YAYASAN PRIMA AGUS TEKNIK

TEKNOLOGI KEAMANAN SIBER

(Cyber Security)

oleh:
Dr. Joseph Teguh Santoso, S.Kom, M.Kom

TEKNOLOGI KEAMANAN SIBER
(Cyber Security)

oleh:
Dr. Joseph Teguh Santoso, S.Kom, M.Kom

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-8120-71-0 (PDF)

Teknologi Keamanan Siber (Cyber Security)

Penulis :
Dr. Joseph Teguh Santoso, S.Kom., M.Kom

ISBN : 9 786238 120710

Editor :
Muhammad Sholikan, M.Kom

Penyunting :
Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

Desain Sampul dan Tata Letak :
Irdha Yunianto, S.Ds., M.Kom

Penebit :
Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

Redaksi :
Jl. Majapahit no 605 Semarang
Telp. (024) 6723456
Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :
Universitas STEKOM
Jl. Majapahit no 605 Semarang
Telp. (024) 6723456
Fax. 024-6710144
Email : info@stekom.ac.id

KATA PENGANTAR

Puji syukur penulis panjatkan atas kehadirat Tuhan Yang Maha Esa karena diberikan kelancaran dalam menyusun buku yang berjudul ***"Teknologi Keamanan Siber (Cyber Security)".*** Cybersecurity adalah praktik melindungi sistem komputer, jaringan, perangkat, dan data dari ancaman keamanan yang berasal dari dunia maya. Tujuan utama dari keamanan cyber adalah menjaga kerahasiaan, integritas, dan ketersediaan informasi. Ancaman keamanan cyber melibatkan serangan dari berbagai bentuk, termasuk serangan siber, malware, peretasan, phishing, dan banyak lagi. Cybersecurity merupakan elemen kritis dalam dunia digital yang terus berkembang, dan keberlanjutan bisnis serta keamanan informasi sangat tergantung pada efektivitas sistem keamanan cyber.

Keamanan Siber (Cybersecurity) memiliki peran sentral dalam melindungi dan memastikan keamanan infrastruktur digital, data, dan informasi di era teknologi informasi saat ini. Salah satu manfaat utama keamanan siber adalah melindungi data pribadi dan informasi sensitif dari akses yang tidak sah atau pencurian, menjaga integritas data agar tidak terpengaruh oleh manipulasi yang tidak sah, serta memastikan ketersediaan sistem dan layanan bagi pengguna yang berhak. Keamanan siber juga berperan dalam meningkatkan kepercayaan dalam transaksi online, mencegah serangan malware yang dapat merusak atau mencuri informasi, dan mengamankan infrastruktur kritis seperti sistem energi dan keuangan dari potensi ancaman siber. Selain itu, keamanan siber membantu organisasi untuk mematuhi peraturan dan undang-undang terkait keamanan data, mengurangi risiko pencurian identitas, dan meningkatkan kesadaran keamanan di kalangan pengguna dan staf organisasi. Dengan meminimalkan dampak serangan siber, keamanan siber juga berkontribusi pada perlindungan reputasi bisnis, efisiensi operasional, dan meningkatkan overall keamanan jaringan komputer serta perangkat Internet of Things (IoT). Melalui manfaat-manfaat ini, keamanan siber menjadi kritis dalam menjaga keberlanjutan dan integritas sistem informasi di lingkungan digital yang terus berkembang.

Buku ini terdiri dari 12 bab, yang terdiri dari bagian-bagian tersendiri, yang memberikan pandangan utuh baik tersendiri maupun saling berhubungan dengan bagian-bagian relevan di dalam buku. Di bawah ini kami merangkum secara singkat isi setiap bab. Pada Bab 1, penulis membahas pertimbangan Desain dan Arsitektur untuk Platform Intelijen, Deteksi, dan Mitigasi Ancaman Siber Tingkat Lanjut. Secara khusus, kerangka dan pendekatan arsitektur diperkenalkan yang menjamin efisiensi yang lebih baik. Bab 2 mengeksplorasi aspek prosedural yang merinci bagaimana proses penilaian dampak diatur dan dilakukan di dalam platform keamanan siber yang kompleks, mengacu pada kasus Cyber-Trust. Penulis Bab3 menguraikan sistem yang menggabungkan dan memperluas alat dan teknik terkini dari siklus hidup Cyber-Threat Intelligence dengan memberikan pandangan holistik dalam proses Cyber-Threat Intelligence.

Teknik Moving Target Defense untuk mitigasi IoT (Internet of Things) yang canggih merupakan inti dari Bab 4 yang menyajikan implementasi sistem respons intrusi. Para penulis

juga menunjukkan bahwa hasil evaluasi menunjukkan efektivitas yang tinggi terhadap ancaman tradisiona l, dan peningkatan efektivitas terhadap ancaman baru. Bab 5 berfokus pada Deteksi Ancaman Cyber di IoT. Di sini penulis menyajikan gambaran komprehensif tentang pembuatan profil perangkat IoT dan solusi deteksi ancaman yang diusulkan oleh Cyber-Trust untuk mengatasi tantangan besar dalam mengamankan ekosistem perangkat IoT. Selain itu, efektivitas dan kinerja solusi yang diusulkan telah diverifikasi secara mendalam, terutama terhadap botnet dan serangan Zero-day.Untuk Mitigasi Ancaman yang Tidak Diketahui di Honeypots IoT, Pembelajaran Mesin dapat dimanfaatkan untuk mengatasi masalah ini secara efektif, yang dijelaskan secara rinci di Bab 6. Pendekatan yang diperkenalkan dalam bab ini adalah pendekatan baru yang mendeteksi lalu lintas jaringan berbahaya yang menggunakan honeypot dan pembelajaran mesin.

Pada Bab 7, penulis memberikan dukungan teoritis mengenai perkembangan terkini di bidang kriptografi pasca-kuantum (PQC) yang bertujuan untuk menggabungkan primitif kriptografi yang aman ke dalam blockchain. Tantangan bagi peneliti dan industri mengenai penerapan algoritma postquantum dalam aplikasi blockchain telah ditunjukkan. Penulis Bab8 membahas dan mengusulkan pendekatan komputasi kepercayaan di Internet of Things, yang menggabungkan aspek perilaku, status perangkat, dan risiko terkait ke dalam skor kepercayaan komprehensif, yang dapat dikonsultasikan untuk mewujudkan kontrol akses berbasis kepercayaan. Pada Bab 9 memperkenalkan metodologi pengujian, validasi, verifikasi dan evaluasi yang diikuti oleh proyek Cyber-Trust selama fase percontohan siklus hidup proyek. Singkatnya, penulis menyajikan bahwa pengumpulan dan analisis data dari kegiatan percontohan mengungkapkan tingkat kepuasan para pemangku kepentingan dan tingkat kinerja sistem. Dari pengujian dan validasi, beralih ke pengujian untuk bisnis. Bab 10 adalah tentang pengujian Rumah Pintar untuk Bisnis. Penulis menyajikan hasil dari platform SoHo (Smart Home) yang ditiru dan diuji, potensi eksploitasinya di beberapa bidang, terutama dari perspektif bisnis serta dampaknya terhadap bisnis dan potensi perluasan.

Untuk Bab 11, kami mendapat masukan berharga dari para pemimpin industri yang membahas cara mengamankan realitas digital yang kompleks saat ini dengan memperkenalkan pendekatan keamanan siber CGI yang teruji dan terbukti untuk lingkungan kerja modern saat ini. Yang terakhir, Bab 12 buku ini membahas tentang aspek keamanan dan privasi bagi si kembar digital, pengemudi, kekhawatiran, dan rekomendasi tentang cara mengelola risiko. Kasus-kasus praktis juga disediakan.

Demikian buku ajar ini kami buat, dengan harapan agar pembaca dapat memahami informasi dan juga mendapatkan wawasan mengenai bidang sistem informasi manajemen serta dapat bermanfaat bagi masyarakat dalam arti luas. Terima kasih.

Semarang, November 2023
Penulis

Dr. Joseph Teguh Santoso, S.Kom, M.Kom

DAFTAR ISI

BAB 1
METODE ARSITEKTUR MITIGASI ANCAMAN SIBER

Bab ini akan mendemonstrasikan cara merancang dan mengatur arsitektur untuk platform intelijen, deteksi, dan mitigasi ancaman siber tingkat lanjut dengan mengikuti contoh proyek penelitian dan inovasi Siber-Trust EU yang menerapkan metodologi arsitektur yang telah terbukti Arsitektur Berbasis Risiko dan Biaya (RCDA). Pendekatan arsitektur RCDA memiliki keunggulan dibandingkan pendekatan lain yang membantu mitra konsorsium untuk menyepakati tahap awal desain dan pengembangan platform. Menurut prinsip-prinsip RCDA, pekerjaan arsitektur dimulai dengan mengidentifikasi permasalahan arsitektur yang memiliki dampak tertinggi dalam hal risiko dan biaya, dan mengatasi permasalahan tersebut dengan membuat keputusan arsitektur. Oleh karena itu, artikel ini berisi hasil keputusan arsitektur paling berpengaruh yang dibuat. Hal ini memungkinkan arsitektur dan proses persyaratan untuk saling mengambil manfaat dari kemajuan masing-masing, dan menghasilkan kohesi yang baik antara persyaratan dan arsitektur. Harga dari kohesi ini adalah beberapa pengerjaan ulang dalam menjaga ketertelusuran: Dalam artikel ini kami memperkenalkan ketertelusuran persyaratan yang didasarkan pada persyaratan tahap awal dan selanjutnya diperluas menjadi referensi terhadap keluaran persyaratan pengguna akhir serta kerangka hukum, etika, dan perlindungan data.

Kekhawatiran dengan dampak tertinggi dalam hal risiko dan biaya yang diidentifikasi pada awal proyek terutama adalah integrasi, serta kepatuhan dan keamanan. Integrasi menjadi perhatian karena solusi intelijen, deteksi, dan mitigasi siber-treat terdiri dari banyak komponen terpisah yang sedang dikembangkan oleh berbagai tim pengembangan dan penelitian. Kekhawatiran ini diatasi dengan membentuk arsitektur modular yang terdiri dari berbagai komponen yang digabungkan secara longgar dimana antarmuka antara komponen-komponen ini dibentuk melalui pedoman integrasi. Selain itu, arsitektur mencakup pendekatan yang dipilih untuk mengembangkan atau memperoleh elemen-elemen yang dapat disampaikan yang membentuk solusi teknis.

Kepatuhan merupakan perhatian penting, terutama yang berkaitan dengan aturan hukum, etika, sosial, dan privasi. Kekhawatiran ini terutama diatasi dalam skenario kasus penggunaan Siber-Trust, rekomendasi hukum dan etika yang dibutuhkan pengguna akhir, dan penilaian dampak. Keamanan selalu menjadi perhatian utama dalam platform yang kompleks, terutama dalam merancang dan mengembangkan platform intelijen, deteksi, dan mitigasi ancaman dunia maya. Kami mengatasi permasalahan ini, selaras dan melengkapi rekomendasi Hukum dan etika.

1.1 LATAR BELAKANG DAN KEKUATAN PENDORONG

Dengan membangun platform pengumpulan, deteksi, dan mitigasi intelijen ancaman dunia maya yang inovatif, serta melakukan penelitian interdisipliner berkualitas tinggi di bidang-bidang utama, proyek Siber-Trust bertujuan untuk mengembangkan teknologi dan

konsep baru untuk mengatasi tantangan besar menuju pengamanan. ekosistem perangkat IoT. Hal ini disusun berdasarkan tiga pilar: a. teknologi proaktif utama, b. deteksi dan mitigasi serangan siber, dan c. teknologi buku besar terdistribusi, seperti terlihat pada Tabel 1.1 di bawah.

Untuk menyiapkan desain platform Siber-Trust, pendekatan iteratif arsitektur digabungkan agar dapat memiliki kesempatan untuk memvalidasi dan mempelajari keputusan arsitektur yang dibuat. Siklus berulang berikut telah diterapkan:

Siklus Iiteratif 1. Persyaratan pengguna dan kerangka peraturan telah ditetapkan untuk membuka jalan bagi desain dan arsitektur sistem. Selama fase ini, tren yang muncul dalam serangan siber telah diidentifikasi untuk memandu definisi skenario kasus penggunaan dan pengumpulan persyaratan pengguna akhir serta kerangka peraturan sedang dianalisis dan dampak metode yang diusulkan terhadap hak-hak dasar, perlindungan data dan privasi sedang dinilai. Kasus penggunaan telah diidentifikasi. Siklus Iteratif 1 mencakup paket pekerjaan

- Lanskap ancaman dunia maya dan persyaratan pengguna akhir;
- Masalah hukum: perlindungan data dan privasi.

***Siklus Iteratif 2*.** Desain platform. Pada fase ini, arsitektur referensi platform Siber-Trust dibuat, menggabungkan masukan dari fase pertama, diterjemahkan ke dalam alat teknologi yang akan dibangun dalam Siklus Iteratif 3. Alat di atas yang terdiri dari platform terintegrasi sedang dirancang dan dibuat prototipe dan konsorsium sedang dalam proses tahap awal desain platform. Desain dan arsitektur sistem diimplementasikan berdasarkan paket pekerjaan

- Kerangka Siber-Trust, desain platform dan arsitektur.

Keluaran utama dari fase ini adalah prototipe platform, dan spesifikasi akhirnya di akhir fase yang dikaitkan dengan tonggak sejarah arsitektur dan spesifikasi desain Siber-Trust. Pada fase ini versi awal desain dan arsitektur sistem ditetapkan termasuk rencana integrasi. Untuk memastikan kepatuhan dan pertimbangan privasi keamanan, aspek etika dan hukum terus aktif dalam fase ini untuk meninjau dan memberikan saran mengenai persyaratan.

***Siklus Iteratif 3*.** Penyempurnaan desain dan arsitektur platform. Dalam siklus berulang ini, arsitektur referensi platform Siber-Trust secara berulang dipantau dan disempurnakan secara paralel dengan pengembangan alat dan selama validasi uji coba. Alat-alat sedang dikembangkan dan arsitektur disempurnakan (jika ada kekurangan) atau divalidasi ulang selama pengembangan dan integrasi perangkat lunak. Ketika platform sudah siap, percontohan akan memvalidasi platform, di mana desain dan arsitektur mengikuti tahap akhir validasi ulang dan penyediaan masukan apa pun yang mungkin dimiliki arsitektur platform agar lebih kokoh.

Dalam menyiapkan desain dan arsitektur Siber-Trust yang kompleks ini, kami menerapkan pendekatan berulang. Pertama, arsitektur awal disampaikan. Kemudian umpan balik dikumpulkan selama lokakarya pengujian dan validasi yang melibatkan anggota dewan penasihat dan kelompok ahli terfokus. Umpan balik ini diproses selama arsitektur referensi Platform dan spesifikasi desain. Para mitra menghasilkan prototipe sebagai versi rancangan komponen perangkat lunak yang berfungsi sebenarnya dan sebagian terintegrasi. Setiap mitra

teknis berkontribusi pada pengembangan, desain dan penyediaan, penjelasan, dan berbagi teknologi yang akan berfungsi sebagai landasan untuk mengimplementasikan platform Siber-Trust selama siklus pengembangan komponen dan perangkat lunak. Dengan mengembangkan perangkat lunak di awal proyek, selama siklus iteratif desain dan arsitektur, arsitektur dan implementasi digabungkan lebih awal, yang memberikan keuntungan dalam memvalidasi dan menyempurnakan arsitektur dan memulai implementasi yang akan dilakukan selama fase pengembangan perangkat lunak inti.

Campuran penelitian dan pengembangan: Teknologi Proaktif Utama dan intelijen ancaman siber, Deteksi dan mitigasi serangan siber tingkat lanjut, dan Teknologi buku besar terdistribusi untuk meningkatkan akuntabilitas, mengikuti (dan sebagian berjalan paralel) paket kerja kerangka kerja Siber-Trust, desain platform, dan kegiatan arsitektur dan bertujuan untuk mengimplementasikan arsitektur solusi (Bukti Konsep). Kegiatan implementasi ini terdiri dari gabungan kegiatan penelitian dan pengembangan, di mana teknologi tercanggih yang relevan diidentifikasi, digunakan dan diperluas, serta alat-alat baru dikembangkan secara khusus. Mitra penelitian dan teknologi fokus bekerja sama dengan peran dan tanggung jawab yang jelas untuk memastikan penyampaian platform Siber-Trust yang efisien, berkualitas tinggi, dan lancar.

Tabel 1.1. Tiga pilar Siber-Trust.

Teknologi proaktif utama	Deteksi dan mitigasi serangan	Teknologi Buku Besar Terdistribusi
• Intelijen ancaman dunia maya • Berbagi ancaman dunia maya • Manajemen reputasi/kepercayaan • Permainan keamanan	• Serangan tertarget tingkat lanjut • Serangan infrastruktur jaringan • Visualisasi jaringan • Mitigasi dan remediasi • Pengumpulan bukti forensik	• Registrasi • Memperbarui • Verifikasi • Pemodelan • Konsensus • Privasi

1.2 PENDEKATAN DAN METODOLOGI ARSITEKTUR

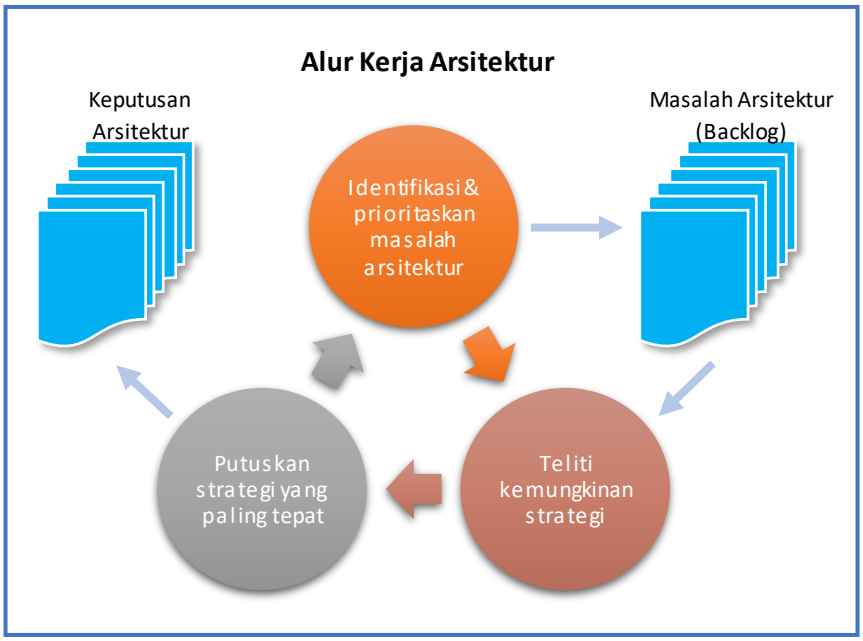
Metodologi Arsitektur Berbasis Risiko dan Biaya (RCDA)

Konsorsium telah memilih kerangka dan pendekatan Arsitektur Berbasis Risiko dan Biaya (RCDA) sebagai metodologi utama untuk desain arsitektur. Keuntungan penerapan metode ini adalah mendukung pengambilan keputusan arsitektural di seluruh proses desain. Kekhawatiran dan keputusan dipertimbangkan selama proses desain dan persyaratan pemangku kepentingan terus-menerus divalidasi terhadap desain tersebut. Proses desain bersifat berulang untuk memastikan hasil berkualitas tinggi. Fakta bahwa RCDA adalah metode yang diakui dalam program Arsitek Bersertifikat Grup Terbuka, merupakan keuntungan ekstra bagi mitra proyek dan konsorsium untuk mendorong keterbukaan dan kolaborasi mengenai cara paling efisien dalam membentuk desain dan arsitektur.

Praktik RCDA diterapkan saat pertama kali membentuk proyek Siber-Trust. Langkah-langkah konkrit berikut ini diterapkan:

- Arsitek dilibatkan selama tahap persyaratan untuk membantu dan membimbing dengan tujuan meningkatkan hubungan antara persyaratan dan desain.
- Arsitektur disampaikan dalam dua tahap, dengan kemampuan untuk memverifikasi dan mempelajari:
  - Arsitektur awal disampaikan pada tahap awal, untuk dapat menyelaraskan rekayasa persyaratan dengan pengembangan perangkat lunak dan memiliki kesempatan untuk memvalidasi keputusan desain.
  - Arsitektur awal ini divalidasi dengan membangun dan menguji perangkat lunak yang berfungsi, yaitu prototipe cepat
  - Arsitektur ditentukan setelah memproses umpan balik yang dikumpulkan melalui arsitektur awal penilaian prototipe cepat dan validasi serta demonstrasi, penilaian, dan validasi mock up UI
- Arsitektur berfokus pada keputusan desain yang penting dan tidak boleh terlalu spesifik, dan dimulai sejak awal proyek, namun pekerjaan arsitektur tidak berhenti sampai di sini. Desain Teknis dan pemilihan alat dilakukan kemudian dalam proyek selama tahap pengembangan (Paket Kerja (WP) 5, 6 dan 7 – WP5, 6, 7 dalam proyek Siber-Trust) dan implementasi percontohan (WP8) yang merupakan tahap akhir menuju evaluasi dan validasi platform, oleh karena itu, arsitektur akhir platform. Arsitek terlibat selama paket pekerjaan ini dimana arsitektur divalidasi dan dielaborasi. Arsitek akan membantu dan membimbing tetapi tidak memimpin.
- Rekomendasi hukum dan etika telah diberikan sepanjang pengerjaan arsitektur.

Selama proyek berlangsung, pada tingkat abstraksi tertinggi, proses spesifikasi arsitektur mengikuti putaran alur kerja sederhana dengan tiga langkah:



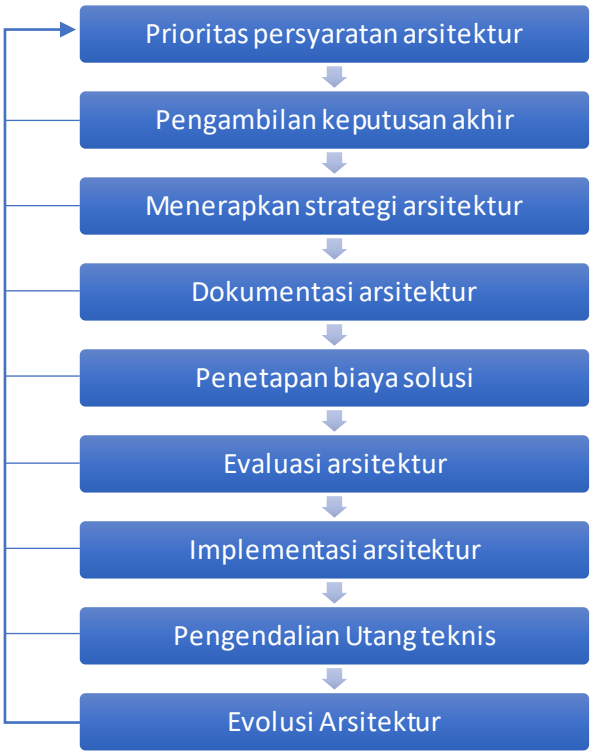
Gambar 1.1. Siklus Mikro Arsitektur RCDA.

Kami menyebutnya *"Siklus Mikro Arsitektur"*. Putaran alur kerja ini didorong oleh tumpukan masalah arsitektur yang belum terselesaikan, akibat praktik prioritisasi kebutuhan

arsitektur. Keputusan-keputusan arsitektural yang diambil, yang dihasilkan dari praktik pengambilan keputusan arsitektur, untuk mengatasi permasalahan ini ditambahkan ke dalam tumpukan Keputusan Arsitektur yang terus bertambah.

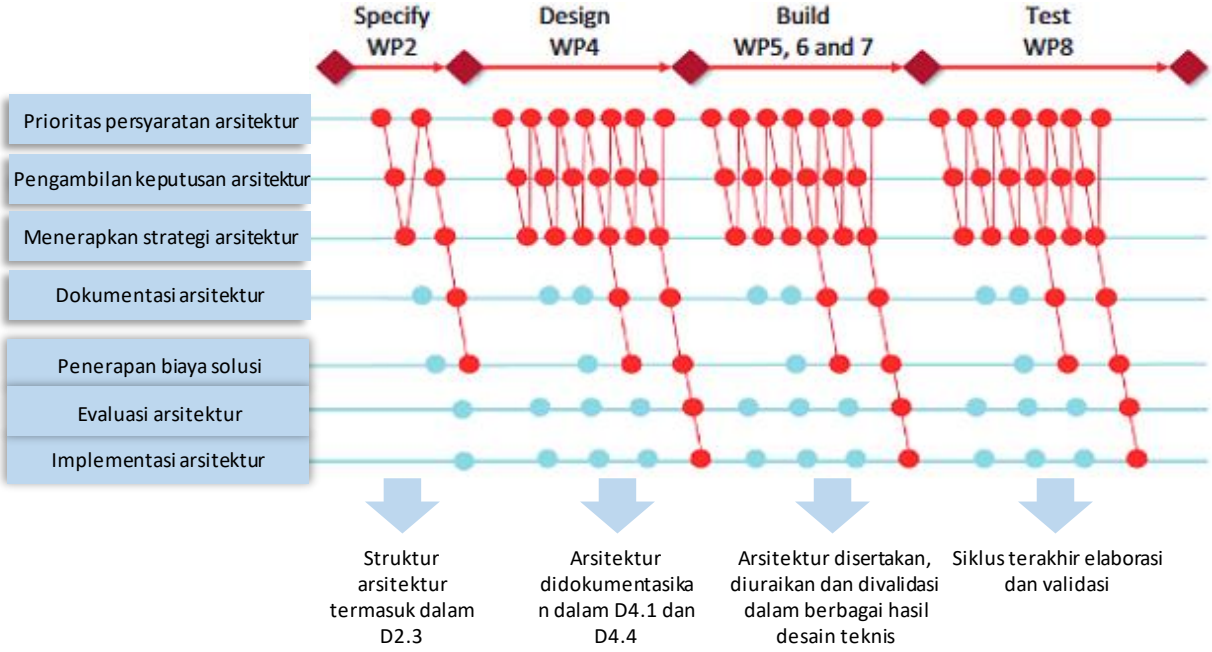
Representasi siklus mikro ini merupakan penyederhanaan yang berlebihan. Dalam kehidupan nyata, keputusan arsitektur biasanya mempengaruhi lebih dari satu hal, dan hampir tidak pernah dapat dibuat secara berurutan. Arsitek harus memastikan bahwa seluruh rangkaian keputusan mendukung seluruh rangkaian permasalahan secara maksimal.

Selain dua praktik pertama (prioritas dan pengambilan keputusan) yang disebutkan di atas, RCDA menawarkan serangkaian praktik inti yang diterapkan sepanjang siklus hidup proyek.



Gambar 1.2. praktik inti RCDA.

Gambar 1.3 menunjukkan bagaimana praktik RCDA diterapkan dalam proses proyek Siber-Trust. Praktik-praktik diterapkan secara bertahap, terus-menerus mengidentifikasi dan memprioritaskan permasalahan serta membuat (serta menerapkan dan mendokumentasikan serta memvalidasi, dll.) keputusan untuk memitigasi permasalahan tersebut.



Gambar 1.3. Tinjauan indikatif tingkat tinggi mengenai praktik RCDA yang diterapkan dalam proses proyek Siber-Trust.

Proyek Siber-Trust pada dasarnya didasarkan pada pendekatan tradisional dan bertahap (waterfall). Meskipun tahapannya tumpang tindih dan arsitek terlibat secara menyeluruh di seluruh siklus hidup, sebagian besar pekerjaan dilakukan dalam tahap desain (WP4).

Gambar 1.4. Pekerjaan arsitektur dilakukan sepanjang siklus hidup proyek.

Tampilan Arsitektur

Arsitektur solusi Siber-Trust dibentuk oleh berbagai persyaratan arsitektur dan keputusan yang dibuat dan didokumentasikan dalam serangkaian pandangan (lihat Tabel1.2).

Pandangan ini fokus pada mengkomunikasikan arsitektur secara efektif kepada pemangku kepentingan terkait. Di luar pandangan ini, dokumentasi tambahan disediakan untuk melengkapi desain sistem teknis. Pandangannya dirinci dalam bab-bab selanjutnya.

Tabel 1.2. Pemandangan arsitektur.

Pandangan arsitektur		
Bab	Melihat	Sasaran
2	Konteks	Jelaskan konteks solusi tingkat tinggi.
3	Persyaratan	Untuk mengidentifikasi, memahami dan memprioritaskan persyaratan arsitektur yang signifikan.
4	Keputusan, kekhawatiran & kesimpulan persyaratan arsitektur	Untuk menggambarkan kekhawatiran, keputusan penting, dan kesimpulan persyaratan arsitektur.
5	Tampilan operasional	Untuk menggambarkan bagaimana sistem berperilaku dalam lingkungan operasional.
6	Tampilan rincian pengiriman	Untuk dijadikan sebagai dasar perencanaan penyampaian solusi.
7	Pandangan infrastruktur	Untuk mengidentifikasi dan menjelaskan aspek perangkat keras, perangkat lunak infrastruktur, dan penerapan solusi.
8	Tampilan data	Jelaskan data yang relevan dan bagaimana data ini didistribusikan dalam solusi.
9	Tampilan keamanan	Untuk menggambarkan serangkaian proses, mekanisme dan komponen yang digunakan untuk membuat sistem aman.

Kepatuhan dan Keamanan

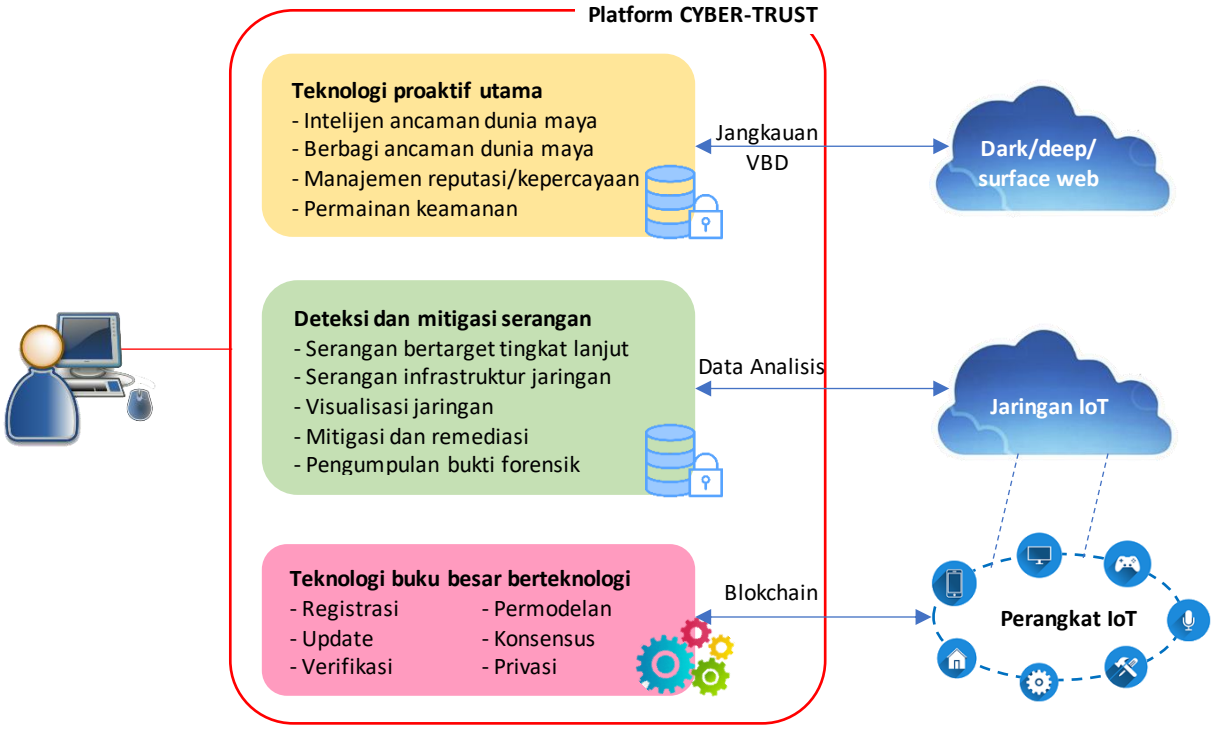
Kepatuhan merupakan perhatian penting, terutama yang berkaitan dengan aturan hukum, etika, sosial, dan privasi. Kekhawatiran ini terutama diatasi dalam skenario kasus penggunaan Siber-Trust, persyaratan pengguna akhir Siber-Trust dan khususnya Rekomendasi Hukum dan etika, yang menjelaskan bagaimana, kekhawatiran kepatuhan bervariasi berdasarkan kasus penggunaan, alat yang akan dikembangkan dalam Siber-Trust. Proyek kepercayaan dan arsitekturnya harus cukup fleksibel untuk mengatasi perbedaan ini. Keamanan selalu menjadi perhatian utama dalam platform yang kompleks, terutama dalam merancang dan mengembangkan platform intelijen, deteksi, dan mitigasi ancaman dunia maya. Rincian lebih lanjut akan diberikan nanti dalam artikel ini yang membahas masalah ini, selaras dan melengkapi rekomendasi hukum dan etika. Pendekatan yang akan kami terapkan dalam merancang platform Siber-Trust adalah sebagai berikut: persyaratan (persyaratan pengguna akhir dan persyaratan arsitektur) harus mematuhi hukum dan etika. Tinjauan

hukum dan etika telah dilakukan oleh mitra ahli yang berdedikasi sepanjang durasi sejak pembuatan sistem hingga validasi saat merancang dan mengembangkan sistem.

1.3 SOLUSI, KONTEKS DAN IKHTISAR

Konteks

Proyek Siber-Trust dibangun berdasarkan tiga tujuan utama penelitian keamanan siber, yaitu teknologi proaktif utama, deteksi dan mitigasi serangan siber, dan teknologi buku besar terdistribusi. Pendekatan yang diusulkan bertujuan untuk menangkap fase-fase berbeda dari serangan siber berskala besar sebelum dan sesudah kerentanan perangkat yang ada (dan mungkin tidak diketahui) telah dieksploitasi secara luas oleh penjahat siber untuk melancarkan serangan. Beberapa metode dan alat baru akan dikembangkan untuk menangani masalah mendasar dalam pencegahan, deteksi, dan mitigasi serangan siber tingkat lanjut yang melibatkan perangkat dan jaringan IoT.



Gambar 1.5. Ikhtisar solusi tingkat tinggi. Sumber.

Ikhtisar Solusi Statis

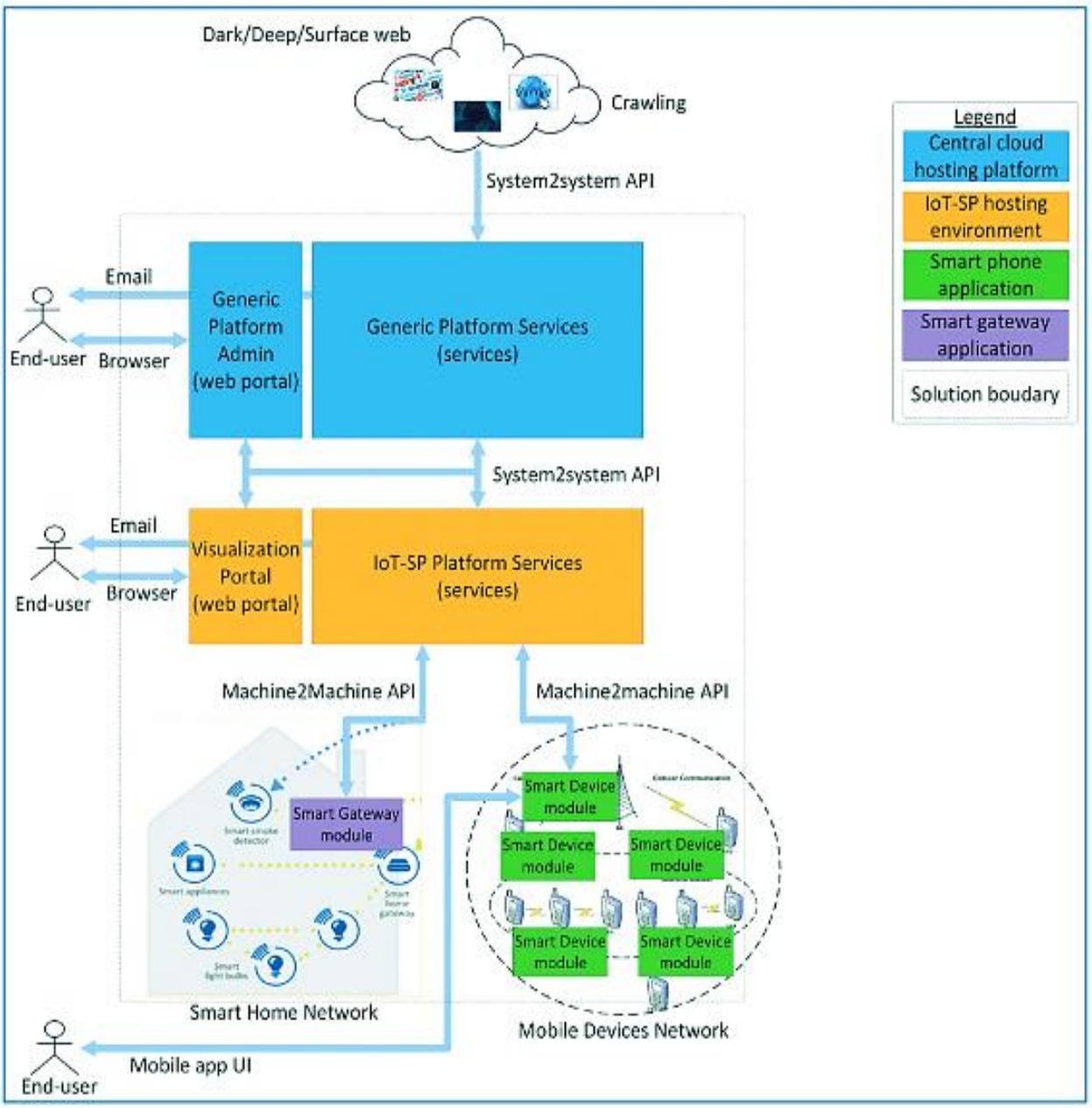
Solusi SiberTrust disusun dalam empat area solusi, ditandai dengan empat warna pada Gambar 1.6 di bawah:

(1) Platform berisi semua layanan dan data pusat (biru)

(2) Platform dengan layanan dan data ISP tertentu (oranye)

(3) Aplikasi yang berjalan di ponsel pintar (hijau)

(4) Aplikasi yang berjalan di gateway pintar (ungu)



Gambar 1.6. Ikhtisar Solusi Statis & Batasan Solusi.

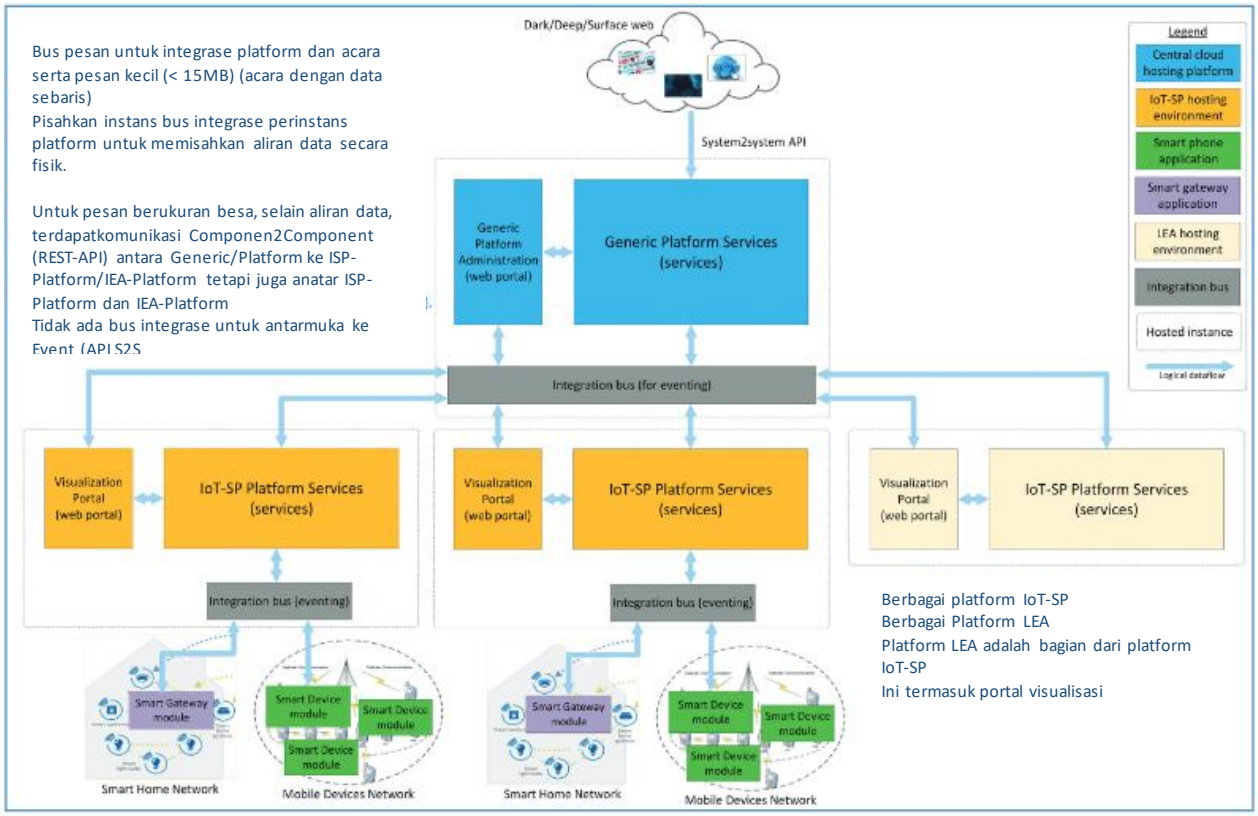
Ikhtisar Solusi Runtime

Gambar di bawah menunjukkan empat area solusi Siber-Trust saat runtime. Setiap ISP menjalankan platform layanan ISPnya sendiri, menghubungkan ke berbagai gateway pintar dan ponsel pintar terkait ISP. Jika Lembaga Penegakan Hukum (LEA) bergabung dengan platform ini, mereka akan menjalankan platform khusus, yang terdiri dari subset platform ISP. Komunikasi dilakukan melalui pesan melalui Bus Integrasi. Sehubungan dengan Gambar 1.7, berikut pertimbangan yang dilakukan

- Bus pesan untuk integrasi platform dan acara serta pesan kecil (<15 mb) (acara dengan data inline).
- Pisahkan instans bus integrasi per instans platform untuk memisahkan aliran data secara fisik.

- Untuk pesan berukuran besar, selain aliran data, terdapat komunikasi Komponen2 Komponen (REST-API) antara GenericPlatform ke ISP-Platform/ LEA-Platform tetapi juga antara ISP-Platform dan LEA-Platform.
- Tidak ada bus integrasi untuk antarmuka perayapan (S2S API).
- Tidak ada bus integrasi untuk antarmuka webportal2platform (API S2S).
- Beberapa platform IoT-SP
- Beberapa platform LEA
- Platform LEA adalah bagian dari platform IoT-SP
- Ini termasuk Portal Visualisasi

Tinjauan solusi statis dan run-time bersama-sama terdiri dari arsitektur utama platform Siber-Trust sebagai platform intelijen, deteksi, dan mitigasi ancaman siber. Pengembangan platform Siber-Trust setiap kemajuan atau pengembangan teknologiArsitektur ini berfungsi sebagai panduan dan landasan dalam pengembangan proyek lebih lanjut, semua pekerjaan teknologi termasuk pengembangan.



Gambar 1.7 Ikhtisar Solusi Run-time.

1.4 KESIMPULAN

Dalam bab ini, kami menyajikan pendekatan untuk menyiapkan desain dan arsitektur platform pengumpulan, deteksi, dan mitigasi intelijen ancaman siber yang canggih. Kami menunjukkan hal ini dengan mengikuti contoh proyek penelitian dan inovasi Siber-Trust European Commission H2020 yang dilaksanakan oleh sembilan mitra multidisiplin dari tujuh

negara yang menyatukan praktik dan pengalaman terbaik yang berasal dari mitra proyek. Pendekatan arsitektur yang diterapkan pada Siber-Trust adalah Risk and Cost Driven Architecture (RCDA) berdasarkan keunggulan dibandingkan pendekatan lain yang disepakati oleh mitra konsorsium pada tahap inisiasi proyek pengembangan platform. Menurut prinsip-prinsip RCDA, pekerjaan arsitektur dimulai dengan mengidentifikasi permasalahan arsitektur yang memiliki dampak paling tinggi dalam hal risiko dan biaya, dan mengatasi permasalahan tersebut dengan membuat keputusan arsitektur. Oleh karena itu, bab ini berisi hasil keputusan arsitektur paling berdampak yang dibuat. Hal ini memungkinkan arsitektur dan proses persyaratan untuk saling mengambil manfaat dari kemajuan masing-masing, dan menghasilkan kohesi yang baik antara persyaratan dan arsitektur. Harga yang harus dibayar untuk kohesi ini adalah beberapa perubahan dalam menjaga ketertelusuran: Dalam artikel ini kami memperkenalkan ketertelusuran persyaratan yang didasarkan pada persyaratan tahap awal dan selanjutnya diperluas menjadi referensi terhadap keluaran persyaratan pengguna akhir serta kerangka hukum, etika, dan perlindungan data. Kami juga mempertimbangkan kekhawatiran dengan dampak paling besar dalam hal risiko dan biaya yang diidentifikasi pada awal proyek, terutama integrasi, kepatuhan, dan keamanan.

BAB 2
PARADIGMA KEPERCAYAAN SIBER DALAM ASPEK PROSEDURAL

Bab ini mengeksplorasi elemen-elemen meta dari penilaian dampak, yang kita sebut sebagai aspek prosedural, sebelum, selama, dan setelahnya. Dengan kata lain, bagaimana prosedur penilaian dampak diatur dan dilakukan di dalam proyek Siber-Trust. Buku ini memusatkan semua pengalaman yang diperoleh dan pembelajaran sejauh ini. Skema struktural yang digunakan dalam proyek Siber-Trust dapat menjadi dasar bagi konsorsium proyek penelitian lain yang mengembangkan solusi inovatif di lapangan, atau sebagai titik awal diskusi mengenai cara meningkatkan dan akhirnya menstandardisasi prosedur tersebut.

2.1 PENDAHULUAN DAN LATAR BELAKANG

Proyek Siber-Trust H2020 bertujuan untuk mengembangkan platform pengumpulan, pencegahan, deteksi dan mitigasi ancaman siber yang holistik dan baru, untuk mengamankan infrastruktur cerdas yang kompleks dan terus berkembang, yang digunakan oleh jutaan orang setiap hari. Konsorsium proyek mengikuti inovasi teknis terkini serta praktik terbaik di lapangan, mengamati perkembangan kerangka hukum dan peraturan yang berlaku, serta menyelidiki pertimbangan etika dan sosial lainnya.

Dalam hal ini, sejak konsepsinya, proyek Siber-Trust telah membentuk mekanisme penilaian dampak, dengan fokus khusus pada perlindungan data dan privasi, sebagai latihan dan saling berhubungan secara berturut-turut. langkah-langkah yang terhubung. Mekanisme ini sesuai dengan penilaian dampak perlindungan data sebagaimana tercantum dalam Pasal 35 GDPR namun mengingat kompleksitas tujuan yang ingin dicapai, konsorsium menyempurnakan prosedur tersebut dengan elemen penilaian dampak yang lebih luas termasuk pertimbangan etika dan sosial yang lebih luas.

Bab ini mengeksplorasi elemen-elemen meta dari penilaian dampak, yang kita sebut sebagai aspek prosedural, sebelum, selama, dan setelahnya. Dengan kata lain, bagaimana prosedur penilaian dampak diatur dan dilakukan di dalam proyek Siber-Trust. Artikel ini memusatkan semua pengalaman yang diperoleh dan pembelajaran sejauh ini. Skema struktural yang digunakan dalam proyek Siber-Trust dapat menjadi dasar bagi konsorsium proyek penelitian lain yang mengembangkan solusi inovatif di lapangan, atau sebagai titik awal diskusi mengenai cara meningkatkan dan akhirnya menstandardisasi prosedur tersebut.

2.2 PENILAIAN DAMPAK PERLINDUNGAN DATA

Dengan berlakunya Peraturan Perlindungan Data Umum pada tahun 2018, Penilaian Dampak Perlindungan Data (atau singkatnya, DPIA) menjadi persyaratan hukum bagi pengontrol data mengenai operasi pemrosesan data tertentu dalam beberapa konteks. DPIA mengacu pada pengembangan atau penerapan sistem, produk, atau proses baru terkait pemrosesan data pribadi, misalnya dalam skala besar atau cara baru. Mereka memungkinkan untuk mengidentifikasi risiko jauh sebelumnya dan mengeksplorasi strategi mitigasi risiko.

Namun, penilaian dampak bukanlah hal baru. Penilaian dampak lingkungan telah dilaksanakan selama bertahun-tahun. Organisasi telah melakukan penilaian dampak privasi, penilaian dampak dari sudut pandang sosial atau etika, atau bahkan penilaian dengan fokus tertentu.

2.3 PENILAIAN DAMPAK SIBER-TRUST

DPIA dianggap perlu dalam konteks Siber-Trust, terlepas dari kenyataan bahwa DPIA merupakan bagian dari kewajiban kontrak proyek, karena dua alasan:

a. sehubungan dengan pemrosesan yang dimaksudkan setelah penelitian, jika sistem tersebut dipasarkan: seperti halnya dengan banyak sistem keamanan siber, ketika beroperasi dan diterapkan secara penuh, pemrosesan data pribadi dapat dilakukan dalam skala besar. Pemrosesan ini cukup sering terjadi dengan penggunaan solusi teknologi inovatif. Dalam proyek Siber-Trust, teknologi baru mencakup penggunaan pembelajaran mesin, Kecerdasan Buatan, dan Teknologi Buku Besar Terdistribusi dan bertujuan untuk menciptakan sistem yang melampaui kecanggihan saat ini. Teknologi tersebut dapat melibatkan bentuk pengumpulan dan penggunaan data baru, yang mungkin menimbulkan risiko tinggi terhadap hak dan kebebasan individu. Selain itu, sistem ini memiliki konstelasi aktor yang terlibat (pengguna dan pengguna akhir) yang kompleks, mulai dari berbagai subjek data hingga penyedia telekomunikasi dan Badan Penegakan Hukum.
b. Pemrosesan yang dimaksudkan selama penelitian: Dalam kasus perayap web, data pribadi mungkin diproses tanpa memberikan pemberitahuan privasi langsung kepada individu tersebut. Mengingat bahwa salah satu bagian dari layanan perayapan akan diterapkan di lingkungan nyata, dengan sedikit dampak manusia terhadap pilihan situs web dan tautan yang akan diakses, khususnya dengan penggunaan Kecerdasan Buatan, kemungkinan untuk merayapi data pribadi bahkan secara instan dari sumber yang tersedia untuk umum tidaklah jauh. Meskipun dalam konteks Siber-Trust, tujuan pengumpulannya bukanlah untuk mengidentifikasi dan membuat profil individu maupun pengumpulan data pribadi, dalam Pedoman Komisi Eropa mengenai etika dan perlindungan data dalam proyek Horizon 2020. Penggunaan perayapan web dianggap menimbulkan kekhawatiran etis dan oleh karena itu, DPIA terdaftar sebagai alat yang tepat untuk mengidentifikasi risiko dan potensi tindakan mitigasi.

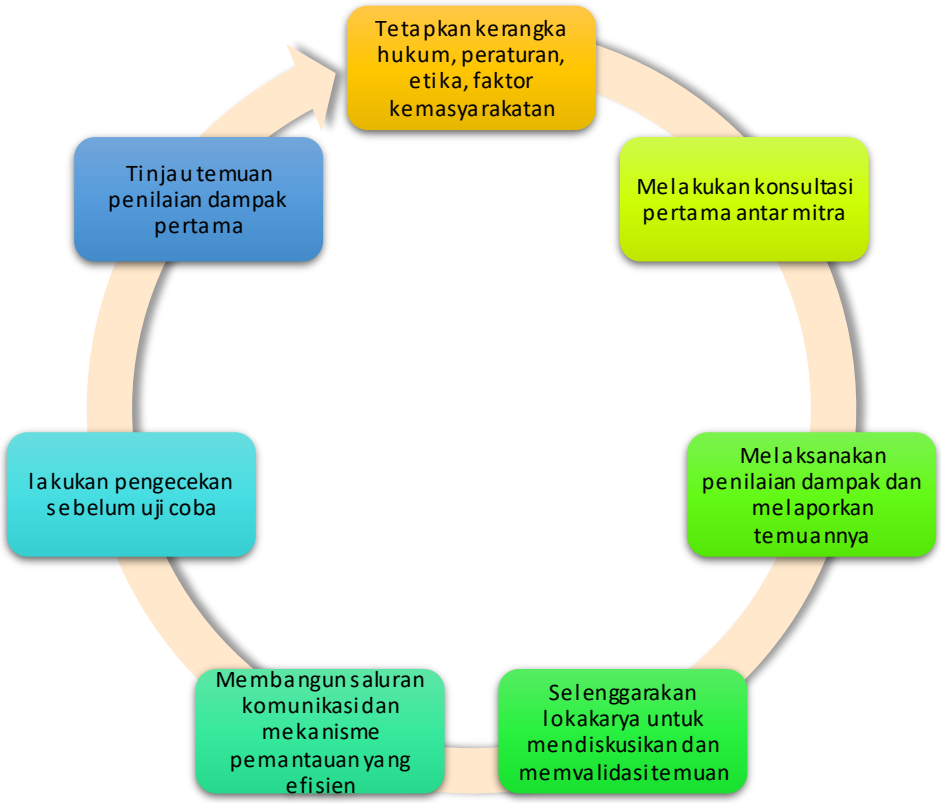
2.4 PANDUAN YANG ADA

Langkah-langkah prosedural saling terkait satu sama lain sehingga menciptakan jaringan arus informasi di dalam konsorsium, berguna untuk pengambilan keputusan dan kebijakan, dan pusat pengetahuan bagi pemangku kepentingan potensial yang di masa depan mungkin ingin menerapkan sistem tersebut. Artikel ini tidak akan menyajikan langkah-langkah analisis aktual yang diharapkan dilakukan selama penilaian dampak. Karena proses ini bergantung pada konteks, hal ini hanya dapat ditentukan berdasarkan kasus per kasus.

Selain itu, terdapat banyak panduan mengenai substansi penilaian dampak. Kelompok Kerja Pasal 29 menerbitkan pedoman mengenai Penilaian Dampak Perlindungan Data pada tahun 2017 untuk memungkinkan penafsiran umum terhadap Pasal 35 GDPR. Otoritas

Pengawasan Nasional Negara-negara Anggota UE juga telah menerbitkan pedoman dan templat untuk membantu pengontrol data, pemroses data, serta peneliti dan produsen untuk mendokumentasikan dan menilai operasi pemrosesan data yang sedang berjalan, direncanakan, atau direncanakan. Misalnya, otoritas Perancis (CNIL) memiliki repositori dengan panduan di situs webnya dan bahkan perangkat lunak khusus. Laboratorium Brussels untuk Penilaian Dampak Perlindungan Data & Privasi di Vrije Universiteit Brussel juga telah menerbitkan serangkaian laporan singkat tentang proses penilaian dampak perlindungan data dalam berbagai bahasa, menyediakan templat interaktif. Pada prinsipnya, metodologi tertentu tidak disarankan dalam GDPR. Hal ini memungkinkan organisasi untuk menggunakan kerangka kerja atau metodologi apa pun, selama kerangka atau metodologi tersebut "menggambarkan sifat, ruang lingkup, konteks, dan tujuan pemrosesan; menilai perlunya, proporsionalitas dan langkah-langkah kepatuhan; mengidentifikasi dan menilai risiko terhadap individu; dan mengidentifikasi tindakan tambahan apa pun untuk memitigasi risiko tersebut."

2.5 TUJUH LANGKAH



Langkah Pertama: Menetapkan Kerangka Hukum dan Peraturan pada Awal Proyek

Konsorsium Siber-Trust bersifat interdisipliner. Mitra-mitranya berasal dari kalangan akademisi, bisnis, administrasi publik dan memiliki latar belakang dan pengalaman berbeda di bidang: teknologi, keamanan siber, kebijakan, hukum, etika, industri, perdagangan, telekomunikasi, penegakan hukum. Oleh karena itu, langkah pertama yang dilakukan adalah mengajak semua mitra untuk merenungkan konteks di mana a) penelitian Siber-Trust akan dilakukan dan b) sistem Siber-Trust di masa depan akan diterapkan. Dalam beberapa bulan

pertama proyek (semester pertama) dan selama tahap konseptualisasi sistem, para mitra mengeksplorasi secara menyeluruh dampak kerangka hukum dan peraturan berdasarkan konsep awal proyek yang sangat kasar. Mereka melakukan hal tersebut dengan mempelajari kerangka peraturan UE dan undang-undang nasional yang berlaku di negara-negara dimana mitra tersebut berada dan merupakan hal yang paling penting jika sistem tersebut dirilis di masa mendatang. Dalam konteks Siber-Trust, yaitu dalam konteks keamanan siber, yang ditinjau secara khusus adalah undang-undang perlindungan data dan privasi, undang-undang yang mengatur telekomunikasi, undang-undang terkait dengan bukti dengan fokus khusus pada bukti elektronik, peraturan terkait dengan kejahatan dunia maya, dan pedoman peraturan atau kebijakan ad-hoc sehubungan dengan teknologi spesifik yang diterapkan selama proyek (sistem DLT, pembelajaran mesin, dll). Studi ini menghasilkan dua laporan tertulis yang menetapkan konsep dasar dan membangun diskusi yang kompleks dan khusus. Pada tahap ini, persyaratan hukum dan etika lainnya juga diselesaikan oleh konsorsium, misalnya keterlibatan atau penunjukan petugas perlindungan data per entitas yang berpartisipasi, penyiapan template, seperti formulir informed consent dan lembar informasi untuk keikutsertaan dalam penelitian. dan pemrosesan data pribadi, kapan pun diperlukan dan sebagainya. Persyaratan tersebut akan berbeda dari satu proyek ke proyek lainnya.

Langkah Kedua: Konsultasi Luas Pertama Antar Mitra untuk Bersama-sama Menentukan Jalan ke Depan

Pada awal semester kedua, dan setelah para mitra mempelajari secara menyeluruh kerangka hukum dan peraturan, konsultasi pertama di antara seluruh mitra teknis dilakukan. Mitra utama diidentifikasi dengan bantuan Koordinator Proyek dan Manajer Teknis. Para mitra tersebut diundang untuk mengisi kuesioner singkat tentang konsep komponen yang mereka kembangkan. Tujuan utamanya adalah untuk mendapatkan gambaran pertama mengenai desain yang diinginkan dan mengumpulkan kekhawatiran atau pertanyaan mengenai hal tersebut, yang muncul berdasarkan kajian kerangka hukum dan peraturan. Hasil dari konsultasi ini adalah penyusunan serangkaian rekomendasi umum dan lebih konkrit untuk membantu mitra-mitra utama lebih lanjut dalam konsep dan desain mereka. Selama periode ini, sejumlah pertemuan bilateral ad-hoc telah dilakukan. Proses ini bertepatan dengan diskusi tentang arsitektur awal dan para mitra menilai perlunya penilaian dampak. Pada tahap ini, para mitra juga mengusulkan metodologi penilaian dampak dan menetapkan prosedur pelaporannya.

Langkah Ketiga: Melaksanakan, Menyelesaikan dan Melaporkan Penilaian Dampak

Sejalan dengan negosiasi yang intens untuk finalisasi arsitektur sistem, para mitra terlibat dalam dialog ekstensif tentang bagaimana menerapkan rekomendasi yang diberikan pada Langkah 2 dengan lebih baik, ke dalam rencana kerja mereka. Para mitra kembali diundang untuk mengisi kuesioner tertulis individual yang dibuat khusus untuk komponen-komponen mereka, menilai masing-masing komponen secara terpisah namun juga dalam konteks sistem secara keseluruhan. Dalam praktiknya, para mitra diajak untuk menguraikan lebih lanjut kekhawatiran dan pertanyaan awal mereka, serta menyatakan secara eksplisit manfaat dari solusi yang diusulkan.

Kuesioner tersebut mencakup pertanyaan terbuka, umum untuk semua komponen, serta pertanyaan spesifik, yang dibuat khusus untuk komponen tertentu. Latihan ini terdiri dari dua langkah: pertama, para mitra memvisualisasikan komponen yang mereka kembangkan, kebutuhan penelitian mereka, operasi pemrosesan data yang mereka rencanakan dan menjelaskan bagaimana mereka bertujuan untuk tetap patuh selama proyek berlangsung, dengan melihat persyaratan dari setiap prinsip perlindungan data ; kedua, para mitra menunjukkan bagaimana mereka membayangkan komponen mereka secara umum sesuai dengan prinsip-prinsip perlindungan data, jika ada kemungkinan komersialisasi di masa depan. Dengan kata lain, penilaian tersebut merujuk pada: (a) pemrosesan data yang diharapkan akan dilakukan selama proyek berlangsung; dan (b) pemrosesan data yang dimaksudkan untuk suatu sistem teknologi baru yang kemungkinan akan digunakan oleh pengontrol data yang berbeda untuk melaksanakan operasi pemrosesan yang berbeda.

Karena perbedaan disiplin ilmu, para mitra juga membuat daftar istilah yang sering digunakan (misalnya, apa yang dimaksud dengan subjek data, apa perbedaan antara hak privasi dan hak atas perlindungan data, dll). Konsorsium diundang untuk mempertimbangkan informasi mana yang harus dikumpulkan dan alasannya, apakah informasi tersebut mencakup data pribadi dan mengapa data tersebut diperlukan untuk tujuan yang mereka inginkan, berdasarkan dasar hukum apa dan untuk berapa lama mereka berencana atau berencana untuk menyimpannya. data.

Pengaturan waktu, ketepatan dan fleksibilitas adalah kuncinya di sini: Meskipun mitra diberikan kuesioner awal, melalui interaksi yang berkelanjutan beberapa pertanyaan disempurnakan dan pertanyaan baru ditambahkan atau dihilangkan. Semua kuesioner dibuat jelas sejak awal, dengan menghubungi Manajer Teknis dan koordinator Proyek, yang bertugas memberikan tanggapan; dengan kata lain, mitra teknis yang memiliki peran utama dalam perancangan operasi pemrosesan data tertentu dan mitra non-teknis yang harus diajak berkonsultasi karena keahlian mereka dalam proyek tersebut. Dalam beberapa kesempatan, mitra didorong untuk berkonsultasi dengan pakar eksternal dan Petugas Perlindungan Data mereka sendiri.

Tergantung pada sistem yang dimaksud seperti yang sering terjadi pada sistem keamanan siber, prosedur pemetaan semua operasi pemrosesan data dari antarmuka pengguna hingga semua sumber backend dan database, mungkin bersifat dinamis, panjang, sangat kolaboratif, agak interaktif, intens dan menuntut sumber daya. Oleh karena itu, disarankan untuk memulainya sesegera mungkin dan setidaknya sebelum pemrosesan yang dimaksudkan. Perlu dicatat bahwa prosedur ini bukan hanya dilakukan sekali saja, melainkan sebagai instrumen hidup yang akan berlangsung bersamaan dengan tahap perencanaan, pengembangan, validasi, dan implementasi aktual.

Hasil dari proses awal kasus Siber-Trust ini adalah laporan tertulis, yang terdiri dari ringkasan tanggapan seluruh mitra, serangkaian pedoman per komponen, matriks pemrosesan data per komponen, dan matriks penilaian risiko per komponen. untuk keseluruhan proyek. Kuesioner lengkap yang diisi oleh mitra juga ditambahkan sebagai Lampiran di akhir laporan tertulis, jika mitra ingin mencari klarifikasi atau rincian yang tidak disertakan dalam laporan utama, sesuai dengan persyaratan transparansi.

Langkah Keempat: Lokakarya untuk Membahas dan Memvalidasi Hasil Penilaian Dampak

Setelah penilaian dampak pertama selesai dan hasilnya dipublikasikan, sebuah lokakarya ad-hoc diselenggarakan dalam pleno untuk membahas hasil penilaian dampak dan menarik perhatian para pengambil keputusan utama di dalam konsorsium. Tujuan utama dari lokakarya ini adalah untuk merefleksikan dan mengklarifikasi kesalahpahaman umum yang diamati selama prosedur penilaian dampak, untuk mengingat kembali persyaratan hukum dan etika dan pada akhirnya untuk memeriksa ruang lingkup substansial dan hasil dari penilaian dampak pertama dan mengevaluasi prosedurnya. aspek. Lokakarya ini juga merupakan titik awal untuk persiapan tinjauan lanjutan atas penilaian dampak yang akan diselesaikan pada akhir proyek dan bertepatan dengan pembahasan awal alur kerja sistem.

Langkah Kelima: Komunikasi Berkelanjutan Selama Pembangunan

Sejak awal proyek dan sepanjang proyek berlangsung, mitra non-teknis telah berpartisipasi dalam pertemuan manajerial dan teknis secara berkala dan memantau proses pembangunan. Semua mitra telah didorong untuk menghubungi mitra hukum ketika mereka memiliki pertanyaan atau kekhawatiran, dan mitra hukum pada gilirannya mengikuti perkembangan hukum dan peraturan serta memberikan pembaruan ketika terjadi perubahan undang-undang yang berpotensi berdampak pada sistem Siber-Trust. atau kasus hukum baru muncul. Berbagai diskusi di antara masing-masing mitra, Manajer Teknis dan Koordinator Proyek, telah menghasilkan penyusunan makalah dan buku kolektif, yang menyelidiki topik-topik antar-disiplin yang menjadi kepentingan global. Topik-topik tersebut mencakup, namun tidak terbatas pada: perlindungan data yang dirancang untuk sistem keamanan siber di rumah pintar, mekanisme pelestarian privasi dalam sistem Teknologi Buku Besar Terdistribusi, perlindungan privasi dan data dalam ekosistem Internet of Things, dan sebagainya. Inisiatif-inisiatif tersebut tidak hanya meningkatkan pemahaman konsorsium terhadap isu-isu kompleks, namun juga memajukan perdebatan di lapangan, memobilisasi perhatian para peneliti, pemangku kepentingan dan masyarakat dengan menyelenggarakan seminar dan acara publik, serta membentuk sinergi dengan penelitian lain. proyek. Selain itu, elemen penting dalam proyek Siber-Trust adalah, untuk memastikan bahwa dampak terhadap kerangka hukum dan peraturan akan dipertimbangkan secara efektif, konsorsium juga telah menetapkan sejumlah hal yang disebut sebagai 'Siber-Trust'. Indikator Kinerja Utama (KPI) hukum dan etika. Misalnya, mitra harus berupaya mewujudkan KPI spesifik yang menetapkan jumlah minimum tindakan pelestarian privasi yang harus disertakan oleh sistem secara default.

Langkah Keenam: Periksa Sebelum Pilot

Sebelum uji coba ini dilakukan, mitra-mitra utama diundang untuk melakukan pemeriksaan akhir untuk memastikan bahwa seluruh kondisi yang terkait dengan kepatuhan telah dipenuhi. Hal ini mencakup ketersediaan dokumentasi penting, seperti lembar informasi peserta penelitian dan formulir persetujuan, melanjutkan dan menyelesaikan komunikasi dengan Petugas Perlindungan Data atau komite Etika mereka dan menerima segala jenis izin atau otorisasi yang diperlukan serta meninjau dan menyelesaikan aliran data.

Langkah Ketujuh: Review dan Laporan Penilaian Kedua

Menjelang akhir siklus hidup proyek, peninjauan laporan penilaian dampak direncanakan. Tujuan dari tinjauan ini adalah untuk menilai upaya para mitra dalam menggabungkan hasil penilaian dampak pertama selama perancangan dan implementasi aktual dalam uji coba, melakukan penilaian risiko komparatif berdasarkan matriks penilaian risiko awal dan merefleksikannya. permasalahan baru apa pun yang mungkin muncul akibat pembaruan teknis atau peraturan, antara laporan pertama dan kedua. Selama peninjauan, mengingat kematangan hasil uji coba, konsorsium pertama-tama akan memeriksa apakah lebih banyak komponen (dibandingkan dengan laporan pertama) yang harus dinilai atau apakah komponen-komponen yang tidak termasuk dalam laporan pertama harus dinilai sekarang. Selama peninjauan, konsorsium juga bertujuan untuk mengatasi permasalahan pada Langkah 4, misalnya meningkatkan pemahaman antara mitra teknis dan non-teknis dengan memperluas glosarium yang sudah ada dan mengoptimalkan metodologi. Kuesioner yang ditargetkan dan dibuat khusus akan digunakan kembali pada tahap ini dan diskusi bilateral dengan para mitra akan dilakukan. Hasilnya akan dikumpulkan dalam laporan tertulis, yang bersama dengan dokumentasi teknisnya, akan menyertai platform Siber-Trust final jika ada potensi pemasaran. Dokumentasi ini akan memungkinkan pemangku kepentingan dan pengontrol data di masa depan untuk memahami manfaat dan risiko platform dan melakukan penilaian mereka sendiri, dengan memiliki dasar yang kuat sebagai titik awal.

Yang terpenting adalah perencanaan ke depan, dimulai sejak dini, termasuk garis besar pertama dalam proposal penelitian. Kemudian, karena ini merupakan prosedur horizontal, alat dan mekanisme yang tepat (misalnya, kuesioner, repositori, glosarium, laporan) harus diidentifikasi dan digunakan agar konsorsium tetap mendapat informasi dan terlibat sepanjang siklus hidup proyek.

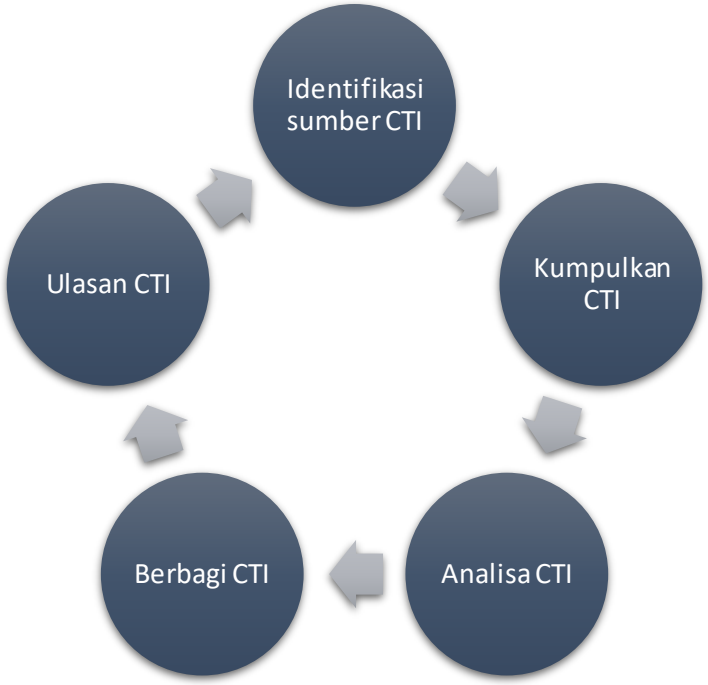
BAB 3
INTELIJEN ANCAMAN SIBER

Di dunia saat ini, teknologi telah hadir dan lebih mudah diakses melalui berbagai perangkat dan platform mulai dari server perusahaan dan PC komoditas hingga telepon seluler dan perangkat yang dapat dikenakan, yang digunakan untuk berinteraksi dan menghubungkan berbagai pemangku kepentingan seperti rumah tangga, organisasi dan infrastruktur penting. Volume dan keragaman sistem operasi yang berbeda, kekhasan perangkat, berbagai domain penggunaan, dan sifat platform yang siap diakses menciptakan lanskap ancaman yang luas dan kompleks yang sulit untuk dibendung. Upaya untuk selalu mengetahui perkembangan ancaman siber ini telah menjadi tugas yang semakin sulit, dan ketepatan waktu dalam penyampaian informasi terkait ancaman siber sangat penting untuk perlindungan dan mitigasi yang tepat. Informasi tersebut biasanya dimanfaatkan dari data yang dikumpulkan, dan mencakup kerentanan dan eksploitasi zero-day, indikator (artefak sistem atau pengamatan yang terkait dengan serangan), peringatan keamanan, laporan intelijen ancaman, serta konfigurasi alat keamanan yang direkomendasikan, dan sering kali disebut sebagai Siber-Threat Intelligence (CTI) dan mencakup pengumpulan, analisis, pemanfaatan, pengelolaan, dan pembagian data dalam jumlah besar. Dalam bab ini, kami menguraikan INTIME, sebuah sistem yang menggabungkan dan memperluas alat dan teknik terkini dari siklus hidup CTI dengan memberikan pandangan holistik dalam proses Siber-Threat Intelligence. Melalui proses ini pembaca akan dapat (i) mengidentifikasi sejumlah alat dan teknologi modern yang terkait dengan siklus hidup CTI yang disebutkan di atas, (ii) mendeteksi permasalahan dan tantangan penelitian yang terlibat dalam perancangan teknologi utama untuk pra-pengintaian Intelijen Ancaman Siber, dan (iii) merencanakan kegiatan tindak lanjut yang memungkinkan penerapan kemajuan terkini di bidang ini.

3.1 PENDAHULUAN

Selama bertahun-tahun, ancaman dunia maya telah meningkat baik dalam jumlah maupun kecanggihannya; Musuh kini menggunakan serangkaian alat dan taktik untuk menyerang korbannya dengan motivasi mulai dari pengumpulan intelijen hingga penghancuran atau keuntungan finansial. Oleh karena itu, organisasi di seluruh dunia, mulai dari pemerintah hingga perusahaan publik dan perusahaan, terus-menerus berada dalam ancaman akibat serangan siber yang terus berkembang ini. Akhir-akhir ini, pemanfaatan perangkat Internet-of-Things (IoT) pada sejumlah aplikasi, mulai dari otomatisasi rumah hingga pemantauan infrastruktur penting, telah menciptakan lanskap pertahanan siber yang semakin rumit. Banyaknya perangkat IoT yang digunakan secara global, yang sebagian besar mudah diakses dan diretas, memungkinkan pelaku ancaman untuk menggunakannya sebagai sistem pengiriman senjata siber pilihan dalam banyak serangan siber saat ini, mulai dari pembuatan botnet untuk Serangan Distributed Denial-of-Service (DDoS) terhadap penyebaran malware dan spam.

Upaya untuk tetap mengikuti perkembangan ancaman siber ini telah menjadi tugas yang semakin sulit, dan ketepatan waktu dalam penyampaian informasi terkait ancaman siber sangat penting untuk perlindungan dan mitigasi yang tepat. Informasi tersebut biasanya dimanfaatkan dari data yang dikumpulkan, dan mencakup kerentanan dan eksploitasi zero-day, indikator (yaitu artefak sistem atau pengamatan yang terkait dengan serangan), peringatan keamanan, laporan intelijen ancaman, serta konfigurasi alat keamanan yang direkomendasikan, dan sering kali disebut sebagai Siber-Threat Intelligence (CTI). Untuk mencapai tujuan ini, dengan istilah CTI kami biasanya mengacu pada informasi apa pun yang dapat membantu organisasi mengidentifikasi, menilai, memantau, dan merespons ancaman dunia maya. Di era big data, penting untuk dicatat bahwa istilah intelijen biasanya tidak mengacu pada data itu sendiri, melainkan pada informasi yang telah dikumpulkan, dianalisis, dimanfaatkan, dan diubah menjadi serangkaian tindakan yang dapat diikuti. pada, yaitu, telah menjadi dapat ditindaklanjuti.



Gambar 3.1. Siklus hidup CTI.

Siklus CTI, diilustrasikan pada Gambar 3.1, adalah proses menghasilkan dan mengevaluasi CTI. Langkah pertama dari proses ini adalah identifikasi sumber CTI. Hal ini berkaitan dengan identifikasi informasi ancaman yang perlu dikumpulkan dari perangkat pemantauan, feed, dan repositori keamanan untuk mendukung pengambilan keputusan dan meningkatkan kesadaran keamanan siber. Langkah selanjutnya, yaitu pengumpulan CTI, adalah pengumpulan data yang diperlukan dari sumber-sumber yang teridentifikasi, beserta alat untuk mengekstraksi berbagai macam informasi, baik informasi taktis maupun strategis. Proses ini tidak hanya dilakukan satu kali saja, namun dilakukan secara berkesinambungan. Tujuan utama pada tahap ini adalah mengumpulkan informasi sebanyak mungkin dan memungkinkan adanya korelasi dan analisis lebih lanjut. Langkah ketiga adalah analisis CTI dan dibangun berdasarkan informasi yang telah dikumpulkan; ini mencakup analisis otomatis

dan berbasis manusia. Langkah keempat adalah berbagi CTI kepada pemangku kepentingan terkait, yaitu entitas yang dapat memanfaatkan intelijen yang dihasilkan, dalam bentuk yang mereka anggap tepat, berguna, dan dalam banyak kasus dapat ditindaklanjuti. Hal ini membuat berbagi sangat bergantung pada audiens (misalnya, pada tingkat taktis, operasional, dan strategis). Tinjauan CTI (juga disebut sebagai umpan balik CTI), yang merupakan langkah terakhir dalam proses di atas, merupakan kunci bagi perbaikan berkelanjutan atas intelijen yang dihasilkan.

Untuk mendukung siklus hidup CTI yang diuraikan di atas, Koloveas dkk. menyajikan INTIME, sebuah kerangka kerja terpadu untuk Penambangan dan Ekstraksi Intelijen Ancaman yang mencakup teknologi utama untuk pengumpulan, analisis, pengelolaan, dan pembagian CTI pra-pengintaian melalui penggunaan alat dan teknologi canggih. INTIME adalah pendekatan yang secara holistik mendukung siklus hidup CTI secara menyeluruh melalui kerangka kerja yang terintegrasi, mudah digunakan, namun dapat diperluas dan mendukung tugas pengumpulan, konsolidasi, dan pengelolaan CTI dari forum atau pasar web dalam dan platform sosial web yang jelas, memanfaatkan informasi ini untuk mengidentifikasi ancaman yang muncul, kerentanan zero-day, dan eksploitasi baru pada perangkat IoT. Tujuan utama bab ini adalah untuk memberikan gambaran umum tentang arsitektur dan implementasi berbagai alat, metode, dan algoritme yang digunakan, dikembangkan, dan diuji di INTIME. Lebih khusus lagi, kami fokus pada komponen INTIME yang mendukung:

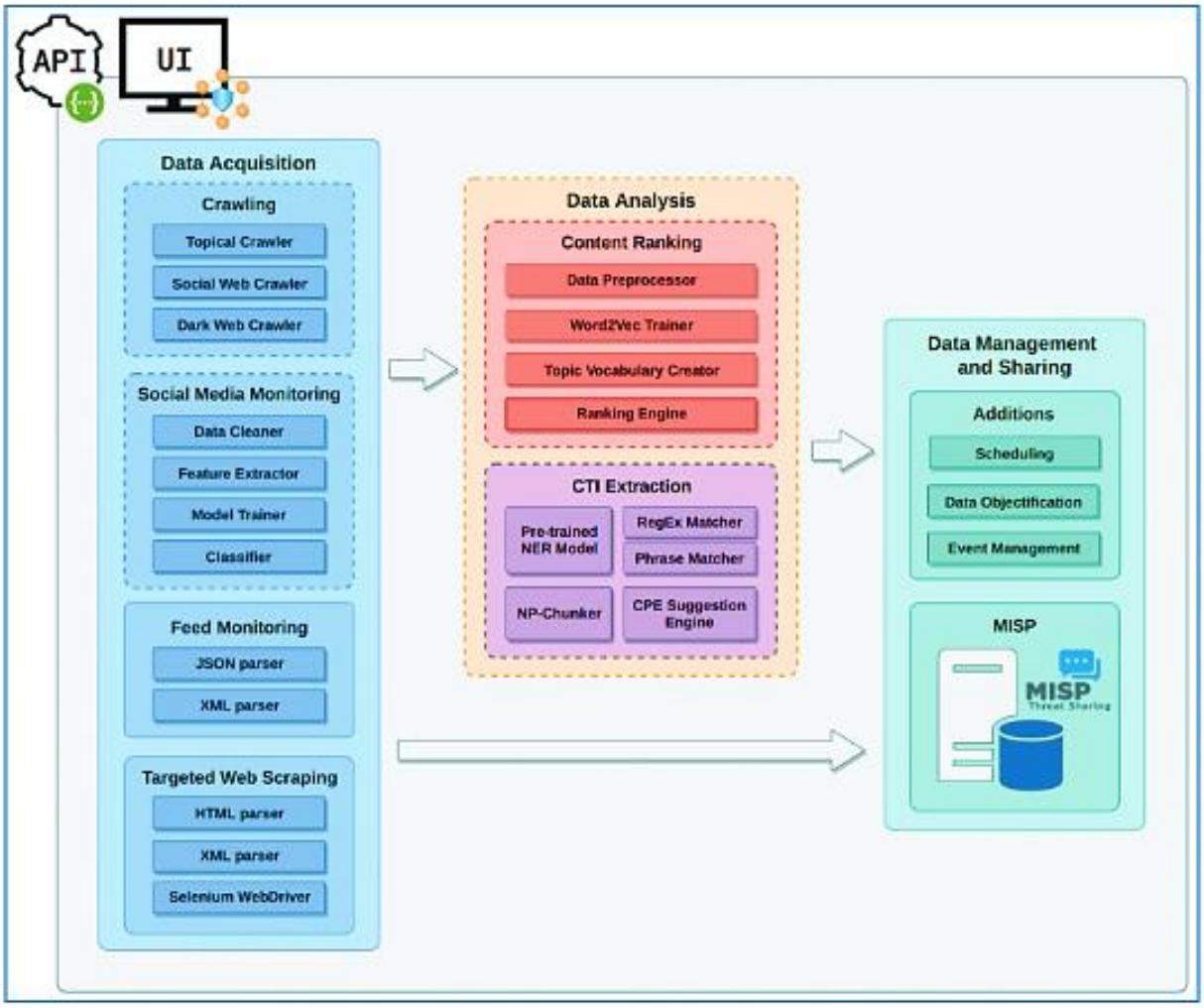
- Memutuskan apakah situs web yang dirayapi berisi CTI yang berguna; hal ini dicapai dengan memberi peringkat pada konten yang dikumpulkan untuk menilai relevansi dan kegunaannya terhadap tugas yang ada.
- Mengekstrak CTI dari konten yang dikumpulkan dan diklasifikasikan sebagai berguna, dengan menggunakan pemahaman bahasa alami yang canggih dan teknik pengenalan entitas bernama.
- Mengelola dan membagikan CTI yang dikumpulkan melalui kombinasi solusi canggih yang dibuat khusus dan diadopsi secara luas yang memungkinkan eksplorasi, konsolidasi, visualisasi, dan pembagian CTI secara lancar ke berbagai organisasi.

INTIME telah sepenuhnya dirancang dan dikembangkan dengan mengandalkan perangkat lunak sumber terbuka termasuk perayap yang berfokus pada sumber terbuka, implementasi penyematan kata sumber terbuka untuk pemodelan topik laten, alat pemahaman bahasa alami sumber terbuka, dan penyimpanan data sumber terbuka untuk penyimpanan model topik dan konten yang dirayapi.

3.2 ARSITEKTUR INTIME

Arsitektur INTIME terdiri dari tiga komponen besar, yaitu (a) Akuisisi Data, (b) Analisis Data, dan (c) Pengelolaan dan Pembagian Data. Modul Akuisisi Data bertanggung jawab untuk memantau dan merayapi berbagai sumber daya web. Tugas ini dicapai dengan menggunakan teknik perayapan dan pengikisan tradisional, serta komponen yang dibantu pembelajaran mesin untuk mengarahkan perayapan ke sumber yang relevan. Meskipun modul ini dapat dengan mudah mengekstrak informasi dari sumber spesifik yang terstruktur dengan baik, analisis lebih lanjut diperlukan jika menyangkut konten web yang dirayapi dari sumber tidak

terstruktur atau semi terstruktur. Untuk menganalisis lebih lanjut konten yang dikumpulkan, modul Analisis Data menampung dua submodul berbasis pembelajaran mesin, submodul Peringkat Konten, yang bertindak sebagai filter internal yang mengurutkan data menurut relevansinya dengan topik yang dibahas, dan submodul Peringkat Konten.



Gambar 3.2. Pandangan tingkat tinggi tentang arsitektur sistem.

Submodul Ekstraksi CTI, yang menggunakan beberapa teknik ekstraksi informasi untuk mengekstrak informasi berguna dari halaman web yang dianggap relevan. Ide di balik pendekatan dua tahap ini berasal dari ketidakmampuan crawler sederhana untuk memodelkan keterbukaan topik secara akurat. Kesulitan muncul dari situs web yang, meskipun relevan dengan topik (misalnya, membahas keamanan IoT secara umum), tidak memiliki informasi aktual yang dapat dimanfaatkan untuk intelijen yang dapat ditindaklanjuti (misalnya, tidak menyebutkan kerentanan spesifik terkait IoT) . Setelah analisis, informasi yang diekstraksi diteruskan ke modul terakhir, bernama Manajemen dan Berbagi Data, yang menampung dan menyalurkan semua Intelijen Ancaman Siber yang dikumpulkan sistem. Arsitektur ini awalnya dikembangkan oleh Koloveas et al dan fokus pada tugas perayapan dan pemeringkatan. Kemudian, hal ini diperluas hingga menjadi seperti sekarang melalui kerangka INTIME.

Yang perlu diperhatikan, Pembelajaran Mesin dan Pembelajaran Mendalam memiliki peran sentral dalam arsitektur kami, karena seluruh modul Analisis Data dibangun berdasarkan teknik Pembelajaran Mendalam seperti Penyematan Kata (peringkat konten) dan Pengenalan Entitas Bernama (ekstraksi CTI). Selain itu, modul Akuisisi Data menggunakan algoritme Pembelajaran Mesin tradisional untuk mengklasifikasikan konten yang dikumpulkan oleh submodul Perayapan dan Pemantauan Media Sosial. Pada Gambar 3.2, setiap modul yang berisi metode Machine Learning diapit oleh garis putus-putus.

3.3 MODUL AKUISISI DATA

Saat ini, informasi berguna terkait keamanan siber yang dapat dimanfaatkan untuk menghasilkan intelijen yang dapat ditindaklanjuti dapat ditemukan di berbagai sumber daring yang berbeda, mulai dari blog yang berfokus pada teknis dan keamanan di web yang jelas, diskusi antar pakar di forum keamanan khusus, media sosial, dan lain-lain. konten, hingga forum peretas web gelap bawah tanah dan pasar yang menjual alat kejahatan dunia maya serta kerentanan dan eksploitasi zero-day. Untuk memenuhi kebutuhan akuisisi data yang meluas ini, arsitektur kami menyediakan Modul Akuisisi Data yang fleksibel namun kuat yang secara konseptual dipisahkan menjadi empat submodul berbeda:

1. Submodul Perayapan memungkinkan pengguna dengan mudah menyiapkan dan menerapkan perayap pengumpulan data otomatis yang mampu menavigasi web yang jelas, sosial, dan gelap untuk menemukan dan mengumpulkan konten yang diinginkan. Submodul Perayapan memungkinkan pengguna untuk memilih di antara beragam opsi termasuk perayapan terfokus (juga disebut sebagai topikal) yang diarahkan oleh metode pembelajaran mesin yang sesuai, pengunduhan seluruh domain berdasarkan perayap mendalam yang kuat namun mudah diatur, berbasis TOR penjelajahan web gelap, dan penanganan metode autentikasi semi-otomatis berdasarkan manajemen cookie. Setelah mengumpulkan konten yang diinginkan, pengguna kemudian dapat menggunakan modul lainnya yang disediakan oleh arsitektur kami untuk memprosesnya lebih lanjut guna mengekstraksi CTI yang berguna darinya.
2. Submodul Pemantauan Media Sosial memungkinkan pengguna memantau aliran media sosial populer untuk konten yang diminati; untuk melakukan hal ini, mereka menggunakan API yang tersedia untuk umum dari platform sosial dan menyediakan serangkaian algoritme klasifikasi yang telah dilatih sebelumnya dan siap digunakan yang dapat digunakan untuk membedakan antara konten yang relevan dan tidak relevan.
3. Submodul Pemantauan Umpan memungkinkan pengguna memantau umpan data berbasis JSON atau RSS terstruktur dari sumber mapan seperti NIST, sekaligus memungkinkan mereka memodifikasi beberapa parameter pemantauan seperti interval pemantauan dan jenis objek yang mereka minati (misalnya, CVE, CPE, atau CWE).
4. Modul Targeted Web Scraping menyediakan akses ke data terstruktur dari sumber terpercaya yang tidak menyediakan kemampuan umpan data. Penyertaan sumber-sumber tersebut merupakan hal yang tidak biasa bagi pengguna akhir, namun karena sifat tugas web scraping, memasukkan sumber-sumber baru memerlukan tingkat teknis tertentu. Untuk mendukung proses ini, arsitektur kami menawarkan seperangkat alat pra-

instal yang dapat digunakan untuk membantu pemrogram, termasuk penguraian HTML standar, kueri XPath, serta alat dan pustaka penanganan JavaScript.

Semua data yang diekstraksi dari submodul Perayapan dan Pemantauan Media Sosial, disimpan dalam database NoSQL internal (MongoDB), di mana data tersebut dianalisis oleh submodul Peringkat Konten dan Ekstraksi CTI dari modul Analisis Data. Selanjutnya dikirim ke modul Pengelolaan dan Pembagian Data dalam bentuk CTI terstruktur. Perhatikan bahwa data yang dikumpulkan oleh submodul Pemantauan Umpan dan Pengikisan Web Bertarget dari sumber data terstruktur langsung disimpan ke modul Manajemen dan Berbagi Data karena tidak memerlukan pemrosesan lebih lanjut. Pada bagian berikut, kami menguraikan lebih lanjut submodul yang diuraikan di atas.

Submodul Perayapan

Submodul Perayapan mengimplementasikan beberapa layanan berbeda yang dapat diminta oleh pengguna untuk memulai pengumpulan data otomatis pada berbagai sumber online di web yang jelas, sosial, atau gelap; infrastruktur perayapan yang mendasarinya dibangun di atas perayap Ache Nyu.

Fungsi perayapan terfokus menggunakan Pengklasifikasi Halaman SMILE, yang menggunakan pengklasifikasi teks Pembelajaran Mesin, yang dilatih dengan pilihan contoh laman web positif dan negatif, untuk mengarahkan perayapan ke situs web yang relevan secara topik (dalam kasus kami, situs web dengan konten yang relevan dengan keamanan siber). Fungsionalitas ini juga dapat dibantu oleh sub-komponen SeedFinder, yang dapat membantu proses pencarian benih awal untuk perayapan terfokus; hal ini dicapai dengan menggabungkan model klasifikasi dengan kueri yang disediakan pengguna yang relevan dengan topik.

Perayapan mendalam pada dasarnya adalah operasi pengunduhan domain berdasarkan perayap ACHE yang melintasi domain tertentu (seperti forum atau situs web) dengan cara penelusuran yang mengutamakan luas dan mengunduh semua laman web di dalamnya. Untuk mengarahkan perayapan ke bagian tertentu dari domain, filter berbasis regex digunakan; filter ini menyediakan fungsionalitas daftar hitam dan daftar putih untuk mengarahkan crawler menjauh dari dan menuju masing-masing bagian domain tertentu. Dengan cara ini pengguna dapat menginstruksikan crawler untuk menghindari mengunduh halaman yang tidak informatif (misalnya, area anggota, halaman login atau bantuan) atau secara aktif mengarahkannya ke rangkaian diskusi tertentu di forum.

Perayapan web gelap juga didukung oleh arsitektur INTIME. Fungsionalitas ini bergantung pada pemanfaatan proxy TOR untuk mengunjungi tautan bawang yang ditentukan pengguna. Perhatikan bahwa pengguna tidak diharuskan memiliki pengalaman apa pun dalam prosedur ini, karena semua tindakan yang diperlukan (yaitu, bergabung dengan jaringan TOR, menggunakan proxy, menginisialisasi crawler) dilakukan secara otomatis melalui panggilan API internal.

Masalah autentikasi apa pun yang mungkin timbul selama perayapan diselesaikan melalui login pengguna manual (pertama kali perayap menemui hambatan autentikasi) dan penyimpanan cookie sesi untuk semua kunjungan perayap berikutnya.

Submodul Pemantauan Media Sosial

Submodul Pemantauan Media Sosial berfokus pada deteksi peristiwa real-time dari aliran sosial menggunakan alat canggih dari domain ilmu data untuk secara otomatis mengklasifikasikan postingan sebagai terkait atau tidak terkait dengan topik yang ditentukan pengguna. Untuk mengumpulkan data dari aliran media sosial, submodul ini menggunakan API platform sosial yang disediakan; pengguna dapat menentukan sekumpulan akun media sosial dan/atau sekumpulan kata kunci yang diminati dan mekanisme pengumpulan konten akan mengambil (dengan cara publikasi/berlangganan berulang) semua konten yang diposting dari akun tersebut atau cocok dengan kata kunci yang disediakan.

Selanjutnya, pengguna dapat mengklasifikasikan konten yang diambil sebagai terkait atau tidak terkait dengan tugas hanya dengan memilih di antara berbagai algoritma klasifikasi populer termasuk (multinomial) Naive Bayes, K-Nearest Neighbors, pohon keputusan, hutan acak, regresi logistik, SVM, serta model pembelajaran mendalam yang telah terbukti seperti Convolutional Neural Networks. Semua algoritma klasifikasi dan pembelajaran mesin telah dilatih sebelumnya pada data dunia nyata dan dengan pengaturan parameter default untuk tugas klasifikasi keamanan, namun pengguna dapat memodifikasi data pelatihan dan parameter pengaturan agar sesuai dengan kebutuhan klasifikasi spesifik mereka. Proses di atas disederhanakan agar dapat langsung digunakan, namun pengguna tingkat lanjut juga dapat menyesuaikan semua bagian proses, termasuk akuisisi konten dari media sosial tanpa API, pengenalan klasifikasi lain atau algoritma pembelajaran mesin, dan pelatihan algoritma khusus tugas.

Submodul untuk Memantau Sumber Terstruktur

Selain data tidak terstruktur dan semi terstruktur yang dikumpulkan oleh fungsi-fungsi yang disebutkan di atas, sistem kami juga dapat dilengkapi dengan data terstruktur dari sumber CTI yang memiliki reputasi baik. Sumber-sumber tersebut dapat dibagi dalam dua kategori utama. Kategori pertama menyediakan umpan data terstruktur dari kumpulan informasi. Kategori kedua tidak menyediakan data feed namun mengekspos konten database mereka pada UI berbasis web secara terstruktur. Arsitektur kami menyediakan fungsionalitas untuk mengekstrak informasi dari kedua kategori.

Untuk kategori pertama, sistem menggunakan teknik parsing JSON/XML standar dengan periode pemantauan variabel bergantung pada frekuensi pembaruan data feed. Sumber tersebut mencakup penyimpanan data kerentanan NVD2 dan JVN3, yang masing-masing menyediakan datanya dalam umpan data JSON dan XML. Untuk kategori kedua, beberapa teknik scraping telah diterapkan, menyediakan seperangkat alat yang fleksibel untuk memperhitungkan berbagai jenis situs web di mana informasi tersebut berada. Teknik-teknik ini berkisar dari penguraian HTML standar dan kueri XPath, hingga WebDriver canggih untuk manipulasi formulir otomatis dan penghapusan pop-up dinamis. Sumber dalam kategori ini mencakup penyimpanan data kerentanan KB-Cert4 dan VulDB5 serta Exploit-DB, yang merupakan arsip eksploitasi publik yang sesuai dengan CVE dan perangkat lunak rentan terkait.

Seperti disebutkan sebelumnya, data yang diperoleh dari sumber-sumber ini dimasukkan langsung ke dalam modul Manajemen dan Berbagi Data tanpa melalui modul Analisis Data, karena sudah terstruktur dalam bentuk CTI yang diinginkan.

3.4 MODUL ANALISIS DATA

Memutuskan apakah suatu situs web yang dikumpulkan berisi Intelijen Ancaman Siber yang berguna merupakan tugas yang menantang, mengingat sifat umum dari banyak situs web yang membahas masalah keamanan umum. Untuk mengatasi masalah ini, kami membuat lapisan pemrosesan tambahan yang awalnya memberi peringkat pada konten yang dikumpulkan untuk menilai relevansi dan kegunaannya terhadap tugas yang ada (submodul Peringkat Konten) dan kemudian mencoba mengekstrak CTI yang dapat ditindaklanjuti dari dokumen dengan peringkat tertinggi (submodul Ekstraksi CTI) .

Submodul Pemeringkatan Konten

Ide di balik pendekatan pemeringkatan kami adalah untuk merepresentasikan topik sebagai distribusi kosakata dengan memanfaatkan vektor distribusi kata-kata terkait; misalnya, topik tentang keamanan IoT dapat ditangkap dengan kata dan frasa terkait seperti “Mirai botnet”, “IoT”, atau “exploit kits”. Frasa penting yang terkait dengan topik tersebut dapat diperoleh dengan pelatihan model topik laten tanpa/semi-pengawasan melalui kumpulan data eksternal seperti IoT dan forum terkait keamanan. Dengan cara ini, kami dapat menangkap ketergantungan semantik dan korelasi statistik antar kata untuk topik tertentu dan merepresentasikannya dalam ruang laten berdimensi rendah. Untuk melakukannya, kami menggunakan Word2Vec; jaringan saraf dua lapis yang dangkal yang dapat dilatih untuk merekonstruksi konteks linguistik dan memetakan kata-kata yang mirip secara semantik di dekat ruang penyematan. Setiap kata dalam ruang penyematan direpresentasikan sebagai kata penyematan. Penyematan kata tersebut dapat menangkap hubungan antara kata-kata dalam kumpulan data, sehingga memungkinkan aritmatika vektor. Metode yang diuraikan di atas, bersama dengan metode memetakan kata-kata ke topik kita, yang akan dibahas nanti, dapat membantu kita membuat Kosakata Topik.

Kosakata Topik. Untuk melatih model Word2Vec, kami harus membuat kumpulan data yang sesuai untuk tugas Pemeringkatan Konten. Kumpulan data kami harus berisi kosakata umum yang digunakan saat topik IoT dan Keamanan sedang dibahas. Untuk menangkap kosakata ini, kami menggunakan sejumlah forum diskusi berbeda dalam ekosistem Stack Exchange. Untuk mencapai tujuan ini, kami memanfaatkan Stack Exchange Data Dump untuk mendapatkan akses ke IoT dan forum diskusi terkait keamanan termasuk Internet of Things, Keamanan Informasi, Arduino, dan Raspberry Pi. Dua yang terakhir dipilih karena merupakan yang paling perangkat terkemuka untuk proyek IoT khusus dengan komunitas yang sangat aktif, sehingga datanya akan membantu model kami untuk menggabungkan kosakata teknis IoT dengan lebih baik. Data dump yang digunakan berisi diskusi pengguna dalam bentuk tanya jawab, termasuk teks dari postingan, komentar, dan tag khusus diskusi dalam format XML. Postingan dan komentar digunakan sebagai masukan utama untuk model.

Dalam banyak kasus, kata-kata dari model yang dilatih terlalu umum atau di luar topik, oleh karena itu, diperlukan metode yang dapat menghilangkan kata-kata tersebut, untuk

menciptakan kosa kata yang lebih kecil, lebih kuat, dan spesifik topik. Untuk melakukannya, kami menggunakan tag yang diekstraksi dan menambahkannya dengan kumpulan N istilah paling terkait di ruang laten untuk setiap tag. Tabel 3.1 menunjukkan contoh istilah yang paling relevan dengan tag pengguna DDoS, untuk N = 5, 10, 15.

Mesin Pemeringkatan. Karena CTI yang berguna diwujudkan dalam bentuk artikel keamanan siber, postingan pengguna di forum keamanan/peretas, atau postingan iklan di pasar kejahatan siber, maka CTI juga dapat dikategorikan sebagai vektor distribusi kata-kata. Dengan begitu, kita dapat membandingkan kesamaan antara vektor distribusi konten yang dikumpulkan dan topik tertentu untuk menilai relevansi dan kegunaan konten.

Untuk melakukannya, kami menggunakan sub-komponen Mesin Pemeringkatan. Komponen ini pertama-tama membuat Vektor Topik, dengan memanfaatkan Kosakata Topik yang dihasilkan, lalu membuat Vektor Postingan untuk setiap entri postingan dalam koleksi yang dirayapi.

Tabel 3.1. Istilah Paling Relevan untuk Tag "DDoS".

Rank	Term
#1	volumetric
#2	dos
#3	flooding
#4	flood
#5	sloloris
#6	denial_of_service
#7	cloudflare
#8	prolexic
#9	floods
#10	aldos
#11	slowloris
#12	Ip_spoofing
#13	loic
#14	drdos
#15	zombies

Vektor Topik T→ dibangun sebagai jumlah dari vektor distribusi semua istilah topik t→i yang ada dalam kosakata topik, yaitu,

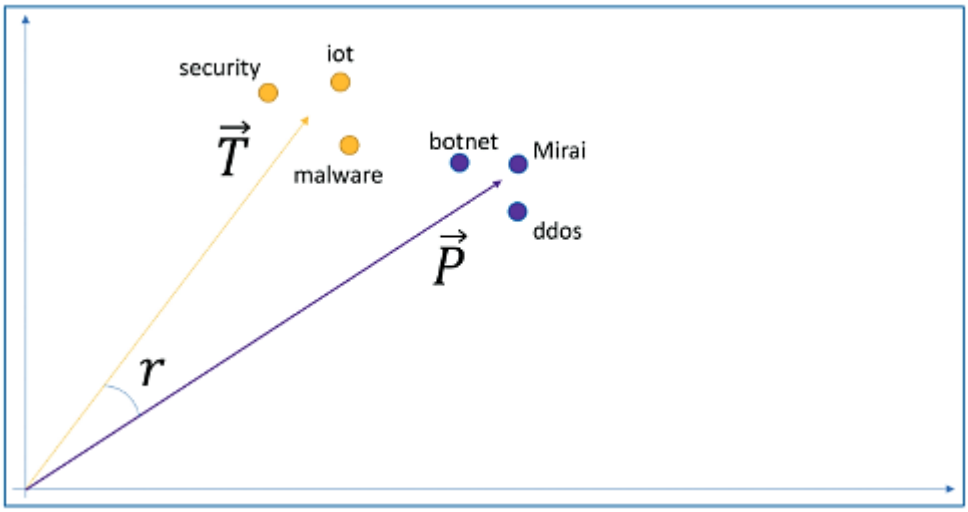
$$\vec{T} = \sum_{\forall_i} \vec{t_\iota}$$

Demikian pula, Post Vector P→ dibangun sebagai jumlah dari vektor distribusi semua post term w→j yang ada dalam kosakata topik. Untuk mempromosikan dampak kata-kata yang terkait dengan topik yang dibahas, kami memperkenalkan skema pembobotan yang bergantung pada topik untuk vektor pos dengan semangat [6]. Yakni untuk topik T dan postingan berisi himpunan kata {w→1, w→2, . . .}, vektor pos dihitung sebagai

$$\vec{P} = \sum_{\forall_j} \cos\,(\vec{w}_j, \vec{T})\vec{w}_j$$

Tabel 3.2. Perhitungan Skor Relevansi.

Kutipan dari:www.iotforall.com/5-worst-iot-hacking-vulnerabilities Mirai Botnet (alias Dyn Attack) Pada bulan Oktober 2016, serangan DDoS terbesar yang pernah diluncurkan pada penyedia layanan Dyn menggunakan botnet IoT. Hal ini menyebabkan sebagian besar internet mati, termasuk Twitter, Guardian, Netflix, Reddit, dan CNN. Botnet IoT ini dimungkinkan oleh malware bernama Mirai. Setelah terinfeksi Mirai, komputer terus mencari perangkat IoT yang rentan di internet dan kemudian menggunakan nama pengguna dan kata sandi default yang diketahui untuk masuk, sehingga menginfeksi perangkat tersebut dengan malware. Perangkat ini seperti kamera digital dan pemutar DVR. Skor Relevansi: 0,8563855440900794



Gambar 3.3. Visualisasi teoritis dari proses komputasi.

Terakhir, setelah kedua vektor dihitung, Skor Relevansi r antara topik T dan postingan P dihitung sebagai kemiripan kosinus dari masing-masing vektor distribusinya di ruang laten.

$$r = \cos(\vec{T}, \vec{P})$$

Setelah menghitung skor relevansi untuk setiap postingan yang dirayapi di penyimpanan data kami, tugas mengidentifikasi informasi yang relevan/berguna dapat dengan mudah direduksi menjadi campuran operasi ambang batas dan pemilihan top-k. Tabel 3.2 menampilkan contoh proses yang diikuti oleh komponen. Gambar 3.3 menunjukkan visualisasi teoritis dari proses komputasi.

Submodul Ekstraksi CTI

Setelah komponen Pemeringkatan Konten menentukan situs web mana yang lebih mungkin berisi Intelijen Ancaman Siber, sistem kami harus dapat mengekstrak CTI tersebut.

Untuk melakukannya, kami menggunakan beberapa mekanisme seperti Pengenalan Entitas Bernama dengan entitas yang dipelajari dan berbasis Regex, Penguraian Ketergantungan untuk mengidentifikasi eksploitasi, malware, dan kerentanan berdasarkan struktur dokumen, serta, mesin saran CPE baru untuk membantu semi- tautan otomatis ke skema penamaan platform/kerentanan yang diketahui.

Pengakuan Entitas Bernama. Teknik utama yang digunakan untuk tugas ini adalah Named Entity Recognition (NER). Teknik ini dapat mengidentifikasi entitas spesifik yang berpotensi mengarah pada penemuan CTI. Daripada melatih model NER dengan data yang dianotasi entitas dari awal, model yang telah dilatih sebelumnya digunakan untuk mendeteksi entitas umum yang tidak terbatas pada topik CTI. Untuk membantu model terlatih dalam menemukan lebih banyak entitas yang terkait dengan topik, fungsi Pencocokan Frasa digunakan. Pencocokan Frasa dapat melakukan pencocokan sebagian dan seluruh frasa multi-kata yang unik dan memetakannya ke entitas bernama tertentu. Frasa yang kami impor ke model adalah nama lengkap perusahaan/organisasi dan produk yang diambil dari JVN dan dipetakan ke entitas ORG dan PRODUK (Tabel 3.3). Selain entitas yang dapat diidentifikasi oleh model terlatih, beberapa entitas khusus domain juga diperkenalkan. Entitas ini dimasukkan ke saluran NER dengan menentukan Ekspresi Reguler untuk masing-masing entitas, melalui fungsi Regex Matcher. Tabel 3.3 menunjukkan entitas yang dapat diidentifikasi oleh INTIME, beserta mekanisme yang bertanggung jawab untuk identifikasi tersebut. Gambar 3.4 menunjukkan beberapa entitas yang teridentifikasi pada contoh teks.

Mesin Saran CPE. Pada bagian sebelumnya, kami menguraikan proses mengekstraksi Entitas Bernama dari dokumen teks tidak terstruktur dalam upaya mengidentifikasi Intelijen Ancaman Siber. Meskipun ini merupakan tugas yang penting, informasi yang diekstraksi sebagian besar masih tidak terstruktur dan karena modul Manajemen dan Berbagi Data sudah berisi sejumlah besar CTI yang terverifikasi dan terstruktur, sebuah mekanisme yang akan membantu pakar keamanan menghubungkan CTI yang baru ditemukan dengan peristiwa yang ada akan bermanfaat bagi keseluruhan jalur pipa CTI.

Entitas paling jelas yang dapat kami gunakan untuk memetakan data yang baru ditemukan ke CTI terstruktur adalah “CVE” dan “CPE”. Namun, pengguna non-teknis cenderung tidak menggunakan jenis pengenal ini ketika mereka berkomunikasi dalam konteks forum web, dll., sehingga kemungkinan bertemu dengan mereka dalam jumlah yang cukup besar adalah rendah. Oleh karena itu, solusi hybrid dirancang, Mesin Saran CPE, yang akan kami uraikan di bawah.

Meskipun entitas CVE dan CPE sangat jarang ditemukan dalam pengaturan teks bebas, entitas Produk muncul dengan frekuensi tinggi pada kumpulan teks relevan. Akibatnya, database produk digunakan untuk membuat mesin rekomendasi, yang dengan memanfaatkan metode pengambilan teks, menyarankan CPE yang paling mungkin terkait dengan entitas Produk tertentu. Saran tersebut ditambahkan ke objek yang dikirim ke komponen Manajemen dan Berbagi Data, di mana pakar keamanan dapat mengevaluasi CPE yang disarankan untuk melihat apakah CPE tersebut benar-benar cocok dengan Peristiwa yang ada, dan selanjutnya, melakukan penautan Objek bila diperlukan.

Tabel 3.3. Jenis entitas yang didukung.

Tingkatan	Ketentuan	Sumber
PERSON	Orang, Termasuk fiksi	Model Terlatih
ORG	Perusahaan, Agensi, Institusi, dll	Model Terlatih, PhraseMatcher
PRODUCT	Benda, Kendaraan, Makanan, dll	Model Terlatih, PhraseMatcher
DATE	Tanggal/Periode absolut/relatif	Model Terlatih,
TIME	Lebih kecil dari sehari	Model Terlatih,
MONEY	Nilai Moneter	Model Terlatih, RegexMatcher
CVE	Pengidentifikasian kerentanan dan Eksposure umum (CVE)	RegexMatcher
CPE	Pengidentifikasian Pencacahan Platform Umum	RegexMatcher
CWE	Pencacahan Kelemahan Umum (CWE) indentifier	RegexMatcher
CVSS2_VECTOR	Sistem penilaian kerentanan umum (CVSS) V2	RegexMatcher
CVSS3_VECTOR	Sistem penilaian kerentanan umum (CVSS) V3	RegexMatcher
IP	Alamat IP	RegexMatcher
VERSION	Versi perangkat lunak	RegexMatcher
FILE	Nama File atau Ekstensi file	RegexMatcher
COMMAND/ FUCTION/ CONFIG	Perintah/fungsi/kode/ pengaturan konfigurasi	RegexMatcher

Gambar 3.4. Entitas yang teridentifikasi.

Saran lebih disukai daripada pencocokan string yang tepat pada entitas Produk terutama karena fakta bahwa dalam pengaturan teks bebas, pengguna mungkin menyingkat bagian dari produk, hanya menggunakan nama populer yang umum dari produk tersebut (misalnya, “Struts” daripada “ Apache Struts”), atau sekadar membuat kesalahan ejaan. Untuk menyajikan saran yang akurat, masalah tersebut didekati dengan melakukan pencarian teks fuzzy. Untuk itu, Mesin Saran CPE menggunakan n-gram, metode umum untuk menghitung kesamaan teks. Awalnya, n-gram untuk setiap produk dalam database dihasilkan dan diindeks. Kemudian, kueri untuk setiap entitas Produk yang ditemukan dilakukan, dan dengan

menggunakan Operator Pencarian Teks MongoDB, modul membandingkan kesamaan n-gram kueri dengan n-gram yang diindeks. Pada akhirnya, 10 hasil teratas dikembalikan, diurutkan berdasarkan skor kecocokan teks.

NP-Chunking. Untuk bagian akhir Ekstraksi CTI, Dependency Parser digunakan untuk melakukan tugas "Noun Phrase Chunking" (NP Chunking). NP Chunking- subset dari Text Chunking yang berhubungan dengan tugas mengenali bagian teks yang tidak tumpang tindih yang terdiri dari frase kata benda (NP).

Meskipun sebagian besar CTI yang dapat kita temukan dapat dimodelkan secara efektif ke Named Entity Recogniser, beberapa konsep spesifik domain tidak dapat didefinisikan secara memadai sebagai entitas bernama. Konsep tersebut mencakup jenis serangan dan kerentanan sistem, nama eksploitasi, nama malware, dll. Konsep tersebut dapat ditambahkan ke Pencocokan Frasa sebagai daftar terminologi, namun karena cara dinamis konsep tersebut dijelaskan dalam teks non-teknis, efektivitas sistemnya tidak akan memuaskan.

Setelah mengamati secara menyeluruh data yang dikumpulkan, kami menemukan pola umum, bahwa konsep-konsep ini secara bawaan diekspresikan sebagai potongan Frasa Kata Benda. Misalnya, frasa seperti "kerentanan injeksi basis data", "serangan brute-force", dan "eksploitasi eskalasi hak istimewa" semuanya merupakan NP yang dapat diklasifikasikan sebagai Intelijen Ancaman Siber, dan kami tidak akan dapat mengidentifikasinya dengan pra-penelitian kami. infrastruktur yang ada.

Untuk tujuan ini, sebagai bagian dari modul Ekstraksi CTI, kami telah menerapkan NP Chunker yang mendeteksi semua potongan NP yang ditemukan dalam dokumen dan mengelompokkannya dalam sebuah objek yang disebut HIGHLIGHTS.

Misalnya, pada dokumen yang disajikan pada Gambar 3.4, HIGHLIGHTS akan menjadi sebagai berikut:

- "Kerentanan Apache Struts",
- "bug eksekusi kode jarak jauh", dan
- "Pembaruan Patch Kritis April 2017"

Metode ini sangat membantu para pakar keamanan untuk dengan cepat mengidentifikasi apakah suatu dokumen berisi CTI yang dapat ditindaklanjuti, atau menghubungkannya ke objek CTI yang ada dari berbagai sumber.

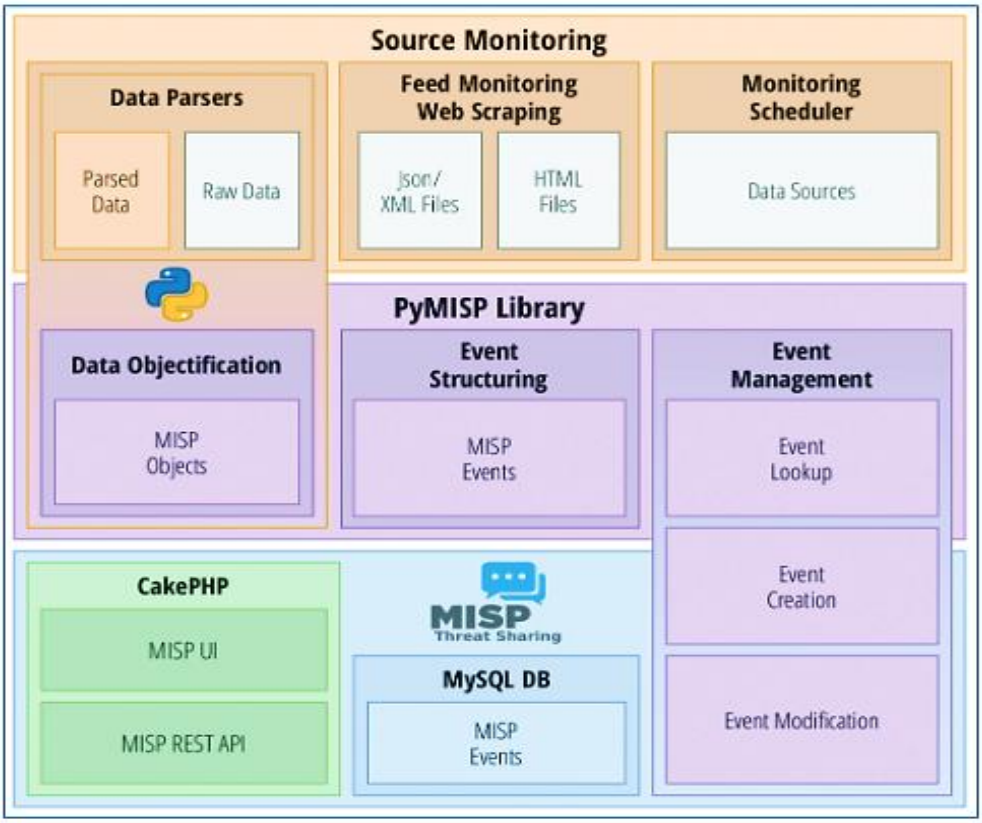
3.5 PENGELOLAAN DAN PEMBAGIAN DATA

Pada bagian ini kami menyajikan komponen Manajemen dan Berbagi Data, yang merupakan solusi full-stack, yang bertujuan untuk menyediakan metodologi proaktif lengkap untuk tugas manajemen dan berbagi CTI. Komponen tersebut mampu menyimpan CTI dari berbagai sumber, menggabungkan artefak yang berkaitan dengan informasi tentang CTI yang sama, dan saling mengkorelasikan CTI serupa. Setelah menyimpan semua CTI yang dikumpulkan, komponen Pengelolaan dan Pembagian Data mampu menyajikan semua informasi yang disimpan dalam format yang dapat dibaca manusia, melalui aplikasi web MISP. Antarmuka memungkinkan pengguna untuk mengedit lebih lanjut, menganalisis, dan memperkaya CTI yang disimpan. Yang terakhir, melalui pemanfaatan MISP, hal ini

memungkinkan pembagian CTI yang disimpan, baik dalam format yang dapat dibaca manusia maupun mesin.

Ikhtisar Komponen

Pertama, kami telah mengidentifikasi berbagai sumber CTI, yaitu database kerentanan dan eksploitasi, yang berisi analisis CTI, dalam bentuk laporan kerentanan dan eksploitasi. Laporan-laporan ini sebagian besar terdiri dari sejumlah informasi intelijen yang berguna dan dapat ditindaklanjuti mengenai kerentanan dan eksploitasi, seperti deskripsi kerentanan yang ada, bukti konsep eksploitasi, daftar konfigurasi produk yang terkena dampak. (CPE), metrik yang memberikan faktor dampak untuk produk yang terkena dampak (CVSS), tanggal publikasi dan modifikasi, referensi ke laporan serupa, dan pengidentifikasi unik yang telah ditetapkan ke kerentanan yang ada (ID CVE). Namun, meskipun sumber-sumber yang disebutkan di atas sering kali memberikan laporan tentang ID CVE unik yang sama, namun laporan tersebut cenderung berbeda. Hal ini terjadi karena dinamisnya informasi yang tersedia pada saat analisis. Dengan demikian, analisis yang terjadi pada waktu berbeda, mungkin memberikan metrik yang berbeda dalam laporan akhir. Untuk mengatasi masalah ini, kami mengumpulkan semua laporan yang tersedia untuk umum dari sumber-sumber ini, kami menguraikannya, satu per satu, untuk mengekstrak CTI yang disediakan, menggunakan modul Feed Monitoring dan Targeted Web Scraping. Kemudian, kami menyimpan CTI yang telah diurai, secara berkelompok, dengan memperhatikan ID CVE unik yang dicakupnya. Platform yang dipilih untuk menyimpan dan menyebarkan CTI yang dikumpulkan adalah MISP.



Gambar 3.5. Arsitektur Berbagi dan Manajemen Data.

Cluster ini disebut peristiwa dalam platform MISP dan pengelompokan laporan terjadi pada fase manajemen peristiwa yang diilustrasikan pada Gambar 3.5, di mana kami menyajikan pandangan abstrak dari arsitektur komponen. MISP menyediakan informasi yang disimpan dalam basis datanya, dalam format yang dapat dibaca manusia dan mesin, dan memungkinkan pengguna untuk mengaksesnya melalui GUI atau melalui REST API. Terakhir, MISP telah menerapkan berbagai alat, tersedia di GUI, yang memungkinkan pengguna UI meninjau CTI yang dikumpulkan dan menghilangkan positif palsu atau mengomentari artefak, dan menganalisis lebih lanjut serta memperkaya CTI melalui proses korelasi.

MISP

MISP memimpin perlombaan platform, sebagai platform yang paling sesuai untuk tujuan dukungan siklus hidup CTI. Oleh karena itu, ini adalah platform pilihan untuk pengelolaan CTI dan berbagi INTIME. Secara khusus, modul Manajemen dan Berbagi Data menggunakan, memperluas dan meningkatkan MISP, untuk memperkaya kemampuan penyimpanannya dengan konteks tambahan. Di bagian selanjutnya, kami akan menjelaskan rincian penting PPAM, yang berkaitan dengan (i) model datanya, (ii) properti dan fitur berbagi CTI, dan (iii) fitur tambahannya.

Tujuan utama dari model data MISP adalah untuk memiliki format minimum yang layak, yang dapat diperluas, sesuai dengan kebutuhan kompleksitas tambahan, daripada mencoba untuk menangkap semua kemungkinan kebutuhan di masa depan terlebih dahulu. Entri baru dalam MISP disebut objek peristiwa, yang ditentukan oleh serangkaian karakteristik, beserta semua jenis deskripsi masing-masing indikator, termasuk lampirannya. Karakteristik ini disebut atribut dalam MISP, dan memberikan semua informasi yang berguna untuk kejadian tersebut, seperti tanggal IoC, tingkat ancaman, komentar, organisasi yang menciptakannya, dan sebagainya. Atribut terutama dijelaskan oleh dua bidang: kategori dan jenis. Perbedaan utamanya adalah bidang kategori menjelaskan apa yang diwakili oleh atribut, seperti aktivitas jaringan, penipuan keuangan, sedangkan bidang jenis menjelaskan bagaimana atribut mewakili kategori yang dipilih. Misalnya, tipe atribut mungkin berupa checksum, nama file, nama host, alamat IP, dan sebagainya. Muatan sebenarnya dari atribut disimpan di bidang nilai.

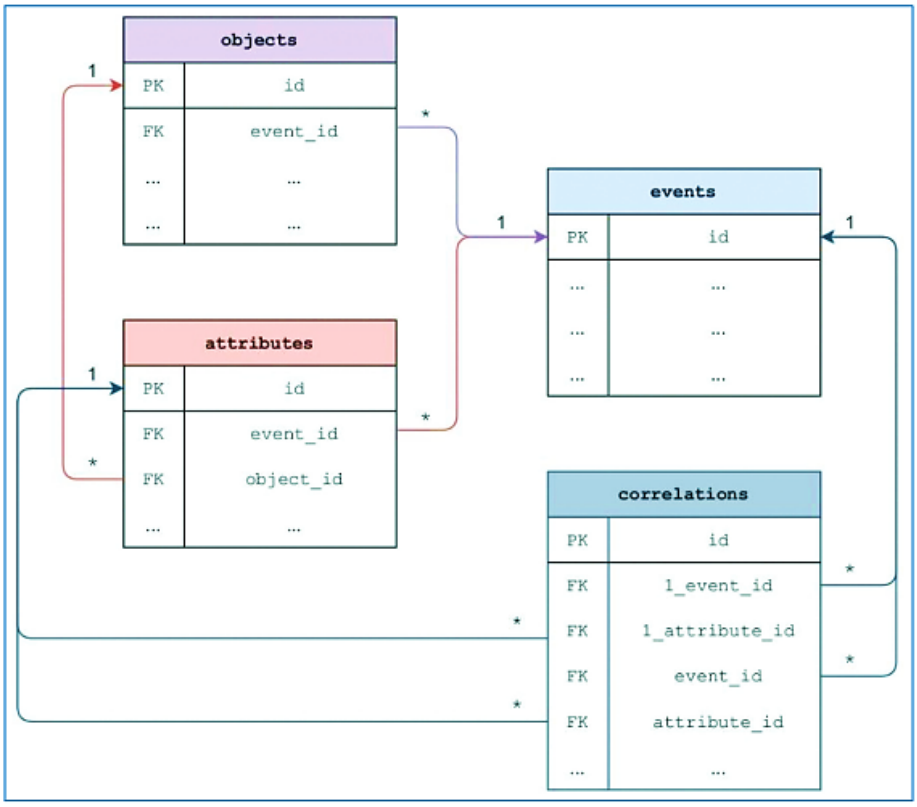
Artefak CTI apa pun, seperti ID CVE kerentanan, disimpan dalam database MISP dalam bentuk atribut. Beberapa atribut dapat dikelompokkan untuk membentuk sebuah objek, yang membentuk artefak CTI yang lebih besar, seperti laporan kerentanan. Baik atribut maupun objek harus dilampirkan pada peristiwa, yang pada dasarnya berfungsi sebagai catatan penyimpanan artefak. Terakhir, MISP memungkinkan suatu kejadian dikorelasikan dengan kejadian lain, melalui teknik pencocokan atributnya. Setiap korelasi yang mungkin terjadi antar peristiwa berfungsi sebagai suatu ikatan, yang juga menunjukkan atribut yang cocok. Pada Gambar 3.6, kami menyajikan gambaran abstrak bagian skema database, yang digunakan untuk menyimpan CTI.

Secara khusus:

- Tabel kejadian adalah skema meta-struktur, dimana atribut, objek dan meta-data tertanam untuk menyusun serangkaian indikator yang memadai, yang mampu menggambarkan kasus tertentu, seperti laporan kerentanan. Suatu peristiwa dapat terdiri

dari sebuah insiden, laporan analisis keamanan, atau analisis pelaku ancaman tertentu. Makna suatu peristiwa semata-mata berasal dari informasi yang tertanam di dalamnya. Dalam kasus kami, salah satu peristiwa adalah kumpulan objek yang digunakan untuk mendeskripsikan artefak CTI.

- Objek berfungsi sebagai ikatan kontekstual antara daftar atribut dalam suatu peristiwa. Tujuan utamanya adalah untuk mendeskripsikan struktur yang lebih kompleks daripada yang dapat dijelaskan oleh satu atribut. Setiap objek dibuat menggunakan Templat Objek dan membawa metadata templat yang digunakan untuk pembuatannya di dalamnya. Objek termasuk dalam kategori meta dan ditentukan oleh sebuah nama.
- Atribut digunakan untuk menggambarkan indikator dan data kontekstual suatu peristiwa. Informasi utama yang terkandung dalam suatu atribut dibentuk oleh triplet kategori-tipe-nilai, dimana kategori dan tipe memberikan makna dan konteks pada nilai tersebut. Melalui berbagai kombinasi tipe kategori, berbagai macam informasi dapat disampaikan.
- Korelasi berfungsi sebagai sistem pengikatan antara peristiwa yang disimpan. Tujuan utamanya adalah untuk mendeskripsikan pencocokan artefak apa pun yang mungkin terjadi di antara peristiwa-peristiwa melalui Mesin Korelasi MISP.



Gambar 3.6. Gambaran abstrak skema database MISP.

Terkait dengan model pembagian MISP, ada dua aspek utama. Pertama, MISP memungkinkan penggunanya untuk memilih tingkat pembagian informasi yang disimpan dalam MISP DB. Misalnya, pihak yang berbagi dapat menyebarkan informasi yang dimilikinya kepada organisasi tertentu, komunitas organisasi, komunitas yang saling berhubungan,

seluruh peserta PPAM, atau bahkan menentukan kelompok berbagi secara manual. Aspek utama MISP selanjutnya adalah fitur proposal. Meskipun modifikasi acara hanya diperbolehkan bagi anggota organisasi pembuat, proposal memungkinkan pengguna memberikan saran untuk perubahan pada suatu acara, yang dibuat oleh organisasi lain. Proposal dilaporkan kembali ke pembuat acara asli, yang mungkin menerima perubahan atau membuangnya. Kemudian, hasil keputusan pencipta akan disebarkan ke seluruh instansi yang saling berhubungan. Contoh fitur ini adalah pelaporan positif palsu kepada pembuat acara, meminta koreksi kesalahan. Terakhir, MISP mampu menyediakan informasi apa pun yang disimpan dalam basis datanya, baik dalam format yang dapat dibaca manusia maupun mesin, dan memungkinkan pengguna untuk mengaksesnya baik melalui GUI atau melalui REST API, sehubungan dengan aspek model berbagi yang disebutkan di atas.

Lebih lanjut, MISP menyediakan berbagai fitur pelengkap, antara lain:

1) *PyMISP12:* Pustaka python untuk implementasi MISP API. PyMISP memberi pengguna kemampuan mengambil, menambah, memperbarui, menghapus, dan mencari melalui peristiwa/atribut atau sampel yang disimpan.
2) *Alat Impor Teks Bebas:* Hal ini memungkinkan pengguna untuk menyalin dan menempelkan data mentah (dalam format teks bebas) ke dalam satu bidang data, yang melalui algoritma heuristik cocok dengan atributnya. Atribut yang dihasilkan kemudian disajikan kepada pengguna yang melanjutkan untuk memvalidasi temuan.
3) *Mekanisme Penandaan MISP:* Hal ini memungkinkan pengguna untuk menentukan tag yang dapat disesuaikan, yang nantinya dapat digunakan untuk memfilter peristiwa dan mengklasifikasikan informasi yang dicakup. Selain itu, tag juga dapat diekspor, sehingga memungkinkan penggunaan kembali tag yang sama dari instance MISP lainnya.
4) *Taksonomi PPAM:* Taksonomi adalah tiga buah tag, yang dideskripsikan dengan nama, predikat, dan nilai. Melalui pemanfaatan gudang taksonomi, organisasi memiliki format umum untuk menggambarkan insiden. Lebih jauh lagi, jika taksonomi yang telah ditentukan sebelumnya tidak sesuai dengan deskripsi suatu peristiwa, pengguna dapat menentukan sendiri taksonominya.
5) *Sinkronisasi Instance MISP:* MISP dilengkapi dengan protokol sinkronisasi, yang mendukung empat fitur utama; tarik, dorong, pemetikan ceri, dan sistem pengumpanan. Fitur tarik memungkinkan instans MISP menemukan peristiwa yang tersedia dan dapat diakses pada instans yang terhubung dan mengunduh peristiwa baru atau yang dimodifikasi. Mekanisme push memungkinkan sebuah instance MISP untuk mengkonversi kejadian ke format JSON yang dapat ditransfer ke instance jarak jauh. Fitur cherry-picking adalah alternatif dari metode penarikan, yang memungkinkan pengguna memutuskan peristiwa mana yang harus ditarik ke instance lokal. Terakhir, mekanisme umpan memungkinkan instans MISP menghasilkan dump
6) *file JSON*: Yang berasal dari pilihan peristiwa yang dipublikasikan oleh organisasi. Kemudian, keluarannya dapat disajikan melalui server web, yang melaluinya instans MISP lainnya dapat mengakses dan mengambil konten melalui UI, serupa dengan cherry-picking.

7) *Penampakan MISP:* MISP menyediakan sistem penampakan, yang memungkinkan pengguna bereaksi terhadap atribut pada suatu peristiwa. Awalnya, ini dirancang untuk memberikan metode yang mudah bagi pengguna untuk memverifikasi atribut tertentu, sehingga meningkatkan kredibilitasnya. Kemudian, penampakan telah diperbaiki untuk memberikan metode untuk memberi sinyal positif palsu, namun juga untuk memberikan tanggal kedaluwarsa untuk beberapa atribut. Seperti yang dinyatakan sebelumnya, Penampakan MISP adalah cara bagi pengguna untuk menyatakan bahwa mereka telah melihat atau memperhatikan suatu atribut dan juga mengkonfirmasi validitasnya. Suatu atribut dapat terlihat beberapa kali oleh pengguna yang sama, sehingga satu pengguna dapat menggunakan penampakan beberapa kali pada satu atribut. Terkadang, beberapa atribut dapat dianggap sebagai positif palsu, dan serupa dengan kasus sebelumnya, pengguna dapat memberi sinyal pada satu atribut sebagai positif palsu beberapa kali. Ada juga beberapa atribut yang valid selama jangka waktu tertentu (misalnya, dalam kasus kampanye phishing yang diasumsikan hanya berlangsung selama satu minggu). Dalam hal ini, pengguna dapat menetapkan tanggal kedaluwarsa pada suatu atribut, namun kali ini, hanya ada satu tanggal kedaluwarsa yang valid per organisasi instans MISP.

Fitur tambahan yang sangat menarik dari MISP adalah mesin korelasinya, yang mencakup semua korelasi antara atribut dan korelasi yang lebih maju seperti korelasi hashing fuzzy (misalnya, ssdeep) atau pencocokan blok CIDR. Korelasi dapat diaktifkan atau dinonaktifkan, untuk setiap kejadian per atribut. Bidang nilai atribut adalah muatan utama atribut, yang dijelaskan oleh kolom kategori dan jenis, dan digunakan oleh mesin korelasi untuk menemukan hubungan antar peristiwa. Khususnya, setelah setiap kejadian dibuat, mesin korelasi MISP memindai database untuk mencari kecocokan atribut-atribut kejadian yang dapat dihubungkan, berkenaan dengan kategori dan jenisnya. Untuk setiap kecocokan, MISP menyimpan dua entri korelasi dalam database; yang menunjuk dari peristiwa yang baru dibuat, ke peristiwa yang disimpan sebelumnya, dan yang menunjuk ke peristiwa yang baru dibuat, dari peristiwa yang disimpan sebelumnya, melalui ID peristiwa uniknya, beserta ID unik atributnya yang sesuai.

Implementasi dan Penyesuaian PPAM

Untuk sepenuhnya mengakomodasi MISP dengan kebutuhan kami, kami menggunakan alat yang disediakan platform untuk menentukan objek khusus yang mampu sepenuhnya mencakup artefak CTI dari sumber yang dipantau. Untuk mendeskripsikan artefak yang dihasilkan dari prosedur penguraian sistem kita dengan baik, kita perlu menyimpannya di MISP pada objek yang paling sesuai; kerentanan dan kelemahan. Selain itu, MISP menyediakan metode untuk membuat objek MISP khusus, yang kita gunakan untuk membuat dua objek khusus untuk komponen kita; yaitu, objek vuldb-vulnerability dan expdb-poc, yang masing-masing memperkaya atribut objek kerentanan dan eksploitasi-poc15. Terakhir, kami membuat satu objek khusus tambahan (crawled_obj), yang mampu merangkum artefak apa pun yang mungkin berasal dari submodul Perayapan dan Pemantauan Media Sosial, karena berasal dari tugas Analisis Data dan Ekstraksi CTI.

Objek kerentanan menggambarkan CVE, yang mengacu pada kerentanan yang dipublikasikan, tidak dipublikasikan, atau sedang ditinjau untuk perangkat lunak, peralatan, atau perangkat keras. Secara khusus, objek kerentanan mampu mendeskripsikan entri CVE, dengan atribut yang berkaitan dengan tanggal publikasi/modifikasi, referensi, konfigurasi rentan (dalam bentuk CPE), deskripsi dan ringkasan kerentanan, metrik CVSS, dan tentu saja, ID CVE.

Objek kelemahan mendeskripsikan CWE yang mengacu pada kelemahan perangkat lunak, peralatan, atau perangkat keras yang dapat digunakan, tidak lengkap, dirancang, atau tidak digunakan lagi. CWE berfungsi sebagai bahasa umum, teknik pengukuran alat keamanan, dan sebagai dasar untuk identifikasi kelemahan, mitigasi, dan upaya pencegahan. Objek tersebut berisi atribut yang menggambarkan CWE terkait, seperti deskripsi, nama, dan status kelemahan, serta ID CWE. Objek kerentanan vuldb adalah versi objek kerentanan yang diperkaya, untuk CVE. Khususnya, ia menyediakan semua atribut yang tepat untuk menyimpan CTI tambahan yang diurai dari sumber yang berorientasi pada kerentanan, seperti estimasi harga, string CVSS dari sumber eksternal (NVD, Vendor, Peneliti), dan status eksploitasi dan remediasi.

Objek expdb-poc adalah versi berbeda dari objek eksploitasi-poc3, yang menggambarkan bukti konsep atau eksploitasi kerentanan. Objek ini sering mempunyai hubungan dengan entri CVE, melalui referensi ID CVE. Perbedaan antara expdb-poc dan eksploitasi-poc adalah kita membuat kolom kredit untuk expdb-poc. Lebih jauh lagi, daripada mengunduh dan menyimpan semua bukti konsep eksploitasi, kami mengarahkan ke tautan kode mentah PoC, melalui referensi.

Objek crawled_obj mendeskripsikan CTI yang mungkin dihasilkan dari submodul Perayapan dan Pemantauan Media Sosial, melalui prosedur Analisis Data dan Ekstraksi CTI. Pertama, objek menyimpan beberapa atribut yang mengacu pada metadata tentang perayapan, seperti id dokumen yang dirayapi, stempel waktu penemuan, judul, teks mentah, dan URL sumber, beserta hash MD5 yang sesuai. Selain itu, ia menyimpan metadata perayapan seperti id, jenis perayap yang menemukan dokumen, skor relevansi yang ditetapkan ke dokumen oleh submodul Peringkat Konten, dan sorotan yang diidentifikasi oleh submodul Ekstraksi CTI. Kemudian, artefak CTI lainnya yang berasal dari submodul Ekstraksi CTI disimpan di bidang yang sesuai dari objek yang ditentukan, dan mungkin merupakan konfigurasi yang rentan, CVE, CWE, organisasi, produk, versi, dan kemungkinan CPE, metrik CVSS, file, IP, perintah, fungsi, konfigurasi, nilai uang, tanggal dan cap waktu.

Terakhir, semua Objek MISP yang digunakan di sistem kami berisi bidang kredit, yang kami gunakan untuk menyimpan sumber CTI yang diurai, menggunakan pengidentifikasi string unik untuk setiap sumber.

Fungsionalitas Komponen

Pada bagian ini kami menjelaskan fungsi komponen Manajemen dan Berbagi Data. Secara khusus, kami menjelaskan prosedur pemantauan sumber, yang bertanggung jawab mengumpulkan CTI secara berkala dari sumber yang kami pantau. Kemudian, kami menjelaskan prosedur pengelolaan data, yang kami rancang khusus untuk (i) menyusun CTI yang masuk ke dalam objek yang sesuai (penataan objek), (ii) memeriksa apakah CTI yang

masuk diindeks oleh komponen kami atau tidak (pencarian peristiwa), (iii) mengelompokkan objek ke dalam entri CTI yang sesuai (pembuatan acara), (iii) mengelola pembaruan dan modifikasi CTI yang disimpan (modifikasi acara). Terakhir, kami menyajikan fungsi MISP yang diterapkan untuk prosedur interkorelasi CTI yang diindeks (korelasi peristiwa), serta pembagian dan peninjauan CTI.

Pemantauan Sumber. Selama fase ini, sistem kami menggunakan modul Feed Monitoring dan Targeted Web Scraping, untuk mengekstrak CTI yang tercakup. Sumber yang dipantau dapat dibagi dalam dua kategori. Kategori pertama berisi sumber yang menyediakan umpan data terstruktur (dalam format JSON dan XML) dari kumpulan informasinya. Untuk kategori ini, kami menggunakan modul Feed Monitoring, yang melanjutkan mengekstrak CTI melalui teknik parsing JSON/XML. Sumber-sumber lain yang dipantau termasuk dalam kategori kedua, yang mengacu pada sumber-sumber yang tidak menyediakan umpan data, namun mengekspos konten database mereka pada antarmuka berbasis web, dengan cara yang terstruktur. Untuk kategori ini kami menerapkan teknik scraping standar seperti query XPath dan parsing HTML, melalui modul Targeted Web Scraping. Prosedur pemantauan sumber dijalankan dengan periode pemantauan yang dapat disesuaikan, yang dapat diinstruksikan dalam modul Penjadwal Pemantauan.

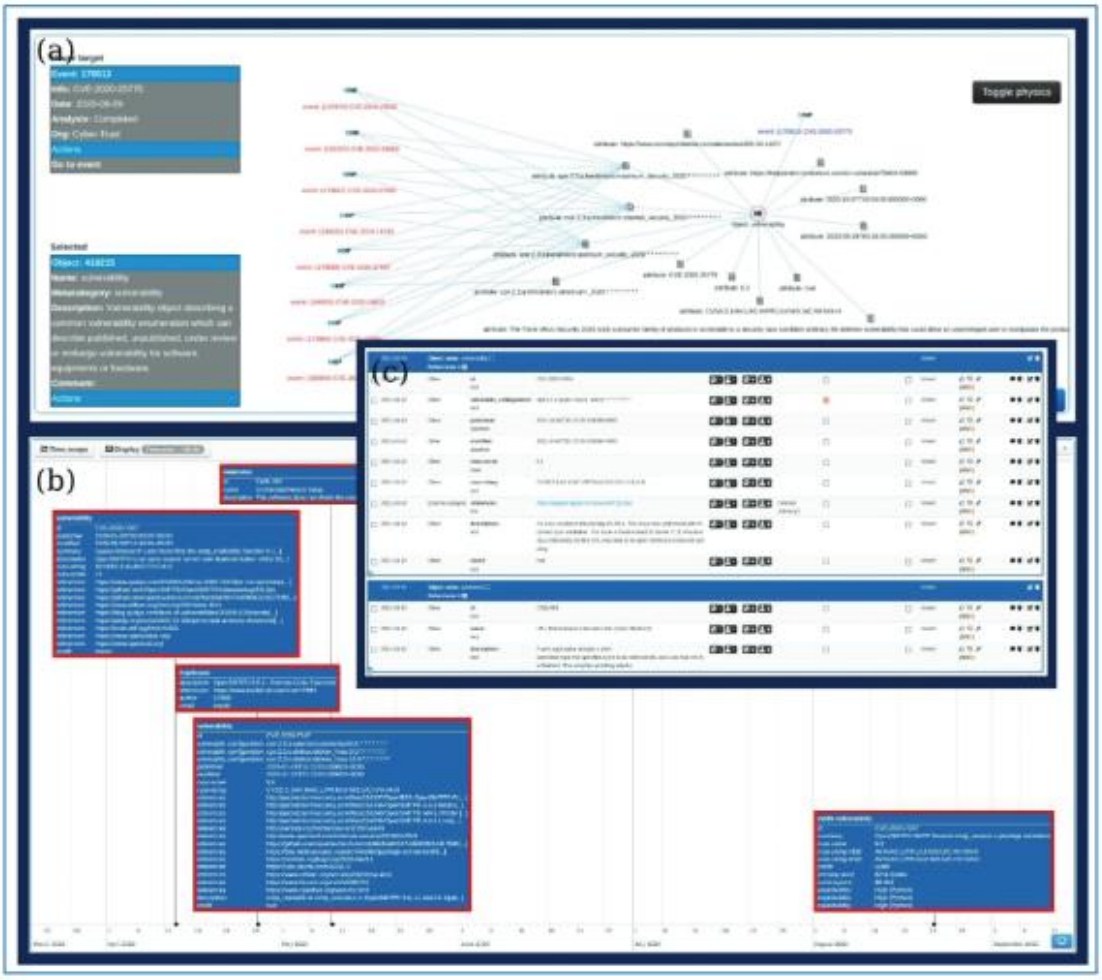
Penataan Objek. Setelah mengekstraksi semua CTI yang dapat ditindaklanjuti dari prosedur penguraian yang dijelaskan di bagian sebelumnya, komponen kami melanjutkan untuk menyusunnya dalam format objek MISP yang sesuai dengan menggunakan perpustakaan PyMISP (seperti yang disajikan pada Gambar 3.5). Untuk mencapai hal tersebut, komponen menghasilkan objek MISP dalam format JSON, sebagai triplet dari bidang atribut, nilai, komentar, dengan nilai yang diekstraksi dari fase penguraian. Bidang komentar digunakan untuk menyimpan informasi yang memperkaya nilai. Misalnya, mendeklarasikan sumber referensi, baik dari vendor yang terkena dampak, atau dari sumber catatan kerentanan lain.

Manajemen acara. Fase manajemen peristiwa dijalankan secara paralel dengan fase perayapan dan penguraian sumber seperti yang dijelaskan di bagian sebelumnya. Apa yang sebenarnya terjadi selama fase ini adalah pembuatan peristiwa baru, setiap kali CTI baru masuk ke komponen Manajemen dan Berbagi Data, atau modifikasi peristiwa yang disimpan sebelumnya, karena artefak CTI yang diperbarui. Ini juga merupakan fase di mana pengelompokan CTI yang dikumpulkan terjadi. Pada bagian berikut, kami menjelaskan proses yang diikuti untuk mencapai hal tersebut.

Pencarian Acara. Pertama-tama, untuk menentukan apakah CTI yang datang tidak dikatalogkan oleh sistem atau tidak, komponen kami menanyakan instance MISP, dengan pengenal unik CTI yang ada. Jadi, melalui penggunaan PyMISP, komponen menanyakan MISP, untuk peristiwa apa pun yang berkaitan dengan ID unik CTI yang saat ini diurai, dengan melihat bidang info peristiwa, yang digunakan untuk menyimpan pengidentifikasi tersebut. Hasil kueri dapat menghasilkan dua kemungkinan hasil; (a) ID CTI yang diurai belum disimpan, sehingga peristiwa baru harus dibuat, atau (b) ID CTI yang diurai sudah ada, sehingga satu atau lebih peristiwa yang sudah ada harus diubah. Untuk kasus kedua, komponen mengembalikan

Peristiwa MISP terkait dalam format JSON, melalui PyMISP, dan juga menyimpan sementara ID Peristiwa MISP terkait, seperti yang disimpan dalam instans MISP.

Pembuatan Acara. Jika CTI yang diuraikan tidak terindeks, maka melalui PyMISP, komponen mengikuti pendekatan tiga langkah, untuk mengkatalogkannya. Pertama, ini menghasilkan peristiwa baru di instans MISP, mengatur bidang info peristiwa, agar sesuai dengan ID CTI unik yang diurai. Kemudian, ia menghasilkan Objek MISP yang diperlukan (berkenaan dengan spesifikasi setiap sumber yang dipantau), dari struktur JSON yang dibangun pada fase penataan objek. Selain itu, validitas objek yang dihasilkan diperiksa baik secara lokal, melalui definisi objek perpustakaan PyMISP, dan secara eksternal, melalui permintaan PyMISP dari definisi objek instance MISP. Kedua definisi tersebut harus sama agar langkah ini berhasil, dan keduanya dinyatakan dalam bentuk file JSON, dalam file pustaka PyMISP, dan file instans MISP. Terakhir, ia melampirkan Objek MISP yang dihasilkan ke peristiwa yang dihasilkan pada langkah pertama, pada instans MISP. Ikhtisar kejadian yang dihasilkan melalui MISP UI disajikan pada Gambar 3.7(c).



Gambar 3.7. Tampilan Acara MISP; (A) Grafik Korelasi Peristiwa, (B) Garis Waktu Peristiwa, (C) Tampilan Objek Dan Atribut Peristiwa.

Modifikasi Acara. Modifikasi peristiwa dapat terjadi dalam dua kasus; sistem menguraikan CTI yang (a) tidak disimpan oleh komponen, namun menganggap entri ID CVE

yang ada (yang terjadi karena CTI yang tumpang tindih dari sumber yang berbeda), (b) versi terbaru dari CTI yang disimpan sebelumnya. Setiap modifikasi yang terjadi selama fase ini, memanfaatkan Peristiwa MISP yang disimpan sebelumnya, yang berasal dari fase pencarian Peristiwa, melalui ID CTI-nya, yang menunjuk pada instans MISP, melalui PyMISP, peristiwa yang akan dimodifikasi. Mengenai kasus pertama, komponen memeriksa bidang kredit setiap objek dalam peristiwa yang ada. Jika tidak ada kecocokan, ia melanjutkan untuk menghasilkan Objek MISP yang diperlukan, dan kemudian melampirkannya ke acara yang ada. Untuk mencapai hal tersebut, komponen memeriksa bidang kredit setiap objek dalam peristiwa yang ada. Untuk kasus kedua, serupa dengan kasus sebelumnya, komponen menghasilkan Objek MISP yang sesuai dan memeriksa bidang kredit setiap objek dalam peristiwa yang ada. Jika ada kecocokan, ia akan memeriksa atribut modifikasi dari objek yang cocok, yang memperhitungkan tanggal modifikasi CTI yang dicakup. Jika tanggal modifikasi CTI yang baru diurai lebih baru daripada tanggal yang disimpan sebelumnya, komponen akan menghapus objek yang disimpan, dan melanjutkan untuk melampirkan objek yang baru dibuat, ke Peristiwa MISP yang ada. Setiap modifikasi atau penambahan artefak CTI pada peristiwa MISP, akan muncul pada tampilan peristiwa MISP, melalui garis waktu peristiwa (Gambar3.7(b)).

Korelasi Peristiwa. Terakhir, penting untuk dicatat bahwa, setelah setiap pembuatan/modifikasi kejadian, komponen melanjutkan menghitung ulang korelasi, melalui Mesin Korelasi MISP, karena ada kemungkinan bahwa CTI yang baru disimpan akan mempertimbangkan peristiwa tersebut. produk yang terkena dampak yang sama, seperti acara lainnya. Setelah proses ini, kejadian yang ada menunjuk ke semua kejadian terkait, seperti yang digambarkan pada Gambar 3.7(a).

Berbagi dan Meninjau CTI. Sejalan dengan pengumpulan semua CTI yang tersedia untuk umum dari sumber-sumber yang dipantau, sistem kami juga dapat melanjutkan ke tahap berbagi dan peninjauan CTI. Pembagian CTI yang tercakup dapat terjadi dalam dua cara. Yang pertama adalah membagikan CTI melalui fitur berbagi MISP. Metode kedua, adalah menanyakan komponen melalui MISP REST API yang disediakan, menggunakan kredensial otorisasi yang diperlukan. Pada bagian berikut, kami memberikan gambaran rinci tentang bagaimana hal ini dapat dicapai.

MISP Rest Api Pencarian Tenang. Seperti disebutkan sebelumnya, MISP menyediakan opsi untuk mencari database tertanamnya, melalui REST API yang disediakan. Selain itu, ia dapat mengekspor CTI dalam berbagai standar berbagi CTI seperti JSON, XML, OpenIOC, Suricata, Snort, STIX, dan banyak lagi. Dengan demikian, dimungkinkan untuk menanyakan MISP REST API, untuk informasi mengenai entri tertentu, dan menerima respons dalam format yang diminta. Untuk tujuan ini, ada dua titik akhir REST; satu yang berkaitan dengan informasi pada tingkat peristiwa, dan satu lagi untuk tingkat atribut. Dalam kasus pertama, pengguna dapat mengambil semua CTI terkait dengan kueri yang diajukan, sedangkan dalam kasus kedua, pengguna dapat mengambil semua atribut terkait dari CTI yang disimpan, yang cocok dengan kueri yang diajukan (misalnya, deskripsi kerentanan). Kedua titik akhir ini menggunakan metode POST HTTP untuk menanyakan MISP REST API. Selain itu, kedua titik akhir memungkinkan pengguna untuk memberikan batasan pada CTI yang diminta, seperti tanggal, nilai (yang mungkin juga berisi karakter pengganti dengan penggunaan karakter “%”),

penomoran halaman hasil, dan banyak lagi. Terakhir, MISP menyediakan fungsionalitas otomasi, yang dirancang untuk secara otomatis memasukkan data dari repositori MISP ke alat dan sistem lain. Agar fungsi ini tersedia untuk alat otomatis, kunci autentikasi digunakan. Jadi, untuk mendapatkan akses ke REST API MISP, pengguna harus menyertakan kunci unik mereka (sebagai header dalam permintaan POST).

Gambar 3.8. Mekanisme Penampakan MISP sebagaimana disediakan di UI MISP pada tampilan peristiwa.

Peninjauan CTI Melalui Penampakan MISP. Untuk mencapai tujuan ini, untuk meninjau CTI yang tercakup, komponen yang diusulkan menggunakan mekanisme Penampakan MISP, yang memungkinkan pengguna untuk menyatakan apakah suatu artefak benar-benar positif atau positif palsu, sehubungan dengan kerentanannya. dan eksploitasi yang disimpan di MISP. Mekanisme penampakan untuk meninjau CTI yang disimpan, dapat digunakan melalui MISP UI pada tampilan peristiwa, seperti yang disorot pada Gambar 3.8.

Kesimpulan

Dalam bab ini, kami berfokus pada memfasilitasi siklus hidup CTI, dengan memanfaatkan alat sumber terbuka yang sesuai, untuk mengotomatisasi pengumpulan dan berbagi tugas CTI. Kami telah menghadirkan INTIME, sebuah solusi yang menyediakan platform manajemen CTI end-to-end yang mampu mendukung pengumpulan, analisis, pemanfaatan, dan pembagian CTI melalui kerangka kerja yang terintegrasi dan dapat diperluas. Kami mempresentasikan solusi arsitektur di balik sistem yang diusulkan, mendiskusikan masing-masing teknologi modul dan memberikan rincian tentang orkestrasi modul.

BAB 4
TEKNIK PERTAHANAN KEAMANAN SIBER

Mengamankan lanskap ancaman IoT yang terus berkembang merupakan masalah yang menantang, dengan konsekuensi yang parah jika tidak ditangani dengan tepat. Menanggapi tantangan tersebut, bidang pertahanan sasaran bergerak telah dikembangkan, untuk mengatasi ancaman-ancaman ini dengan memanfaatkan pendekatan teori permainan untuk merespons ancaman-ancaman tersebut sambil mempertahankan tingkat ketersediaan yang tinggi. Karya ini menyajikan implementasi sistem respons intrusi, yang menggunakan grafik serangan Bayesian untuk memodelkan keadaan kompleks jaringan dan hostnya, dan proses keputusan Markov yang dapat diamati sebagian untuk memilih tindakan mitigasi yang optimal. Untuk mengatasi serangan jaringan yang baru dan tidak diketahui, seperti eksploitasi zero-day, kebijakan manajemen peringatan ditambahkan untuk memfokuskan POMDP pada kondisi jaringan saat ini dan memberikan tindakan mitigasi jangka pendek. Terakhir, sistem dievaluasi berdasarkan lima skenario (Mirai, Zeus, zero-day, 10 pemutaran ulang lalu lintas berbahaya, dan BlackEnergy) yang dijalankan dalam lingkungan SOHO yang disimulasikan. Hasil evaluasi menunjukkan efektivitas yang tinggi terhadap ancaman tradisional, dan sedikit peningkatan efektivitas terhadap ancaman baru.

4.1 PENDAHULUAN

Dalam beberapa tahun terakhir, lanskap ancaman yang terus berkembang telah menyebabkan peningkatan jumlah serangan siber, dengan serangan tingkat jaringan, botnet, dan perangkat lunak berbahaya yang semakin canggih dari waktu ke waktu. Selain itu, ancaman-ancaman yang telah dipahami dengan baik ini juga disertai dengan serangan zero-day (yaitu, eksploitasi kerentanan yang dirahasiakan dan tidak ditambal) yang menurut sifatnya menimbulkan ancaman lebih besar terhadap keamanan jaringan komputasi karena kurangnya informasi tentang kerentanan tersebut.

Deteksi ancaman semacam ini bukanlah hal yang sepele, karena para pembela HAM sering kali harus mengevaluasi kondisi keamanan jaringan mereka melalui sumber informasi yang berisik seperti server log (yang darinya mungkin sulit untuk membedakan kejadian keamanan dari torrent yang tidak penting). Atau peringatan berisik dari sistem deteksi intrusi (yaitu, dengan jumlah positif/negatif palsu yang sangat tinggi). Teknik mitigasi yang ada saat ini, yang seringkali mengandalkan intervensi manusia (misalnya tim tanggap insiden) atau kontrol berbasis jaringan dan host yang ada (misalnya solusi firewall atau antimalware), terbukti tidak memadai dalam hal cakupan. Selain itu, solusi seperti ini biasanya tidak mempertimbangkan ketersediaan layanan sebelum mengambil tindakan misalnya, penerapan aturan firewall yang tidak akurat saat terjadi serangan dapat menyebabkan lebih banyak kerusakan dibandingkan serangan itu sendiri, karena ketersediaan sistem atau sumber daya penting dapat sangat dirugikan. Selain itu, solusi antimalware sering kali gagal melindungi

terhadap sejumlah besar ancaman yang tidak diketahui atau baru terjadi, namun juga memerlukan interaksi manusia untuk menerapkan langkah-langkah mitigasi.

Solusi pertahanan yang lebih maju telah dikembangkan dengan dua tujuan: untuk menghambat perkembangan serangan, dan untuk mendapatkan pemahaman yang lebih baik tentang alat dan metode penyerang. Solusi ini sering kali berinteraksi dengan penyerang dengan mengubah struktur jaringan, atau menghadirkan target yang lebih menarik untuk mengalihkan perhatian dari sistem jaringan lain. Misalnya, honeypots mencapai hal ini dengan menggunakan layanan yang rentan terhadap umpan, sementara honeynets menggunakan sistem yang tampak menarik sebagai pengalih perhatian untuk mengalihkan perhatian penyerang. Namun, serangan ini pun gagal melawan penyerang terampil yang mampu mengidentifikasi dan menghindarinya.

Memperluas gagasan berinteraksi dengan penyerang, teknik pertahanan target bergerak (MTD) dikembangkan untuk merespons ancaman yang beradaptasi dan kompleks secara optimal. Tujuan utama dari teknik MTD adalah untuk mempengaruhi perubahan pada struktur jaringan (atau permukaan serangan) untuk meminimalkan kemampuan pengintaian penyerang, serta untuk merespons ancaman sambil mempertahankan tingkat ketersediaan layanan yang dapat diterima. Lanskap saat ini dalam pendekatan MTD teori permainan cukup menjanjikan tetapi menampilkan pendekatan yang kontras dalam hal pemodelan serangan, dengan beberapa pekerjaan menunjukkan inefisiensi baik dalam efisiensi waktu, kemampuan beradaptasi, atau dalam pilihan pemilihan respons. Selain itu, banyak karya yang menilai modelnya sebagian besar melalui simulasi, yang menghadirkan keterbatasan terkait penerapannya di dunia nyata. Dalam upaya untuk memberikan liputan penuh mengenai kemungkinan skenario serangan, pekerjaan terkait memiliki waktu respons yang lambat atau menggunakan metode pemodelan serangan yang tidak akurat ketika mencocokkan ancaman keamanan dengan berbagai lingkungan yang dapat diterapkan (misalnya, rumah pintar). Selain itu, sebagian besar pendekatan teori permainan tidak menangani proses pencocokan peringatan, sehingga menyebabkan pemodelan status jaringan tidak akurat. Meskipun pendekatan ini dikembangkan untuk memberikan respons optimal dalam jangka panjang, tanpa mempertimbangkan respons jangka pendek, sebagian besar ancaman jaringan yang umum tidak ditangani dengan tepat.

Selama bertahun-tahun, terdapat motivasi untuk mengotomatiskan proses mitigasi serangan yang mengarah pada pengembangan sistem respons intrusi (IRS). Upaya awal menerapkan pemetaan statis antara ancaman yang terdeteksi dan tindakan penanggulangan yang tersedia tetapi kurang fleksibel. Karya ini menyajikan implementasi IRS yang memanfaatkan fungsionalitas inti dari berbagai model keamanan jaringan grafis (GNSM) untuk menyajikan template yang ringan dan efisien untuk penerapan proses pengambilan keputusan. Selain itu, penerapan metode yang efektif untuk menghitung respons jangka pendek yang optimal, untuk menghadapi ancaman sesaat dan kerentanan zero-day di lingkungan internet of things (IoT), juga akan disajikan dan dievaluasi berdasarkan skenario serangan yang realistis dalam simulasi. jaringan komputer.

4.2 LATAR BELAKANG DAN PEKERJAAN TERKAIT

MTD adalah bidang luas yang mencakup teknik dan mekanisme yang bertujuan untuk menipu penyerang dengan mengubah topologi jaringan (dengan menerapkan mekanisme peralihan) dan memanfaatkan informasi berbasis peristiwa apa pun yang tersedia untuk memantau aktivitas jahat di jaringan. Lei dkk. MTD dapat dipelajari dengan mengelaborasi elemen-elemen penentu yang dapat mengukur efektivitas mekanisme yang diterapkan.

Sengputa dkk. dalam menunjukkan bahwa teknik MTD paling menguntungkan ketika mekanisme yang diterapkan tidak bersifat deterministik, dengan alasan bahwa penyerang pada akhirnya akan mampu mengantisipasi perubahan tindakan di masa depan dan menghitung strategi serangan mereka dengan tepat. Penulis membahas lebih lanjut penerapan teknik MTD, dengan fokus pada jaringan dan lapisan aplikasi model interkoneksi sistem terbuka (OSI). Mereka mencatat bahwa implementasi middlebox MTD, yang memanfaatkan perangkat jaringan yang ada yang digunakan untuk memanipulasi lalu lintas jaringan (misalnya proxy, firewall), bermasalah karena sifatnya yang statis dan bahkan dapat mengungkapkan informasi tentang jaringan kepada penyerang. Oleh karena itu, mereka menjelaskan bagaimana teknologi jaringan canggih, seperti jaringan yang ditentukan perangkat lunak (SDN) dan virtualisasi fungsi jaringan (NFV), dapat digunakan untuk menambah dinamika pada teknik MTD. Dengan teknologi sebelumnya, SDN menjadi pendekatan pilihan di bidang MTD karena solusi yang lebih terukur dan efektif, selain menyediakan metode yang dioptimalkan untuk pemetaan jaringan dan perlindungan serangan multi-tahap. Cho dkk. dalam membedakan tiga pendekatan MTD yang luas: (a) teori permainan, (b) berbasis algoritma genetika, dan (c) berbasis pembelajaran mesin. Meskipun ketiganya menjanjikan, pekerjaan mereka berfokus pada pendekatan teori permainan karena memberikan keuntungan besar dalam hal fleksibilitas implementasi, pemodelan lingkungan yang realistis, dan penggabungan skenario serangan yang beragam.

Zonouz dkk. dalam mengusulkan penggunaan proses keputusan Markov kompetitif (CMDP) yang diterapkan pada model keamanan pohon sebagai respons otomatis dan mesin pemulihan yang menjaga ketersediaan. Pendekatan ini menghadirkan solusi holistik yang memodelkan penyerang sebagai entitas yang cukup cerdas, yang menghindari tindakan dengan imbalan rendah, namun kurang dalam manajemen penskalaan dan waktu respons.
Shameli-Sendi dkk. Dalam menampilkan IRS otomatis dan interaktif yang secara dinamis mengevaluasi tindakan respons sehubungan dengan ketergantungan jaringan dan proses penting, dengan membangun GNSM yang statis namun fleksibel. Model yang diusulkan secara membabi buta memicu respons dari peringatan yang diterima, yang dievaluasi berdasarkan metrik keamanan yang sama (seperti yang didefinisikan untuk aset) untuk menunjukkan, ketika terjadi serangan, dampak negatif dari respons pada titik pertahanan yang berbeda. Batasannya adalah penghitungan dampak positif respons bersifat statis dan status keamanan tidak diperbarui saat respons diterapkan. Namun, evaluasi respon yang akurat diberikan sepanjang proses respon karena pemilihan respon tersebut mempertimbangkan kerugian akibat serangan, tingkat kepercayaan penyerang dan kemungkinan terjadinya serangan.

Miehling dkk. Memgembangkan sistem otonom untuk pertahanan jaringan yang diserang berdasarkan grafik serangan Bayesian (BAG). Model probabilistik diterapkan untuk

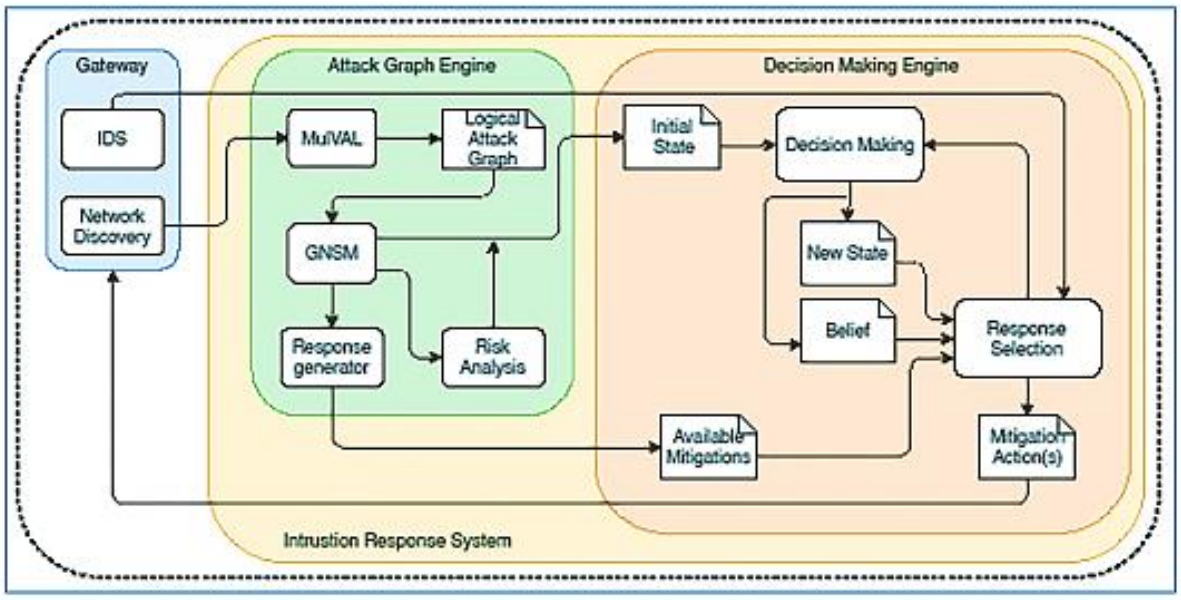
menangkap perilaku penyerang saat maju melalui jaringan. Dalam model mereka, pembela HAM adalah pengamat parsial, karena strategi penyerang tidak diketahui, yang mencoba menghalangi kemajuan penyerang melalui jaringan dengan melakukan tindakan mitigasi terkait layanan jaringan. Penulis menggambarkan masalah ini sebagai proses keputusan Markov yang dapat diamati sebagian (POMDP) waktu diskrit dan mempertimbangkan atribut jaringan (layanan, kerentanan, dll.) dan representasinya dalam GNSM (jalur serangan, status kepercayaan, dll.) dari masalah keputusan , agar berhasil memprediksi tindakan penyerang di masa depan. Penulis menyajikan IRS yang memanfaatkan grafik serangan ketergantungan untuk memodelkan POMDP dengan cara yang mirip. Model dinamis yang lebih baru ini mampu menangani alarm palsu dan mengukur perkembangan penyerang sambil menghitung respons efektif jangka panjang dengan mensimulasikan efektivitas keputusan menggunakan algoritma perencanaan Monte-Carlo yang dapat diobservasi sebagian (POMCP).

4.3 PEMODELAN SISTEM

Bagian ini menyajikan pemodelan yang kami usulkan untuk mengatasi ancaman saat ini di rumah pintar, kantor pintar/kantor rumah (SOHO) dan jaringan IoT dengan memanfaatkan model berbasis grafik dan karakteristik uniknya, sehingga membentuk kerangka kerja serbaguna untuk penerapan MTD teknik. Implementasi IRS dibagi menjadi dua sub-komponen, seperti terlihat pada Gambar 4.1, generator grafik serangan dan mesin pengambilan keputusan.

Fungsionalitas tingkat tinggi IRS adalah sebagai berikut:

- Awalnya, IRS menerima informasi tentang topologi jaringan dari modul penemuan jaringan gateway, termasuk: alamat IP host, tabel perutean, definisi subjaringan, dan kerentanan apa pun yang ditemukan.
- Kemudian, mesin grafik serangan memproses informasi ini untuk menghasilkan GNSM dasar, melakukan analisis risiko, dan melakukan pra-perhitungan semua kemungkinan tindakan mitigasi (aturan firewall) oleh generator respons.
- Informasi ini kemudian diteruskan ke mesin pengambilan keputusan, dengan GNSM membentuk keadaan awal model teori permainan dan tindakan mitigasi yang telah diperhitungkan sebelumnya menjadi tindakan pembela HAM.
- Terakhir, peringatan jaringan yang dihasilkan oleh sistem deteksi intrusi (IDS) gateway dipetakan ke GNSM, yang dianalisis melalui proses pemilihan respons dan tindakan mitigasi yang sesuai dipilih.



Gambar 4.1. Arsitektur tingkat tinggi IRS.

Grafik Serangan

GNSM banyak digunakan untuk memodelkan status keamanan jaringan (atau host, bergantung pada aplikasinya) menggunakan grafik terarah, untuk mengidentifikasi kemungkinan jalur serangan (urutan tindakan) yang mungkin diambil penyerang untuk mencapai kondisi yang diinginkan (kondisi tujuan). dan untuk melakukan metode analisis risiko yang lebih kompleks. Jalur ini menggambarkan status jaringan dengan node dan transisi status dengan tepi terarah. Node-node ini biasanya dikonseptualisasikan sebagai prakondisi (kemampuan yang harus dimiliki penyerang untuk melangkah lebih jauh) atau pascakondisi (kemampuan yang dapat diperoleh penyerang, selama prasyaratnya terpenuhi); Kemampuannya meliputi: hak istimewa yang diperoleh, kerentanan yang ada, atribut atau tindakan jaringan, dan lain-lain. Ada dua kategori utama GNSM: pohon serangan dan grafik serangan; dengan yang pertama menggambarkan kondisi tujuan tunggal dan setiap tindakan yang diperlukan untuk mencapainya, dan yang terakhir menggambarkan serangan multi-tahap yang tidak terbatas pada kondisi tujuan tunggal yang berfokus pada tindakan penyerang daripada konsekuensi dari tindakan tersebut. tindakan itu.

Berbagai model keamanan berbasis grafik serangan telah diusulkan selama bertahun-tahun dengan yang paling penting adalah grafik serangan negara (SAG) , grafik serangan logis (LAG) dan grafik serangan Bayesian (BAG). Meskipun SAG lebih baik dalam hal penerapannya, SAG berkembang secara eksponensial dalam upaya untuk mencakup semua kemungkinan kombinasi gerakan penyerang, dengan tidak memperhitungkan pembuatan jalur serangan duplikat. LAG mendeskripsikan ketergantungan logis di antara sasaran serangan dengan menggunakan node (fakta) sebagai pernyataan logis dan dianggap sebagai solusi terukur untuk pembuatan grafik serangan. BAG adalah grafik asiklik terarah di mana node mewakili variabel acak dan tepinya menggambarkan ketergantungan bersyarat antara pasangan node; mereka terutama digunakan untuk melakukan analisis risiko probabilistik pada jaringan yang ditandai dengan perubahan cepat dalam topologi atau atribut hostnya.

Pengembangan model grafis IRS kami didasarkan pada Multi-host, Multi-stage Vulnerability Analysis Language (MulVAL), sebuah kerangka kerja yang banyak digunakan untuk memproduksi LAG di jaringan skala besar. Ketergantungan logisnya menggambarkan bagaimana serangan dapat dilakukan dengan mempertimbangkan fakta logis sebagai tindakan, yang diterjemahkan ke dalam rangkaian derivasi Datalog. Informasi tentang jaringan dan kerentanan yang ditemukan diterjemahkan ke tupel Datalog dan diproses oleh mesin penalaran XSB internal untuk menghasilkan LAG. Model ini berisi tiga jenis node: node OR & LEAF yang menggambarkan keadaan perangkat jaringan (kondisi keamanan), dan node AND yang menggambarkan hubungan penghubung antara node OR & LEAF (eksploitasi). Tepi dalam model ini menghubungkan prakondisi ke pascakondisi melalui node eksploitasi. Di IRS, LAG yang dihasilkan MulVAL diubah menjadi BAG dengan melakukan eliminasi siklus dan dengan mengaitkan metrik sistem penilaian kerentanan umum (CVSS) dengan tepinya.

Pembuatan Respon

Tindakan remediasi yang dapat ditindaklanjuti, yang akan digunakan oleh mesin pengambil keputusan dan model POMCP untuk mengubah topologi jaringan yang digambarkan oleh GNSM, telah dihitung sebelumnya oleh submodul pembuatan respons. Ini adalah aturan firewall yang mengubah interkonektivitas host, baik di dalam maupun di seluruh sub jaringan, dengan tujuan memblokir akses ke layanan atau host yang rentan.

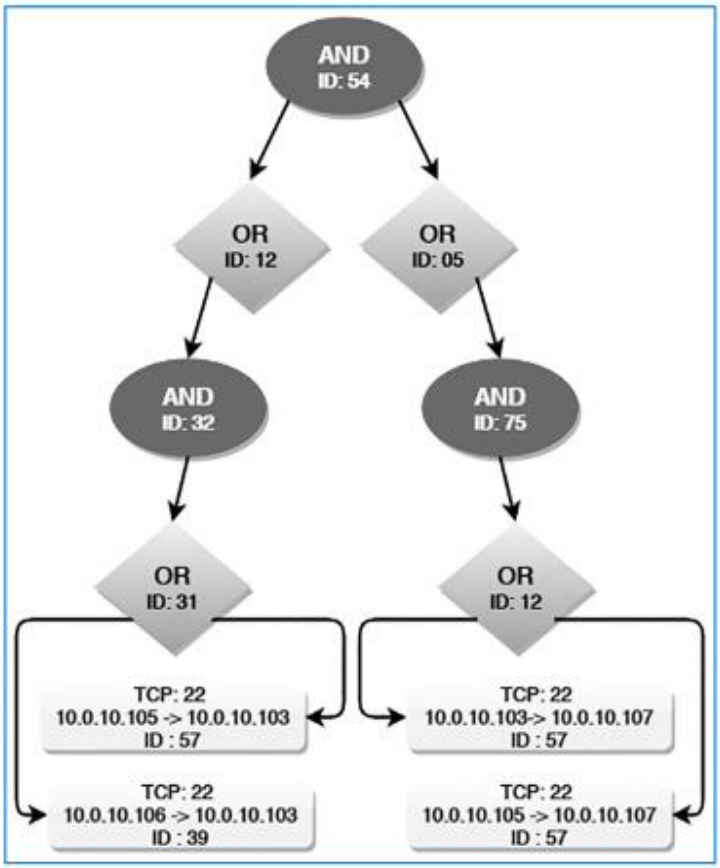
Algoritme dimulai dengan memilih node yang akan diblokir (biasanya semua eksploitasi terdapat dalam BAG) dan, menggunakan depth-first search (DFS), mengeksplorasi subgraf terkait hingga node LEAF tercapai. Selama proses ini, node diperiksa secara berurutan dan semua yang berisi informasi yang cukup dan menggambarkan status akses, diperhitungkan untuk pembuatan aturan firewall dan dengan demikian dimasukkan ke dalam struktur pohon. Selain itu, setiap node OR yang dikunjungi ditambahkan ke pohon sebagai operator AND (karena setiap anak harus diinvalidasi untuk membuat node OR tidak valid) dan setiap node AND yang dikunjungi ditambahkan ke pohon sebagai operator OR (karena hanya diperlukan satu anak untuk melakukan hal tersebut. menjadi tidak valid untuk membuat node AND tidak valid). Semua jalur yang pada akhirnya tidak mewakili keadaan tersebut, di akhiri dengan node NULL. Aturan Datalog MulVAL mampu mendeskripsikan layanan yang terdeteksi secara akurat, serta informasi terkait layanan seperti port dan alamat IP. Selanjutnya, semua jalur pohon yang diakhiri dengan node NULL dihapus dari pohon untuk membuat pemrosesan lebih mudah, dan jalur yang tersisa kemudian diciutkan untuk menghilangkan urutan operator yang berlebihan (lihat Gambar 4.2). Pohon sisanya mewakili solusi dalam bentuk normal disjungtif (DNF).

$$(R_1 \cap \cdots \cap R_k) \cup (R_1 \cap \cdots \cap R_n) \cup \cdots \cup (R_1 \cap \cdots \cap R_m)$$

Untuk mengelola ketidakpastian yang muncul akibat serangan yang tidak diketahui, aturan firewall yang memblokir semua layanan dari setiap host jaringan (aturan global) juga dibuat. Meskipun solusi ini dianggap tidak optimal dalam hal ketersediaan, terdapat beberapa serangan tingkat jaringan yang menyebabkan perubahan cepat pada jaringan yang tidak dapat

digambarkan oleh mesin grafik serangan dalam BAG secara real-time. Misalnya, serangan yang berkomunikasi melalui port yang ditetapkan secara dinamis pada host jaringan yang ditargetkan perilaku umum terhadap ancaman malware seperti Zeus yang menggunakan API yang disediakan OS untuk membuka koneksi ke server perintah dan kontrol (C&C), sehingga setiap upaya komunikasi terjadi melalui port yang berbeda.

Terakhir, setiap solusi dikaitkan dengan daftar node BAG yang terpengaruh (yaitu, node yang akan dianggap tidak valid/dihapus setelah penerapan aturan) yang digunakan oleh mesin pengambil keputusan untuk menentukan dampak dari setiap solusi, dan memilih solusi yang secara optimal mencakup keyakinannya tentang node mana yang diyakini akan dieksploitasi oleh penyerang.



Gambar 4.2. Contoh pohon dari proses pembuatan respons.

Proses Pengambilan Keputusan

Tujuan utama mesin pengambil keputusan IRS adalah memilih tindakan mitigasi yang optimal, dari serangkaian tindakan yang telah dihitung sebelumnya yang diterima oleh submodul pembangkit respons, sebagai respons terhadap serangan jaringan yang canggih. Model teori permainan yang diimplementasikan didasarkan pada model POMDP yang disajikan pada yang dieksekusi di atas BAG yang dihasilkan oleh mesin grafik serangan.

Model ini menggambarkan permainan antara penyerang dan pemain bertahan yang merupakan pengamat parsial, artinya strategi penyerang tidak diketahui oleh pemain bertahan. Dalam permainan ini, penyerang bertujuan untuk mengeksploitasi kerentanan atau

melakukan serangan jaringan lainnya untuk maju melalui jaringan dan mencapai kondisi tujuan. Pembela bertujuan untuk memblokir kemajuan penyerang melalui jaringan dengan memilih tindakan mitigasi yang tepat berdasarkan keyakinannya tentang keadaan jaringan (probabilitas keyakinan pada BAG) dan jenis penyerang (anggapan terhadap strategi penyerang). Tiga jenis perilaku penyerang dimodelkan, mewakili gagasan yang telah ditetapkan tentang strategi penyerang yang sebenarnya (agresi, tingkat pengetahuan, dan kerahasiaan).

Metrik probabilistik pada keputusan dan tindakan yang berorientasi pada eksploitasi, seperti probabilitas upaya eksploitasi dan probabilitas keberhasilan eksploitasi, ditetapkan melalui proses analisis risiko yang dilakukan oleh mesin grafik serangan pada BAG dasar. Eksekusi model POMDP dilakukan secara real-time, dengan setiap putaran (langkah waktu diskrit) memanfaatkan informasi yang diterima oleh IDS gateway untuk mengamati tindakan penyerang di jaringan. Pengamatan ini merupakan pencocokan peringatan yang diterima pada node BAG (status keamanan) yang dianggap telah dijangkau oleh penyerang. Selain itu, proses pengambilan keputusan didasarkan pada matriks kepercayaan yang merupakan distribusi gabungan berdasarkan negara keamanan dan jenis penyerang. Keyakinan tersebut diperbarui setiap putaran sesuai dengan pengamatan pemain bertahan dan disimpan sebagai metrik yang memikirkan secara rekursif semua keputusan sebelumnya. Semua solusi yang berlaku telah dihitung sebelumnya, sehingga memungkinkan pelaksanaan tindakan yang diperlukan secara optimal dan cepat. Biaya paling rendah adalah ketika aturan firewall (atau serangkaian aturan, tergantung keadaan) mencakup area node terluas di BAG.

Penyesuaian Lebih Lanjut

Awalnya, prosedur spesifik mengenai pemilihan peringatan yang akan dipicu. Peringatan dianggap valid ketika prasyarat terkait eksploitasi dikompromikan. Pada saat yang sama, model asli mengabaikan peringatan apa pun yang memiliki postconditions yang sesuai dan kemudian mengambil sampel peringatan acak, disaring menggunakan distribusi binomial, sesuai dengan pekerjaannya.

Dalam banyak kesempatan, struktur GNSM yang mendasarinya secara signifikan mempengaruhi perkembangan penyerang dalam jaringan yang dimodelkan ketika peringatan diterima dengan cara tersebut. Kadang-kadang, kondisi tujuan grafik dapat tercapai secara instan atau kadang tidak pernah tercapai sama sekali, sehingga mengakibatkan tidak adanya tindakan mitigasi. Untuk mengatasi hal ini, model POMDP yang diterapkan menerapkan kebijakan manajemen peringatan, sehingga serangan yang tidak diketahui dapat dimitigasi bersamaan dengan serangan jaringan tradisional dan upaya eksploitasi. Kebijakan ini beroperasi dalam dua mode: ketat dan tangkas. Untuk kedua mode, tiga set eksploitasi (DAN node BAG). Yang pertama didefinisikan sebagai kumpulan eksploitasi yang diaktifkan E_{ac}; yang kedua didefinisikan sebagai kumpulan eksploitasi yang tersedia E_{av}, yang mencakup eksploitasi yang prasyaratnya terganggu dan keyakinannya melebihi ambang batas; sedangkan yang terakhir didefinisikan sebagai kumpulan eksploitasi yang diblokir E_{bl}, yang mencakup eksploitasi yang telah diblokir oleh tindakan mitigasi sebelumnya. Akibatnya, kami mendefinisikan kebijakan ketat Ps sebagai:

$$P_S = (E_{bl})^C \cap E_{ac}$$

dan kebijakan tangkas PA sebagai:

$$P_A = E_{av} \cap E_{ac}$$

Tergantung pada kebijakan yang dipilih, peringatan akan dicocokkan dengan salah satu rangkaian eksploitasi yang disebutkan di atas, selama tersedia cukup informasi dari IDS. Model POMDP yang diimplementasikan berfokus pada keadaan jaringan saat ini, sehingga memungkinkan IRS merespons serangan dengan lebih baik dengan memberikan respons tindakan mitigasi jangka pendek jika dibandingkan dengan pekerjaan lain, karena penerapannya tidak mencakup perencanaan optimal yang tidak terbatas. Jalur serangan yang digambarkan dalam BAG dibangun dengan tindakan yang lebih sedikit dibandingkan dengan jaringan yang kompleks, sehingga tidak perlu mengembangkan sistem yang berupaya untuk berpikir lebih dulu dari musuh. Untuk itu, kompleksitas sistem dikurangi dengan membatasi model POMDP hanya pada satu putaran simulasi.

4.4 STRATEGI SERANGAN

Pekerjaan ini bertujuan untuk mengatasi ancaman dan kerentanan tingkat jaringan yang relevan dengan lingkungan IoT dan SOHO. Perangkat di lingkungan ini dicirikan oleh variabilitas sistem operasi dan teknologi tertanamnya, yang jika dipadukan dengan lingkungan komputasi yang berkembang pesat saat ini, memungkinkan terciptanya banyak vektor serangan. Keandalan operasi, kerahasiaan, dan ketersediaan adalah salah satu tujuan keamanan yang paling penting untuk dipertimbangkan dalam konteks pengamanan sistem tersebut, terutama karena kontrol keamanan yang moderat tidak diterapkan baik di tingkat host maupun tingkat jaringan, dan sebagai penggunanya tidak diberi pendidikan yang memadai tentang cara mengkonfigurasi dan mengamankannya dengan benar. Oleh karena itu, dalam lanskap ancaman dunia maya saat ini, ekosistem ini menjadi target utama serangan berskala besar, termasuk botnet IoT dan Trojan. Bagian ini menyajikan dan menganalisis dua karakteristik skenario serangan yang terkait dengan sistem IoT dan SOHO, yang akan diperiksa lebih lanjut di bagian berikut melalui simulasi skenario dunia nyata.

Botnet Mirai

Ancaman pertama yang menjadi perhatian adalah botnet IoT. Untuk tujuan evaluasi, botnet Mirai dipilih, karena pada puncak aktivitasnya, bot ini menjadi peringatan bagi industri keamanan, dengan perkiraan jumlah 600.000 sistem yang terinfeksi pada puncak aktivitas awalnya. Perangkat yang terinfeksi menjadi sumber salah satu kasus serangan penolakan layanan (DDoS) terdistribusi yang paling parah di masa lalu, menargetkan web host Perancis OVH dengan ukuran lalu lintas puncak 1,1 Tbps. Pengungkapan kode sumbernya, bukannya mengarah pada pemberantasannya, malah meningkatkan jumlah serangan secara signifikan dan menjadi titik awal untuk penciptaan varian yang lebih tangguh.

Mirai terdiri dari empat komponen:

- Bot yang dapat dieksekusi, yang bertanggung jawab atas infeksi melalui penggunaan serangan kamus, menggunakan pasangan nama pengguna dan kata sandi yang umum, terhadap perangkat IoT yang salah dikonfigurasi.

- Server laporan yang memelihara database botnet, menangani laporan masuk untuk perangkat yang terinfeksi dan bertindak sebagai salah satu dari dua entitas perantara antara server C&C dan bot. Komunikasi bot dan server laporan dicapai melalui jaringan Tor sehingga pendeteksiannya menjadi tugas yang menantang.
- Server C&C adalah unit pusat, yang menyediakan antarmuka manajemen botnet kepada penyerang sekaligus memungkinkan pelaksanaan perintah infeksi dan serangan.
- Loader beroperasi sebagai entitas perantara lain antara server C&C dan perangkat yang terinfeksi, dengan mengirimkan biner berbahaya ke korban sesuai dengan perintah infeksi server.

Deteksi Mirai sangat bergantung pada sistem deteksi intrusi jaringan (NIDS) yang digunakan untuk deteksi berbasis tanda tangan dalam paket yang dikirimkan di lingkungan IoT. Serangan tersebut mungkin dapat dideteksi dalam tiga tindakan berbeda: (a) selama infeksi pada korban baru, (b) selama serangan DDoS, dan/atau (c) selama transmisi biner berbahaya antara loader dan korban yang terinfeksi. . Mengenai serangan DDoS, perlu disebutkan bahwa Mirai mampu menggunakan sepuluh variasi serangan antara lain HTTP Flood, SYN Flood, UDP Flood, ACK Packet Flood, dan lain sebagainya. Namun, kebanyakan dari mereka dapat dengan mudah dideteksi oleh NIDS.

Selama eksekusi skenario serangan Mirai, IDS di gateway diharapkan menghasilkan sejumlah peringatan tentang lalu lintas yang mencurigakan, IRS akan memprosesnya untuk menghasilkan aturan firewall untuk memblokir lalu lintas yang mencurigakan. Bergantung pada peringatannya, respons yang paling sesuai akan ditentukan oleh model POMDP dengan merumuskan strategi yang tidak hanya menyelesaikan masalah tetapi juga mempertimbangkan bagaimana setiap tindakan yang dihasilkan akan mempengaruhi ketersediaan di lingkungan SOHO atau IoT.

Serangan Zero-Day

Serangan zero-day mengeksploitasi kerentanan yang belum diungkapkan dan belum ditambal, yang tidak memiliki tindakan penanggulangan atau tindakan mitigasi yang diketahui pada saat eksploitasi. Khususnya di lingkungan IoT, beragam perangkat komunikasi (terlepas dari teknologi operasionalnya) dan antisipasi integrasinya, merupakan sistem yang kompleks dan beragam yang tidak bergantung pada campur tangan manusia hal ini mengakibatkan patch atau mekanisme keamanan tidak selalu ditangani sebagaimana mestinya. sebaiknya. Seperti yang dicatat oleh, fitur-fitur penting yang diperlukan dalam aplikasi IoT, memungkinkan akses ke seluruh jaringan ketika dieksploitasi. Hal yang sama juga berlaku pada serangan zero-day di lingkungan SOHO dimana terdapat perangkat yang rentan.

Mirip dengan skenario Mirai, deteksi serangan zero-day sangat bergantung pada NIDS dan mode operasinya. Jenis eksploitasi ini sering kali disertai dengan muatan paket jaringan yang mencurigakan, sehingga membuat proses pendeteksian dapat dilakukan sampai batas tertentu. Meskipun demikian, langkah eksploitasi zero-day sering kali tidak mencerminkan tujuan akhir penyerang, melainkan merupakan langkah pertama dari serangan multi-tahap (jalur serangan pada BAG). Seorang penyerang dalam hal ini, mungkin saja memanfaatkan kerentanan yang ada dan berpindah dari satu host ke host lainnya hingga kondisi tujuan yang diinginkan tercapai. Di sisi lain, penyerang yang lebih canggih mungkin mengambil jalur

alternatif sehubungan dengan kecepatan dan kelayakan. Serangan zero-day diselidiki dengan mempertimbangkan transisi berbobot di masa depan untuk menghitung metrik keyakinan dari status serangan terkait. Peringatan yang diterima mengarahkan IRS menuju respons optimal yang terkait dengan status penyerang dalam grafik, sesuai dengan node eksploitasi di sekitarnya.

4.5 PENGATURAN EKSPERIMENTAL

Implementasi IRS yang dijelaskan pada bagian sebelumnya, dievaluasi dalam lingkungan simulasi SOHO yang realistis yang mencakup perangkat yang disajikan pada Tabel 4.1. Masing-masing, sejumlah perangkat eksternal terletak di WAN, dari mana gateway SOHO dapat dijangkau di 172.16.4.36. Komponen inti eksternal Mirai (C&C, loader, dan server laporan) terletak di 172.16.4.21, sedangkan target DDoS terletak di 172.16.4.26. Selain itu, server Zeus C&C terletak di 172.16.4.67

Tabel 4.1. Ikhtisar lingkungan SOHO.

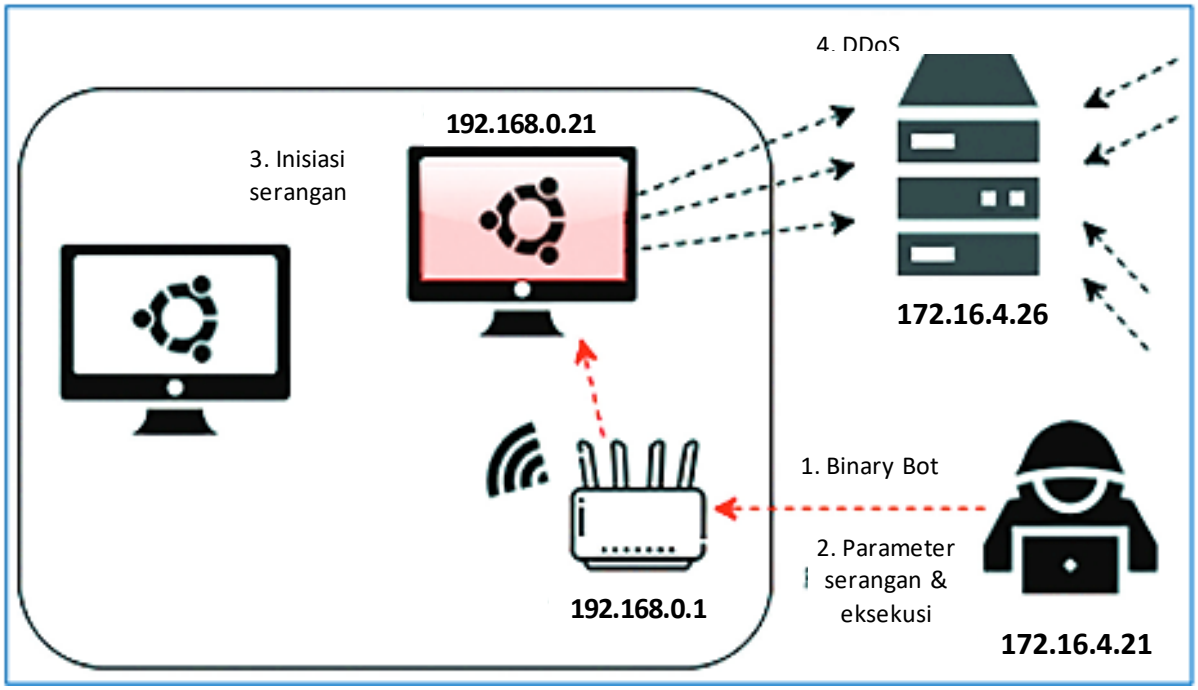
Nama perangkat	alamat IP	Keterangan
Gateway	192.168.0.1	Selain fungsi gatewaynya, ia menghosting instans Suricata IDS bersama dengan alat penemuan jaringan.
IRS	192.168.0.3 & .4	Dua bagian implementasi IRS (masing-masing mesin grafik serangan dan mesin pengambilan keputusan).
DHCP	192.168.0.7	Server DHCP khusus yang berdiri sendiri.
Android Device	192.168.0.9	Docker-Android Image1 berjalan di mesin virtual Ubuntu.
Windows XP	192.168.0.36	Mesin Windows XP tujuan umum bertindak sebagai target serangan (dengan paket layanan 3 diinstal).
Windows 7	192.168.0.17	Mesin Windows 7 tujuan umum bertindak sebagai target serangan (dengan paket layanan 1 diinstal).
Metasploitable 2	192.168.0.20	Perangkat Ubuntu2 yang sengaja rentan dirancang untuk pengujian eksploitasi jarak jauh dan lokal.
BusyBox	192.168.0.21 & .35	Rangkaian perangkat lunak yang mengimplementasikan sejumlah utilitas dasar Unix yang biasa digunakan pada perangkat yang disematkan IoT. Dua instance diterapkan di mesin virtual Ubuntu yang sama dengan perangkat Docker-Android.

Skenario Serangan Mirai

Untuk mendemonstrasikan lebih lanjut prosedur evaluasi IRS, eksekusi skenario serangan Mirai akan disajikan secara rinci, sedangkan gambaran umum diberikan pada Gambar 4.3. Skenario serangan ini melibatkan host BusyBox yang terinfeksi Mirai di dalam jaringan SOHO di 192.168.0.21, berkomunikasi dengan komponen Mirai eksternal di 172.16.4.21 untuk melakukan serangan DDoS di 172.16.4.26.

Bot biasanya melakukan serangan kamus terhadap port TCP 23 & 2323 (terkait dengan protokol TELNET) menggunakan daftar pasangan nama pengguna/kata sandi default umum untuk membuat koneksi dan mendapatkan akses shell. Skenario ini dimulai dengan biner bot

x86/x64 diunggah ke host BusyBox SOHO yang ditargetkan, dengan IDS gateway dan IRS keduanya beroperasi secara normal.



Gambar 4.3. Eksekusi serangan Mirai DDoS.

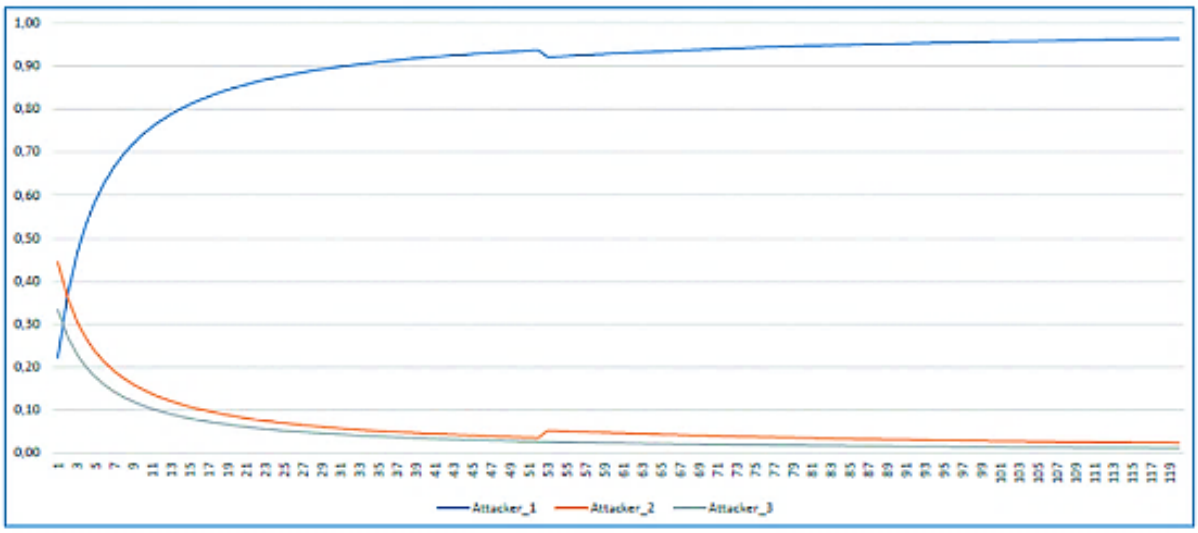
Informasi yang dihasilkan dilaporkan kembali ke server laporan Mirai. Pada titik ini, penyerang dapat memindai target potensial dengan mengirimkan permintaan ARP, untuk menemukan topologi SOHO.

Setelah itu, serangan dimulai dengan penyerang memilih parameter serangan dan mengkonfirmasi tindakannya. Serangkaian serangan DDoS yang dapat dipilih oleh penyerang, dalam hal ini serangan banjir SYN digunakan. Host yang terinfeksi akan mulai menyerang mesin eksternal dengan mengirimkan paket SYN berulang kali, dalam upaya untuk membuka koneksi TCP sebanyak mungkin dan menghabiskan sumber daya target.

Dalam demonstrasi ini, SOHO dipantau oleh IDS berbasis tanda tangan Suricata3, sehingga mitigasinya bergantung pada analisis paket yang ditangkap yang melewati gateway. Namun, bot Mirai berkomunikasi dengan komponen sisi server melalui Tor, sehingga membuat proses pendeteksiannya menjadi tugas yang sulit. Selama serangan berlangsung, pesan peringatan event_type = alert yang diterima digunakan oleh mesin pengambil keputusan.

IDS menghasilkan peringatan untuk tiga tindakan berikut:

- Penemuan target menggunakan paket ARP.
- Mencoba infeksi pada perangkat LAN dengan serangan kamus (192.168.0.21).
- Serangan banjir SYN pada perangkat target eksternal (192.168.0.21 → 172.16.4.26).



Gambar 4.4. Keyakinan penyerang untuk setiap negara keamanan.

Peringatan ini mengawali proses pengambilan keputusan IRS yang menghasilkan 120 status keamanan berbeda di GNSM. Secara total, satu tindakan mitigasi respons dipilih, sebuah aturan global yang memblokir semua komunikasi yang berasal dari host yang terinfeksi Mirai, yang mampu mencegah serangan DDoS:

```
iptables -A INPUT -s 192.168.0.21 -j DROP
iptables -A OUTPUT -s 192.168.0.21 -j DROP
```

Terlepas dari kenyataan bahwa terdapat pembatasan deteksi, IRS menjadi lebih yakin terhadap keyakinan negara dan keyakinan penyerang seiring berjalannya waktu, yang mengakibatkan pemblokiran terus-menerus terhadap host yang terinfeksi yang berlokasi di 192.168.0.21 dengan aturan firewall global. Keyakinan tipe penyerang sepanjang eksekusi skenario disajikan pada Gambar 4.4. Ketidakpastian awal mengenai tipe penyerang dapat dilihat di bagian paling kiri grafik karena niat penyerang tidak jelas pada beberapa putaran pertama. Ketika serangan berlanjut, keyakinan tipe penyerang dengan cepat mendekati kepastian, dengan POMDP berasumsi bahwa penyerang mengikuti perilaku yang ditetapkan pada penyerang tipe 1 (yang paling tidak tersembunyi dari ketiganya). Demikian pula, keyakinan pembela HAM terhadap keamanan negara semakin meningkat dan semakin pasti. Masing-masing, waktu komputasi keyakinan ditampilkan pada Gambar 4.5.

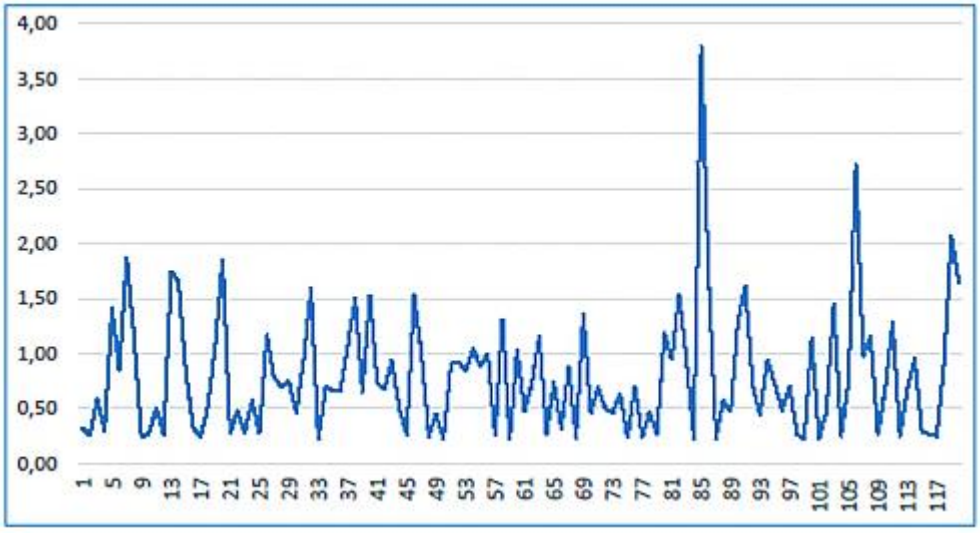
Setelah penerapan aturan firewall oleh gateway, bot dibatasi untuk menginfeksi lebih lanjut calon korban baru di SOHO, apalagi mengambil bagian dalam serangan DDoS. Selain itu, hasil positif yang didapat dari respons sebelumnya juga mencegah penyerang berkomunikasi dengan bot. Masing-masing, bot dilarang mengirimkan laporan relatif, kembali ke server laporan.

4.6 EVALUASI IRS

IRS telah dievaluasi berdasarkan total lima skenario serangan. Yang pertama, skenario Mirai, telah dijelaskan di bagian sebelumnya. Empat skenario sisanya meliputi: simulasi

serangan zero-day dari vsftpd eksploitasi4 di testbed SOHO, serangan tingkat jaringan yang diulang, dan botnet BlackEnergy & Zeus.

Secara khusus, kerentanan zero-day yang telah dieksploitasi adalah pintu belakang yang ada di binari vsftpd v2.3.4 yang membuka shell jarak jauh pada port TCP 6200. Kerentanan spesifik ini ada di mesin virtual Metasploitable 2 yang berada di dalam SOHO dan dipicu selama proses login FTP ketika nama pengguna yang dibentuk secara khusus dimasukkan. Untuk mensimulasikan serangan zero-day secara efektif, semua informasi tentang kerentanan dan tanda tangan terkait dihapus dari semua komponen pertahanan siber.



Gambar 4.5. Waktu komputasi keyakinan per status keamanan.

Selama fase pengujian dan evaluasi, kumpulan data file pcap telah dihasilkan dari lalu lintas malware yang realistis di lingkungan SOHO, termasuk enumerasi pengguna, serangan bruteforce, dan eksploitasi Metasploit. Daftar lengkapnya meliputi: (a) pintu belakang Java-RMI, (b) pintu belakang distcc_exec, (c) pintu belakang UnrealIRCD, (d) eksploitasi Web Tomcat, (e) Eksekusi kode Ruby DRb, (f) Brute force Hydra FTP, (g) Bruteforce Hydra SSH, (h) eksploitasi vstfpd, (i) Pencacahan Pengguna SMTP dan (j) kerentanan eksekusi kode jarak jauh NetBIOS-SSN. Sebagian besar serangan ini dilakukan di mesin virtual Metasploitable 2.

Skenario serangan ketiga adalah botnet Black Energy, yang tujuannya adalah memulai serangan DDoS jarak jauh. Malware menyembunyikan prosesnya di driver sistem dan menghindari deteksi melalui teknik kebingungan. Serangan DDoS yang dipilih adalah serangan banjir SYN yang meluncurkan beberapa permintaan sinkronisasi ke perangkat eksternal SOHO. Selanjutnya, botnet dikelola melalui server C&C eksternal (ke SOHO) yang bertanggung jawab untuk mengeluarkan perintah. Target untuk langkah infeksi adalah mesin Windows XP (192.168.0.36) dari testbed, sedangkan transmisi malware yang dapat dieksekusi dilakukan melalui HTTP.

Botnet Zeus adalah skenario serangan terakhir dari evaluasi; trojan perbankan yang dikenal luas yang tujuan utamanya adalah menangkap kredensial melalui suntikan web dan logging penekanan tombol, namun juga memiliki kemampuan untuk membentuk botnet.

Setiap host yang terinfeksi Zeus berkomunikasi dengan server C&C eksternal untuk laporan berkala dan ketika diminta oleh operator botnet, semua komunikasi dienkripsi menggunakan algoritma RC4 dan terjadi melalui HTTP. Botnet memiliki dua langkah deteksi yang berbeda yang mengarah pada pembuatan peringatan NIDS: (1) langkah infeksi, di mana botnet memulai komunikasinya dengan K&C, dan (2) pembentukan koneksi TCP dengan server C&C, tempat laporan tersebut dikirim ke penyerang. Selain itu, pada langkah terakhir, penyerang dapat menjalankan perintah pada mesin yang terinfeksi (misalnya mengambil tangkapan layar desktop, mengunduh dan menjalankan program lain, dll.). Mesin Windows 7 (192.168.0.17) di dalam SOHO adalah target skenario ini.

Opsi Konfigurasi

Enam belas opsi konfigurasi dievaluasi berdasarkan lima skenario serangan yang disebutkan di atas untuk menentukan efektivitas sejumlah fitur IRS; yang paling penting adalah:

- Penggunaan metrik berbasis CVSS atau yang telah ditentukan sebelumnya untuk menghitung risiko host awal dan probabilitas upaya eksploitasi (dari node OR ? AND) dan keberhasilan (dari node AND → OR).
- Batas keyakinan di mana node eksploitasi (AND) dianggap telah disusupi oleh penyerang. Lebih khusus lagi, ambang batas ini mengontrol node mana yang akan dimasukkan dalam set Eav. Awalnya, semua node OR & AND pada BAG diberi keyakinan 0, sedangkan node LEAF yang mewakili kemampuan penyerang untuk mengeksekusi kode pada sebuah host diberi keyakinan 0,5 dan semua node LEAF yang tersisa diberi keyakinan 1.
- Apakah generator respons akan menghasilkan aturan firewall spesifik (menargetkan port dan protokol tertentu) dan global (memblokir semua upaya koneksi host), atau apakah akan dibatasi hanya pada aturan firewall global. Opsi ini secara efektif membatasi rangkaian tindakan remediasi yang tersedia bagi pembela HAM.
- Kebijakan manajemen peringatan, ketat atau tangkas, yang mengontrol proses pencocokan peringatan dan apakah kondisi keyakinan IRS akan dikesampingkan oleh penerimaan peringatan (kebijakan ketat) atau apakah akan diperhitungkan (kebijakan tangkas) .

Hasil Evaluasi

Evaluasi IRS dilakukan terhadap kelima skenario dengan masing-masing skenario diulang enam belas kali, satu untuk setiap opsi konfigurasi. Hasil evaluasi dirangkum pada Tabel 4.2 berikut.

Tabel 4.2. Hasil Evaluasi IRS.

	Konfigurasi				**Skenario**				
#	Metrik	Kompromi ambang	Aturan FW Global	Manajer peringatan	Mirai	Zeus	Zero-Day	Reply	Black Energy
1	P	0.5	Benar	Strict	√	√	×	9/10 √	√

2				Agile	√	√	×	9/10 √	√
3			Salah	Strict	√	√	*√	8/10 √	√
4				Agile	√	√	×	8/10 √	√
5		1	Benar	Strict	√	√	×	9/10 √	√
6				Agile	×	×	×	0/10 ×	×
7			Salah	Strict	√	√	×	9/10 √	√
8				Agile	×	×	×	0/10 ×	×
9		0.5	Benar	Strict	√	√	×	9/10 √	√
10				Agile	√	√	×	9/10 √	√
11			Salah	Strict	√	√	*√	10/10 √	√
12				Agile	√	√	×	10/10 √	√
13	CVSS-Based	1	Benar	Strict	√	√	×	9/10 √	√
14				Agile	×	×	×	0/10 ×	×
15			Salah	Strict	√	√	*×	9/10 √	√
16				Agile	×	×	×	0/10 ×	×

√ dan × masing-masing menunjukkan bahwa serangan tersebut berhasil dan tidak berhasil dimitigasi.

* menunjukkan bahwa aturan tertentu (menargetkan port dan protokol tertentu) digunakan untuk mengurangi serangan.

Kombinasi dari ambang batas kompromi yang tinggi dan kebijakan manajemen peringatan tangkas pada konfigurasi #6, #8, #14 dan #16 membuat konfigurasi tersebut selalu gagal. Karena ambang batas yang tinggi tidak memungkinkan node eksploitasi (AND) apa pun dianggap telah disusupi, karena tidak ada keyakinan node LEAF yang berhasil melampauinya, dan kebijakan agile tidak mengesampingkan keyakinan untuk mempertimbangkan node yang cocok dengan peringatan IDS.

Untuk konfigurasi selebihnya, mengenai:

- Skenario Mirai, Zeus, dan BlackEnergy: peringatan dicocokkan dengan BAG menggunakan kriteria terluas yang tersedia, yang memaksa mesin pengambil keputusan untuk memilih aturan firewall global apa pun opsi konfigurasinya. Hal ini karena skenario ini memulai komunikasi melalui port yang ditetapkan secara dinamis, karena semuanya menggunakan API sistem operasi yang membuka port acak pada setiap panggilan. Perubahan ini cukup cepat sehingga proses pembangkitan GNSM harus diulang beberapa kali per menit, hal ini tidak optimal dan tidak layak saat ini, untuk menangkap port yang berubah dengan cepat pada GNSM yang dihasilkan.
- Skenario zero-day: (a) untuk konfigurasi #3, #11, dan #15 peringatan IDS telah dicocokkan dengan benar ke port TCP 5000 yang menghasilkan pilihan aturan tertentu yang memblokir komunikasi semua host dengan router melalui TCP port 5000, dan (b) untuk konfigurasi lainnya, peringatan diterima mengenai eksploitasi zero-day namun tidak cocok dengan bagian BAG yang sama sekali berbeda, sehingga menyebabkan pilihan tindakan mitigasi yang salah; akibat kurangnya informasi mengenai kerentanan yang dieksploitasi.
- Skenario replay yang tidak berhasil dimitigasi adalah: (a) backdoor Java RMI (gagal dua kali), (b) eksekusi kode Ruby DRb (gagal satu kali), (c) enumerasi pengguna SMTP (gagal lima kali), (d) eksploitasi web Tomcat (gagal dua kali), dan (e) pintu belakang UnrealIRCD

(gagal dua kali). Sekali lagi, selama pelaksanaan skenario ini, peringatan IDS diterima, namun seperti halnya skenario zero-day, peringatan tersebut salah dicocokkan dengan BAG.

4.7 KESIMPULAN

Memindahkan target pertahanan tidak diragukan lagi merupakan bidang yang mencakup banyak implementasi berbeda untuk mengatasi masalah yang sama dengan beragam teknologi dan mekanisme. Pertarungan pembela-penyerang adalah permainan yang tidak pernah berakhir, menandakan bahwa keamanan yang sangat mudah tidak akan pernah tercapai dalam sistem apa pun dan terutama dalam jaringan kecil dan seringkali tanpa pengawasan. Selanjutnya, MTD berupaya menyediakan kerangka pertahanan keamanan dengan efektivitas yang memadai.

Dalam karya ini, solusi terukur yang telah diuji dalam lingkungan SOHO yang realistis dan secara efisien mengatasi situasi yang disebutkan di atas telah disajikan. IRS yang disajikan dalam karya ini didasarkan pada GNSM yang dihasilkan oleh kerangka MulVAL yang diubah menjadi BAG, untuk melakukan analisis risiko dan menjadi dasar proses pengambilan keputusan. Mesin pengambilan keputusan mengimplementasikan model POMDP dengan banyak modifikasi untuk mengatasi serangan yang tidak diketahui dan tingkat jaringan dengan lebih baik. Di antara modifikasi tersebut adalah penerapan kebijakan peringatan yang mampu mempertimbangkan ancaman di seluruh kemungkinan kondisi GNSM.

Untuk mengevaluasi efektivitas penerapan IRS terhadap situasi realistis, seperti serangan botnet Mirai, lima skenario serangan (Mirai, Zeus, zero-day, 10 pemutaran ulang lalu lintas berbahaya, dan BlackEnergy) dieksekusi dalam lingkungan simulasi SOHO. Enam belas konfigurasi IRS diuji, untuk menentukan konfigurasi optimal, menguji efektivitas modifikasi tersebut di atas, dan untuk mengidentifikasi keterbatasannya.

Pada akhirnya, sistem ini sangat efektif melawan ancaman yang lebih tradisional, seperti Mirai, Zeus, dan BlackEnergy, namun efektivitasnya terhadap ancaman baru (yaitu zero-day), meskipun sedikit meningkat, masih kurang. Pekerjaan ini merupakan titik awal untuk pekerjaan di masa depan, karena sejumlah keterbatasan diidentifikasi dari proses ini, termasuk: a) ketidakmampuan GNSM IRS untuk secara tepat memodelkan keadaan jaringan dengan perubahan topologi yang cepat (misalnya dengan memasukkan koneksi baru perangkat) atau untuk meng-host atribut (misalnya port yang baru dibuka); dan b) kesalahan pencocokan peringatan IDS dengan GNSM yang diamati selama zero-day dan beberapa skenario pemutaran ulang yang menyebabkan banyak penalti efektivitas selama pelaksanaan skenario ini.

BAB 5
DETEKSI ANCAMAN SIBER DI IOT

Ekosistem Internet of Things (IoT) sebagian besar terdiri dari perangkat berbasis internet yang heterogen, yang menghasilkan data dalam jumlah besar setiap hari; ini termasuk sensor, perangkat pintar, dan modul industri lainnya. Namun, kompleksitas ekosistem IoT dan kuantitas perangkat IoT yang tersedia telah secara dramatis meningkatkan volume kerentanan keamanan yang muncul dan terus-menerus dari infrastruktur komputasi edge hingga cloud, terutama karena masalah keamanan yang timbul dari perangkat yang tertanam dan perangkat keras lama lainnya. Lebih lanjut, dengan munculnya teknologi IoT, kampanye malware dan motivasi kriminal semakin mengeksploitasi layanan-layanan mendasar dan kerentanan yang ada. Dalam proyek Siber-Trust, kami bertujuan untuk mengatasi masalah keamanan ini guna mendukung pertumbuhan ekosistem IoT sekaligus memitigasi kompleksitas dan kerentanan yang diakibatkannya saat melindungi perangkat IoT. Bab ini menyajikan ikhtisar pembuatan profil perangkat IoT dan solusi deteksi ancaman yang diusulkan oleh Siber-Trust untuk mengatasi tantangan besar dalam mengamankan ekosistem perangkat IoT. Selain itu, efektivitas dan kinerja solusi yang diusulkan telah diverifikasi secara mendalam, terutama terhadap botnet dan serangan Zero-day.

5.1 ANCAMAN BESAR DUNIA MAYA TERHADAP IOT

Meningkatnya adopsi teknologi Internet of Things (IoT) menghasilkan dunia yang lebih cerdas dan terhubung. Menurut statistik IoT terakhir , ada lebih dari 10 miliar perangkat IoT aktif pada tahun 2022. Selanjutnya, diperkirakan pada tahun 2025, akan ada lebih dari 152.200 perangkat IoT yang terhubung ke Internet per menit. Jumlah data yang dihasilkan oleh perangkat ini diperkirakan mencapai 73,1 ZB . Namun, menghubungkan sejumlah besar perangkat IoT secara global, yang sebagian besar mudah diakses dan disusupi, memungkinkan peretas dan pelaku kejahatan untuk menggunakannya sebagai sistem pengiriman senjata siber pilihan dalam banyak serangan siber saat ini, misalnya, mulai dari pembuatan botnet untuk meluncurkan serangan penolakan layanan terdistribusi, hingga penyebaran malware dan spam.

Di sisi lain, perangkat IoT pada dasarnya memiliki keterbatasan sumber daya dalam komputasi, daya baterai, konektivitas intermiten, dan protokol jaringan. Keterbatasan ini menghambat pelaksanaan tugas keamanan yang kompleks dan menjadikannya rentan terhadap serangkaian serangan seperti malware, kebocoran data, spoofing, gangguan layanan (DoS/DDoS), kebocoran energi, gateway tidak aman, suntikan, ransomware, dan lain-lain. pembajakan perangkat. Mengarah pada masalah keamanan dan keselamatan yang berpotensi membahayakan nyawa manusia.

Keamanan IoT telah menjadi topik yang semakin umum selama beberapa tahun terakhir, terutama dengan meningkatnya insiden keamanan yang melibatkan perangkat yang terhubung secara cerdas. Dalam konteks ini, proyek IoT Proyek Keamanan Aplikasi Web

Terbuka (OWASP)1; yang merupakan komunitas relawan profesional keamanan, bekerja untuk menyelidiki kerentanan IoT paling kritis yang dapat dieksploitasi oleh peretas sebagai dasar untuk semua jenis perilaku jahat, termasuk serangan DDoS terdistribusi, distribusi malware, kampanye spam, phishing, penipuan, pencurian data, dan masih banyak lagi. yang lain. Selain itu, proyek ini bertujuan untuk membantu produsen, pengembang, organisasi, dan pelanggan perangkat pintar untuk lebih memahami risiko keamanan IoT yang sedang berlangsung dan mengambil tindakan yang tepat untuk memitigasinya. Menurut laporan terakhir yang dirilis oleh proyek OWASP IoT, ancaman IoT paling parah pada tahun 2018 adalah:

1. Kata sandi yang lemah: menurut laporan, kata sandi yang lemah, dapat ditebak, atau dikodekan secara keras adalah kelemahan keamanan IoT. Jika kredensial login tidak diubah dari pengaturan defaultnya, serangan brute force sederhana dapat dengan mudah digunakan untuk menyusupi perangkat ini dan menggunakannya untuk melancarkan serangan skala besar terhadap infrastruktur siber yang penting.
2. Layanan jaringan tidak aman: Ini adalah masalah besar lainnya dalam jaringan IoT, dimana layanan jaringan standar yang berjalan pada perangkat, seperti Telnet, SSH, dan protokol HTTP yang tidak aman, mewakili masalah keamanan signifikan yang belum dipertimbangkan oleh produsen. Setiap port yang terbuka pada perangkat pintar memberikan peluang baru bagi pelaku kejahatan untuk mendapatkan akses ke perangkat tersebut.
3. Antarmuka tidak aman: Antarmuka standar yang digunakan untuk berkomunikasi dengan perangkat yang terhubung tidak selalu aman. Ini termasuk antarmuka web, API cloud, dan antarmuka seluler. Ekosistem antarmuka yang tidak aman pada akhirnya menyebabkan perangkat dikompromikan melalui kerentanan pada tingkat ini, seperti enkripsi yang lemah, pemfilteran data, dan metode otentikasi yang lemah.
4. Mekanisme pembaruan yang tidak aman: Masalah keamanan IoT terkait dengan kurangnya mekanisme pembaruan yang aman, seperti tidak adanya pembaruan otomatis sebagai fitur dan tidak adanya pemberitahuan perubahan keamanan. Oleh karena itu, produsen perangkat IoT harus menyediakan pembaruan/patch keamanan secara berkala untuk menjamin keamanan perangkat mereka.
5. Penggunaan komponen yang tidak aman dan ketinggalan jaman: Beberapa produsen menggunakan perangkat di luar merek dan komponen/pustaka perangkat lunak yang tidak aman untuk membuat perangkat IoT yang lebih murah. Namun, praktik ini juga membawa banyak kerentanan bagi pengguna akhir dan menciptakan pintu masuk bagi potensi serangan siber. Menurut Symantec [8], serangan rantai pasokan merupakan bagian besar dari lanskap ancaman, dengan peningkatan serangan sebesar 78% pada tahun 2019.
6. Masalah privasi: Penyimpanan, pemrosesan, dan pengungkapan data pribadi yang tidak aman tanpa persetujuan tertulis dapat menyebabkan banyak masalah privasi dan bahkan membahayakan keselamatan orang-orang di dunia fisik. Selain itu, pernyataan kebijakan privasi dari beberapa penyedia layanan IoT tidak jelas mengenai pengumpulan data dan tidak mengidentifikasi kemampuan sistem.

7. Penyimpanan dan transfer data yang tidak aman: Biasanya, data yang dikumpulkan oleh perangkat pintar berpindah melalui jaringan atau disimpan di lokasi pihak ketiga (misalnya, penyimpanan cloud). Oleh karena itu, potensi untuk disusupi semakin meningkat, terutama dengan kurangnya enkripsi yang efisien dan kontrol akses ke data dan transfer sensitif perangkat.
8. Kurangnya manajemen perangkat: Manajemen IoT menimbulkan sejumlah tantangan terkait keamanan, dimana sebagian besar perangkat yang terhubung ke jaringan tidak memiliki manajemen keamanan yang efisien, seperti kurangnya pemantauan sistem dan mekanisme pembaruan/patch, yang menjadikannya menarik target penyerang dunia maya.
9. Pengaturan default tidak aman: Sebagian besar perangkat IoT dikirimkan dengan konfigurasi default yang tidak aman dan modifikasi terbatas. Namun, mempertahankan pengaturan default seperti kata sandi default akan menimbulkan risiko keamanan yang serius, tidak hanya pada perangkat, tetapi juga pada seluruh jaringan.
10. Kurangnya pengerasan fisik: Penguatan fisik adalah salah satu aspek paling penting dari keamanan IoT karena akses fisik dapat menjadi bencana bagi perangkat dan memungkinkan penyerang potensial mendapatkan informasi sensitif (misalnya, kata sandi yang tertanam), memasukkan kode berbahaya, dan bahkan menulis ulang firmware perangkat.

Semua masalah keamanan ini dan banyak masalah lainnya menjadikan perangkat IoT sebagai sasaran empuk bagi peretas dan pelaku jahat, bahkan menggunakannya sebagai sarana untuk serangan siber besar-besaran seperti serangan Distributed Denial of Service (DDoS). Oleh karena itu, terdapat kebutuhan penting akan teknik baru yang dirancang khusus untuk lingkungan IoT guna mengidentifikasi dan memitigasi potensi serangan keamanan terkait IoT yang mengeksploitasi beberapa kerentanan keamanan ini. Pada bagian berikut, kami menyajikan tinjauan komprehensif tentang teknik terbaru yang dirancang untuk pembuatan profil perangkat IoT dan deteksi ancaman di IoT.

Metode Deteksi Ancaman IoT

Beberapa penelitian telah mencoba merancang sistem deteksi intrusi baru yang dapat mengidentifikasi potensi serangan siber di jaringan IoT dalam beberapa tahun terakhir. Teknik-teknik ini diklasifikasikan ke dalam dua kategori utama: teknik deteksi berbasis tanda tangan dan berbasis perilaku. Metode berbasis tanda tangan adalah teknik paling sederhana dan efektif untuk mendeteksi intrusi dan serangan siber. Mereka mengacu pada kumpulan data tanda tangan (atau pola) malware yang dikenal. Tanda tangan mencakup informasi (misalnya hash kriptografi) yang dapat mengidentifikasi malware (serangan) secara unik. Aktivitas jaringan saat ini dibandingkan dengan tanda tangan untuk mengidentifikasi potensi serangan. Jika tanda tangan lalu lintas jaringan sesuai dengan salah satu tanda tangan yang ada, maka tanda tangan tersebut dianggap berbahaya, dan tindakan pertahanan lebih lanjut akan dilakukan. Teknik-teknik ini memberikan tingkat akurasi 100% dalam mendeteksi serangan yang diketahui; namun, mereka tidak dapat mendeteksi serangan baru dan tidak diketahui (serangan Zero-day) yang tidak memiliki tanda tangan yang sesuai. Dengan

keterbatasan ini, serangan menggunakan teknik Kebingungan untuk mengubah tanda serangan dan menghindari deteksi.

Teknik deteksi berbasis anomali telah diusulkan untuk mengatasi keterbatasan metode deteksi berbasis tanda tangan. Metode ini memantau aktivitas jaringan berdasarkan serangkaian persyaratan yang ditentukan yang mengacu pada model dasar untuk perilaku jaringan yang diharapkan. Setiap penyimpangan dari profil rata-rata ini akan dianggap sebagai anomali dan memulai tindakan defensif yang sesuai. Teknik pendeteksian berbasis anomali secara umum dimulai dengan mengumpulkan informasi yang dapat membedakan perilaku yang diharapkan dari jaringan dari perilaku abnormal. Kemudian, informasi ini digunakan untuk melatih pengklasifikasi pembelajaran mesin untuk mendeteksi potensi serangan. Dalam konteks ini, keakuratan prediksi dari banyak algoritma pembelajaran yang diawasi dan tidak diawasi telah dipelajari dalam beberapa penelitian. Misalnya, Verma Abhishek dkk. mempelajari kinerja berbagai algoritma pembelajaran terawasi dalam mengamankan perangkat IoT terhadap serangan DDoS. Algoritma yang dipelajari adalah Random Forest (RF), AdaBoost (AB), Extreme Gradient Boosting (XGB), Gradient Boosted Machine (GBM), dan Extremely Randomized Trees (ETC). Hasil eksperimen menunjukkan bahwa pengklasifikasi Multilayer perceptron (MLP) menggunakan kumpulan pemilihan fitur yang berasal dari metode pemilihan fitur, mengungguli semua pengklasifikasi lainnya dengan tingkat akurasi 83%, tingkat True Positive (TP) 90%, dan tingkat False Positive (FP) 23% .

Efektivitas algoritma pembelajaran mendalam juga telah diselidiki dalam banyak penelitian. Teknik-teknik ini memberikan paradigma baru yang kuat yang dapat secara otomatis mengekstraksi fitur-fitur yang diperlukan untuk membangun profil jaringan dari data besar tanpa diprogram secara khusus. Misalnya, Recurrent Neural Network (RNN) telah digunakan dalam banyak penelitian untuk memodelkan aktivitas jaringan untuk deteksi intrusi di IoT, terutama dua varian utamanya, Long Short-Term Memory (LSTM) dan Unit Berulang Berpagar (GRU). Selain itu, Convolutional Neural Network (CNN), yang memperoleh kesuksesan besar dalam klasifikasi gambar, juga telah digunakan dalam banyak metode deteksi intrusi untuk jaringan IoT. Hasil dari banyak penelitian menunjukkan bahwa Pembelajaran mendalam dapat meningkatkan akurasi deteksi intrusi secara signifikan. Misalnya, metode yang diusulkan dalam telah mencapai akurasi rata-rata 98,9%. Manfaat penting lainnya dari teknik ini adalah bahwa teknik ini berpotensi mengidentifikasi serangan Zero-day dan serangan tak terduga; namun, mereka memiliki tingkat positif palsu yang lebih tinggi. Tabel 5.1 menyajikan contoh algoritma pembelajaran yang digunakan dalam metode deteksi intrusi untuk IoT dan hasil yang dicapai dalam hal akurasi, FP, dan TP.

Metode Pembuatan Profil Perangkat IoT

Secara umum, pembuatan profil perangkat IoT mengacu pada pemantauan dan pencatatan data yang dapat diambil dari berbagai sumber (misalnya perangkat IoT, aset jaringan) untuk mengkarakterisasi perilaku pribadi perangkat IoT yang terhubung ke jaringan. Dalam konteks ini, perilaku abnormal perangkat IoT dapat diidentifikasi dengan membandingkan aktivitas perangkat saat ini dengan profil yang ada yang dibangun dari aktivitas historis selama periode tertentu. Jika perilaku saat ini cukup menyimpang dari

perilaku normal yang telah ditentukan sebelumnya, maka hal tersebut akan dianggap sebagai potensi serangan dan memulai tindakan pertahanan yang sesuai.

Tabel 5.1. Algoritma pembelajaran populer yang digunakan dalam metode deteksi intrusi untuk IoT.

Study	Classification	Test Dataset	Best Results
V. Abhishek *et al.* [11]	Random forest (RF), AdaBoost (AB), Extreme Gradient Boosting (XGB), Gradient boosted machine (GBM), and Extremely Randomized Trees (ETC), Multilayer Perceptron (MLP).	• CIDDS-001, • UNSW-NB15, • NSL-KDD	MLP • Accuracy: 83%, • TP: 90%, • FP: 23%
K. K. Sai *et al.* [12]	SVM, Naïve Bayes, Decision Tree, Adaboost.	Sensor480 with 480 samples	Decision Tree • Accuracy: 100%
Z. Marzia *et al.* [13]	Radial Basis Function (RBF),	Kyoto 2006+	RBF • Precision: 90%
R. Bipraneel *et al.* [15]	Recurrent Neural Network (RNN)	NSL-KDD dataset	Accuracy: 89.00%
K. Jihyun *et al.* [16]	Long Short-Term Memory (LSTM)	KDD Cup 1999	Accuracy: 96.93%
G. Mengmeng *et al.* [18]	Feedforward Neural Network (FNN)	BoT-IoT dataset	Accuracy: 96.82%
V. Huong *et al.* [17]	Convolutional Neural Network (CNN)	IoT intrusion dataset with 357952 samples	Accuracy: 98.90%

Biasanya, proses pembuatan profil dapat dilakukan pada perangkat IoT dan tingkat jaringan (yaitu pembuatan profil jaringan) untuk mengambil informasi masing-masing dari perangkat pengguna akhir dan aset jaringan (misalnya gateway).

Beberapa karya penelitian telah menyajikan proposal untuk pembuatan profil perangkat IoT dengan menggunakan teknik berbeda seperti fusi sensor dan SDA dengan Layanan Cloud untuk memantau penggunaan perangkat dan mengambil informasi tentang file penting, status keamanan, termasuk status patching dan integritas firmware. Namun, dalam bab ini, kami fokus pada teknik pembuatan profil tingkat jaringan. Profil jaringan mengacu pada proses pemantauan dan pencatatan semua aktivitas jaringan dengan mencatat informasi dari metadata paket seperti IP sumber/tujuan paket, waktu mulai, durasi, identitas sensor, protokol lapisan aplikasi yang digunakan. Pembuatan profil Jaringan IoT dapat dilakukan di

enam bidang utama, dengan perangkat lunak sumber terbuka dan komersial yang menyediakan alat yang diperlukan operator jaringan untuk memahami, mengendalikan, dan mengelola jaringan yang berada di bawah kendali mereka. Enam bidang utama, termasuk contoh penerapannya, dirangkum dalam Tabel 5.1.

Seperti yang ditunjukkan pada Tabel 5.2, beberapa alat bersumber terbuka dan berpemilik dapat digunakan untuk pembuatan profil jaringan dan menyelidiki potensi ancaman dunia maya, seperti SiLK (Sistem untuk Pengetahuan Tingkat Internet), perangkat yang sangat skalabel dan kuat untuk menangkap dan menganalisis aliran jaringan data. Selain itu, alat berpemilik seperti NetFlow (Sisco), ntopng (ntop) dan PRTG Network Monitor menawarkan fungsionalitas lengkap untuk penawaran komersialnya masing-masing.

Tabel 5.2. Area utama pembuatan profil jaringan dengan contoh alat.

Areas	Examples of Tools
Network Spoofing and Redirection	DNSMasq, Ettercap.
Executable Reverse Engineering	Java Decompiler, NET Reflector, IDA Pro, Hopper, ILSpy.
Web App Testing	Mitmproxy, Zed Attack Proxy, Burp Suite.
Active Network Capture and Analysis	Canape, Canape Core, Mallory.
Passive Network Protocol Capture and Analysis	Wireshark, SiLK, LibPCAP, TCPDump, MS Message Analyser.
Fuzzing, Packet Execution and Vulnerability Exploitation Frameworks	American Fuzzy Lop (AFL), Kali Linux, Metasploit, Scapy, Sully.

Menuju arah yang sama, Satuan Tugas Rekayasa Internet (IETF) telah memperkenalkan spesifikasi Deskripsi Penggunaan Pabrikan (MUD) untuk meningkatkan keamanan jaringan IoT dengan mencegah perangkat IoT dari akses tidak terbatas ke jaringan dan hanya mengizinkan perangkat tersebut terhubung ke layanan khusus. Untuk itu, MUD mengharuskan produsen IoT menyediakan profil perilaku perangkat mereka. Misalnya, kamera IP mungkin perlu menggunakan protokol DNS dan DHCP untuk berkomunikasi dengan pengontrol berbasis cloud dan server NTP (Network Time Protocol). Informasi ini dapat digunakan untuk menghasilkan daftar kontrol akses (ACL) khusus perangkat yang menetapkan batasan pada perangkat ini dan, oleh karena itu, mengurangi potensi permukaan serangan pada jaringan. Namun, spesifikasi MUD masih dalam pengembangan sehingga belum diterapkan oleh produsen.

Di sisi lain, banyak penelitian telah mengusulkan pendekatan profil lalu lintas jaringan IoT yang berbeda. Misalnya, Jonathan Roux dkk, telah mengusulkan pendekatan deteksi intrusi untuk IoT berdasarkan profil komunikasi radio. Solusi yang diusulkan menargetkan serangan siber yang mungkin terjadi melalui komunikasi nirkabel dengan membuat profil dan memantau Indikasi Kekuatan Sinyal Radio (RSSI) yang terkait dengan transmisi nirkabel pada perangkat yang terhubung. Informasi ini dikumpulkan oleh probe radio yang ditempatkan di

area pintar (jaringan). Kemudian, jaringan saraf dilatih untuk mengklasifikasikan area sah dan tidak sah di mana perangkat biasanya berkomunikasi dalam smart place. Namun, solusi yang diusulkan tidak sepenuhnya diterapkan, dan makalah ini tidak memberikan informasi tentang kinerja pendeteksiannya (seperti akurasi, positif palsu, dan negatif palsu.).

Dalam karya lain, Andrei Bytes dkk, telah mengembangkan perangkat lunak baru untuk pembuatan profil fitur otomatis perangkat IoT. Profil perangkat dibuat berdasarkan kemampuan teknisnya seperti firmware perangkat, mode akses perangkat, topologi operasi jaringan, dan antarmuka nirkabel. Informasi ini dikumpulkan dari berbagai lokasi, termasuk sumber langsung dan tidak langsung. Profil yang dibuat kemudian digunakan untuk mengkategorikan dan membandingkan kemampuan sensitif keamanan perangkat IoT.

5.2 METODE DETEKSI KEPERCAYAAN DUNIA MAYA

Tujuan utama proyek Siber-Trust adalah untuk mengusulkan platform pengumpulan, deteksi, dan mitigasi intelijen ancaman siber yang inovatif untuk mengatasi tantangan besar dalam mengamankan ekosistem perangkat IoT. Pendekatan yang diusulkan mencakup berbagai fase serangan IoT yang muncul, sebelum dan sesudah kerentanan yang diketahui atau tidak diketahui (Zero-day). Bab ini fokus pada fase deteksi, yang melibatkan dua komponen utama: pembuatan profil jaringan dan deteksi intrusi.

Pendekatan Profil Jaringan

Komponen pembuatan profil jaringan, juga dikenal sebagai repositori jaringan, secara otomatis memindai perangkat yang terhubung pada jaringan yang tersedia secara lokal untuk mencari potensi kerentanan umum dan layanan yang sedang berjalan. Untuk setiap perangkat yang terhubung ke jaringan, daftar potensi kerentanan dikumpulkan dari dataset publik CVE Mitre1 dan dipetakan ke layanan jaringan yang tersedia, yang ditemukan melalui alat pemindaian port jaringan seperti Nmap. Informasi ini kemudian digunakan untuk membuat profil perangkat dan informasi lainnya tentang informasi perutean, nama host yang dilaporkan, aliran jaringan, dan topologi. Berdasarkan profil yang dibuat untuk setiap perangkat, komponen pembuatan profil jaringan menghitung perilaku profil jaringan di luar batas; ini dihitung dengan pemantauan terus menerus terhadap arus lalu lintas jaringan dari setiap perangkat di seluruh jaringan. Ini menggunakan profil heuristik tingkat informasi untuk menciptakan pola throughput yang diharapkan untuk setiap perangkat di LAN yang terhubung dengannya. Profil ini kemudian dibandingkan dengan tiga profil berbeda yang telah ditentukan sebelumnya yang merujuk pada profil jaringan yang diperoleh dari penangkapan paket yang disegarkan setiap jam (HP, Profil Per Jam), harian (DP, Profil Harian) dan mingguan (WP, Profil Mingguan). Tujuan penggunaan profil berbeda yang dipisahkan dan diperbarui berdasarkan periode adalah untuk memberikan peta kondisi jaringan yang lebih akurat yang akan dialami perangkat dari waktu ke waktu. Meningkatkan akurasi profil dan membuat sistem lebih mudah beradaptasi dengan kondisi jaringan yang bervariasi dan penggunaan perangkat yang bervariasi. Metrik Tarif (RM) untuk pengambilan ini dihitung sebagai berikut:

$$RM = \frac{n}{t} \qquad (5.1)$$

Dimana n adalah jumlah total byte yang dikirimkan, dan t adalah waktu penangkapan. Komponen kemudian dapat mengambil tangkapan jaringan berkala atas lalu lintas LAN dari gateway, tangkapan baru ini kemudian dijalankan melalui sistem pembuatan profil yang sama dengan tangkapan profil berwaktu, dan metrik laju baru dihitung. Terakhir, perbedaan persentase (Δ) dihitung, dengan membandingkan profil laju penangkapan baru dengan setiap profil waktunya sebagai berikut:

$$\Delta = \frac{CRM}{PRM} \times 100 \qquad (5.2)$$

Delta (Δ) adalah perbedaan persentase antara CRM, metrik tarif terhitung, dan PRM, metrik tarif profil. Misalkan nilai delta melewati nilai ambang batas yang dapat dikonfigurasi per implementasi bergantung pada volatilitas jaringan. Dalam hal ini, aktivitas jaringan perangkat ditandai sebagai di luar profil, dan pemindaian ulang jaringan dimulai untuk memindai ulang kemungkinan permukaan serangan yang dieksploitasi secara aktif pada jaringan. Proses ini cepat namun minimal dalam hal dampak jaringan dan tidak akan menurunkan kinerja jaringan, bahkan pada jaringan kecil, karena skala pemindaian akan bertambah atau berkurang intensitasnya secara otomatis tergantung pada waktu pemindaian dan throughput. Selain itu, ambang batas ini dapat dinaikkan atau diturunkan tergantung pada apakah pemindaian terlalu sering; ambang batas dapat ditingkatkan pada jaringan beban variabel yang dinamis, misalnya. Tangkapan lalu lintas, disimpan dalam format PCAP yang digunakan komponen pembuatan profil jaringan untuk menghitung dan membuat profil setiap perangkat, kemudian dapat ditransfer ke komponen pembelajaran mesin untuk memeriksa pola lalu lintas yang dapat mengindikasikan lalu lintas berbahaya, termasuk serangan aktif atau eksploitasi yang sedang berlangsung. . Profil ini kemudian dapat digunakan untuk menginformasikan tindakan mitigasi di seluruh jaringan yang terkena dampak.

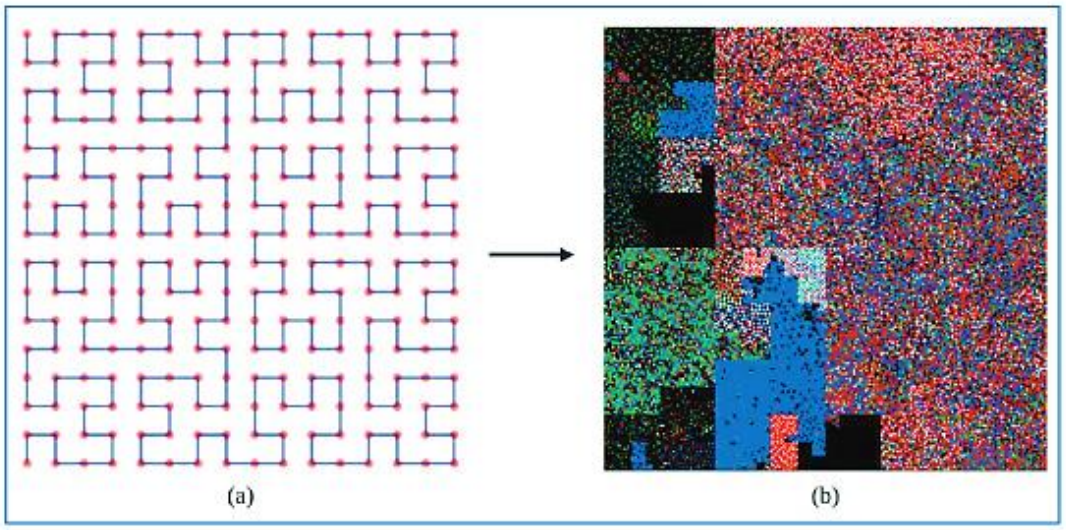
Metode Deteksi Intrusi

Proyek Siber-Trust mengusulkan solusi deteksi intrusi cerdas hibrid untuk deteksi ancaman siber berbahaya yang tepat dan efektif di tingkat host dan jaringan. Solusi yang diusulkan menggabungkan pembelajaran mendalam dan teknik visualisasi gambar untuk mendeteksi serangan siber yang canggih dan baru dirilis di jaringan IoT dengan cepat. Pembelajaran mendalam adalah teknik pembelajaran canggih yang semakin dominan di berbagai bidang, termasuk deteksi intrusi. Beberapa peneliti telah menyarankan penerapan visualisasi gambar pada sistem deteksi intrusi.

Dalam konteks ini, laboratorium Intel dan tim intelijen ancaman Microsoft berkolaborasi dalam proyek penelitian terkait yang disebut STAMINA (Static Malware-as-Image Network Analysis), yang mengubah file input biner menjadi gambar skala abu-abu sehingga algoritma pembelajaran mendalam dapat memprosesnya. dan mengklasifikasikannya. Pendekatan utama proyek penelitian ini adalah mengubah konten file biner masukan menjadi aliran piksel sederhana dan mengubahnya menjadi gambar 2D yang bervariasi tergantung pada aspek seperti ukuran file. Kemudian, pengklasifikasi jaringan saraf

terlatih digunakan untuk menganalisis dan mengklasifikasikan gambar keluaran sebagai gambar sah atau malware. Algoritme pembelajaran dilatih berdasarkan sejumlah besar data dunia nyata (2,2 juta hash file PE) yang dikumpulkan Microsoft dari instalasi Windows Defenders. STAMINA telah terbukti efektif, dengan akurasi lebih dari 99,00% dalam mengklasifikasikan malware dan tingkat positif palsu sedikit di bawah 2,6%. Namun, hal itu ada batasnya. Misalnya, ia bekerja dengan baik dengan file kecil, namun kesulitan dengan file yang lebih besar.

Dalam proyek Siber-Trust, kami telah mengusulkan solusi deteksi intrusi inovatif yang mengubah lalu lintas jaringan menjadi gambar RGB menggunakan alat representasi visual Binvis1. Kemudian, gambar yang dihasilkan dianalisis dan diklasifikasikan menggunakan algoritma pembelajaran yang berbeda, termasuk Residual Neural Network (ResNet50), Self-Organizing Inkremental Neural Networks (SOINN) dan MobileNet. Pendekatan kami diumumkan pada tanggal 1 April 2018, yang berarti dua tahun sebelum pengumuman proyek STAMINA.



Gambar 5.1. Pemetaan kurva pengisian ruang Hilbert dan (b) gambar 2D.

Gambar 5.1 menunjukkan gambar yang dihasilkan dari lalu lintas jaringan dengan menggunakan alat visualisasi BinVis. Pertama, gambar keluaran dibuat dengan memberikan warna tertentu pada setiap byte file PCAP dan diubah menjadi gambar 2D dengan menggunakan algoritma clustering Hilbert space-filling curve. Konversi ini dilakukan pada setiap byte bergantung pada referensi karakter ASCII-nya:

- Biru untuk karakter yang dapat dicetak
- Hijau untuk karakter kontrol
- Merah untuk karakter tambahan
- Hitam untuk karakter null, atau 0x00
- Putih untuk spasi yang tidak terputus, atau 0xFF

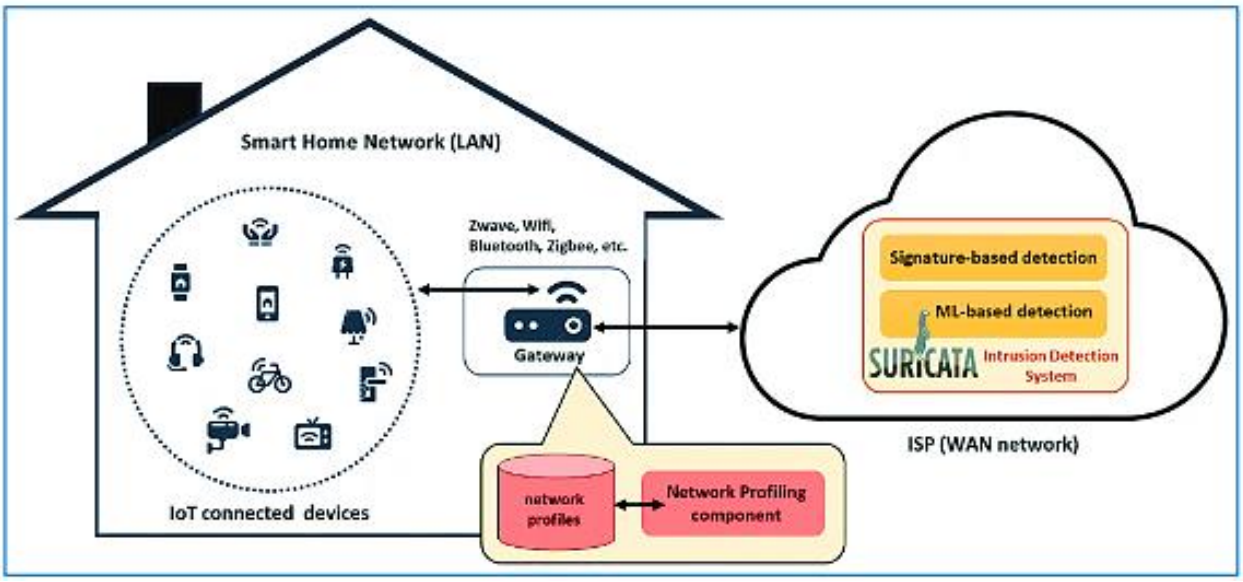
5.3 IMPLEMENTASI DAN PENGUJIAN SISTEM

Pengaturan Tempat Tidur Uji

Di domain rumah pintar, eksperimen dilakukan di testbed Siber-Trust, yang melibatkan sejumlah besar (750) Kantor/Rumah Kecil (SOHO) yang ditiru dan disimulasikan. Setiap SOHO mencakup beberapa perangkat virtual dan VM Ubuntu terpisah yang bertindak sebagai gateway. Seperti yang ditunjukkan pada Gambar 5.1, komponen profil jaringan disebarkan di VM gateway karena komponen tersebut perlu berkomunikasi dengan jaringan rumah pintar (LAN) dan mengumpulkan informasi tentang perangkat yang terhubung. Secara konseptual, komponen ini mungkin berada di gerbang rumah pintar untuk pengumpulan data dan komunikasi atau mengingat persyaratan komputasi tambahan, komponen ini mungkin dipindahkan pada perangkat keras terpisah namun terhubung erat ke gerbang pintar. Lalu lintas jaringan memang dapat dikumpulkan dari antarmuka LAN dan WAN gateway pintar dan selanjutnya diproses untuk penyimpanan menggunakan NetFlow. Infrastruktur jaringan disimpulkan menggunakan kombinasi mekanisme penemuan (khususnya Nmap) dan menanyakan layanan pada gateway pintar (dari penyewaan ARP dan DHCP hingga VLAN dan informasi perutean). Komponen deteksi intrusi yang mencakup modul deteksi pembelajaran mesin diterapkan di VM terpisah lainnya yang menjalankan Debian GNU/Linux 10.2 di tingkat ISP (jaringan WAN). Komponen ini diterapkan dalam VM terpisah karena daya komputasi yang dibutuhkan oleh modul pembelajaran mesin. Untuk perangkat tervirtualisasi, Oss berbeda yang digunakan dalam perangkat IoT digunakan dalam VM atau bentuk dockerized. Konfigurasi jaringan rumah pintar dilakukan melalui gateway VM, yang diberi dua Kartu Antarmuka; dari sini, kami mengontrol penetapan jaringan untuk lalu lintas WAN dan LAN. Kartu antarmuka eth0 direferensikan sebagai NIC1 (172.16.4.1/24) dan memiliki konektivitas Internet (WAN). Sebaliknya, antarmuka kedua eth1 direferensikan sebagai NIC2 (192.168.1.1/26) dan bertindak sebagai IP gateway untuk jaringan terisolasi rumah pintar (LAN).

Uji Kumpulan Data

Untuk menguji pendekatan deteksi yang diusulkan, pertama-tama kami membuat kumpulan data awal untuk melatih modul pembelajaran mesin. Namun, keseluruhan proses pelatihan algoritme pembelajaran mesin dilakukan secara bertahap setiap kali ditemukan lalu lintas berbahaya baru, tanpa mengabaikan informasi yang diidentifikasi pada fase pelatihan sebelumnya. Pembelajaran tambahan ini secara signifikan meningkatkan akurasi deteksi modul pembelajaran mesin. Kumpulan data ini terdiri dari lebih dari 900 gambar lalu lintas berbahaya BinVis yang bersumber dari beberapa repositori analisis lalu lintas malware1. File PCAP berbahaya berisi lalu lintas berbahaya nyata yang dihasilkan oleh Trojan, Botnet, spyware Keylogger, dan Backdoors, dan masih banyak lagi. Sementara file PCAP standar berisi lalu lintas reguler yang diambil dari proyek Siber-Trust yang diuji dari berbagai perangkat bersih di jaringan menggunakan tcpdump. Kumpulan data file PCAP berbahaya dan gambar BinVis terkait tersedia untuk umum di situs web IEEE DataPort2 dengan akses terbuka. Tabel 5.3 menunjukkan persentase sampel lalu lintas berbahaya dalam kumpulan data pelatihan.



Gambar 5.2. Tempat Uji Coba yang Diimplementasikan.

Tabel 5.3. Persentase lalu lintas berbahaya menurut jenis serangan.

				Other		
Malware Type	**Trojan**	**DDoS**	**Botnets**	**Zero-day Exploits**	**Backdoors**	**Others**
Percentage	33%	16%	19%	8%	6%	18%

Tabel 5.4. Metrik yang digunakan dalam pengujian.

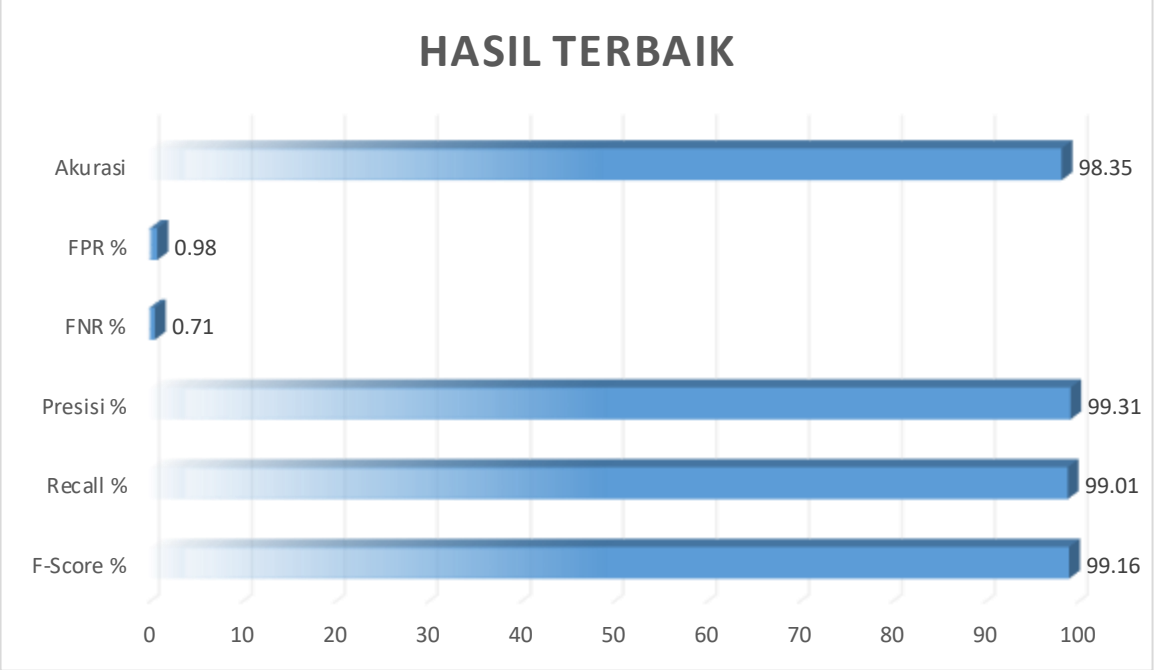
Metrik	**Keterangan**	**DDos**
Akurasi	Mengacu pada jumlah sampel yang diprediksi dengan benar dari semua sampel	$A = \frac{TP + TN}{TP + TN + FP + FN}$
Tingkat Positif Palsu	Mengukur tingkat alarm palsu yang dihasilkan oleh sistem deteksi intrusi	$FPR = \frac{FP}{FP + FN}$
Tingkat Negatif Palsu	Mengukur tingkat serangan yang tidak tertangkap oleh sistem deteksi intrusi	$FNR = \frac{FN}{FP + TP}$
Presisi	Mengukur presentase sampel yang diklasifikasikan positif dan benar-benar positif	$P = \frac{TP}{TP + FP}$
Recall	Penarikan kembali mewakili jumlah sampel normal yang diklasifikasikan dengan benar	$R = \frac{TP}{TP + FN}$
F-Score	F-Score adalah rata-rata tertimbang antara	$F - Score = 2 \times \frac{P \times R}{P + R}$

Kami telah membuat koleksi file PCAP yang disediakan oleh lalu lintas malware nyata di pengujian Siber-Trust untuk kumpulan data pengujian. Lebih tepatnya, file PCAP berbahaya dibuat dari berbagai skenario serangan dunia nyata, termasuk Mirai Botnet, BlackEnergy Botnet, Zeus Botnet, dan skenario serangan ulang, yang terdiri dari beberapa jenis serangan Java-RMI Backdoor, distcc exec backdoor, Web Tomcat Exploit dan serangan Hydra

Bruteforce. File PCAP dihasilkan dengan menjalankan demo langsung dari setiap skenario serangan dan merekam komunikasi jaringan antar perangkat menggunakan tcpdump.

Modul Deteksi Pembelajaran Mesin

Beberapa pengujian dilakukan untuk mengevaluasi keberhasilan solusi deteksi intrusi yang diusulkan dan menentukan keakuratannya. Metrik yang digunakan untuk menyelidiki hasil modul ML adalah Akurasi (A), False Positive Rate atau alarm palsu dan False Negative Rate. Dalam eksperimen ini, lalu lintas berbahaya mewakili kejadian positif sedangkan lalu lintas normal mewakili kejadian negatif. True Positive (TP) adalah jumlah kejadian berbahaya yang telah diklasifikasikan dengan benar. False Positive (FP) adalah jumlah kejadian normal yang salah diklasifikasikan sebagai normal. True Negative (TN) adalah jumlah sampel lalu lintas normal yang telah diklasifikasikan dengan benar. False Negative (FN) adalah jumlah file PCAP normal yang salah diklasifikasikan sebagai kejadian anomali.



Gambar 5.3. Hasil pengujian secara keseluruhan.

Dengan memproses tayangan ulang PCAP ini ke komponen A04, kami dapat menilai metrik ini dengan data yang dapat diukur; hasil pengujian ini menghasilkan statistik keseluruhan sebagai berikut. Gambar5.3 menyajikan hasil pengujian secara keseluruhan, yang mencapai akurasi deteksi keseluruhan sebesar 98,35%, yang merupakan tingkat tinggi dan memenuhi tingkat akurasi yang disyaratkan dalam penggunaan praktis. Dengan menjalankan pengujian beberapa kali dan lebih dari 100 kali dijalankan, hasil akurasi (A) terbaik adalah 98,35%, tingkat positif palsu 0,98%, dan tingkat palsu negatif 0,71%. Hasil presisi (P) juga sangat tinggi, dengan tingkat 99,3%, yang menunjukkan kepercayaan yang kuat secara keseluruhan dalam proses pengenalan pola. Dalam pengujian ini, presisi sangat penting karena mendapatkan False Negatives (FN), ketika lalu lintas malware dianggap normal, memerlukan biaya lebih besar daripada False Positives (FP), ketika lalu lintas normal dianggap

sebagai lalu lintas berbahaya. Persentase recall (R) memperoleh hasil sebesar 99,01%. Nilai F1 (F1) yang dicapai sebesar 99,16%.

Pembuatan profil jaringan

Pendekatan pembuatan profil jaringan yang diusulkan digunakan oleh platform Siber-Trust IoT untuk secara dinamis dan aktif membuat profil dan memantau semua perangkat yang terhubung ke jaringan untuk mendeteksi upaya gangguan perangkat IoT dan transaksi jaringan yang mencurigakan. Selama pengujian yang dilakukan pada solusi yang diusulkan, ambang batas diatur ke 80% dari persentase perbedaan (PD) dalam waktu pengambilan 60 detik yang ditetapkan. Perbedaan yang signifikan dari tingkat transmisi standar dalam setiap penangkapan merupakan dasar yang baik untuk kasus penggunaan kami. Namun, penting untuk dicatat bahwa pengguna akhir dapat mengkonfigurasi ambang batas ini agar sesuai dengan kasus penggunaan jaringan mereka jika throughput aktivitas jaringan mereka jauh lebih fluktuatif atau stabil dibandingkan jaringan SOHO, kami menguji konfigurasi tersebut. Seperti yang ditunjukkan pada Tabel 5.5, selama pengujian yang dilakukan, sampel berbahaya yang terdeteksi di luar profil untuk perangkat yang terkena dampak diidentifikasi dengan benar, sehingga menghasilkan tingkat keberhasilan deteksi 100% untuk serangan yang diuji. Selanjutnya, dengan menjalankan pengujian beberapa kali untuk lalu lintas jaringan berbahaya dan jinak, hasil akurasi (A) terbaik adalah 100% dan tingkat positif palsu sebesar 8,3%.

Tabel 5.5. Hasil untuk setiap jenis serangan.

Type Malware	Diluar profile	Deteksi Profil	Δ %
Eksploitasi zero-day	Ya	D	28.37 %
Serangan DDoS dengan Mirai Botnet	Ya	H, D, W	98.53 %
Serangan DDoS dengan Black Energy	Ya	H, D, W	128.42 %
java_rmi	Ya	D, W	96.88 %
distcc_exec_backdoor	Ya	D, W	98,64 %
Unreallred	Ya	D, W	97.69 %
Tomcat	Ya	W	395.52 %
ruby_drb_code_exec	Ya	D, W	682.16 %
hydra_ftp	Ya	D, W	95.15 %
hydra_ssh	Ya	D, W	99.14 %
Smtp	Ya	D, W	93.50 %
netbios_ssn	Ya	D, W	307.39 %
Zeus Malware	Ya	W	96.70 %

5.4 KESIMPULAN

Dalam bab ini, kami telah memperkenalkan pendekatan Siber-Trust untuk mendeteksi serangan tingkat jaringan di lingkungan IoT. Pendekatan ini menggabungkan profil jaringan, visualisasi biner, dan teknik pembelajaran mesin untuk mendeteksi vektor ancaman tingkat lanjut dan baru di jaringan IoT. Pengujian solusi yang diusulkan dilakukan di testbed Siber-Trust, yang terdiri dari banyak jaringan rumah pintar yang disimulasikan dan ditiru. Untuk pelatihan dan pengujian solusi yang diusulkan, kami telah membuat kumpulan data baru yang mencakup banyak gambar 2D yang sesuai dengan lalu lintas jaringan berbahaya dan reguler

yang dikumpulkan dari berbagai sumber. Sebagai perbandingan, sampel berbahaya yang digunakan dalam tahap pengujian dibuat di pengujian Siber-Trust dari skenario serangan nyata yang mencakup berbagai serangan kritis, termasuk serangan DDoS berdasarkan Botnet, serangan Zero-day, Malware, eksploitasi. dan pintu belakang. Kumpulan data tersebut sekarang tersedia untuk umum dan dapat diakses oleh para peneliti di bidang ini, terutama karena kurangnya data yang difitnah untuk menguji algoritme pembelajaran mesin.

Hasil pengujian secara keseluruhan cukup baik, terutama jika mempertimbangkan hasil komponen pembelajaran mesin, yang mencatat akurasi sebesar 98,35% dalam 100 pengujian dengan hanya FPR 0,98% dan peringkat presisi 99,31%. Hasil ini diperoleh dari pengujian terhadap eksploitasi perangkat dari kerentanan umum yang tidak diketahui dan diketahui serta botnet berdampak tinggi yang telah mengalami infeksi ekstensif di dunia nyata; ini menunjukkan kemanjuran solusi yang tinggi. Namun, keakuratan solusi yang diusulkan secara keseluruhan masih dapat ditingkatkan nilainya dengan pelatihan lebih lanjut. Perlu dicatat bahwa ketika menjelaskan pekerjaan di masa depan, pengujian dapat dilakukan untuk menilai apakah model ini dapat meningkatkan akurasinya dengan bentuk pelatihan dan teknik visualisasi biner yang lebih luas atau alternatif. Pembuatan profil jaringan telah mencapai hasil yang baik, di mana serangan diidentifikasi sebagai di luar profil untuk perangkat yang terkena dampak berdasarkan ambang batas yang telah ditentukan selama pengujian. Hasil yang diperoleh untuk komponen ini dapat ditingkatkan secara signifikan selama tahap pengujian berikutnya dengan menjalankan lebih banyak sampel dalam jangka waktu yang lama.

BAB 6
MEMANFAATKAN DETEKSI INTRUSI TERHADAP ANCAMAN SIBER

Keamanan IoT kini telah muncul sebagai salah satu isu terpenting dalam keamanan jaringan. Teknik keamanan konvensional, seperti firewall dan sistem deteksi intrusi berbasis tanda tangan, telah terbukti tidak efektif dalam melindungi jaringan IoT dari serangan dan malware yang semakin canggih. Karena kendala ini, para peneliti terpaksa membangun solusi deteksi intrusi baru dengan memanfaatkan berbagai teknologi seperti IoT Honeypots dan Machine Learning (ML). Bab ini menjelaskan cara memanfaatkan deteksi intruksi terhadap ancaman siber serta pendekatan baru untuk mendeteksi lalu lintas jaringan berbahaya yang menggunakan honeypot dan pembelajaran mesin. Sistem honeypot IoT digunakan untuk mengumpulkan intelijen tentang serangan yang menargetkan perangkat IoT. Data yang dikumpulkan digunakan untuk memahami senjata penyerang, strategi dan teknik baru yang digunakan. Ini juga digunakan untuk melatih model pembelajaran mesin yang digunakan pada IDS secara terus menerus untuk meningkatkan akurasi pendeteksiannya. Metode ini paling berhasil melawan serangan yang tidak diketahui dan serangan zero-day pada komputer IoT.

6.1 PENDAHULUAN

Perangkat IoT sepertinya ada dimana-mana saat ini, dan semakin banyak digunakan di sektor infrastruktur penting seperti layanan kesehatan, keamanan, energi, dan layanan darurat. Semua perangkat ini menambahkan titik masuk baru ke jaringan, meningkatkan risiko keamanan. Satu perangkat yang disusupi dan terhubung ke jaringan dapat menimbulkan potensi ancaman terhadap jaringan dan berfungsi sebagai titik masuk untuk berbagai upaya peretasan. Berdasarkan lingkungan ancaman terkini, teknik penjahat siber telah mencapai titik di mana mereka sangat sulit untuk diidentifikasi dan diremediasi. Menurut laporan terbaru dari Universitas Maryland, mereka kini berhasil menembus perangkat IoT setiap 39 detik. Lebih jauh lagi, insiden keamanan menegaskan bahwa masalah keamanan yang lebih besar adalah kelemahan keamanan perangkat ini dapat dengan mudah dieksploitasi oleh peretas yang membentuk botnet besar (yaitu tentara zombi) dan dengan demikian meluncurkan serangan DDoS yang signifikan. Menurut laporan terbaru A10 Networks, hampir 6 juta serangan DDoS terjadi pada kuartal keempat tahun 2019. Studi ini menegaskan bahwa Mirai tetap menjadi malware pilihan botnet, dan WD-Discovery telah melampaui SNMP (Simple Network Management Protocol) dan SSDP (Simple Service Delivery Protocol) sebagai sumber DDoS terpopuler ketiga. Meskipun ada upaya besar (dan anggaran) yang dilakukan oleh organisasi dan komunitas keamanan untuk melindungi perangkat yang terhubung, penyerang terus merancang strategi baru untuk mengaburkan operasi mereka dan menghindari deteksi oleh mekanisme pertahanan siber. Sistem Deteksi Intrusi (IDS) berbasis tanda tangan saat ini khususnya tidak efektif dalam mendeteksi malware yang tidak dikenal dan dikaburkan yang tidak memiliki tanda tangan. Selain itu, tanda tangan malware harus diperbarui secara berkala, yang memerlukan sumber daya yang signifikan dan

keterlibatan/keahlian manusia untuk membuat tanda tangan ini. Oleh karena itu, teknologi deteksi intrusi yang inovatif menjadi penting untuk melindungi diri dari ancaman-ancaman ini sebelum menimbulkan bahaya yang serius.

Dalam artikel ini, kami mengusulkan solusi deteksi intrusi hibrid yang dapat meningkatkan sistem IDS yang saat ini digunakan untuk melindungi jaringan IoT dari penyusup, ancaman yang tidak jelas, dan ancaman zero-day menggunakan pembelajaran mesin dan teknologi honeypot yang sudah mapan. Kerangka kerja honeypot sengaja menarik peretas dan menggunakan upaya intrusi mereka untuk mempelajari lebih lanjut tentang aktor jahat dan cara mereka beroperasi. Selain itu, data mentah yang dihasilkan oleh sistem honeypot digunakan untuk pelatihan model pembelajaran mesin yang efektif dan dinamis, sehingga meningkatkan akurasi pendeteksiannya. Model pembelajaran mesin yang memenuhi syarat digunakan untuk mengidentifikasi kemungkinan ancaman keamanan siber yang tidak diketahui secara otomatis. Sisa bab ini disusun sebagai berikut: bagian pertama memberikan konteks tentang honeypots dan survei pekerjaan sebelumnya yang dilakukan di bidang ini menggunakan teknik pembelajaran mesin dan perangkat lunak honeypots. Subbab 6.3 kemudian menawarkan penjelasan tentang sistem deteksi intrusi yang diusulkan. Hal ini juga membahas strategi dan algoritma yang paling sesuai untuk keberhasilan implementasi sistem yang diusulkan. Terakhir, segmen terakhir mengakhiri bab ini dan membahas pekerjaan di masa depan.

6.2 LATAR BELAKANG DAN PEKERJAAN TERKAIT

Intrusion Detection System (IDS) adalah mekanisme keamanan yang digunakan untuk melindungi host dan jaringan dari potensi ancaman yang biasanya melewati perangkat firewall biasa. IDS secara tradisional diklasifikasikan menjadi dua jenis: sistem deteksi intrusi berbasis host (HIDS) dan sistem deteksi intrusi berbasis jaringan (NIDS). HIDS biasanya digunakan untuk memantau dan menganalisis aktivitas internal pada mesin tertentu serta paket jaringan pada antarmuka jaringannya. Di sisi lain, NIDS digunakan untuk terus-menerus melacak lalu lintas jaringan, mencari masukan yang berpotensi berbahaya dan tidak sah yang dapat membahayakan keamanan jaringan dan melakukan tindakan pencegahan otomatis untuk menguranginya dengan mengirimkan peringatan ke administrator jaringan. NIDS dapat diimplementasikan dengan dua cara: berbasis tanda tangan dan berbasis anomali. Sebagian besar sistem pertahanan keamanan telah menggunakan metode klasifikasi berbasis tanda tangan sejak awal deteksi ancaman. Bentuk NIDS ini melacak lalu lintas jaringan dan membandingkannya dengan database tanda tangan atau atribut ancaman yang diketahui, di mana pola yang menentukan karakteristik unik setiap ancaman dihasilkan, sehingga malware tertentu dapat dideteksi di masa depan. Teknik deteksi berbasis tanda tangan biasanya sangat berhasil dalam mendeteksi malware yang dikenal, namun sebagian besar tidak efektif dalam mendeteksi malware baru dan tidak dikenal yang tidak memiliki tanda tangan. Karena pembatasan ini, penyerang modern sering memutasi kreasi mereka untuk mempertahankan fungsi jahat dengan memodifikasi tanda tangan file, seperti malware polimorfik, yang dapat membuat varian baru setiap kali dijalankan, sehingga menghasilkan tanda tangan baru.

Karena kelemahan teknik deteksi berbasis tanda tangan, para peneliti kini berkonsentrasi pada pendekatan deteksi berbasis anomali. Teknik ini mengklasifikasikan lalu lintas jaringan berdasarkan tren yang dihasilkan dengan melacak karakteristik operasi tipikal dari waktu ke waktu. Lalu lintas jaringan sebenarnya kemudian dibandingkan dengan profil yang telah ditentukan, dan setiap penyimpangan besar dari pola tersebut diklasifikasikan sebagai berbahaya. Sistem ini sangat efektif untuk mendeteksi ancaman yang tidak diketahui dan dikaburkan. Dengan munculnya bentuk-bentuk baru ancaman IoT secara rutin, banyak metode dan teknik untuk deteksi berbasis anomali telah diusulkan dalam literatur. Banyak dari pendekatan ini telah meneliti pembelajaran mesin (ML), dengan fokus pada algoritma pembelajaran mendalam (DL), yang memberikan paradigma kuat untuk secara otomatis menentukan fitur yang diperlukan untuk deteksi lalu lintas berbahaya. Penelitian yang lebih baru mengamati penggunaan honeypot untuk meningkatkan NIDS. Strategi Honeypot bertujuan untuk mengubah strategi pertahanan terhadap serangan dengan memungkinkan organisasi mengambil inisiatif. Bagian berikut mencakup lebih banyak informasi tentang pekerjaan sebelumnya dalam klasifikasi lalu lintas jaringan berbahaya menggunakan metodologi pembelajaran mesin, serta sejarah honeypots dan survei pekerjaan terkait honeypot.

Penggunaan pembelajaran mesin untuk mempertahankan diri dari intrusi dalam jaringan IoT baru-baru ini mendapatkan banyak perhatian di dunia akademis. Biasanya, teknik ini memeriksa informasi lalu lintas jaringan yang dapat digunakan untuk mengekstrak fitur yang dapat digunakan untuk memisahkan lalu lintas berbahaya dari lalu lintas yang sah. Fitur-fitur tersebut kemudian digunakan untuk melatih pengklasifikasi untuk mendeteksi kemungkinan serangan, dengan setiap contoh data diberi label sebagai standar atau anomali. Hasil output biasanya disajikan dalam format biner, dengan dua kemungkinan nilai: lalu lintas alami atau malware. Di bidang ini, algoritma pembelajaran yang diawasi seperti pengklasifikasi tetangga terdekat, mesin vektor pendukung, dan skema berbasis aturan seperti pohon keputusan dan hutan acak telah menunjukkan hasil yang menjanjikan. Dalam , sebuah survei mengusulkan klasifikasi sistem deteksi intrusi berbasis pembelajaran dan membahas kinerja berbagai algoritma pembelajaran yang diawasi dan tidak diawasi yang digunakan dalam bidang ini dalam hal akurasi dan tingkat alarm palsu. Menurut laporan tersebut, tantangan paling signifikan terhadap pembelajaran yang diawasi adalah kurangnya kumpulan data yang dapat diakses dengan data berlabel. Menurut sebuah penelitian yang diterbitkan dalam, teknologi deteksi intrusi saat ini untuk jaringan IoT masih perlu ditingkatkan dalam hal skalabilitas, akurasi deteksi, tingkat positif sebenarnya, dan konsumsi energi.

Sejalan dengan itu, penulis mengeksplorasi kemanjuran berbagai teknik pembelajaran mesin dalam melindungi perangkat IoT dari serangan DoS. Tujuan dari penelitian ini adalah untuk mengusulkan metode yang efektif untuk mengembangkan IDS untuk aplikasi IoT menggunakan pembelajaran ansambel. Hutan Acak (RF), AdaBoost (AB), Peningkatan Gradien Ekstrim (XGB), Mesin Peningkatan Gradien (GBM), dan Pohon Acak Ekstrim adalah pengklasifikasi yang dievaluasi (ETC). Dalam karya yang lebih baru, penulis telah menguji lima algoritma pembelajaran yang diawasi untuk membedakan paket IoT normal dari paket serangan DoS. Pengklasifikasi pengujiannya adalah algoritma K-nearest neighbour “KDTree”

(KN), Support vector machine with linear kernel (LSVM), Decision tree menggunakan Gini impurity score (DT), Random Forest menggunakan Gini impurity score (RF) dan Neural Network (NN) dengan 4 lapis. Tingkat akurasi pengklasifikasi berkisar antara 91% hingga 99%.

Pembelajaran mendalam juga mendapat banyak perhatian dalam beberapa tahun terakhir. Karena kemampuannya untuk secara otomatis mengekstrak fitur-fitur canggih dari data yang tidak berlabel, algoritme ini dianggap penting untuk deteksi intrusi di jaringan IoT. Penulis membandingkan pendekatan pembelajaran mendalam dengan teknik NIDS konvensional tertentu. Para penulis menemukan bahwa pendekatan berbasis pembelajaran mendalam mengungguli teknik deteksi intrusi konvolusional dalam hal akurasi deteksi di berbagai ukuran sampel dan jenis anomali lalu lintas. Dan telah menggunakan Recurrent Neural Network (RNN) dan variannya untuk deteksi intrusi jaringan dalam pengertian yang sama. Convolutional Neural Network (CNN), yang telah mencapai kesuksesan besar dalam klasifikasi gambar dan pengenalan pola, juga telah digunakan di banyak sistem deteksi intrusi (IDS) dengan menganalisis gambar yang dihasilkan oleh karakteristik lalu lintas jaringan. Output dari solusi deteksi intrusi berbasis CNN dievaluasi pada menggunakan dataset sintetis KDDCup 99 dan NSL-KDD. Auto-encoder dan Variational Auto-encoder adalah dua teknik pembelajaran mendalam umum lainnya yang saat ini digunakan dalam penelitian. Banyak penelitian terbaru telah melihat kekokohan strategi ini dalam deteksi intrusi. Dalam hal akurasi deteksi, penulis melaporkan bahwa IDS berbasis autoencoder yang diusulkan mengungguli IDS berdasarkan Prinsip Analisis Komponen (PCA) lebih dari 15%. Hasilnya, beberapa pendekatan terbaru telah menyelidiki kemanjuran penggunaan teknik pembelajaran mendalam untuk deteksi intrusi. Meskipun ada kemajuan dalam bidang ini, topik penggunaan pembelajaran mendalam untuk deteksi intrusi masih kurang dimanfaatkan.

Teknologi Honeypot bertujuan untuk mengkompensasi kelemahan dalam sistem deteksi intrusi dengan mengumpulkan informasi tentang ancaman saat ini pada jaringan dan mendeteksi munculnya ancaman baru. Honeypot adalah perangkat siber yang meniru target tertentu (misalnya layanan, database, atau sistem operasi) untuk menarik serangan siber dan menggunakan upaya intrusinya untuk mengumpulkan informasi tentang penyusup dan cara kerjanya. Kecerdasan yang diperoleh dari honeypot akan sangat membantu peningkatan keamanan sistem produksi di dunia nyata. Honeypots secara historis dinilai berdasarkan tingkat kontaknya, yang menunjukkan seberapa banyak aktivitas yang mungkin dilakukan penyerang terhadapnya. Ada dua jenis honeypot dalam konteks ini: honeypot dengan interaksi rendah dan honeypot dengan interaksi tinggi. Honeypot dengan tingkat interaksi yang tinggi memungkinkan penyerang untuk berkompromi dan mendapatkan akses ke layanan atau program yang sebenarnya rentan. Karena mereka tidak meniru layanan apa pun, Honeypot Interaksi Tinggi membantu mendeteksi kerentanan yang tidak diketahui dan mengumpulkan informasi terperinci mengenai prosedur penyerang. Namun, mereka lebih rentan terhadap infeksi, dan sebagai hasilnya, penyerang akan mendapatkan kendali penuh atas mereka untuk berkompromi dan menargetkan sistem produksi aktual lainnya di jaringan. Selain itu, teknologi ini rumit dan mahal untuk diterapkan dan dipertahankan. IoTPOT adalah salah satu honeypot interaksi tinggi pertama yang diterapkan di bidang IoT untuk meniru modul IoT. SIPHON juga merupakan jaringan honeypot dengan interaksi tinggi dan terukur

untuk aplikasi Internet of Things. Honware adalah contoh lain dari honeypot interaksi tinggi yang baru dibuat yang mampu mensimulasikan berbagai produk IoT.

Honeypots Interaksi Rendah, di sisi lain, beroperasi sebagai emulator layanan dan sistem operasi, sehingga penyerang hanya dapat melakukan interaksi minimal. Sebagai konsekuensinya, Honeypot ini tidak rentan dan tidak dapat dirusak oleh eksploitasi; namun, penyerang dapat dengan mudah mendeteksinya dengan menjalankan perintah yang tidak didukung emulator. Alat umum honeyd, yang menyediakan metode sederhana untuk mensimulasikan layanan berbeda yang disediakan oleh beberapa mesin pada satu komputer, adalah contoh honeypot dengan interaksi rendah. Sistem honeypot dengan interaksi rendah telah digunakan di bidang IoT untuk menangkap perilaku IoT yang berbahaya. Honeypot dengan interaksi rendah seperti Nepentes dan Dionaea juga digunakan untuk pengumpulan data skala besar tentang malware yang mereplikasi dirinya sendiri di alam liar. Untuk mensimulasikan perilaku komputer IoT, Dionaea honeypot menggunakan protokol MQTT. Pengembang menggunakan honeypot interaksi rendah untuk mengidentifikasi dan memperbaiki kerentanan pada perangkat IoT. Honeypot dirancang secara otomatis memanfaatkan teknologi pembelajaran mesin untuk mempelajari karakteristik perilaku berbagai jenis perangkat IoT.

MIHs (Medium Interaction Honeypots) adalah campuran honeypots interaksi rendah dan tinggi. Para peneliti mengenali sistem honeypot jenis ini menawarkan solusi honeypot lengkap untuk pemantauan dan deteksi intrusi. Beberapa model honeypot MIH IoT telah diusulkan dalam literatur. Misalnya, penulis mengusulkan arsitektur honeypot hybrid berdasarkan honeypot interaksi rendah (honeyds) yang berfungsi sebagai emulator layanan dan sistem operasi. Lalu lintas berbahaya yang dipandu ke honeyds kemudian dengan mulus dialihkan ke honeypot dengan interaksi tinggi, tempat penyerang dapat berkomunikasi dengan layanan nyata. Dalam makalah berikutnya penulis mendefinisikan arsitektur honeypot IoT hibrid dengan pembelajaran mesin untuk memerangi serangan DDoS zero-day. Sejalan dengan itu, penulis mengembangkan honeynet hybrid baru yang saling terhubung dan kolaboratif untuk jaringan IoT. Penulis mendefinisikan jaringan honeynet berbasis IoT yang mencakup perangkat IoT virtual dan fisik. Untuk analisis lalu lintas, sistem honeypot yang diusulkan menggunakan algoritma pembelajaran mesin yang diawasi. Contoh honeypot IoT yang baru terbentuk ditunjukkan pada Tabel 6.1.

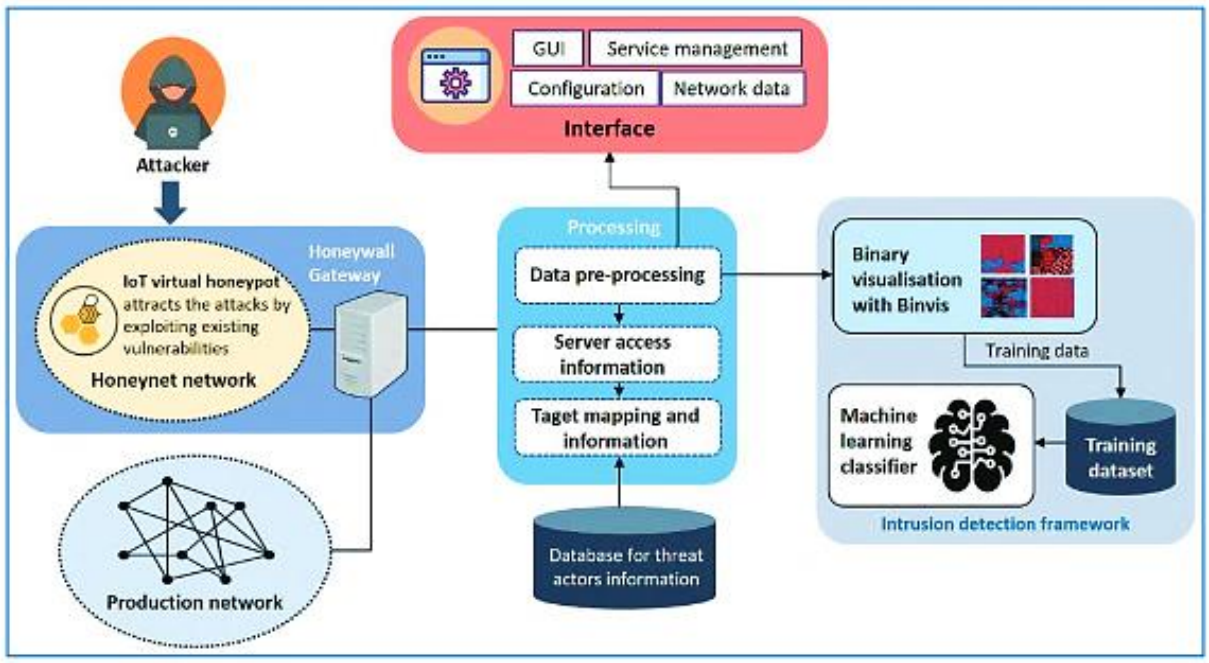
Tabel 6.1. Contoh honeypot IoT yang baru dikembangkan.

– Dionaea: menggunakan protokol MQTT untuk mensimulasikan perilaku IoT.
– U-POT: untuk perangkat yang menggunakan protokol Universal Plug and Play (UPnP).
– ZigBee Honeypot: menyimulasikan gateway ZigBee .
– SIPHON: platform honeypot interaksi tinggi untuk perangkat IoT, dengan 80 perangkat interaktif tinggi.
– Honware: kerangka honeypot interaksi tinggi yang dapat meniru perangkat IoT yang berbeda.
– Thingpot: Mengemulasi protokol komunikasi IoT yang berbeda.
– HIoTPOT: Mengemulasi layanan Telnet dari berbagai perangkat IoT.

– Multiport Honeypots: honeypot IoT interaksi menengah-tinggi yang dapat mensimulasikan layanan UPnP dan port layanan SOAP.

6.3 KERANGKA DETEKSI INTRUSI

Kami terutama tertarik untuk mendeteksi dan memitigasi malware tak dikenal yang bertanggung jawab atas serangan Zero-Day dalam sistem deteksi yang diusulkan ini. Kata "zero-day eksploitasi" mengacu pada kode berbahaya yang ditulis oleh pelaku jahat untuk mengeksploitasi "kerentanan zero-day." Bentuk malware ini bisa luput dari perhatian selama beberapa tahun dan sangat berbahaya karena hanya pelakunya yang mengetahui sifatnya, sehingga tidak ada perbaikan keamanan yang tersedia untuk mengatasi kerentanan ini dan memblokir eksploitasi zero-day berikutnya. Kami mengusulkan pendekatan deteksi dan mitigasi baru berdasarkan honeypot dan pembelajaran mesin untuk mengatasi masalah ini. Kerangka kerja honeypot dirancang untuk menarik peretas untuk melacak, menangkis, dan menganalisis upaya peretasan untuk mendapatkan akses tidak sah ke perangkat IoT. Sebagai perbandingan, sistem deteksi berbasis Machine Learning (ML) yang merupakan aplikasi pembelajaran mesin bersama dengan teknik visualisasi biner digunakan untuk mengidentifikasi kemungkinan ancaman keamanan siber yang tidak diketahui.



Gambar 6.1. Alur proses untuk solusi yang diusulkan dengan pembelajaran mesin honeypot dan kerangka deteksi berbasis.

Seluruh mekanisme sistem yang diusulkan digambarkan pada Gambar6.1. Seperti yang ditunjukkan pada Gambar 6.1, Honeywall dibangun dalam sistem honeypot untuk mengisolasi jaringan honeynet dari infrastruktur produksi organisasi. Honeywall juga digunakan sebagai titik masuk utama ke jaringan honeynet, memberikan kendali penuh atas semua lalu lintas masuk dan keluar ke dan dari jaringan. Setiap tindakan yang dilakukan dengan sistem honeynet dianggap berbahaya dan diarahkan ke modul pra-pemrosesan untuk pemeriksaan

lebih lanjut. Data ini juga dikonversi ke format yang sesuai (gambar 2D) sehingga dapat digunakan untuk terus melatih model pembelajaran mesin dan meningkatkan akurasi pendeteksiannya. Pra-pemrosesan data juga memerlukan analisis data yang dikumpulkan untuk lebih memahami alat, strategi, teknik, dan motif penyerang. Hal ini dapat dicapai dengan memasukkan sumber daya dan kerangka kerja ke dalam honeypots untuk mencatat semua aktivitas sistem.

Total data yang dikumpulkan dari pemeriksaan mendalam pada jaringan dan interaksi tingkat sistem dengan perangkat honeynet dimasukkan ke dalam basis data pelaku ancaman pusat, ini termasuk informasi tingkat rendah yang diperlukan untuk menghasilkan gambar 2D yang disebutkan di atas dari pemeriksaan paket mendalam pada lalu lintas jaringan yang ditangkap. yang kemudian digunakan dalam pelatihan sistem NIDS melalui modul berbasis ML. Ini menggunakan gambar-gambar ini sebagai dasar metode yang diusulkan. Dan memberikan ringkasan resmi dari interaksi yang telah terjadi, interaksi ini ditugaskan ke database bersama dengan informasi yang dapat diidentifikasi seperti alamat IP asal, stempel waktu, dan informasi layanan terkait untuk layanan jaringan yang ditargetkan.

Sistem Honeypot

Dalam solusi yang diusulkan, sistem honeypot terutama digunakan untuk mengumpulkan informasi intelijen tentang upaya serangan pada perangkat IoT. Ini melibatkan dua komponen utama: honeynet dan Honeywall. Jaringan honeynet digunakan untuk menarik penyerang karena sengaja mengeksploitasi kerentanan yang ada di perangkat IoT, di mana semua interaksi dengan jaringan ini dianggap berbahaya. Pengumpulan data dilakukan di gateway Honeywall, yang merupakan titik masuk utama ke jaringan honeynet. Setelah data diambil, data tersebut dikirim dengan aman ke sistem prapemrosesan untuk analisis lebih lanjut dan untuk melatih model klasifikasi.

Jaringan honeynet terdiri dari berbagai perangkat IoT yang menangkap berbagai perilaku berbahaya. Namun, membangun jaringan madu perangkat IoT merupakan tantangan jika menggunakan metode tradisional karena karakteristik khusus dari IoT. Oleh karena itu, banyak peneliti telah mencoba merancang honeypot baru untuk perangkat IoT. Seperti disebutkan sebelumnya, Tabel 6.1 memberikan beberapa contoh honeypot IoT yang baru-baru ini dikembangkan.

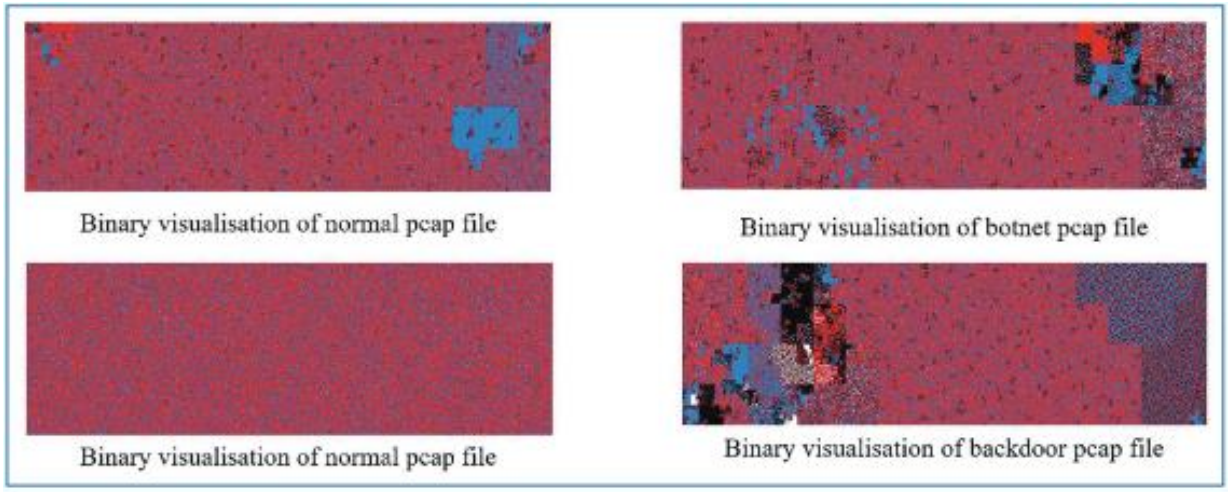
Namun, penerapan sistem honeynet berbasis IoT yang paling tepat harus mensimulasikan seluruh platform IoT beserta semua protokol yang didukung dalam komunikasi IoT. Misalnya, Thingpot adalah honeypot virtual IoT yang mampu menangkap berbagai botnet berbasis IoT dengan meniru protokol komunikasi IoT yang berbeda serta seluruh perilaku platform IoT. Selain itu, honeypot IoT harus mampu menyediakan interaksi tingkat tinggi untuk memotivasi penyerang melakukan aktivitas jahatnya dan oleh karena itu, melacak lanskap ancaman yang dinamis.

Kerangka Deteksi Pembelajaran Mesin

Kerangka kerja deteksi berbasis pembelajaran mesin merupakan komponen penting dalam solusi yang diusulkan. Seperti yang ditunjukkan pada Gambar 6.1, kerangka kerja ini terdiri dari dua langkah utama, pertama memperoleh representasi visual yang sesuai dari lalu lintas jaringan yang dikumpulkan, dan kedua, memproses representasi visual ini dengan

model pembelajaran mesin yang terlatih. Ide utama dari kerangka ini didasarkan pada pendekatan Malware-Squid yang diusulkan dalam, yang mewakili layanan pertahanan siber dalam proyek Siber-Trust . Dalam pendekatan ini, kami menggunakan kurva pengisian ruang Hilbert sebagai algoritma pengelompokan utamanya, hal ini dicapai dengan menetapkan warna tertentu pada setiap byte saat diubah menjadi gambar 2D. Algoritma pengelompokan ini mengungguli kurva lainnya dalam menjaga lokalitas antar objek dalam ruang multidimensi, yang membantu menciptakan gambar RGB yang jauh lebih sesuai untuk proses klasifikasi. Konversi dilakukan pada setiap byte tergantung pada referensi karakter ASCII-nya sebagai berikut:

- Biru untuk karakter yang dapat dicetak
- Hijau untuk karakter kontrol
- Merah untuk karakter tambahan
- Hitam untuk karakter null, atau 0x00
- Putih untuk spasi yang tidak terputus, atau 0xFF



Gambar 6.2. Gambar Binvis dari lalu lintas jaringan normal dan malware dibuat dengan kurva pengisian ruang Hilbert.

Array byte yang dihasilkan ini kemudian diproses menggunakan algoritme Hilbert, mengubahnya menjadi gambar yang mempertahankan lokalitas optimal untuk pengenalan pola, sehingga memungkinkannya diproses oleh model klasifikasi gambar pembelajaran mesin. Ukuran gambar RGB keluaran adalah 784 (1024*256) byte. Gambar 6.2 menunjukkan gambar Bin-Vis untuk lalu lintas jaringan normal dan malware, yang dibuat menggunakan kurva pengisian ruang Hilbert.

Ada sejumlah algoritma pembelajaran yang tersedia untuk melakukan klasifikasi lalu lintas jaringan berdasarkan gambar 2D yang dihasilkan. Namun, dalam penelitian ini, kami tertarik pada algoritma pembelajaran tanpa pengawasan yang dapat secara akurat mengklasifikasikan lalu lintas jaringan sebagai “normal” atau “berbahaya” dengan tingkat alarm palsu yang wajar. Dalam konteks ini, berbagai pengklasifikasi tanpa pengawasan seperti Autoencoders, Self-Organizing Inkremental Neural Network, Residual Neural Network (ResNet) dan MobileNet telah terbukti efektif dalam mendeteksi lalu lintas jaringan yang tidak

normal. dengan nilai akurasi keseluruhan yang memenuhi nilai yang disyaratkan dalam penggunaan praktis (dari 94% menjadi 96%).

6.4 KESIMPULAN

Dalam bab ini, kami memperkenalkan pendekatan baru untuk deteksi intrusi jaringan berdasarkan pembelajaran mesin dan teknologi honeypot. Untuk implementasi kerangka deteksi intrusi yang diusulkan, kami telah membahas teknologi yang sudah dikembangkan di bidang honeypots IoT dan pembelajaran mesin. Penggunaan honeypot IoT yang dapat menyimulasikan seluruh platform IoT akan memastikan pencatatan vektor besar karakteristik ancaman keamanan berbasis IoT, khususnya vektor ancaman baru. Lalu lintas malware yang dikumpulkan juga dapat digunakan untuk melatih sistem deteksi berbasis ML secara efektif, yang tentunya akan meningkatkan akurasi pendeteksiannya dan oleh karena itu, melindungi seluruh jaringan produksi dari ancaman keamanan baru yang muncul.

Untuk cakupan masa depan, kami akan menerapkan kerangka kerja IDS yang diusulkan dalam lingkungan dunia nyata dan menyelidiki secara mendalam isu-isu terbuka terkait honeypot IoT melalui skenario waktu nyata. Kami juga bermaksud membandingkan kinerja solusi yang diusulkan dengan model representatif di bidang ini.

BAB 7
MENUJU PLATFORM BLOCKCHAIN PASCA-QUANTUM

Dua dari kemajuan teknologi paling signifikan yang sedang berlangsung dan menunjukkan penyebaran yang terus meningkat baik di bidang industri maupun akademik, adalah blockchain dan munculnya komputasi kuantum. Karena blockchain telah mengalami kemajuan pesat dalam beberapa tahun terakhir dan telah menemukan banyak aplikasi di banyak bidang dengan harapan dapat meningkatkan keamanannya secara signifikan, teka-teki terkait ancaman kuantum dan penerapan tanda tangan pasca-kuantum dalam blockchain adalah sebuah tantangan. trending topik di komunitas ilmiah saat ini. Seperti halnya produk apa pun yang didasarkan pada kriptografi primitif, teknologi ini dipengaruhi oleh munculnya komputasi kuantum, karena teknologi ini pada dasarnya tidak berbeda dengan aplikasi lain yang tangguh dan aman dalam hal tersebut. Bab ini memberikan dukungan teoritis dari perkembangan terkini di bidang kriptografi pasca-kuantum (PQC) yang bertujuan untuk menggabungkan primitif kriptografi yang aman ke dalam teknologi blockchain. Oleh karena itu, bab ini menilai algoritma PQC kontemporer dan menyajikan situasi terkini dari kandidat PQC putaran ke-3 NIST. Selain itu, ini menunjukkan dampak komputasi kuantum pada blockchain dan menyelidiki penggabungan primitif PQC ke berbagai platform blockchain. Oleh karena itu, bab ini bertujuan untuk memberikan pedoman dan menunjukkan tantangan bagi peneliti dan industri mengenai implementasi algoritma post-quantum dalam aplikasi blockchain.

7.1 PENDAHULUAN

Sejak evolusi Bitcoin, teknologi blockchain semakin diminati dalam beberapa tahun terakhir sebagai teknologi baru yang memfasilitasi tingkat desentralisasi yang dibutuhkan oleh aplikasi dan layanan modern dengan cara yang efisien dan kuat. Blockchain adalah database catatan terdistribusi, atau buku besar bersama dari semua transaksi atau peristiwa digital yang telah dijalankan dan dipertukarkan di antara sejumlah pihak. Blockchain telah mengadopsi dasar kriptografi primitif, seperti fungsi hash dan tanda tangan digital, yang digunakan untuk mencapai konsensus dan mengautentikasi transaksi. Sebagian besar platform blockchain paling populer menggunakan daftar blok tertaut, di mana setiap blok berkaitan dengan penunjuk hash sebelumnya, sedangkan data setiap blok disusun menggunakan pohon Merkle. Namun skema dan algoritma tersebut tidak dapat menjamin kebutuhan keamanan yang mungkin terjadi di masa depan. Meskipun masyarakat komputer modern cenderung menuju globalisasi, tujuan keamanan tidak hanya merupakan persyaratan dasar, seperti ketahanan terhadap gangguan dan kepercayaan, namun juga tuntutan keamanan yang mendesak untuk mekanisme pelestarian privasi dan kebutuhan untuk menegakkan akuntabilitas dalam banyak aplikasi. Sejak itu, teknologi blockchain telah diadopsi tidak hanya pada industri keuangan, namun juga pada banyak bidang lainnya; keamanan dan arsitektur bisnisnya tidak dapat dengan mudah dimodifikasi. Oleh karena itu, keamanan blockchain harus mempertimbangkan

tidak hanya cara serangan yang sedang berlangsung, namun juga masalah keamanan yang mungkin muncul di masa depan.

Pada dasarnya, untuk otentikasi transaksi, blockchain didasarkan pada algoritma tanda tangan digital kurva elips (ECDSA), yang tidak cukup memadai untuk menangani ancaman kuantum. Algoritme Shor telah terbukti menunjukkan supremasi kuantum dibandingkan komputasi klasik. Jika algoritma ini digunakan oleh penyerang, maka kunci privat korban dapat diambil dari kunci publik dan keamanan sistem dapat dikompromikan. Demikian pula jika penyerang memalsukan tanda tangan pengguna, maka seluruh aset dan privasi pengguna akan hilang. Oleh karena itu, dengan mempertimbangkan dasar-dasar kriptografi dari blockchain, bab ini menggarisbawahi aspek keamanan pasca-kuantum yang dapat diadopsi dalam teknologi blockchain dan memungkinkannya untuk melawan serangan kuantum berdasarkan algoritma Shor dan Grover.

7.2 KRIPTOGRAFI PASCA-KUANTUM

Kriptografi pasca-kuantum (PQC) mengacu pada sistem kriptografi yang akan memberikan keamanan bahkan jika komputer kuantum menjadi kenyataan. Lebih tepatnya, komputasi kuantum memanfaatkan fenomena mekanika kuantum, sehingga menjadi lebih kuat daripada komputer klasik. Dengan kata sederhana, komputer klasik beroperasi pada bit, yang dapat memiliki salah satu dari dua nilai (keadaan), yaitu 0 atau 1, sedangkan komputer kuantum beroperasi pada qubit, yang berada dalam superposisi keadaan, yaitu 0, 1, atau keduanya. Oleh karena itu, algoritma kuantum dapat memanfaatkan superposisi keadaan ini untuk memberikan solusi efisien terhadap beberapa masalah matematika di mana komputer klasik secara praktis gagal memberikan solusi. Meskipun tidak semua permasalahan dapat diselesaikan secara efisien; Meskipun terdapat beberapa masalah yang dianggap sulit saat ini, namun masalah tersebut dapat dipecahkan secara efisien oleh komputer kuantum. Beberapa dari masalah ini merupakan landasan bagi algoritma kriptografi kontemporer, sehingga menjadikannya tidak aman sepenuhnya di era pasca kuantum.

Algoritme kuantum yang paling terkenal, yang mempunyai dampak langsung pada keamanan sistem kriptografi, adalah algoritma faktorisasi bilangan bulat Shor, yang merupakan algoritma kuantum yang memfaktorkan bilangan bulat N dalam waktu polinomial terhadap panjang N dan algoritma Grover, yang adalah algoritma kuantum untuk mencari database tidak terstruktur.

Cipher simetris saat ini dengan kunci 256-bit seperti AES-256, diyakini tahan terhadap kuantum. Demikian pula, fungsi hash dengan parameter yang tepat (yaitu, panjang nilai hash) juga dianggap aman pasca-kuantum, dalam hal ketahanan benturan. Oleh karena itu, penelitian kriptografi post-kuantum berfokus pada algoritma asimetris, sehingga dapat menggantikan RSA, (EC)DH dan (EC)DSA. Algoritme aman pasca-kuantum ini didasarkan pada permasalahan matematika yang diyakini sulit dalam kasus klasik dan kuantum. Selain itu, karena fungsi hash juga aman pasca-kuantum, beberapa skema tanda tangan digital pasca-kuantum yang keamanannya bergantung pada keamanan fungsi hash juga ada.

Lebih tepatnya, algoritma kriptografi pasca-kuantum terutama diklasifikasikan ke dalam salah satu kategori berikut, sementara masing-masing algoritma tersebut menyandarkan keamanannya pada satu masalah matematika spesifik yang sulit:

- Kriptografi berbasis kode,
- Kriptografi berbasis kisi,
- Kriptografi multivariat,
- Kriptografi berbasis hash,
- Kriptografi isogeni kurva elips supersingular.

Sedangkan pendekatan hibrida juga dipertimbangkan. Selain itu, beberapa algoritme didasarkan pada keamanan bukti tanpa pengetahuan, yang akan dijelaskan selanjutnya.

Kriptografi Berbasis Kode

Keamanan algoritma kriptografi yang termasuk dalam kelas ini didasarkan pada teori pengkodean yaitu, dengan masalah yang berbeda secara inheren dalam memecahkan kode kata kode yang salah yang dihasilkan melalui kode koreksi kesalahan yang tidak diketahui. Sistem yang paling klasik adalah kriptosistem McEliece, yang keamanannya didasarkan pada masalah penguraian sindrom. Kriptosistem McEliece menyediakan enkripsi cepat dan dekripsi yang relatif cepat, yang merupakan keuntungan untuk melakukan transaksi blockchain dengan cepat. Namun, sistem kriptografi McEliece memerlukan matriks besar yang bertindak sebagai kunci publik dan privat, yang mungkin menjadi batasan dalam lingkungan terbatas.

Kriptografi Berbasis Kisi

Golongan ini mencakup algoritma kriptografi yang konstruksinya didasarkan pada kisi-kisi, yaitu himpunan titik-titik dalam ruang berdimensi n dengan struktur periodik. Algoritme ini menyandarkan keamanannya pada tingkat kesulitan yang diketahui dalam permasalahan matematika tertentu dalam bidang kisi, seperti Masalah Vektor Terpendek (SVP), karena merupakan NP-hard, yang terkait dengan penemuan vektor bukan nol terpendek dalam sebuah kisi. Masalah sulit berbasis kisi serupa lainnya juga ada, seperti Masalah Vektor Terdekat (CVP), Solusi Integer Terpendek (SIS) atau Masalah Vektor Independen Terpendek (SIVP). Masalah berbasis kisi yang penting, yang "hadir" di beberapa sistem kriptografi berbasis kisi, adalah masalah "belajar dengan kesalahan" (LWE), yang memiliki pengurangan keamanan pada varian SVP.

Kriptografi multivariat

Kriptografi multivariat bergantung pada kompleksitas sistem penyelesaian persamaan multivariat, yang telah terbukti bersifat NP-hard atau NP-complete. Secara umum, diketahui bahwa skema kriptografi tersebut memiliki beberapa keterbatasan dalam kecepatan dekripsinya (karena adanya "perkiraan". Saat ini, beberapa skema berbasis multivariat yang paling menjanjikan didasarkan pada Hidden Field Equations (HFE) untuk survei umum masalah matematika di bidang kriptografi multivariat.

Kriptografi Berbasis Hash

Skema ini mencakup skema tanda tangan digital kriptografi yang keamanannya bergantung pada keamanan fungsi hash yang mendasarinya, bukan pada tingkat kesulitan permasalahan matematika. Skema semacam ini dimulai sejak akhir tahun 70an, ketika Lamport mengusulkan skema tanda tangan berdasarkan fungsi satu arah.

Kriptografi Isogeni Kurva Elips Supersingular

Skema ini mencakup algoritma kriptografi yang keamanannya bergantung pada protokol isogeni untuk kurva elips biasa tetapi ditingkatkan untuk menahan serangan kuantum. Kriptosistem seperti ini biasanya menggunakan ukuran kunci dalam urutan beberapa ribu bit.

Pendekatan Lain

Kriptografi pasca-kuantum berdasarkan bukti tanpa pengetahuan: Berdasarkan konsep klasik bukti tanpa pengetahuan, algoritma kriptografi ini adalah generalisasi dari skema kriptografi berbasis hash, diperkaya dengan sifat kriptografi yang bagus dari sandi simetris menuju konstruksi nol- bukti pengetahuan.

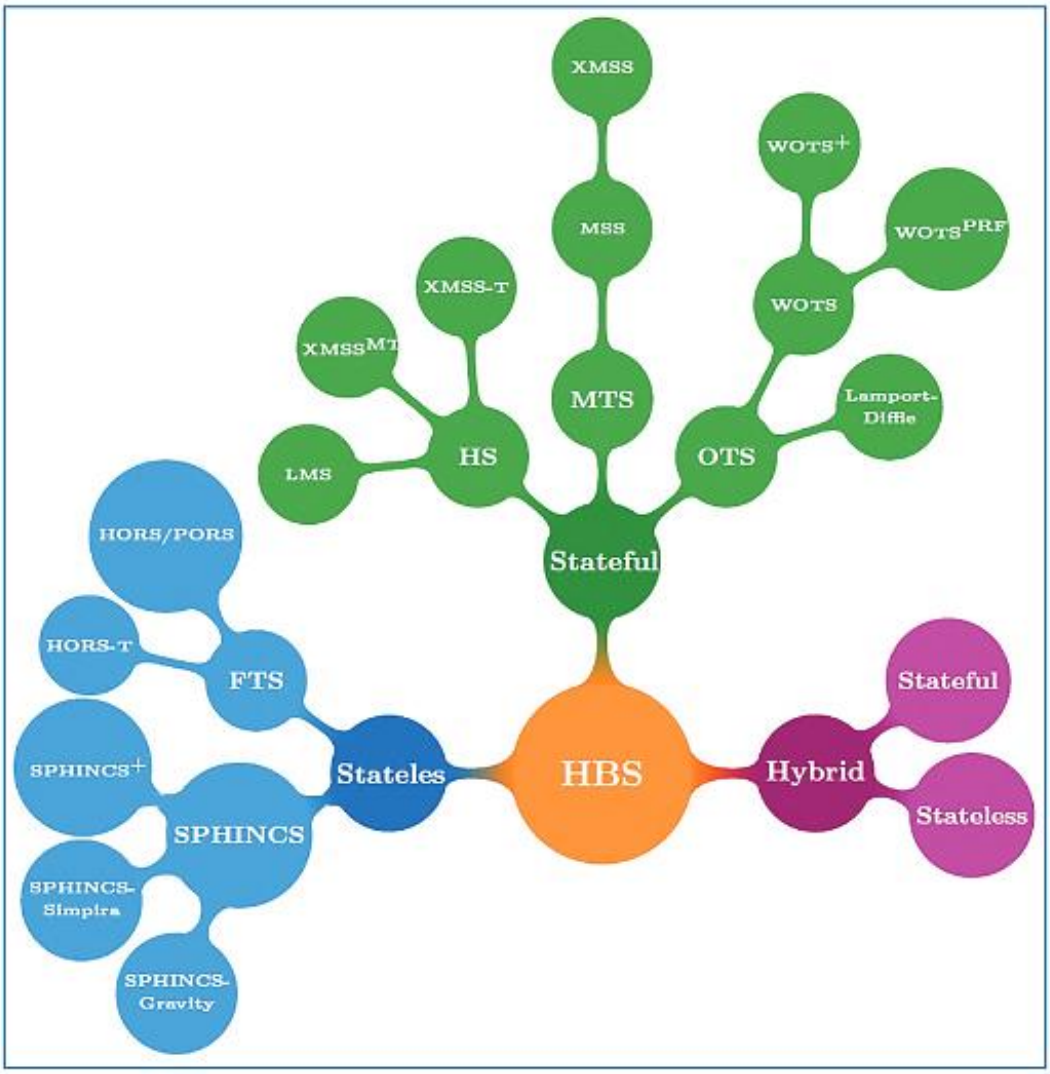
Pendekatan hibrid: Skema hibrid nampaknya merupakan langkah selanjutnya menuju keamanan pasca-kuantum, karena skema ini secara tepat menggabungkan kriptosistem pra-kuantum dan pasca-kuantum, yang bertujuan untuk melindungi data yang dipertukarkan baik dari serangan kuantum maupun dari serangan terhadap data yang digunakan. skema pasca-kuantum. Namun, skema tersebut melibatkan penerapan dua sistem kriptografi yang kompleks, yang memerlukan sumber daya komputasi yang signifikan dan konsumsi energi yang lebih banyak. Oleh karena itu, pengembang sistem kriptografi pasca-kuantum hibrida untuk blockchain di masa depan harus mencari trade-off antara keamanan, kompleksitas komputasi, dan konsumsi sumber daya.

Algoritma Penandatanganan Pasca-Quantum

Dalam aplikasi dunia nyata saat ini, skema kriptografi yang paling banyak digunakan untuk tanda tangan digital adalah RSA, Digital Signature Algorithm (DSA), dan Elliptic Curve Digital Signature Algorithm (ECDSA). Namun, seperti telah disebutkan, skema tanda tangan digital seperti itu tidak diposkan. -aman kuantum. Oleh karena itu, penting bagi aplikasi blockchain untuk memberikan keamanan jangka panjang dan memastikan bahwa tanda tangan digital aman terhadap komputer pasca-kuantum. Untuk tujuan ini, kami kemudian fokus secara eksplisit pada algoritma penandatanganan pasca-kuantum.

Tanda Tangan Digital Berbasis Hash

Algoritme tanda tangan berbasis hash (HBS) adalah skema dengan persyaratan keamanan minimal, cukup cepat, menyediakan tanda tangan berukuran kecil dan memiliki jaminan keamanan yang kuat (bukti keamanannya relatif terhadap properti yang masuk akal dari fungsi hash kriptografi).



Gambar 7.1. Taksonomi skema kriptografi HBS.

Skema HBS dapat diklasifikasikan menjadi skema stateless dan stateful yang selanjutnya dapat dikategorikan menjadi One-Time Signature (OTS), Few-Time Signature (FTS), Multi-Time Signature (MTS), dan Hierarchical Signature (HS), bergantung pada pada pembuatan kunci dan tanda tangan. Taksonomi skema ini dapat dilihat pada Gambar 7.1.

Skema tanda tangan satu kali (OTS) stateful: Skema Lamport, skema Winternitz, dan variannya WOTS+, WOTSPRF adalah algoritma karakteristik yang termasuk dalam kelas ini. Untuk menandatangani pesan dengan skema OTS, kunci privat dihasilkan secara acak secara seragam, sedangkan kunci publik diperoleh dari kunci privat, dengan melibatkan fungsi hash secara tepat; fungsi hash yang tidak dapat diubah, serta ketahanannya terhadap benturan, memastikan bahwa pengetahuan tentang kunci publik tidak memungkinkan penghitungan kunci privat. Skema Lamport, meskipun memiliki sifat keamanan yang tinggi, sebenarnya tidak tepat karena beberapa keterbatasan; pertama adalah skema tanda tangan satu kali (yaitu, setiap tanda tangan hanya dapat digunakan satu kali), sedangkan skema ini memerlukan ukuran kunci yang sangat besar; tanda tangan turunannya juga berukuran besar (lihat Tabel 7.1).

Fakta bahwa ini adalah skema OTS menyiratkan bahwa setiap kunci rahasia hanya digunakan satu kali untuk penandatanganan; jika tidak, penyerang mungkin dapat memperoleh informasi berguna untuk meniru pengguna melalui pengaturan tanda tangan yang valid (karena penyerang akan dapat mempelajari bagian dari kunci rahasia). Kelemahan yang terkait dengan efisiensi skema Lamport diatasi dengan skema Winternitz One Time Signature (WOTS), yang menggunakan apa yang disebut parameter Winternitz yang mengontrol trade-off waktu/memori. Oleh karena itu, pada prinsipnya, mengurangi ruang yang diperlukan untuk kunci dan tanda tangan menjadikan WOTS pilihan yang baik untuk perangkat tertanam dengan memori terbatas, namun dengan mengorbankan proses penandatanganan dan verifikasi yang lebih lambat.

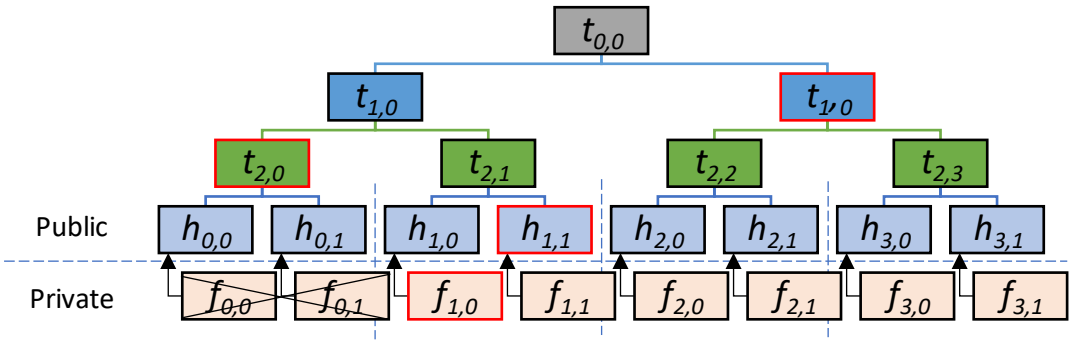
Tabel 7.1. Skema OTS dan FTS untuk panjang pesan 384-bit dan tingkat keamanan pasca-kuantum sekitar 128-bit.

Signature Scheme	Type	Signature Size (Kb)	Key Size (Kb)
Lamport	OTS	18.4	36.9
WOTS	OTS	4.8	4.8
WOTS+	OTS	3.2	3.2
$WOTS^{PRF}$	OTS	3.2	3.7
HORS-T	FTS	17.3	0.05

Stateful Multi-time Signature Schemes (MTS): Untuk mengatasi keterbatasan yang melekat pada skema OTS, skema MTS diusulkan untuk membuat tanda tangan berkali-kali dengan menggunakan OTS sebagai primitif yang mendasarinya. Skema pertama yang diusulkan oleh Merkle disebut Merkle Signature Scheme (MSS). Skema ini menggunakan apa yang disebut pohon Merkle, yang cukup untuk menggabungkan sejumlah besar pasangan kunci OTS ke dalam struktur pohon hash biner tunggal (seperti yang ditunjukkan pada Gambar 7.2). Akar pohon merupakan kunci publik global. Karena sifat dari fungsi hash yang mendasari yang digunakan untuk membangun pohon Merkle, penandatangan (dan tidak ada orang lain) dapat dengan mudah membuktikan bahwa kunci publik satu kali (misalnya kunci publik WOTS+) dikaitkan dengan kunci publik global. kunci publik, dengan mengungkapkan simpul pohon yang sesuai, menentukan jalur autentikasi, yang memungkinkan validator merekonstruksi jalur dari kunci publik satu kali yang relevan ke akar pohon setelah verifikasi tanda tangan.

Selain itu, ada beberapa cara lain yang efisien untuk menangani pohon Merkle, khususnya otentikasi (yaitu menyimpan cache jalur otentikasi dari tanda tangan sebelumnya dengan tepat). Teknik cerdas seperti ini menghasilkan skema tanda tangan yang lebih efisien berdasarkan pohon Merkle dengan Extended Merkle Signature Scheme (XMSS) sebagai contohnya. Skema XMSS adalah hypertree Merkle yang dimodifikasi dengan tepat, di mana daun yang melekat pada pohon tersebut didasarkan pada skema WOTS+. Lebih tepatnya, skema XMSS menggunakan pohon Merkle dengan perbedaan besar adalah penggunaan

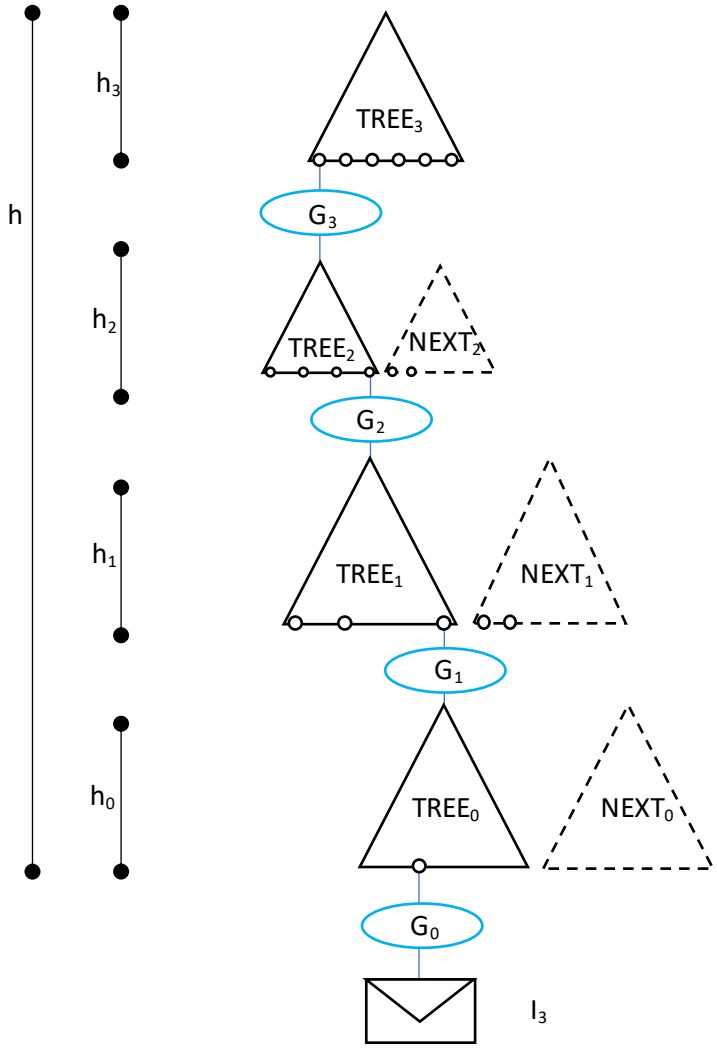
bitmask XOR dari node anak sebelum penggabungan hash ke dalam node induk. Penggunaan bitmask XOR memungkinkan penggantian rangkaian fungsi hash tahan benturan. Setiap daun pohon adalah akar pohon anak (juga pohon XMSS) yang disebut pohon-L, yang menyimpan kunci publik OTS.



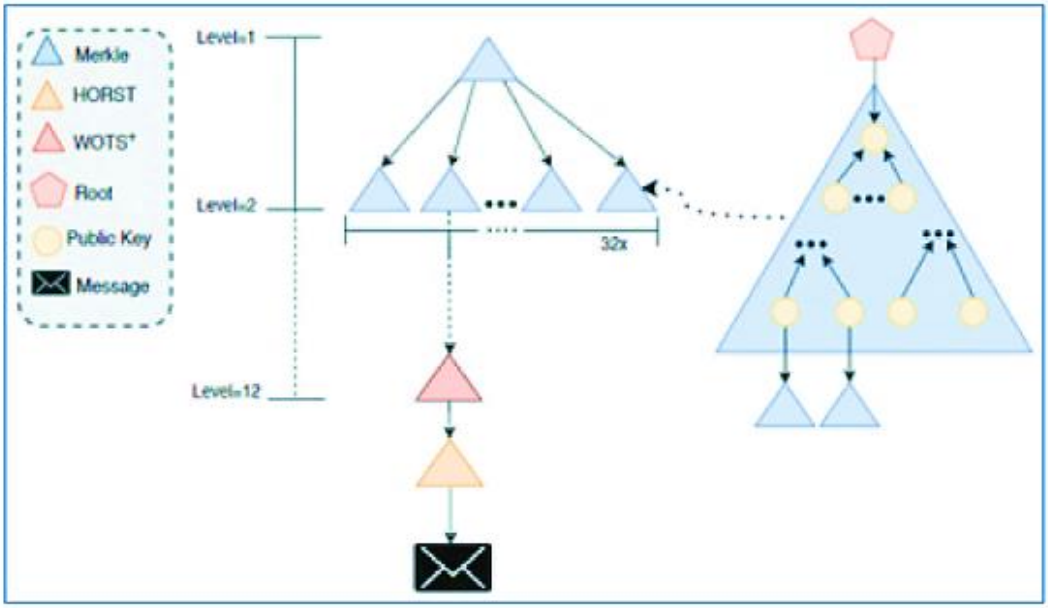
Gambar 7.2. Pohon Merkle dengan jalur verifikasi untuk kunci publik OTS h1,0.

Skema Tanda Tangan Hierarki Stateful (HS): Skema tanda tangan berbasis hash tanpa status umumnya dianggap lambat, karena perlu membuat pohon baru untuk menghasilkan pasangan kunci baru. Oleh karena itu, skema tanda tangan hierarki (HS) merupakan langkah selanjutnya menuju peningkatan efisiensi. Skema HS sebenarnya adalah skema MTS yang menggunakan tanda tangan berbasis hash lainnya dalam konstruksinya. Ide HS didasarkan pada pembentukan hyper-tree yang melibatkan rangkaian pohon dengan menggunakan beberapa lapisan pohon MSS. Dengan cara ini, lapisan atas digunakan untuk menandatangani akar lapisan di bawahnya sementara hanya lapisan terbawah yang digunakan untuk menandatangani pesan. Contoh penting dari HS adalah XMSS-MultiTree (XMSSMT) (lihat juga Gambar 7.3), XMSS dengan keamanan yang diperketat (XMSS-T) dan Leighton Micali Scheme (LMS). XMSSMT adalah pilihan yang bagus untuk aplikasi yang memerlukan banyak pesan untuk ditandatangani, asalkan teknik optimasi yang disebutkan di atas (penggunaan PNRG, cache jalur otentikasi, dll.) masih ada.

Skema HBS stateful lainnya yang lebih baru, yang memanfaatkan blockchain untuk menyimpan "jalur autentikasi" adalah apa yang disebut skema BPQS. BPQS sebenarnya adalah skema XMSS yang dimodifikasi, menggunakan jalur otentikasi tunggal (yaitu rantai dan bukan pohon). Para peneliti di berpendapat bahwa BPQS cocok dengan blockchain.



Gambar 7.3. XMMSMT dengan 4 lapisan.



Gambar 7.4. Struktur hypertree digunakan dalam SPHINCS.

Skema Tanda Tangan Hierarki Tanpa Negara (HS): Properti mail dari skema tanda tangan hierarki berstatus adalah bahwa proses penandatanganan memerlukan pembaruan kunci rahasia. Dengan kata lain, untuk skema tanda tangan stateful, penandatanganan memerlukan penyimpanan status kunci satu kali yang digunakan dan memastikan kunci tersebut tidak pernah digunakan kembali. Namun, ada juga skema tanda tangan hierarki tanpa kewarganegaraan, dengan contoh yang paling menonjol adalah SPHINCS [8] dan variannya SPHINCS-Simpira, Gravity-SPHINCS, dan SPHINCS+. Mirip dengan XMSSMT, SPHINCS menggunakan hypertree sehingga lapisan atas menggunakan XMSS dengan WOTS+ untuk menandatangani akar nenek moyangnya, sedangkan lapisan bawah menggunakan konstruksi pohon Merkle dengan HORS-T untuk menandatangani pesan (seperti yang ditunjukkan pada Gambar 7.4). Karena skema stateless tidak menyimpan catatan pasangan kunci yang digunakan, maka untuk memastikan penggunaan pasangan kunci yang benar beberapa kali, SPHINCS menyebarkan beberapa pasangan kunci HORS-T dan memilih satu pasangan kunci secara acak untuk setiap pembuatan tanda tangan (HORS-T beberapa kali – bukan satu kali – primitif tanda tangan (FTS)). Oleh karena itu, tidak diperlukan pelacakan jalur-negara.

Dalam skema stateless seperti SPHINCS, menghasilkan semua kunci pribadi (HORS-T dan WOTS+) dengan PRNG dan menghitung satu pohon di setiap lapisan untuk menghasilkan tanda tangan akan menghasilkan komputasi yang efisien. Meskipun demikian, skema tanpa kewarganegaraan menimbulkan permasalahan kinerja sebagai berikut. Pertama, pembuatan tanda tangan lebih mahal karena pasangan kunci digunakan dalam urutan acak dibandingkan urutan berturut-turut; karenanya, beberapa algoritma optimasi yang digunakan dalam skema stateful tidak dapat diterapkan. Selain itu, berbeda dengan WOTS+, tanda tangan HORS-T relatif jauh lebih besar. Perhatikan bahwa Tabel 7.1 juga memberikan informasi yang relevan tentang HORS-T, sebagai primitif FTS, dibandingkan dengan primitif OTS. Ringkasan antara skema HBS stateless (SPHINCS) dan stateful (MSS, XMSS, XMSSMT) yang dibahas diberikan pada Tabel 7.2, sedangkan evaluasi keseluruhan diberikan pada Tabel 7.3.

Meskipun keamanan pasca-kuantum dianggap ada dalam skema HBS, semua potensi serangan juga harus diperiksa, terutama yang berasal dari serangan implementasi – misalnya, serangan saluran samping dan serangan kesalahan. Dalam serangan saluran samping, penyerang memperoleh informasi ekstra penting (yaitu, relatif terhadap kunci rahasia) dengan memantau dan/atau mengukur kuantitas seperti konsumsi daya, kebocoran elektromagnetik, waktu untuk melakukan eksekusi, dll. Dalam serangan kesalahan, kesalahan, yang bisa bersifat alami atau berbahaya, adalah perilaku buruk perangkat yang menyebabkan komputasi menyimpang dari spesifikasinya, yang juga dapat menghasilkan beberapa informasi tentang kunci rahasia. Skema HBS rentan terhadap serangan kesalahan perangkat keras baik yang bersifat alami maupun yang berbahaya, sehingga perhatian khusus harus diberikan pada penerapan skema tersebut dengan tepat. Selain itu, masalah lain dalam skema tanda tangan stateful adalah apa yang disebut kloning. Ancaman seperti ini terjadi ketika kunci pribadi disalin dan kemudian digunakan tanpa koordinasi dengan unit eksekusi (dikenal sebagai kloning non-volatile) atau tanpa koordinasi dengan unit penyimpanan, yang dikenal sebagai kloning volatil.

Beberapa peneliti menganggap XMSS dan SPHINCS tidak praktis untuk aplikasi blockchain karena kinerjanya (kecepatan penandatanganan yang relatif lambat, sedangkan ukuran tanda tangan di SPHINCS adalah 41kb), sehingga alternatif telah disarankan.

Tabel 7.2. Perbandingan antara skema tanda tangan stateful dan stateless pada.

Signature Scheme	Instantiation	Base Scheme	Key Re-use Capability	Signature Size (Kb)	Key Size (Kb)
MSS	SHA-384	WOTS	2^{60}	7.7	0.05
XMSS	SHA-256	$WOTS^{PRF}$	2^{60}	4.7	0.03
$XMSS^{MT}$	AES-128	$WOTS^{PRF}$	2^{80}	10.7	Private key = 26.1 Public key = 1.8
SPHINCS	SHA-256	HORS-T & WOTS+	Unlimited	41.0	1.0

Tanda Tangan Digital Berbasis Kode

Beberapa algoritma penandatanganan berbasis kode pasca-kuantum telah diusulkan; mungkin yang paling dikenal adalah skema dari Niederreiter dan CFS (Courtois, Finiasz, Sendrier), yang mirip dengan sistem kriptografi McEliece. Penandatanganan skema seperti ini pendek dan dapat diverifikasi dengan sangat cepat, namun mirip dengan kriptosistem McEliece, penggunaan ukuran kunci yang besar memerlukan sumber daya komputasi yang signifikan dan, sebagai konsekuensinya, pembuatan tanda tangan mungkin menjadi tidak efisien [10].

Tabel 7.3. Evaluasi umum keseluruhan skema HBS stateful dan stateless.

Type	Pros	Cons	Use Case
Stateful	– Shorter signature size – Faster signature generation time	– State synchronization problem synchronization failure – Face cloning problem	Performance-constrained environment
Stateless	– No state synchronization. problem – No cloning problem	– Longer signature size – Slower signature generation time	Resource-constrained environment

Skema Tanda Tangan Digital Multivariat

Kelas tanda tangan pasca-kuantum ini biasanya menghasilkan kunci publik yang besar, namun tanda tangan yang sangat kecil. Beberapa skema berbasis multivariat yang paling populer mengandalkan algoritma Matsumoto-Imai atau varian HFE, yang dapat menghasilkan

tanda tangan dengan ukuran yang sebanding dengan tanda tangan berbasis RSA atau ECC yang saat ini digunakan. Skema tanda tangan digital berbasis multivariat lain yang relevan telah diusulkan, seperti Rainbow. Secara umum, diasumsikan secara luas bahwa sistem kriptografi tersebut perlu ditingkatkan lebih lanjut dalam hal ukuran kunci.

Skema Tanda Tangan Digital Berbasis Kisi

Di antara beberapa skema tanda tangan berbasis kisi yang dijelaskan dalam literatur, skema yang didasarkan pada Solusi Integer Pendek (SIS) tampaknya menjanjikan karena ukuran kuncinya yang lebih kecil. Selama beberapa tahun, diasumsikan bahwa BLISS-B (Bimodal Lattice Signatures B), yang keamanannya bergantung pada beratnya masalah SIS, bisa menjadi pilihan yang sangat bagus karena kinerjanya yang baik. Namun, diketahui bahwa BLISS rentan terhadap serangan saluran samping. Selain BLISS, terdapat literatur skema tanda tangan berbasis kisi lainnya yang mengandalkan masalah SIS namun dirancang khusus untuk blockchain. Selain itu, skema tanda tangan buta berbasis kisi telah digunakan untuk memberikan anonimitas dan tidak dapat dilacak dalam aplikasi berbasis blockchain terdistribusi untuk IoT.

Skema Tanda Tangan Digital Isogenies

Meskipun isogeni kurva elips supersingular dapat digunakan untuk membuat skema tanda tangan digital pascakuantum, tidak banyak skema seperti itu yang diketahui, dan skema tersebut juga tidak efisien. Beberapa skema kelas ini menunjukkan bahwa "permasalahan ukuran utama perlu diatasi ketika mengimplementasikan sistem kripto berbasis isogeni dan Supersingular Isogeny Diffie-Hellman (SIDH), terutama dalam kasus perangkat dengan sumber daya terbatas".

Bukti Tanpa Pengetahuan Untuk Tanda Tangan Digital

Ada satu skema tanda tangan digital pasca-kuantum yang penting, yang disebut Piknik, yang memiliki prinsip desain yang sangat berbeda dibandingkan skema sebelumnya. Piknik yang diajukan ke kompetisi NIST didasarkan pada bukti pengetahuan nol non-interaktif, dimana bukti pengetahuan tersebut dibuat dengan menggunakan pendekatan MPC-in-the-head. Tanda tangan adalah bukti pengetahuan kunci rahasia untuk cipher blok yang mengenkripsi blok teks biasa publik ke blok teks sandi publik, yang bersama-sama membentuk kunci publik dari skema tanda tangan. Semua blok penyusun kriptografi dapat dipakai menggunakan primitif kunci simetris (blok cipher dan fungsi hash), sedangkan protokol MPC (Multi-Party Computation) dapat dipakai dengan keamanan teori informasi.

7.3 BLOCKCHAIN DAN KRIPTOGRAFI PASCA KUANTUM

Untuk mengatasi ancaman kuantum dalam teknologi blockchain, beberapa peneliti telah mengusulkan solusi blockchain pasca-kuantum atau bahkan beberapa penyesuaian terhadap pemimpin terdistribusi yang populer. Blockchain komersial juga telah menganalisis dan mengatasi dampak komputer kuantum. Ini termasuk Quantum Resis-tant Ledger (QRL) yang menggunakan XMSS, IOTA yang menggunakan WOTS dan Corda yang menggunakan BPQS.

Bitcoin

Platform Bitcoin menggunakan ECDSA dengan algoritma kurva Koblitz secp256k1 dan fungsi hash SHA-256 untuk mengotorisasi transfer koin dan aset. Didefinisikan oleh Standards for Efficient Cryptography Group (SECG), kurva Koblitz memberikan beberapa keuntungan, seperti efisiensi, pengurangan ukuran kunci dan keamanan, namun kelemahan utamanya adalah kelemahannya terhadap serangan kuantum. Oleh karena itu, untuk mengamankan tanda tangan digital yang termasuk dalam transaksi Bitcoin terhadap algoritma Shor, menerapkan skema tanda tangan berdasarkan algoritma TESLA#, yang menggunakan fungsi BLAKE2 dan SHA-3, maka menghasilkan skema penandatanganan dan verifikasi penandatanganan yang cepat. Namun qTESLA tidak hadir pada evaluasi putaran ketiga kompetisi NIST.

Penelitian kriptografi berbasis kisi, yang meletakkan dasar bagi desain skema tanda tangan serangan anti-kuantum, tidak hanya bermanfaat untuk melawan ancaman kuantum, namun juga cocok untuk blockchain. Oleh karena itu, sistem blockchain e-voting yang transparan, yang dapat diterapkan di Bitcoin. Dalam skema ini, pemilih yang beroperasi secara jahat diaudit, sementara kriptografi berbasis kode digunakan untuk melawan ancaman kuantum. Lebih tepatnya, algoritma tanda tangan cincin tanpa sertifikat yang dapat dilacak diperkenalkan dalam usulan sistem e-voting yang mendukung blockchain untuk memecahkan masalah verifikasi sertifikat kunci publik dan sistem kriptografi berbasis kode Niederreiter diadopsi untuk mengatasi ancaman kuantum dalam e-voting. protokol pemungutan suara.

Etereum

Para penulis di mengusulkan kerangka kerja yang mengenkripsi dan data industri sensitif, sementara pengunggah memutuskan dengan siapa data ini dapat dibagikan. Arsitekturnya dimodelkan untuk beroperasi dengan platform Ethereum yang populer dan Inter Planetary File System (IPFS). Namun, platform serupa dan tradisional juga mampu menyediakan persyaratan yang diperlukan untuk pengoperasian kerangka kerja tersebut. Kerangka kerja ini menggunakan Elliptical-Curve Diffie-Hellman Key Exchange (ECDH) dan algoritma SIDH. Dengan demikian, kelebihan dan kekurangan masing-masing algoritma dibahas dalam makalah tersebut, menyimpulkan bahwa SIDH adalah pendekatan yang paling cocok karena aman pasca-kuantum dan menjamin keamanan terhadap penyerang dengan kemampuan komputasi kuantum. Platform Ethereum juga dimodifikasi di mana penulis menerapkan kriptosistem berbasis multivariat (skema tanda tangan Rainbow) dan membandingkan efisiensinya dengan versi Ethereum saat ini, yang didasarkan pada ECDSA.

IOTA

IOTA adalah buku besar terdistribusi populer yang dirancang untuk ekosistem IoT. Platform ini dianggap sebagai buku besar yang tahan terhadap kuantum, bukan sebagai buku besar yang tahan terhadap kuantum. Secara khusus, ini tidak menggunakan kriptografi kunci publik konvensional, tetapi IOTA Signature Scheme (ISS) yang didasarkan pada WOTS. Dalam platform ini, pengguna di IOTA menandatangani hash pesan, yang berarti bahwa keamanan ISS didasarkan pada kekuatan kriptografi dari fungsi hash. Oleh karena itu, transaksi IOTA bersifat tahan kuantum, namun memerlukan kunci privat/publik baru untuk dihasilkan setiap

kali transaksi ditandatangani dengan kunci privat, karena sebagian dari kunci privat terungkap dalam proses penandatanganan.

QRL

Saat merancang QRL, penekanan besar diberikan pada keamanan kriptografi skema tanda tangannya, agar aman dari serangan klasik dan kuantum, tidak hanya pada saat ini, namun juga pada dekade mendatang. QRL menggantikan secp256k1 dengan XMSS, menggunakan fungsi hash SHA-256 dan menawarkan keamanan 196-bit dengan keamanan yang diharapkan terhadap serangan brute force hingga tahun 2164. Skema tanda tangan hypertree asimetris yang digunakan dalam QRL terdiri dari rantai Pohon XMSS dan memberikan keuntungan ganda menggunakan skema tanda tangan yang divalidasi dan izin untuk menghasilkan alamat buku besar dengan kemampuan menandatangani transaksi tanpa penundaan pra-perhitungan yang diamati dalam konstruksi XMSS.

Kabel

Corda biasanya mendukung algoritma tanda tangan kunci publik konvensional, seperti ECDSA dan RSA (tanda tangan default adalah ECDSA dengan kurva NIST P-256 – yaitu, secp256p1). Namun, pada tingkat eksperimental, SPHINCS telah digunakan untuk menyediakan keamanan pasca-kuantum. Selain itu, baru-baru ini, para peneliti dari R3 (yaitu perusahaan yang mendukung Corda) mengusulkan skema tanda tangan BPQS yang disebutkan di atas, membentuk penyempurnaan dari XMSS (dan, sebenarnya, blockchain itu sendiri memainkan peran tersebut, sehingga terdiri dari skema tanda tangan yang di-blockchain).

Kain Hyperledger

Hyperledger Fabric tidak menyediakan (secara default) keamanan pasca-kuantum. Namun, telah diumumkan bahwa mencapai keamanan pasca-kuantum adalah salah satu prioritas sehubungan dengan kemajuan lebih lanjut dari buku besar. Untuk mencapai tujuan ini, pendekatan seperti itu baru-baru ini disarankan dalam sebuah makalah penelitian [17]. Para peneliti menyajikan apa yang disebut PQFabric, yang merupakan versi pertama dari blockchain berizin perusahaan Hyperledger Fabric yang tanda tangannya aman terhadap ancaman komputasi klasik dan kuantum. Dalam makalah ini, para peneliti menerapkan dan menganalisis tanda tangan hibrid yang dapat dikonfigurasi dengan algoritma tanda tangan pasca-kuantum apa pun.

Para penulis mendesain ulang prosedur dan spesifikasi manajemen kredensial jaringan Fabric dan mereka menciptakan tanda tangan hibrid yang merupakan kombinasi tanda tangan digital klasik dan aman kuantum. Tolok ukur perbandingan PQ-Fabric dilakukan dengan beberapa kandidat dan pengganti NIST, yaitu Falcon-512, Falcon-1024, Dilithium-2, Dilithium-3, Dilithium-4 dan qTesla-p-I.

Sistem yang diusulkan dibangun di atas Fabric v.1.4 dan LIBOQS v0.4, yang digunakan untuk implementasi algoritma kriptografi pasca-kuantum. Tidak mudah, dan oleh karena itu tiga modul inti dari basis kode Fabric dimodifikasi untuk memungkinkan penggabungan tanda tangan kuantum hibrid, (1) Penyedia Layanan Kriptografi Blockchain (BCCSP) yang menawarkan implementasi seragam antarmuka. Antarmuka ini memanggil skema tanda tangan yang relevan berdasarkan jenis kunci yang digunakan; (2) Penyedia Layanan Keanggotaan (MSP) lokal yang mengekstraksi kunci kriptografi, baik publik maupun privat –

karena kriptografi kuantum-klasik hibrid memerlukan dua kunci – dari sertifikat X.509; dan (3) kriptogen, yaitu templat yang digunakan untuk membuat materi kriptografi yang diperlukan untuk menjalankan platform Fabric dari file konfigurasinya. Oleh karena itu, MSP yang dimodifikasi memperoleh kunci privat dan publik dari sertifikat X.509, menyimpannya untuk setiap node dalam struktur internal dan kemudian memberikannya ke modul BCCSP setiap kali pesan ditandatangani. Skema tanda tangan yang sederhana memungkinkan LibOQS untuk melakukan hashing ulang pada pesan yang sudah di-hash, namun tindakan ini berdampak pada kinerja platform. Khususnya, kecepatan algoritma tanda tangan merupakan faktor kunci yang mempengaruhi kinerja skema dengan ukuran tanda tangan dan kunci yang lebih besar.

7.4 KINERJA BLOCKCHAIN PASCA-QUANTUM CRYPTOSYSTEMS

Kinerja tanda tangan digital pasca-kuantum telah dipelajari secara luas dalam literatur. Evaluasi kinerja seperti itu telah dipertimbangkan sehubungan dengan beberapa platform perangkat keras yang mendasarinya, serta beberapa protokol jaringan dengan beberapa asumsi pada saluran komunikasi yang mendasarinya. Dalam kasus FALCON, penulis mengukur kinerjanya berdasarkan waktu yang dihabiskan, bukan siklus. Untuk Rainbow, nilai tersebut menunjukkan performa versi kompresi kunci yang memerlukan upaya komputasi lebih besar dibandingkan versi reguler karena melibatkan proses dekompresi. Namun, sebagian besar kriptosistem telah dievaluasi setelah mengoptimalkannya untuk AVX2, set instruksi 256-bit yang disediakan oleh Intel. Satu-satunya pengecualian adalah kinerja SPHINCS untuk versi HARAKA, yang versi optimalnya diimplementasikan untuk memanfaatkan set instruksi AES-NI.

Menarik untuk diperhatikan bahwa evaluasi kinerja yang disajikan pada Tabel 7.4 didasarkan pada perangkat keras yang sesuai yang dapat digunakan untuk menjalankan node blockchain biasa (yaitu node yang hanya berinteraksi dengan blockchain) atau node blockchain penuh (yaitu, node yang hanya berinteraksi dengan blockchain) atau node blockchain penuh (yaitu, sebuah node yang menyimpan dan memperbarui salinan blockchain secara berkala dan mampu memvalidasi transaksi blockchain).

Kesimpulan yang diperoleh dapat diringkas sebagai berikut: pertama, sehubungan dengan kriptosistem berbasis multivariat, MQDSS menyediakan kunci kecil, versi paling ringannya cukup cepat, namun ukuran tanda tangannya termasuk yang terbesar jika dibandingkan (sedangkan multivariat lainnya skema memiliki ukuran yang besar. Sebaliknya, skema berbasis multivariat lainnya yang dibandingkan memiliki kunci dengan ukuran besar, namun menghasilkan tanda tangan yang pendek; perhatikan juga bahwa MQDSS tidak dilanjutkan pada putaran ketiga.

Tabel 7.4. Evaluasi kinerja keseluruhan pada tanda tangan pasca-kuantum hadir dalam evaluasi NIST putaran ke-3.

Skema	Algoritma	Waktu Eksekusi (ms)	Ukuran (Bits)
Dilithium	Dilithium II	*KeyGen = 0.18*	$K_s = 22.400$
		Sign = 0.82	$K_p = 9.472$
		Ver = 0.16	$\sigma = 16.352$

Falcon	Falcon-512	*KeyGen = 16.77*	K_s *= 10.248*
		Sign = 5.22	K_p *= 7.176*
		Ver = 0.05	σ *= 5.52*
Rainbow	Rainbow-Ia-Cyclic	*KeyGen = 0.48*	K_s *= 743.680*
		Sign = 0.34	K_p *= 465.152*
		Ver = 0.83	σ *= 152*
GeMSS	GeMSS128	*KeyGen = 13.1*	K_s *= 107.502*
		Sign = 188	K_p *= 2.817.504*
		Ver = 0.03	σ *= 258*
Picnic	Picnic-L1-FS	*KeyGen = 0.005*	K_s *= 128*
		Sign = 4.09	K_p *= 256*
		Ver = 3.25	σ *= 272.256*
SPHINCS+	SPHINCS+ -SHA256-128f – simple	*KeyGen = 2.95*	K_s *= 512*
		Sign = 93.37	K_p *= 256*
		Ver = 3.92	σ *= 135.808*

Selanjutnya, sehubungan dengan tanda tangan berbasis kisi, skema ini umumnya memerlukan kunci yang lebih kecil dibandingkan skema multivariat, namun menghasilkan tanda tangan yang lebih besar. Di antara semuanya, FALCON – yang berlanjut ke putaran ketiga kompetisi NIST – menggunakan ukuran kunci dan panjang tanda tangan terkecil. qTESLA juga cepat, tetapi kelemahan utamanya adalah ukuran kunci yang besar; qTESLA tidak hadir dalam evaluasi putaran ketiga kompetisi NIST. Skema tercepat adalah Dilithium (di antara semua jenis tanda tangan pasca-kuantum – tidak hanya yang berbasis kisi). DILITHIUM memperoleh, dalam hal kinerja, hasil yang sangat mirip dengan ECDSA-256. Sayangnya, ukuran kunci DILITHIUM jauh lebih besar dibandingkan yang digunakan oleh ECDSA-256.

Tabel 7.5. Waktu (ms) pembuatan pasangan kunci, sign dan verifikasi.

Skema	KeyGen	Sign	Verify
BPQS (w = 4, SHA256)	0.569	0.08	0.10
BPQS (w = 4, SHA384)	1.107	0.16	0.19
BPQS (w = 16, SHA256)	0.872	0.19	0.20
BPQS (w = 16, SHA384)	1.719	0.39	0.38
ECDSA SECP256K1 (SHA256)	0.10	0.34	0.25
Pure EdDSA Ed25519 (SHA512)	0.10	0.08	0.16
RSA3072 (SHA256)	561.1	5.39	0.17
SPHINCS-256 (SHA512)	0.69	144.5	1.76

Namun, selain Dilithium, opsi lain yang menghasilkan kinerja baik adalah versi paling ringan dari Rainbow. Hal ini juga diverifikasi, terlepas dari hasil yang disebutkan di dalam evaluasi protokol TLS. Perhatikan juga bahwa Rainbow memerlukan parameter yang lebih kecil dibandingkan Dilithium, sehingga menjadikan algoritma ini kandidat yang sangat kuat untuk aplikasi masa depan (termasuk blockchain). Falcon memberikan waktu verifikasi terbaik, namun lambat dalam penandatanganan. Algoritma tanda tangan digital yang paling lambat adalah Picnic, GeMSS dan SPHINCS (semuanya merupakan algoritma alternatif dalam

kompetisi NIST). Untuk meringkas hasil (dalam hal kinerja), kami mengilustrasikan hasil kinerja para kandidat (dan penggantinya) pada NIST putaran ketiga (lihat Tabel 7.4). Tabel ini didasarkan pada hasil , yang sepenuhnya sesuai dengan survei yang disajikan pada.

Sebagaimana dinyatakan di atas, SPHINCS umumnya merupakan algoritma penandatanganan yang sangat lambat. Menarik untuk dicatat bahwa BPQS, yang juga berbasis hash (dan di luar kompetisi NIST) sudah cukup untuk mencapai kinerja yang lebih baik daripada SPHINCS, padahal ia berorientasi pada blockchain. Hal ini diilustrasikan pada Tabel7.5. Dapat dilihat bahwa, meskipun terdapat parameter BPQS yang relevan, BPQS jauh lebih cepat dibandingkan SPHINCS dalam hal penandatanganan dan verifikasi (dengan kinerja yang sebenarnya sebanding dengan skema tanda tangan digital kunci publik tradisional). Kelemahan utamanya adalah waktu pembangkitan kunci, yang dalam beberapa kasus sebanding dengan SPHINCS. Mengenai ukuran tanda tangan, semua mode BPQS mengungguli XMSS untuk jumlah tanda tangan pertama. Namun, tanda tangan BPQS tumbuh secara linier seiring dengan berapa kali kunci digunakan kembali, sehingga panjang keluaran tanda tangan bersifat dinamis (mulai dari yang kecil dan bertambah setiap tanda tangan tambahan).

Tabel 7.6. Saatnya membuat pohon XMSS untuk dompet QRL.

Tinggi Pohon XMSS	Jumlah Sign OTS	Fungsi/Algoritma Hash	Jenderal Waktu
18	262.144	SHA2_256 / SHA2	1 jam 10 menit 49 detik
10	1.024	SHAKE_128 / SHA3	11 detik
12	4.096	SHA2_256/ SHA2	1 jam 20 detik
12	4.096	SHAKE_128/ SHA3	48 detik
12	4.096	SHAKE_256/ SHA3	46 detik

Tabel 7.7. Informasi transaksi di QRL.

Ukuran Transaksi (Byte)	Waktu sign	Ukuran sign (Byte)	Waktu Verifikasi	Memblokir #	Ukuran Blok (Byte)
2662	1 detik	2500	4 menit 36 detik	81188	2915
2662	1 detik	2500	9 detik	81168	2915
2662	1 detik	2500	3 menit 0 detik	80944	2915
2704	–	2500	–	80939	2958
2662	1 detik	2500	1 menit 2 detik	80205	2915
2662	1 detik	2500	24 detik	66804	2915
2705	–	2500	–	66739	2959

Menarik juga untuk lebih fokus pada XMSS, dan khususnya pada QRL yang merupakan buku besar yang mendukung XMSS untuk mencapai, secara default, keamanan pasca-kuantum. Diketahui bahwa XMSS memiliki beberapa keterbatasan (itulah sebabnya SPHINCS dan BPQS dianggap sebagai penyempurnaan dari XMSS); namun, XMSS memang merupakan salah satu kriptografi primitif yang saat ini digunakan dalam blockchain komersial yang aman pasca-kuantum.

Kami selanjutnya menyajikan hasil eksperimen terbaru pada QRL, yang bertujuan untuk melihat dalam praktik kinerja QRL (implementing XMSS) di workstation konvensional.

Percobaan telah dilakukan pada prosesor Intel Core2Duo E6750 @ 2,66GHz, dengan RAM 6 Gb (DDR2 @ 400MHz) dan Windows 10 Pro, 64 bit, sebagai sistem operasi. Untuk melakukan beberapa pengukuran, peneliti menghasilkan beberapa dompet berbeda dengan parameter berbeda untuk XMSS. Hasilnya ditunjukkan pada Tabel 7.6.

Selain itu, peneliti sebelumnya melanjutkan melakukan beberapa transaksi dalam lingkungan pengujian (disediakan oleh QRL), dengan tujuan akhir untuk melihat dalam praktik waktu penandatanganan dan verifikasi yang sesuai. Hal ini ditunjukkan pada Tabel 7.7, untuk dompet kedua. Seperti yang ditunjukkan dalam tabel ini, ukuran tanda tangan adalah konstan, yang diharapkan karena ukuran tanda tangan berhubungan dengan tinggi pohon XMSS (atau, setara, dengan jumlah tanda tangan OTS). Lebih tepatnya, dalam QRL ukuran tanda tangan diberikan oleh relasi 2180 + (tinggi $*$ 32) byte. Variasi waktu verifikasi mungkin disebabkan oleh beban penambang di blockchain yang diuji dan alat eksperimen yang ditempatkan.

Serangan Terhadap Primitif PQC

Seperti yang telah dinyatakan NIST pentingnya serangan saluran samping (SCA) dan tindakan penanggulangannya. Lebih tepatnya, dalam seruan proposal NIST PQC pada tahun 2016, dinyatakan bahwa " Skema yang tahan terhadap SCA dengan biaya lebih rendah lebih disukai daripada skema yang kinerjanya sangat terhambat oleh upaya apa pun untuk melawan serangan saluran samping. " NIST juga berharap untuk melihat implementasi yang memiliki mekanisme perlindungan terhadap serangan saluran samping, seperti serangan waktu, serangan kesalahan, serangan pemantauan daya, dll. Oleh karena itu, pada bagian ini, disajikan sejumlah serangan SCA dan ISD terhadap kandidat putaran ke-3 NIST PQC.

Serangan-serangan terhadap kandidat putaran ke-3 NIST ini dikategorikan sebagai:

- Kriptanalisis Klasik (CC), yang menganalisis secara matematis sistem kriptografi yang bersangkutan.
- Static Timing Analysis (STA), yang memanipulasi runtime variabel suatu algoritma.
- Fault Attacks (FA), yang merupakan teknik semi-invasif untuk secara sengaja menimbulkan kesalahan dan mengungkap keadaan internal kriptografi.
- Analisis Daya Sederhana (SPA) dan Analisis Daya Tingkat Lanjut (diferensial/korelasi) (APA), yang secara non-invasif mengeksploitasi variasi konsumsi daya algoritma kriptografi.
- Serangan elektromagnetik (EMA), yang mengeksploitasi radiasi dari algoritma kriptografi.
- Serangan template (TA) yang menggunakan perangkat sensitif untuk mendapatkan akses ke rahasia.
- Serangan cold-boot (CBA), yang mengeksploitasi sisa memori untuk membaca data dari memori komputer ketika komputer dimatikan.
- Penanggulangan (CM) yang melindungi/menghalangi serangan melalui teknik penyembunyian atau penyembunyian.

Oleh karena itu, tabel berikutnya (Tabel 7.8) menyajikan skema mana yang rentan terhadap serangan yang disebutkan di atas.

Tabel 7.8. Ringkasan serangan terhadap kandidat putaran ke-3 NIST PQC.

			SCA								
		Algoritma	**CC**	**STA**	**FA**	**SPA**	**APA**	**EMA**	**TA**	**CBA**	**CM**
Finalists	KEMs	Clasic McEliece			√			√		√	
		Kyber			√	√		√	√	√	
		NTRU				√				√	
		Saber						√			√
	Sign	Dilithium			√			√			√
		Falcon			√						
		Raibow	√				√			√	
Alternatif	KEMs	BIKE		√	√						
		FrodoKEM		√		√	√	√	√	√	√
		HQC		√			√				
		NTRU Prime					√		√		√
		SIKE	√	√							
	Sign	GEMSS	√				√				
		Picnic	√				√				
		SPHINC+			√						

7.5 KESIMPULAN DAN ARAH MASA DEPAN DALAM BLOCKCHAIN PQC

Bab ini membahas aspek keamanan pasca-kuantum dalam teknologi blockchain. Lebih tepatnya, ia telah menilai algoritma PQC kontemporer dan situasi terkini dari kandidat PQC putaran ke-3 NIST. Selain itu, laporan ini juga menyajikan dampak serangan komputasi kuantum terhadap blockchain dan menyelidiki penggabungan primitif PQC ke dalam blockchain.

Saat ini, komputasi kuantum merupakan bidang yang banyak diminati baik dari kalangan akademisi maupun industri. Secara berurutan, serangan baru mungkin dikembangkan terhadap sistem kriptografi pasca-kuantum. Oleh karena itu, baik peneliti maupun industri perlu menyadari bidang komputasi kuantum dan kemajuannya dan oleh karena itu, kami menyajikan tantangan dan arah masa depan dalam blockchain PQC.

Transisi ke Blockchain Pasca-kuantum

Transisi ke blockchain pasca-kuantum memerlukan langkah-langkah yang harus dipertimbangkan dengan cermat. Oleh karena itu, beberapa peneliti telah menemukan metode baru untuk penerapan keamanan pasca-kuantum pada teknologi blockchain. Misalnya, dalam penulis memperkenalkan skema yang memperluas validitas blockchain, jika keamanan tanda tangan digital atau fungsi hash terancam. Namun, hard fork atau smooth-fork mungkin terjadi dan untuk kasus ini, penulis mengusulkan mekanisme soft-fork. Dalam karya lain, sebuah protokol commit-delay-reveal diusulkan yang memungkinkan pengguna Bitcoin untuk memindahkan dana dari protokol yang tidak tahan kuantum ke versi yang mematuhi skema tanda tangan yang tahan kuantum. Protokol transisi ini dapat bekerja dengan baik meskipun ECDSA sebelumnya telah disusupi.

Kunci Ukuran Khas dan Tantangan Kinerja

Ukuran kunci dalam sistem kriptografi pasca-kuantum adalah antara 128 dan 4.096 bit, yang berarti bahwa sistem kriptografi pasca-kuantum memerlukan ukuran kunci yang jauh lebih besar daripada sistem kriptografi kunci publik. Beberapa kriptosistem tanda tangan,

yang didasarkan pada isogeni supersingular, tampaknya bermanfaat untuk memecahkan masalah ukuran kunci, namun skema tersebut menghasilkan tanda tangan yang besar dan memberikan kinerja tuang dibandingkan dengan kriptosistem kunci publik. Ketika satu masalah tampaknya terselesaikan, beberapa masalah lainnya tercipta, karena blockchain menyimpan sejumlah besar tanda tangan. Demikian pula, sistem kriptografi berbasis hash memiliki ukuran kunci yang relatif kecil, yang bertentangan dengan ukuran tanda tangan mereka, yang seringkali lebih dari 40 KB. Di sisi lain, sebagian besar kriptosistem berbasis multivariat menghasilkan tanda tangan pendek, namun kunci yang digunakan untuk pembuatan dan verifikasinya mungkin memerlukan beberapa kilobyte. Kriptosistem kisi, yang didasarkan pada DILITHIUM, sangat cepat, tetapi panjang tanda tangannya adalah 2701 byte dan ukuran kuncinya kira-kira 1500 byte.

Kriptosistem pasca-kuantum memerlukan (a) waktu eksekusi, (b) komputasi, dan (c) sumber daya penyimpanan dalam jumlah besar. Sampai batas tertentu, beberapa skema mengurangi jumlah pesan yang ditandatangani dengan kunci yang sama. Praktik ini menghasilkan pembuatan kunci baru berulang kali dan dedikasi sumber daya komputasi untuk tujuan ini yang dapat digunakan untuk proses blockchain tertentu. Namun demikian, penelitian terkini mengenai sistem kriptografi pasca-kuantum tidak cukup untuk menghasilkan trade-off yang baik antara ukuran kunci dan kinerja skema untuk blockchain. Oleh karena itu, diperlukan pendekatan baru yang akan meminimalkan konsumsi energi sistem kriptografi dan kinerja jaringan blockchain.

Petunjuk Umum

Jaringan terdistribusi yang besar, seperti blockchain, memerlukan pertimbangan yang luar biasa ketika bermigrasi ke kriptografi pasca-kuantum, karena keterbatasan waktu henti dan pembaruan sinkron. Transisi seperti itu tidak hanya memerlukan jaminan performa dan kompatibilitas ke belakang, namun juga peluncuran dan rollback yang lambat. Oleh karena itu, implementasi jaringan blockchain pasca-kuantum memerlukan langkah-langkah berikut:

a. Peluncuran perangkat lunak: Peluncuran perangkat lunak secara perlahan ke semua jaringan sejenis. Migrasi ini harus kompatibel ke belakang, dengan node agar dapat terus menandatangani dan memverifikasi tanda tangan, serta memvalidasi sertifikat X.509 secara klasik hingga berubah ke mode pasca-kuantum.
b. Rollover kunci: Meskipun otoritas sertifikat akan dimodifikasi dengan kunci pasca-kuantum, sertifikat node harus diterbitkan ulang mengikuti metode rollover kunci.
c. Peluncuran kunci PQC yang lambat: Ketika pasangan kunci kunci pasca-kuantum akan dihasilkan, file konfigurasi setiap node milik jaringan harus diperbarui.
d. Langkah terakhir adalah peluncuran kunci pasca kuantum ke rekan klien.

BAB 8
ARSITEKTUR SISTEM MANAJEMEN KEPERCAYAAN IOT

Internet of Things telah memungkinkan interkoneksi miliaran perangkat, yang bekerja sama untuk mendukung sejumlah besar aplikasi dan fitur aplikasi. Dalam konteks ini, jumlah perangkat yang perlu berinteraksi untuk mewujudkan fungsi yang diinginkan telah bertambah secara substansial, dan hal ini menjadikan metode kontrol akses tradisional sulit untuk dikelola dan tidak efektif. Untuk menjawab tantangan ini, kontrol akses berbasis kepercayaan telah muncul, di mana setiap perangkat diberi tingkat kepercayaan, dan tingkat ini dikonsultasikan untuk menentukan apakah akses data dan operasi harus diizinkan atau ditolak. Dalam bab ini, kami mengusulkan pendekatan komputasi kepercayaan di Internet of Things, yang menggabungkan aspek perilaku, status perangkat, dan risiko terkait ke dalam skor kepercayaan komprehensif, yang dapat dikonsultasikan untuk mewujudkan kontrol akses berbasis kepercayaan. Pendekatan yang diusulkan juga mempertimbangkan hubungan kepemilikan perangkat dan hubungan kepercayaan pemilik-ke-pemilik, yang digunakan dalam proses komputasi kepercayaan.

8.1 PENDAHULUAN

Dalam konteks komputasi, pihak-pihak berinteraksi satu sama lain untuk mengakses layanan dan informasi. Secara tradisional, mekanisme kontrol akses digunakan untuk menjaga akses tersebut: mekanisme otentikasi memberikan jaminan yang diperlukan tentang identitas pihak-pihak yang berinteraksi (yaitu, bahwa pemohon layanan/informasi atau server memang benar seperti yang mereka klaim), sedangkan mekanisme otorisasi menegakkan kebijakan akses informasi/layanan, memastikan bahwa hanya klien yang berwenang yang dapat mengakses sumber daya informasi/layanan yang disediakan oleh server. Meskipun pendekatan ini memadai untuk sejumlah kasus penggunaan sistem informasi, dan terutama dalam sistem klien-server di mana sekelompok klien atau kelompok klien yang tertutup berinteraksi dengan sekelompok server terbatas yang diketahui secara apriori, komputasi skala internet modern memerlukan interaksi antara pihak-pihak yang tidak dikenal, dimana masing-masing pihak dapat meminta sekaligus menawarkan layanan dan/atau informasi. Dalam lingkungan seperti ini, sistem kontrol akses tradisional dianggap tidak cukup, karena pihak-pihak yang berinteraksi kemungkinan besar tidak saling mengenal sebelum interaksi dimulai. Dalam hal ini, diperlukan pendekatan berbeda yang memungkinkan pihak-pihak yang berinteraksi untuk memutuskan:

1. Apakah pemohon berhak mengakses layanan/informasi yang diminta dan
2. Apakah penyedia layanan tersebut dapat dipercaya sebagai sumber layanan/informasi tertentu.

Untuk mengatasi permasalahan yang disebutkan di atas, konsep Manajemen Kepercayaan telah diperkenalkan. Para penulis di mendefinisikan manajemen kepercayaan sebagai landasan yang memfasilitasi penegakan kebijakan keamanan dengan memverifikasi tindakan

terhadap kebijakan ini, secara otomatis. Sesuai dengan definisi tersebut, maka pelaksanaan suatu tindakan diperbolehkan jika pihak yang berinteraksi telah memberikan kredensial yang dinilai cukup; jika hal ini terjadi, identitas sebenarnya dari pihak yang berinteraksi tidak perlu diketahui atau diverifikasi. Dengan kata lain, pemeriksaan yang dilakukan hanya perlu memproses dan memverifikasi beberapa representasi simbolis dari tingkat kepercayaan pihak yang meminta, yang kini secara jelas dibedakan dari pihak yang meminta itu sendiri (seseorang atau agen yang bertindak atas nama orang tersebut). Untuk lebih meningkatkan manfaat pendekatan berbasis kepercayaan, presentasi dan validasi kredensial dapat digantikan dengan inspeksi dan penilaian serangkaian properti, yang disaksikan dan divalidasi oleh beberapa pihak yang berinteraksi, sementara sertifikat digital digunakan untuk mewakili properti yang disebutkan di atas dan menjaga validitasnya.

Mengikuti alasan ini, kumpulan awal elemen sistem manajemen kepercayaan yang tercantum direvisi sebagaimana dijelaskan di bawah ini:

1. Kebijakan keamanan, yang terdiri dari sekelompok pernyataan kepercayaan yang dianggap sebagai “kebenaran dasar” dan oleh karena itu dipercaya dalam semua kasus.
2. Properti terkait kepercayaan, yang mewakili karakteristik pihak-pihak yang berkomunikasi yang berkaitan dengan penegakan kebijakan keamanan; biasanya, sifat-sifat tersebut diperiksa sebagai pendahuluan dari aturan-aturan yang mencakup kebijakan keamanan. Kebijakan terkait kepercayaan dilindungi melalui tanda tangan digital atau sarana penting lainnya.
3. Hubungan saling percaya, yaitu jenis khusus kebijakan keamanan.

Meskipun skema yang disajikan di atas secara eksplisit mencantumkan dua pihak yang berinteraksi, yaitu, pemohon layanan/informasi dan server, pembentukan kepercayaan mungkin melibatkan lebih banyak pihak, sehingga menghasilkan model yang sangat terdesentralisasi: pertama, properti yang terkait dengan kepercayaan mungkin (dan biasanya memang demikian) disediakan dan disaksikan oleh pihak ketiga. Kedua, hubungan kepercayaan dapat menunjuk entitas sistem manajemen kepercayaan lainnya yang menjadi penghubung antara sistem manajemen kepercayaan untuk bertukar elemen sistem apa pun yang tercantum di atas (kebijakan keamanan, properti terkait kepercayaan, atau hubungan kepercayaan), termasuk juga penilaian kepercayaan yang dapat dilakukan. diperhitungkan ketika contoh sistem manajemen kepercayaan menilai tingkat kepercayaan pihak yang berinteraksi.

Tingkat kepercayaan dari rekan interaksi dapat dihitung dengan mempertimbangkan semua karakteristik yang dapat diamati: hal ini mencakup (a) karakteristik keamanan dari rekan interaksi, bersama dengan evaluasi penilaian integritas rekan saat ini (kemungkinan kompromi dari firmware, sistem operasi, file sistem; versi patch keamanan; dll.) dan pertahanan keamanan yang digunakan oleh perangkat (firewall; IDS/IPS; dll.) dan (b) karakteristik perilaku rekan interaksi, berkaitan dengan apakah rekan interaksi (i) berfungsi sesuai dengan deskripsi penggunaan yang telah ditentukan sebelumnya dan (ii) menunjukkan perilaku abnormal.

Layanan, informasi, dan sumber daya sebenarnya adalah aset yang memiliki nilai bagi pemiliknya masing-masing dan karenanya memerlukan perlindungan melalui manajemen

kepercayaan atau cara terkait lainnya. Perlindungan bertujuan untuk menjaga aset dari sejumlah ancaman, yang menimbulkan risiko terhadap aset tersebut, dan pada akhirnya dapat menyebabkan penurunan nilainya. Oleh karena itu, proses perlindungan aset harus mencakup penilaian risiko pada setiap interaksi, serta pilihan dan penerapan tindakan pertahanan yang tepat sebagaimana ditentukan oleh hasil penilaian. Hal ini sejalan dengan prosedur yang dijelaskan dalam standar ISO/IEC 27001 untuk mengatasi risiko, yang mencakup dua langkah berikut:

1. penilaian risiko keamanan informasi, yang selanjutnya disempurnakan dalam (i) penetapan dan pemeliharaan kriteria risiko keamanan informasi yang mencakup kriteria penerimaan risiko (ii) identifikasi risiko informasi dan (iii) analisis risiko keamanan informasi dan (iv) evaluasi risiko keamanan informasi dan
2. perlakuan risiko keamanan informasi, dimana (i) pilihan yang sesuai untuk memitigasi risiko keamanan informasi dipilih, setelah mempertimbangkan hasil penilaian risiko, (ii) pengendalian yang tepat untuk realisasi pilihan perlakuan risiko keamanan yang dipilih, juga dengan mempertimbangkan memperhitungkan rasio biaya/manfaat dari penerapan opsi perlakuan risiko keamanan yang dipilih dan (iii) pendekatan perlakuan risiko keamanan informasi divalidasi, setelah meninjau sisa risiko keamanan informasi dan dengan sadar menerima kehadirannya (atau kembali ke langkah memilih yang sesuai). kontrol).

Kepercayaan dan penilaian risiko adalah dua konsep yang terkait erat, mengikuti dasar pemikiran bahwa evaluasi risiko keamanan informasi melibatkan penghitungan kemungkinan terjadinya risiko tersebut, dan hasil penghitungan ini bergantung pada tingkat kepercayaan yang ditetapkan pada sistem yang terbukti menjadi agen ancaman. Dasar pemikiran ini tercermin pada definisi kepercayaan yang ditemukan dalam literatur: “Kepercayaan adalah kesediaan suatu pihak untuk rentan terhadap tindakan pihak lain berdasarkan harapan bahwa pihak lain akan melakukan tindakan tertentu yang penting bagi pihak tersebut. pemberi amanah, terlepas dari kemampuan untuk memantau atau mengendalikan pihak lain tersebut”; pada catatan yang sama, mendefinisikan kepercayaan sebagai “Sikap ekspektasi percaya diri dalam situasi online yang penuh risiko bahwa kerentanan seseorang tidak akan dieksploitasi”. Hal ini membawa kita pada kesimpulan bahwa kepercayaan mengurangi tingkat risiko, berdasarkan keyakinan bahwa sistem yang tepercaya pada akhirnya tidak akan berfungsi sebagai agen ancaman. Secara keseluruhan, penilaian kepercayaan suatu sistem harus dimasukkan sebagai parameter penting dalam penilaian risiko.

Akhirnya, penyerang semakin banyak menggunakan metode serangan yang lebih kompleks yang mencakup jalur serangan multi-tahap dan multi-host, dengan masing-masing jalur mewakili serangkaian eksploitasi yang digunakan oleh penyerang untuk menyusupi jaringan. Untuk mencapai tujuan ini, grafik serangan dapat digunakan untuk melakukan analisis risiko jaringan secara komprehensif, dengan mempertimbangkan hubungan sebab-akibat yang terlibat dalam perubahan status jaringan. Selain itu, kemungkinan eksploitasi hubungan tersebut juga dapat dipertimbangkan.

8.2 DASAR-DASAR MANAJEMEN KEPERCAYAAN

Pada bagian ini kita akan meninjau tiga landasan utama kepercayaan dan manajemen risiko yaitu (a) metode berbasis perilaku, yang berfokus pada interaksi perangkat yang diamati, (b) metode berbasis status, yang berfokus pada aspek keamanan perangkat. dan (c) metode yang berorientasi pada penilaian risiko, dengan fokus pada kuantifikasi risiko yang terkait dengan perangkat dan operasi. Untuk masing-masing dari ketiga landasan tersebut, kami menyajikan metode, alat dan sumber informasi yang dapat digunakan untuk mewujudkan kepercayaan dan manajemen risiko dalam konteks yang relevan.

Aspek Perilaku

Perilaku perangkat dapat dipantau dan digunakan dalam proses penilaian kepercayaan dan risiko. Istilah "perilaku" dalam konteks ini mengacu pada aktivitas yang dapat diamati yang dilakukan oleh perangkat, dan ini terutama mencakup lalu lintas jaringan yang diarahkan ke node lain. Lalu lintas jaringan ini dapat berupa:

- Dibandingkan dengan model perilaku statis yang telah ditentukan sebelumnya yang telah ditentukan untuk perangkat dan menentukan pengoperasian perangkat yang tidak berbahaya. Penyimpangan dari perilaku yang ditentukan kemudian diperlakukan sebagai indikasi perilaku jahat dan menurunkan tingkat kepercayaan, sehingga meningkatkan tingkat risiko. Deskripsi Penggunaan Pabrikan File spesifikasi adalah alat utama di bidang ini.
- Dibandingkan dengan model perilaku perangkat yang dibangun secara dinamis; dalam pendekatan ini, perilaku instance perangkat diprofilkan pada keadaan yang diketahui tidak berbahaya, dan perilaku selanjutnya dibandingkan dengan garis dasar dalam profil. Penyimpangan dari garis dasar ditandai sebagai anomali, sehingga mengurangi tingkat kepercayaan dan meningkatkan risiko terkait. Ketentuan untuk evolusi dinamis dari profil dapat dibuat.
- Dicocokkan dengan serangkaian permintaan berbahaya yang diketahui. Dalam pendekatan ini, lalu lintas jaringan yang berasal dari perangkat dicocokkan dengan database tanda tangan permintaan berbahaya, untuk mengidentifikasi apakah perangkat tersebut merupakan sumber serangan ke perangkat lain; jika demikian, dapat disimpulkan bahwa perangkat tersebut telah disusupi, dan akibatnya penilaian kepercayaan dan risiko pun disesuaikan.

Aspek lain yang dapat dipertimbangkan dalam hal ini adalah mengenai konsekuensi arus informasi yang dapat diamati, dan bukan arus informasi itu sendiri. Berdasarkan sudut pandang ini, informasi yang bocor dari suatu perangkat (misalnya kata sandi pengguna atau data pribadi) merupakan bukti bahwa perangkat tersebut tidak memberikan tingkat keamanan yang memadai (termasuk jika perangkat tersebut mengungkapkan informasi kepada entitas yang tidak dapat dipercaya), dan atas dasar ini tingkat kepercayaan terhadap perangkat ini berkurang.

Pendekatan Berbasis Status

Pendekatan berbasis status terhadap penilaian kepercayaan dan risiko memeriksa keadaan perangkat yang berinteraksi saat ini, terkait dengan aspek keamanannya. Tujuannya adalah untuk menentukan apakah (a) telah terjadi pelanggaran pada perangkat, yang

mengakibatkan gangguan pada perangkat lunak atau konfigurasinya, dan (b) seberapa rentan perangkat terhadap pelanggaran, dalam arti bahwa kerentanan yang diketahui belum ditangani secara tepat dan tepat waktu. melalui pemasangan patch. Kontrol keamanan yang diterapkan pada perangkat juga diperhitungkan karena mengontrol tingkat kerentanan perangkat. Secara lebih rinci, aspek-aspek berikut dipertimbangkan dalam pendekatan berbasis status:

- Apakah file penting telah dirusak? Validasi yang relevan mencakup:
  - firmware perangkat;
  - sistem operasi dan perangkat lunak lainnya;
  - file konfigurasi sistem/jaringan;
  - audit dan log peristiwa.
- Apakah patch terbaru sudah diinstal? Patch yang hilang akan meningkatkan tingkat kerentanan perangkat dan karenanya menurunkan tingkat kepercayaan.
- Kontrol keamanan apa yang berlaku untuk melindungi perangkat?

Penilaian Risiko

Saat ini, keamanan dan kepercayaan terhadap sistem digital telah menjadi perhatian yang semakin besar karena teknologi memainkan peran yang semakin penting dalam masyarakat kita. Manifestasi penting dari aspek ini adalah banyaknya serangan yang dilakukan terhadap organisasi, badan pemerintah, dan masyarakat. Mitigasi serangan-serangan tersebut biasanya memerlukan penilaian risiko keamanan siber yang membantu dalam identifikasi aset-aset penting, ancaman-ancaman yang dihadapi, kemungkinan keberhasilan serangan, dan potensi konsekuensinya. Pendekatan ini, bersama dengan penentuan prioritas risiko yang teridentifikasi, adalah satu-satunya cara untuk mengidentifikasi tindakan yang tepat untuk diterapkan.

Penilaian risiko mencakup identifikasi, estimasi, dan penentuan prioritas risiko yang terkait dengan aset dan operasi organisasi. Kegiatan ini memainkan peran penting dalam konteks manajemen risiko, dengan memberikan dasar bagi penanganan risiko yang teridentifikasi. Pendekatan penanganan yang mungkin dilakukan adalah: penerimaan risiko ketika tingkat risiko dianggap dapat diterima setelah mempertimbangkan kebijakan manajemen risiko organisasi; mitigasi risiko – melalui kontrol keamanan; pengalihan risiko dengan mendelegasikan akuntabilitas kepada perusahaan asuransi; atau penghindaran risiko melalui penghapusan aset terkait. Beberapa konsep inti penilaian risiko termasuk namun tidak terbatas pada: aset, kerentanan, ancaman, kemungkinan serangan, dan dampak.

Aset dapat berupa barang apa pun yang memiliki nilai bagi organisasi, dan ditandai dengan beberapa properti. Aset dapat diklasifikasikan menjadi berwujud (misalnya perangkat keras) atau tidak berwujud (misalnya citra publik suatu bisnis); selain itu, aset dapat menjadi bagian konstituen dari suatu sistem atau menjadi keseluruhan sistem. Kerentanan adalah properti aset yang dapat dieksploitasi, dan dapat didefinisikan sebagai kelemahan aset itu sendiri atau kelemahan pengendalian yang melindunginya. Ancaman adalah tindakan yang dapat membahayakan suatu aset, dan biasanya dikaitkan dengan eksploitasi kerentanan. Ancaman dapat terjadi secara sengaja (misalnya, menerapkan serangan brute force untuk menemukan kata sandi administrator) atau tidak sengaja (misalnya, menghapus file melalui

tindakan yang salah). Konsep-konsep ini digabungkan dalam istilah risiko siber (siber-risk) yang mendefinisikan kemungkinan munculnya ancaman (serangan) yang berhasil dan konsekuensinya terhadap aset yang terlibat.

8.3 PERMODELAN SISTEM MANAJEMEN KEPERCAYAAN

Model manajemen kepercayaan menargetkan untuk mengaktifkan node yang berpartisipasi dalam sistem manajemen kepercayaan untuk menentukan nilai metrik kepercayaan untuk node lain dalam sistem. Pendekatan bagaimana model kepercayaan mendekati komputasi kepercayaan bervariasi dalam berbagai aspek, termasuk input yang digunakan untuk menghitung kepercayaan, cara nilai kepercayaan diperbarui, konsensus yang dicari untuk perhitungan nilai kepercayaan, skala pengukuran kepercayaan, ketahanannya terhadap serangan dan sebagainya. Selain itu, model manajemen kepercayaan bervariasi sehubungan dengan paradigma arsitektur yang mereka ikuti, yaitu cara komponen yang berpartisipasi dalam sistem manajemen kepercayaan diterapkan di jaringan target, hubungan antara komponen dan arus informasi. Pada subbagian berikut ini kami mensurvei model kepercayaan yang ada dan arsitekturnya, serta mengomentari kelebihan dan kekurangannya.

Tinjauan Model Kepercayaan yang Ada

Bagian ini mengulas model kepercayaan yang telah diusulkan oleh literatur untuk mencoba menemukan metode perhitungan kepercayaan yang efektif dan efisien. Dalam jaringan berorientasi layanan, perangkat IoT yang bertindak sebagai peminta layanan memerlukan cara untuk mengevaluasi rekan-rekannya yang mana yang dapat dipercaya untuk menyediakan layanan yang diminta, sambil mempertimbangkan kebutuhan energi untuk melakukan evaluasi tersebut. Inilah tantangan yang ingin dipecahkan oleh model manajemen kepercayaan. Kami menyajikan model manajemen kepercayaan seperti yang terlihat dalam literatur dan kami mengkategorikan setiap model berdasarkan dimensi kepercayaan, ketahanan terhadap serangan tertentu, dan karakteristik kualitatif.

Dimensi kepercayaan

Model kepercayaan terdiri dari beberapa dimensi kepercayaan yang dapat bervariasi tergantung pada pendekatan yang diikuti. Pada bagian ini kami menyajikan lima dimensi kepercayaan yang paling penting, yaitu komposisi kepercayaan, penyebaran kepercayaan, agregasi kepercayaan, pembaruan kepercayaan, dan pembentukan kepercayaan.

Komposisi kepercayaan. Mengacu pada komponen yang diperhitungkan oleh model tersebut. Komponennya adalah Quality of Service (QoS) dan Social trust.

- Kepercayaan QoS mengacu pada tingkat kepercayaan yang diberikan pada sebuah node berdasarkan evaluasi kompetensinya dalam memberikan layanan yang diminta. Ini dianggap sebagai evaluasi kepercayaan yang “objektif”. Untuk menghitung kepercayaan QoS, model menggunakan berbagai properti kepercayaan termasuk kompetensi, kerja sama, keandalan, penyelesaian tugas, dll.
- Kepercayaan sosial mengacu pada hubungan sosial antara pemilik perangkat IoT. Kepercayaan sosial digunakan dalam sistem di mana perangkat IoT tidak harus dievaluasi hanya berdasarkan QoS tetapi juga berdasarkan sosial, yaitu komitmen dan kemauan

perangkat untuk bekerja sama. Bisa juga karena kesamaan perangkat. Sifat kepercayaan sosial meliputi konektivitas, kejujuran, tidak mementingkan diri sendiri, dll.

Penyebaran kepercayaan. Mengacu pada cara nilai kepercayaan disebarluaskan antar entitas. Secara umum pendekatannya ada dua yaitu terdistribusi dan terpusat.

- Dalam penyebaran kepercayaan terdistribusi, setiap perangkat bertindak secara mandiri dengan menyimpan nilai kepercayaan dan menyebarkannya sebagai rekomendasi ke perangkat lain sesuai kebutuhan.
- Dalam penyebaran kepercayaan terpusat, terdapat entitas pusat yang bertanggung jawab untuk menyimpan nilai kepercayaan dari jaringan yang dipantau dan menyebarkannya sesuai kebutuhan.

Agregasi kepercayaan. Mengacu pada teknik komputasi yang digunakan suatu model untuk menggabungkan kepercayaan yang diperoleh dari observasi langsung dengan kepercayaan tidak langsung yang berasal dari rekomendasi. Teknik agregasi utama meliputi penjumlahan tertimbang, inferensi Bayesian, dan logika fuzzy.

- Jumlah tertimbang adalah teknik di mana bobot diberikan pada nilai-nilai yang berpartisipasi baik secara statis maupun dinamis. Misalnya, satu model dapat menggunakan properti kepercayaan, misalnya kompetensi, untuk menetapkan bobot yang lebih tinggi atau lebih rendah.
- Inferensi Bayesian menganggap kepercayaan sebagai variabel acak yang mengikuti distribusi probabilitas. Ini adalah model yang sederhana dan masuk akal secara statistik.
- Logika fuzzy menggunakan penalaran perkiraan yang berarti tidak menggunakan variabel evaluasi biner melainkan variabel yang nilainya berkisar antara 0 dan 1 misalnya, atau bahkan batasan linguistik seperti Tinggi dan Rendah yang diterjemahkan menggunakan fungsi keanggotaan.

Pembaruan kepercayaan. Menjelaskan kapan nilai kepercayaan diperbarui. Ada dua pendekatan: berdasarkan peristiwa dan berdasarkan waktu.

- Berbasis peristiwa (event-driven) adalah pendekatan di mana nilai-nilai kepercayaan diperbarui ketika suatu peristiwa terjadi.
- Berbasis waktu adalah pendekatan di mana nilai-nilai kepercayaan diperbarui secara berkala.

Pembentukan kepercayaan. Mengacu pada bagaimana keseluruhan kepercayaan terbentuk dari properti kepercayaan yang dipertimbangkan. Trust dapat dibentuk dengan mempertimbangkan hanya satu properti trust (Single-trust) atau banyak properti (Multi-trust).

- Kepercayaan tunggal adalah ketika hanya satu properti yang dipertimbangkan ketika menghitung kepercayaan dan biasanya merupakan properti QoS. Pendekatan ini dianggap sebagai pendekatan yang sempit karena kepercayaan bersifat multidimensi, namun berguna dalam kasus-kasus dengan sumber daya yang terbatas.
- Multi-kepercayaan adalah pendekatan multi-dimensi dalam menghitung kepercayaan, karena pendekatan ini menggunakan lebih dari satu properti kepercayaan untuk membentuk evaluasi kepercayaan keseluruhan dari suatu perangkat.

Model Manajemen Kepercayaan

Pada bagian ini kami mensurvei berbagai model kepercayaan yang diusulkan dalam literatur. Untuk setiap model, pendekatan yang diadopsi untuk komputasi kepercayaan disajikan, dengan gambaran umum diberikan pada Tabel 8.1.

Tabel 8.1. Ikhtisar Model Kepercayaan Yang Berbeda.

Models	Composition		Propagasi		Agregasi			Update	Formasi	
	QoS	Sosial	Distrib	Central	Weight	Fuzzy	Bayes	E/T	Sin	Mul
Bao, 2012; Chen, 2016a; Bao, 2013, Chen 2016b; Chen, 2011;	X	X	X		X			E/T		X
Mahalle, 2013; Prajapati, 2013	X	X	X		X		X	E/T	X	
Said, 2013	X		X		X	X		T	X	
Mendoza, 2015	X	X	X		X	X		T	X	
Namal, 2015	X		X		X			E	X	
Khan, 2017	X			X	X			T	X	
Djedjig, 2017b	X		X	X	X			E		X
Medjek, 2017	X			X	X			E/T	X	
Nitti, 2014	X			X	X			E	X	
Wu, 2017	X		X	X	X			T	X	
Mahmud, 2018	X		X					T	X	
Arabsorkhi, 2016	X		X		X			E	X	
Yuan, 2018		X	X	X	X	X		E		X

Bao, 2012. Model ini diusulkan untuk sistem IoT sosial (SIoT) berdasarkan Community of Interest (CoI). Sebuah perangkat memiliki satu pemilik dan satu pemilik dapat memiliki beberapa perangkat. Pemiliknya memesan daftar dengan teman-temannya. Node-node yang menjadi bagian dari komunitas serupa mempunyai peluang lebih besar untuk memiliki minat dan kemampuan serupa. Para penulis mempertimbangkan komposisi QoS dan kepercayaan sosial dan mendefinisikan tiga sifat kepercayaan: kepentingan komunitas (Sosial), kegotongroyongan (QoS), dan kejujuran (QoS); pembaca yang berminat dapat merujuk ke (Tabel 8.1) untuk rincian lebih lanjut. Nilai kepercayaan merupakan bilangan real pada rentang dimana 1 menunjukkan kepercayaan penuh, 0,5 ketidaktahuan, dan 0 ketidakpercayaan. Nilai kepercayaan dihitung dengan memperhatikan pengamatan langsung; jika pengamatan langsung seperti itu tidak tersedia, nilai kepercayaan dapat bersumber dari rekomendasi. Agregasi kepercayaan dilakukan menggunakan jumlah tertimbang, sedangkan model mengikuti arsitektur terdistribusi. Perlu disebutkan bahwa bobot yang digunakan untuk pengalaman masa lalu dapat disesuaikan secara dinamis ketika bukti baru muncul untuk menyeimbangkan kembali tingkat konvergensi kepercayaan dan tingkat fluktuasi kepercayaan. Dalam hasil simulasi, efek perubahan bobot diamati, namun cara untuk menyesuaikannya secara dinamis tidak disebutkan.

Chen, 2016a. Model ini sangat mirip dengan Bao, 2012. Perbedaan utama meliputi: 1. Pendekatan umum untuk penghitungan kepercayaan secara keseluruhan tidak dibahas. Sebaliknya, perhitungan kepercayaan secara keseluruhan untuk skenario tertentu akan dibahas. 2. Daftar teman (node) yang dipertukarkan antar node pada saat interaksi dienkripsi

dengan fungsi satu arah sehingga node hanya dapat mengidentifikasi teman umum. Hashing hemat biaya. 3. Model diuji dalam dua skenario dunia nyata, yaitu “Smart City Air Pollution Detection” dan “Augmented Map Travel Assistance”.

Bao, 2013. Model ini diusulkan untuk sistem IoT sosial (SIoT) berdasarkan konsep Community of Interest (CoI). Sebuah perangkat hanya dapat memiliki satu pemilik dan satu pemilik dapat memiliki beberapa perangkat. Pemilik memelihara daftar teman pribadi. Node-node yang merupakan bagian dari komunitas serupa mempunyai kemungkinan lebih tinggi untuk berbagi minat dan kemampuan serupa. Penulis mempertimbangkan komposisi QoS dan kepercayaan sosial. Nilai kepercayaan merupakan bilangan real pada rentang [0,1] dimana 1 menunjukkan kepercayaan penuh, 0,5 ketidaktahuan, dan 0 ketidakpercayaan. Sifat kepercayaan yang dipertimbangkan adalah kejujuran, kerjasama dan kepentingan masyarakat;. Penyebaran kepercayaan didistribusikan. Skema agregasi kepercayaan model ini menggunakan inferensi Bayesian untuk menghitung kepercayaan langsung, dan jumlah tertimbang digunakan untuk menggabungkan rekomendasi menjadi kepercayaan tidak langsung. Aspek penting dari model ini adalah pengenalan strategi baru untuk manajemen penyimpanan yang dapat diterapkan secara efisien pada sistem IoT skala besar.

Chen, 2016b. Model ini merupakan perpanjangan dari Bao, 2013. Perluasannya meliputi: 1. Dalam evaluasi pemberi rekomendasi, diperkenalkan dua sifat tambahan, yaitu persahabatan dan kontak sosial. Dalam agregasi kepercayaan, ini menggabungkan kepercayaan langsung dan tidak langsung untuk membentuk kepercayaan keseluruhan. 3. Simulasinya mengungguli EigenTrust dan PeerTrust dalam konvergensi kepercayaan, akurasi, dan ketahanan serangan.

Chen, 2011. Model ini hanya mempertimbangkan metrik QoS untuk mengevaluasi kepercayaan, yaitu rasio penerusan paket ujung ke ujung (EPFR), konsumsi energi (EC), dan rasio pengiriman paket (PDR). Setiap node menyimpan tabel transaksi penerusan data yang mencakup nilai: (1) Sumber: node yang mengevaluasi kepercayaan dan evaluasi, (2) Tujuan: node tujuan yang dievaluasi, (3) RFi,j: waktu keberhasilan transaksi yang dilakukan antara node i dan j, dan (4) Fi,j : transaksi positif. Ini mengikuti skema terdistribusi dalam hal penyebaran kepercayaan. Dalam agregasi kepercayaan, model kepercayaan fuzzy digunakan, dan kepercayaan keseluruhan dibentuk menggunakan jumlah kepercayaan langsung dan tidak langsung yang tertimbang berdasarkan rekomendasi. Kepercayaan langsung dihitung dengan terlebih dahulu menggabungkan metrik QoS yang disebutkan di atas, kemudian memberi label hasilnya sebagai pengalaman positif atau negatif berdasarkan ambang batas, dan kemudian fungsi keanggotaan fuzzy menghitung kepercayaan langsung berdasarkan jumlah pengalaman positif dan negatif. Selain itu, model ini diuji pada simulasi dan mencapai kinerja yang lebih baik dari BTRM-WSN dan DRBTS dalam rasio pengiriman paket dan probabilitas deteksi node jahat.

Mahalle, 2013. Model ini mempertimbangkan tiga metrik QoS: peringkat Pengalaman (EX), Pengetahuan (KN) dan Rekomendasi (RC). Ini mengikuti skema terdistribusi, karena setiap perangkat mempertimbangkan peringkat tetangganya untuk menghitung skor kepercayaan. Kepercayaan dihitung secara berkala menggunakan aturan fuzzy tipe Mamdani (mewakili hubungan If-Then antara variabel masukannya) dari nilai linguistik ketiga metrik

tersebut di atas. Skor kepercayaan (sebagai nilai linguistik) kemudian dipetakan ke serangkaian izin kontrol akses. Pengalaman (EX) adalah jumlah tertimbang dari sejumlah peringkat interaksi sebelumnya antara dua perangkat (+1 untuk interaksi yang berhasil dan −1 untuk interaksi yang gagal), Pengetahuan (KN) adalah jumlah tertimbang dari peringkat pengetahuan langsung dan tidak langsung , dan Rekomendasi (RC) adalah jumlah tertimbang peringkat RC dari sejumlah perangkat tentang perangkat yang dapat dipercaya. Ketiga metrik tersebut dipetakan ke variabel linguistiknya menggunakan rentang numerik (tajam) yang telah ditentukan sebelumnya. Model ini diuji dalam lingkungan simulasi sensor nirkabel dengan komunikasi antar sensor dikendalikan oleh peringkat kepercayaan, sehingga menghasilkan komunikasi yang lebih hemat energi, dan terbukti dapat diskalakan.

Prajapati, 2013. Model ini mengusulkan pembentukan nilai kepercayaan berdasarkan seberapa memuaskan respons node terhadap permintaan layanan spesifik yang diberikan padanya: kuantifikasi kepuasan ini digabungkan untuk membentuk nilai Direct Trust. Jika nilai Direct Trust tersedia, maka nilai ini digunakan; jika tidak ada nilai Kepercayaan Langsung, nilai Kepercayaan yang Direkomendasikan dihitung dengan mengambil dan menggabungkan penilaian kepercayaan dari node rekan lainnya. Jika node target bergabung dengan cloud untuk pertama kalinya, dan oleh karena itu nilai Direct Trust maupun Recommended Trust tidak tersedia, maka Ignorance Value yang telah ditentukan sebelumnya akan digunakan. Kepercayaan Langsung didefinisikan sebagai jumlah tertimbang dari peringkat kepuasan layanan dari waktu ke waktu (dengan bobot yang menurun seiring waktu, sehingga mendukung peringkat yang lebih baru). Kepercayaan yang Direkomendasikan didefinisikan sebagai jumlah tertimbang dari nilai Kepercayaan Langsung dari node lainnya. Bobot yang digunakan dalam perhitungan setiap nilai Direct Trust didasarkan pada dua faktor. Yang pertama adalah jumlah interaksi positif antara dua node (trustor dan trustee). Yang kedua adalah Tingkat Kepuasan yang bergantung pada faktor-faktor seperti waktu pemulihan, kinerja beban maksimum, konektivitas dan ketersediaan sebagaimana ditentukan dalam perjanjian layanan.

Semua node memelihara Tabel Kepercayaan Langsung dan Tabel Kepercayaan yang Direkomendasikan yang berisi nilai kepercayaan masing-masing dengan kedua tabel diperbarui secara berkala. Model ini mengikuti model terdistribusi seperti dalam kasus Kepercayaan yang Direkomendasikan, nilai kepercayaan dari semua node jaringan dipertimbangkan.

Said, 2013. Model ini mempertimbangkan peringkat yang diberikan pada node dan layanan tertentu pada waktu tertentu dan juga mempertimbangkan statusnya (misalnya usia, kapasitas sumber daya, dll.) Model ini mengikuti skema terpusat dengan node Trust Manager (TM) yang menerima laporan dari jaringan dan menghitung nilai kepercayaan sesuai permintaan. Hal ini menyebabkan berkurangnya overhead komunikasi – karena nilai kepercayaan dihitung dan dikirimkan sesuai permintaan, penggunaan memori yang lebih sedikit untuk setiap node – karena nilai kepercayaan dapat diminta lagi dari TM, sehingga hemat energi. Model ini beroperasi dalam lima fase: (1) TM menerima laporan dari node jaringan, (2) TM menghitung nilai kepercayaan dari sejumlah kandidat node dan mengirimkan daftar node yang dapat dipercaya ke node yang meminta, (3) node yang meminta menerima

daftar tersebut dan berinteraksi dengan node tepercaya yang dipilih, (4) node yang meminta menilai layanan yang disediakan oleh node tepercaya yang dipilih dan mengirimkan peringkat tersebut ke TM, dan terakhir (5) TM memperbarui nilai kepercayaannya sesuai dengan itu. Kepercayaan dihitung sebagai rata-rata tertimbang dari skor yang diberikan pada sebuah node dengan mempertimbangkan reputasi node yang memberikan skor, kesamaan kontekstual dari semua laporan mengenai node yang sama, dan usia laporan – menyukai laporan terbaru. Kesamaan kontekstual dihitung dari kemampuan node antara dua node – untuk menemukan node yang serupa, dan/atau dari perbedaan sumber daya yang diperlukan antara dua layanan untuk menemukan node yang mampu menjalankan layanan serupa. Awalnya semua node jaringan dianggap dapat dipercaya.

Mendoza, 2015. Model ini merupakan versi terdistribusi dari model yang dikemukakan oleh Saied et al. Perlu dicatat bahwa skema terpusat mungkin tidak cocok untuk sistem IoT karena instalasi server dan biaya server mungkin mahal. Skema pemeringkatan model ini menentukan peringkat untuk node dan layanan tertentu. Operasi model ini terdiri dari tiga fase: (1) node mengumumkan kehadiran mereka kepada tetangganya dan memelihara daftar tetangganya, (2) node meminta layanan dari tetangganya dan menilai interaksi secara positif atau negatif, dan (3) node menghitung dan menyimpan kepercayaan. nilai-nilai bagi tetangga mereka, berdasarkan interaksi ini. Peringkat respons didefinisikan sebagai nilai tetap dari layanan yang diberikan yang ditimbang dengan faktor penyesuaian, dengan peringkat respons negatif sama dengan dua kali peringkat respons positif. Nilai layanan yang diberikan sebanding dengan kebutuhan pemrosesan layanan, semakin banyak daya pemrosesan atau energi yang diperlukan untuk menjalankan suatu layanan, semakin tinggi nilai layanannya. Nilai kepercayaan sebuah node dihitung sebagai jumlah dari semua peringkat interaksi. Model tersebut telah diuji terhadap Serangan On-Off (OOA) dan tercatat bahwa sejumlah besar tetangga dapat menyebabkan penundaan dalam penetapan skor ketidakpercayaan maksimum ke node jahat.

Namal, 2015. Model ini mempertimbangkan empat parameter: ketersediaan sumber daya bagi penggunanya, keandalan informasi yang dihasilkan, ketidakteraturan waktu respons, dan kapasitas. Ini mengikuti skema terpusat dengan modul Trust Manager (TM), yang dihosting di cloud, menerima data yang disaring dari Trust Agents (TA) yang didistribusikan di jaringan yang pada gilirannya menerima data mentah dan memantau keadaan node jaringan. TM mengimplementasikan loop kontrol umpan balik Monitor, Analyze, Plan, Execute, Knowledge (MAPE-K) dan menghitung kepercayaan menggunakan jumlah tertimbang dari parameter kepercayaan untuk semua parameter yang dipertimbangkan. Parameter kepercayaan juga merupakan jumlah tertimbang dari nilai saat ini dan nilai sebelumnya yang dihitung. Model ini menunjukkan keunggulan dalam: ketersediaan dan aksesibilitas – karena TMS dihosting di cloud dan dapat diakses dari internet, skalabilitas – karena TMS menggunakan TA yang memfilter data mentah, dan fleksibilitas – karena TA dapat diterapkan dengan cara yang fleksibel .

Khan, 2017. Model ini mempertimbangkan peringkat yang diberikan pada sebuah simpul oleh tetangganya, peringkat ini merupakan kombinasi dari tiga variabel: keyakinan, ketidakpercayaan, dan ketidakpastian – sebagaimana didefinisikan dalam Logika Subjektif

Jøsang. Model ini diusulkan sebagai bagian dari perpanjangan protokol perutean RPL yang memanfaatkan model yang diusulkan untuk mengisolasi node jahat. Ini mengikuti skema terpusat dengan node pusat (misalnya, router perbatasan RPL atau cluster-head) menghitung nilai kepercayaan untuk semua node jaringan dan memutuskan untuk mengisolasi node berbahaya. Setiap node dalam jaringan diasumsikan mampu mendeteksi dan menilai kinerja node tetangganya; masing-masing dari ketiga variabel tersebut didefinisikan sebagai berikut: keyakinan adalah jumlah interaksi positif dibagi jumlah total interaksi & konstanta k, ketidakpercayaan didefinisikan dengan cara yang sama tetapi jumlah interaksi negatif yang digunakan sebagai pengganti interaksi positif, dan ketidakpastian juga didefinisikan kesamaan tetapi dengan konstanta k yang digunakan sebagai pengganti jumlah interaksi positif/negatif. Node pusat menghitung nilai kepercayaan setiap node jaringan dengan kombinasi nilai kepercayaan mengenai node yang akan dipercaya dan menggunakan ambang batas, node pusat mengisolasi node berbahaya dari jaringan.

Djedjig, 2017b. Model ini mempertimbangkan dua parameter QoS: keegoisan dan energi, dan satu parameter sosial: kejujuran sebagai peringkat yang diberikan tentang sebuah node dari tetangganya. Model ini merupakan perpanjangan yang diusulkan dari protokol routing RPL, seperti dalam Khan et al. Untuk mengisolasi node berbahaya. Ini mengikuti skema terdistribusi dengan setiap node menghitung nilai kepercayaan dari tetangga satu hopnya sambil juga mempertimbangkan nilai kepercayaan dari tetangga satu hopnya. Perhitungan kepercayaan dilakukan sebagai berikut: (1) setiap node menghitung nilai kepercayaan langsung dari tetangga satu lompatannya sebagai jumlah tertimbang dari metrik kejujuran, energi, dan tidak mementingkan diri sendiri (definisinya tidak dibahas secara rinci) dengan setiap metrik menjadi metriknya. jumlah tertimbang dari nilai metrik saat ini dan nilai metrik sebelumnya, (2) setiap node menerima nilai kepercayaan langsung yang dihitung oleh tetangga satu lompatannya mengenai node yang akan diberi peringkat, dan (3) kepercayaan tidak langsung kemudian dihitung oleh setiap node sebagai rata-rata kepercayaan langsung yang dihitung oleh node itu sendiri dan tetangganya. Semua node diasumsikan dilengkapi dengan chip Trusted Platform Module (TPM).

Medjek, 2017. Model ini didasarkan pada yang dikemukakan oleh Djedjig dkk. dengan perbedaan dalam metrik yang dipertimbangkan: kejujuran, energi, dan mobilitas. Perbedaan utamanya adalah arsitektur jaringan karena model ini berlaku untuk jaringan RPL yang terdiri dari Backbone Router (BR) yang menggabungkan beberapa jaringan 6LoWPAN, masing-masing terdiri dari 6LoWPAN Border Router (6BR) yang terhubung ke BR dan node jaringan lainnya. Model ini mengikuti skema terdistribusi dengan masing-masing node jaringan menghitung kepercayaan dari tetangga satu hopnya, seperti pada [36], dengan langkah-langkah tambahan untuk memberitahukan 6BR-nya jika sebuah node ditemukan tidak dapat dipercaya dan dengan 6BR pada gilirannya memberitahukan node tersebut. BR dari node jahat. Semua node diasumsikan dilengkapi dengan Trusted Platform Module (TPM) dan semua node terdaftar di BR pada waktu instalasi, dengan setiap node memiliki ID unik yang ditetapkan oleh BR. Beberapa daftar dikelola oleh berbagai node jaringan; BR menyimpan dua daftar: satu dari node yang berpotensi berbahaya dan satu dari semua node beserta statusnya; 6BR menyimpan tiga daftar: satu dari semua node area 6BR, satu dari semua node

seluler, dan satu dari node yang berpotensi berbahaya; akhirnya node yang tersisa juga menyimpan tiga daftar: satu node yang berpotensi berbahaya, satu node yang mencurigakan, dan salinan daftar node seluler dari 6BR. Tiga modul beroperasi pada berbagai node jaringan: IdentityMod mengontrol akses ke jaringan dan memastikan bahwa setiap node memiliki ID unik, MobilityMod memastikan bahwa BR dan 6BR mengetahui node seluler dan statusnya, dan IDSMod bertanggung jawab atas serangan deteksi dan mitigasi. Kepercayaan dihitung dengan cara yang mirip dengan dengan nilai metrik kejujuran yang disediakan oleh IDSMod dan nilai metrik mobilitas yang disediakan oleh MobilityMod; ketiga metrik tersebut tidak dibahas secara rinci.

Nitti, 2014. Karya ini mengusulkan dua model, yaitu model "subjektif" dan model "objektif". Model ini mempertimbangkan parameter berikut: (i) kredibilitas node, (ii) peringkat layanan, (iii) faktor transaksi – mengidentifikasi transaksi mana yang penting untuk menghindari peningkatan tingkat kepercayaan hanya dengan banyaknya transaksi kecil, (iv) jumlah transaksi per node – untuk mendeteksi kelainan dalam jumlah transaksi pada node tertentu, (v) kapasitas komputasi – node dengan kemampuan komputasi yang lebih tinggi dapat menimbulkan lebih banyak kerusakan jika mereka berbahaya, (vi) gagasan sentralitas – sebuah node berperan lebih besar peran sentral jika terlibat dalam banyak koneksi atau transaksi dalam jaringan, dan (vii) faktor hubungan – dengan mempertimbangkan jenis hubungan dua node.

Model subjektif mengikuti skema terdistribusi di mana setiap node menyimpan informasi yang diperlukan untuk menghitung nilai kepercayaan secara lokal. Ada dua situasi yang dibahas berkaitan dengan hubungan sosial antar node: ketika node pemeringkat memiliki hubungan sosial dengan node yang diberi peringkat dan ketika kedua node tidak memiliki hubungan sosial langsung. Dalam situasi pertama, kepercayaan bergantung pada: pada sentralitas node yang diberi peringkat dalam kaitannya dengan node yang diberi peringkat – berdasarkan jumlah teman bersama dari semua node yang bertetangga, pengalaman langsung dari node yang diberi peringkat – selanjutnya didefinisikan sebagai jumlah tertimbang dari keduanya. pendapat jangka pendek dan jangka panjang, dan pengalaman tidak langsung dari teman-teman simpul pemeringkat – didefinisikan sebagai rata-rata tertimbang dari nilai kepercayaan yang diberikan kepada simpul yang diberi peringkat oleh teman-teman simpul pemeringkat, yang ditimbang berdasarkan kredibilitas mereka. Dalam situasi kedua, kepercayaan bergantung: pada opini dari rantai pertemanan yang menghubungkan dua titik, sekali lagi ditimbang oleh kredibilitas mereka. Umumnya, setelah setiap transaksi, peringkat (positif/negatif) diberikan kepada node yang menyediakan layanan dan kepada node yang pendapatnya dipertimbangkan dalam menghitung nilai kepercayaan. Peringkat rekomendasi negatif diberikan kepada node jahat dan node di lingkungannya, sehingga semakin mengisolasi node jahat dan pengaruhnya.

Model obyektif mengikuti skema yang lebih terpusat di mana setiap node melaporkan umpan baliknya ke node khusus, yang disebut sebagai Pre-Trusted Objects (PTO), yang bertanggung jawab semata-mata untuk memelihara sistem penyimpanan terdistribusi, dalam hal ini Distributed Hash Table (DHT) dan lebih khusus lagi yang mengikuti arsitektur Chord. Kepercayaan dihitung dengan cara yang sama seperti pada model subjektif; sentralitas node

didefinisikan sebagai jumlah total transaksi yang dilakukan oleh node untuk menyediakan layanan dibagi dengan jumlah total transaksi yang dilakukan untuk menyediakan atau meminta layanan, dan opini jangka pendek dan jangka panjang mempertimbangkan peringkat dari node tersebut. setiap node jaringan diberi bobot berdasarkan kredibilitasnya. Node dengan sedikit hubungan sosial, kemampuan komputasi tinggi, dan node yang terlibat dalam sejumlah besar transaksi di antara mereka diberi kredibilitas rendah, karena mereka lebih cenderung menjadi jahat.

Wu, 2017. Model sistem terdiri dari empat entitas dengan tiga hubungan kepercayaan di antara mereka. Empat entitas didefinisikan: tag RFID, pembaca RFID, pusat otentikasi dan satu pusat administrasi, dengan tiga yang pertama dikelompokkan dalam domain. Sebuah domain memiliki beberapa pembaca RFID yang terhubung dengan pusat otentikasi domain yang memberi wewenang kepada pembaca untuk berinteraksi dengan tag RFID, dan pusat otentikasi domain terhubung dengan pusat administrasi. Hubungan kepercayaan model sistem ini didefinisikan sebagai: kepercayaan intra-domain – hubungan kepercayaan antara tag RFID dan pembaca domain yang sama, kepercayaan antar-domain – hubungan kepercayaan antara pusat otentikasi, dan kepercayaan lintas-domain – hubungan kepercayaan antara tag RFID dan pembaca yang berasal dari domain berbeda.

Model manajemen kepercayaan terdiri dari dua lapisan: lapisan kepercayaan pusat otentikasi – sistem manajemen kepercayaan terpusat yang mengelola kepercayaan pusat otentikasi, dan lapisan kepercayaan pembaca – dua skema manajemen kepercayaan yang diusulkan yang mengelola kepercayaan pembaca RFID. Tag RFID selalu dianggap dapat dipercaya.

Skema lapisan manajemen kepercayaan pembaca pertama yang diusulkan menggunakan teori bukti Dempster-Shafer dan terdiri dari empat langkah: (1) interaksi pembaca RFID dicatat oleh tetangganya, (2) tetangga menghitung nilai kepercayaan lokal yang kemudian ditransmisikan ke pusat autentikasi, (3) pusat autentikasi menghitung kepercayaan global pembaca RFID dengan menggunakan aturan pengetahuan Dempster, dan terakhir (4) jika pembaca RFID berbahaya atau tidak berfungsi, pusat administrasi akan diberitahu. Kemungkinan peristiwa interaksi pembaca RFID diidentifikasi dan ditandai sebagai: perilaku berbahaya, perilaku tidak berfungsi, dan perilaku normal oleh pembaca RFID tetangga, masing-masing menghitung jumlah peristiwa dalam jangka waktu tertentu. Dengan menggunakan jumlah kejadian yang terekam, pembaca RFID di dekatnya dapat menghitung nilai kepercayaan lokal untuk setiap jenis kejadian interaksi sebagai: jumlah kejadian yang ditandai sebagai berbahaya/tidak berfungsi/normal dibagi dengan jumlah total kejadian yang terekam. Nilai akhir dari nilai kepercayaan lokal kemudian dipilih dari nilai kepercayaan lokal spesifik peristiwa menggunakan ambang batas. Pusat otentikasi menghitung kepercayaan global pembaca RFID dengan menggabungkan skor kepercayaan lokal spesifik peristiwa yang dihitung oleh pembaca RFID tetangga dan kemudian memilih skor spesifik peristiwa terintegrasi akhir menggunakan ambang batas.

Skema lapisan manajemen kepercayaan pembaca kedua yang diusulkan mempertimbangkan fakta bahwa kejadian mungkin tidak terdeteksi oleh tetangga pembaca RFID dan dengan demikian skema lapisan manajemen kepercayaan pembaca pertama

mungkin tidak dapat diterapkan pada situasi tertentu. Setiap tag RFID menyimpan catatan interaksi terakhir dengan pembaca RFID, lebih khusus lagi ID pembaca RFID, stempel waktu, dan peringkat yang diberikan ke pembaca RFID berdasarkan tag tersebut. Catatan ini dikirim pada saat berikutnya tag RFID berinteraksi dengan pembaca RFID mana pun (dan kemudian dihapus dari tag RFID), dengan pembaca RFID meneruskan catatan tersebut ke pusat autentikasinya yang memeriksa ketidaknormalan dan jika timbul masalah, itu memberi tahu pusat administrasi serta pusat otentikasi milik pembaca RFID sebelumnya.

Skema lapisan kepercayaan pusat otentikasi yang diusulkan mempertimbangkan laporan kejadian abnormal oleh pembaca RFID dan mempengaruhi nilai kepercayaan dari pusat otentikasi domain tempat pembaca menjadi bagiannya. Perhitungan kepercayaan dalam hal ini dapat dilakukan dengan salah satu dari dua metode yang diusulkan untuk skema manajemen kepercayaan pembaca.

Mahmud, 2018. Model ini mempertimbangkan tiga metrik kepercayaan sosial untuk sepasang node, yaitu: frekuensi interaksi relatif, keintiman dan kejujuran, serta penyimpangan data yang dihasilkan dari data historis node yang menghasilkan metrik kepercayaan dan tetangganya. Dua dimensi kepercayaan didefinisikan: kepercayaan perilaku node dan kepercayaan data; keduanya dihitung dengan kombinasi interaksi langsung (dari node pemeringkat) dan tidak langsung (dari tetangga node pemeringkat), dengan interaksi tidak langsung diberi bobot berdasarkan jarak tetangga ke node yang diperingkat. Kepercayaan perilaku node dihitung menggunakan Adaptive Neuro-Fuzzy Inference System (ANFIS), sebuah sistem fuzzy yang menggunakan propagasi balik untuk menyetel dirinya sendiri. Tiga masukan pada ANFIS didefinisikan sebagai: frekuensi interaksi relatif didefinisikan sebagai rasio interaksi dengan node pemeringkat dari seluruh interaksi node yang diberi peringkat dalam jangka waktu tertentu, keintiman didefinisikan sebagai rasio jumlah waktu yang dihabiskan untuk berinteraksi dengan node pemeringkatan dari total waktu yang dihabiskan untuk berinteraksi dengan semua node kecuali node pemeringkat, dan kejujuran didefinisikan sebagai rasio interaksi yang berhasil dari jumlah total interaksi node yang diberi peringkat dengan node pemeringkatnya. Tiga istilah linguistik digunakan dalam ANFIS untuk masing-masing dari tiga masukan: Rendah, Sedang dan Tinggi. Penyimpangan data yang dihasilkan, yang digunakan untuk menghitung kepercayaan data, didefinisikan sebagai berikut: kepercayaan data langsung didefinisikan sebagai penyimpangan data sesaat dari data historis yang dihasilkan oleh node yang diperingkat, dan kepercayaan data tidak langsung didefinisikan sebagai penyimpangan data sesaat dari data historis dari data historis yang dihasilkan oleh tetangga node yang diberi peringkat.

Arabsorkhi, 2016. Karya Arabsorkhi dkk. menyajikan prinsip umum di balik banyak model manajemen kepercayaan yang diusulkan dengan mempertimbangkan peringkat yang diberikan kepada node jaringan untuk kualitas layanan yang diberikan selama periode waktu tertentu. Jika node pemeringkat mempunyai informasi yang cukup untuk menentukan nilai kepercayaan dari peringkatnya sendiri selama jangka waktu tertentu (melalui pengamatan langsung), maka node tersebut dapat melanjutkan untuk menghitung nilai kepercayaan dari node yang akan diberi peringkat. Jika tidak, maka node pemeringkat dapat menanyakan

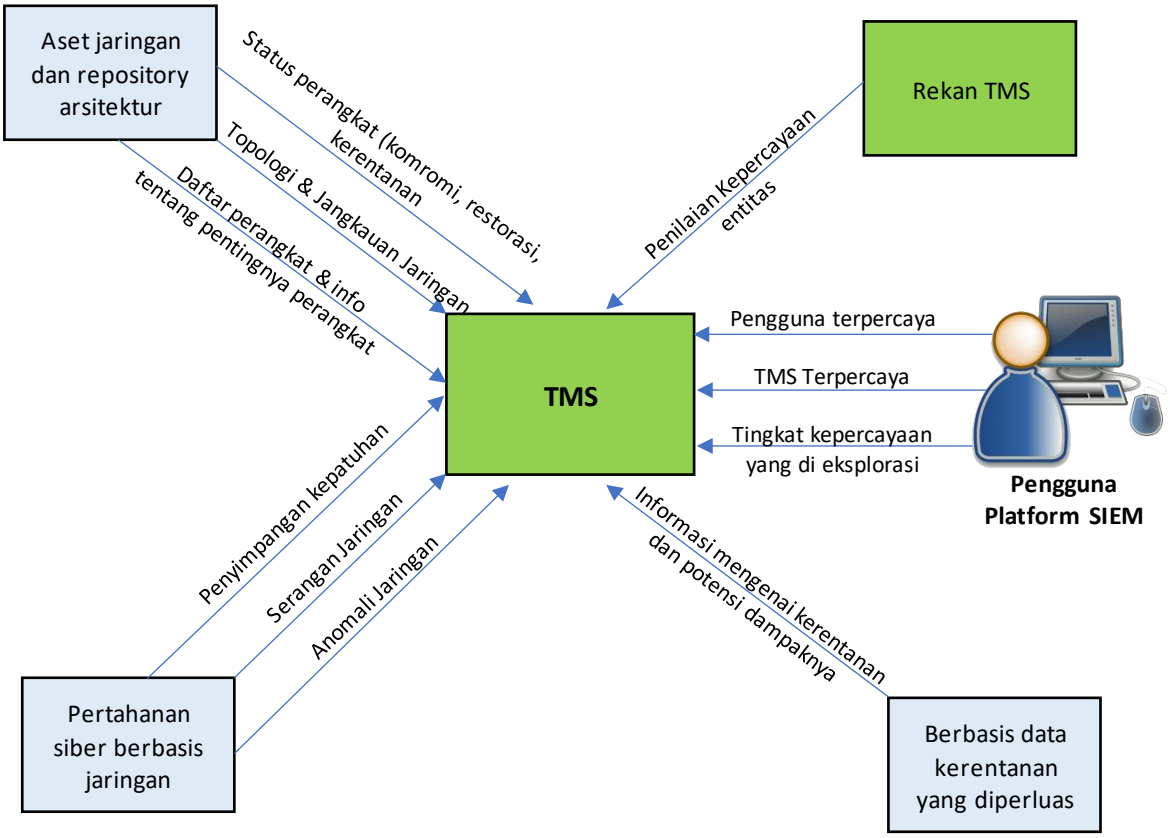
seluruh jaringan dan mengagregasi nilai kepercayaan yang diberikan oleh node jaringan lain ke node yang diberi peringkat.

Yuan, 2018. Model ini mempertimbangkan peringkat yang diberikan setelah interaksi node untuk kualitas layanan yang diberikan. Model jaringan terdiri dari node tepi IoT yang menjadi bagian dari domain yang difederasi oleh node broker tepi, yang kemudian menghubungi server cloud pusat yang bertanggung jawab atas penghitungan akhir nilai kepercayaan. Tiga nilai kepercayaan dihitung: kepercayaan langsung tentang perangkat ke perangkat lain (kepercayaan langsung D2D), kepercayaan umpan balik tentang sebuah node oleh edge broker (kepercayaan umpan balik B-to-D), dan kepercayaan keseluruhan (nilai kepercayaan akhir) tentang suatu perangkat. Kepercayaan langsung D-to-D diperbarui dan berdasarkan riwayat interaksi langsung antar node, ini didefinisikan sebagai rasio interaksi positif dan jumlah total interaksi antara dua node. Kepercayaan umpan balik B-to-D diperbarui oleh edge broker secara berkala dan didasarkan pada semua nilai kepercayaan langsung D-to-D mengenai node edge (kecuali penilaian mandiri); broker tepi mengumpulkan nilai kepercayaan langsung D-ke-D menggunakan bobot yang diperoleh dengan menggunakan teori entropi informasi objek, mengatasi keterbatasan dalam menetapkan bobot secara manual. Nilai kepercayaan keseluruhan dihitung sebagai jumlah tertimbang dari kepercayaan langsung D-ke-D dan kepercayaan umpan balik B-ke-D, sehingga mempertimbangkan opini dari node pemeringkat serta opini seluruh jaringan tentang node yang diberi peringkat.

8.4 SISTEM MANAJEMEN KEPERCAYAAN

Tujuan dari sistem manajemen kepercayaan adalah untuk melayani otoritas dalam perimeter infrastruktur Internet of Things yang dilindungi, yang melakukan tugas-tugas berikut:

- Menggabungkan pengamatan terhadap status, perilaku, dan risiko terkait perangkat ke dalam skor kepercayaan komprehensif, yang menunjukkan sejauh mana setiap perangkat dianggap dapat dipercaya.
- Dapat ditanyakan oleh entitas lain dalam perimeter infrastruktur Internet of Things yang dilindungi, untuk memberikan penilaian yang disebutkan di atas, agar entitas tersebut dapat dibaca dengan teliti. Secara indikatif, penilaian kepercayaan dapat digunakan untuk memvisualisasikan kepercayaan dalam jaringan, untuk membuat keputusan apakah tindakan yang berasal dari atau diarahkan ke suatu perangkat harus diperbolehkan atau tidak, untuk meningkatkan peringatan kepada petugas keamanan dan sebagainya.
- Memberikan pemberitahuan tepat waktu kepada entitas lain dalam perimeter infrastruktur Internet of Things yang dilindungi, untuk memperingatkan mereka tentang peristiwa penting terkait dengan tingkat kepercayaan yang terkait dengan perangkat. Secara khusus, penurunan tingkat kepercayaan perangkat di bawah ambang batas tertentu dan pemulihan kepercayaan perangkat yang sebelumnya diturunkan akan dilakukan, sehingga memungkinkan komponen yang relevan dari perimeter infrastruktur Internet of Things yang dilindungi, untuk mengambil tindakan yang tepat, seperti mengaktifkan atau menonaktifkan mekanisme pertahanan.



Gambar 8.1. Elemen platform SIEM memberikan informasi ke TMS.

Konteks TMS

TMS diharapkan dapat beroperasi dalam konteks platform yang luas dengan mengikuti prinsip Sistem Informasi Keamanan dan Manajemen Peristiwa (SIEM), yang memperoleh informasi yang diperlukan untuk pengoperasiannya dari modul platform lain, seperti yang digambarkan pada Gambar8.1.

Secara lebih rinci, informasi yang bersumber dari elemen platform lain yang berperan sebagai penyedia informasi keamanan dan manajemen peristiwa (SIEM) adalah sebagai berikut:

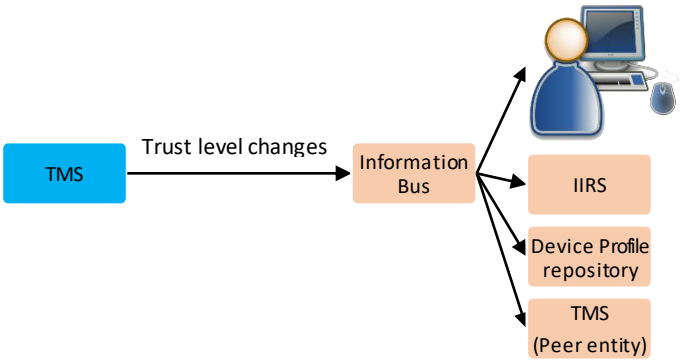
- pengguna platform memberikan informasi mengenai pengguna sejawat yang mereka percayai, TMS sejawat yang tepercaya, dan spesifikasi kepercayaan perangkat yang eksplisit. Tentu saja, interaksi pengguna dengan TMS dimediasi melalui aplikasi yang sesuai.
- Modul SiberDefense menyediakan data mengenai anomali jaringan yang terdeteksi (penyimpangan dari nominal perangkat dan perilaku jaringan), lalu lintas yang tidak patuh (arus lalu lintas yang belum dimasukkan dalam daftar putih sebagai “perilaku yang dapat diterima” untuk perangkat) dan serangan jaringan (terutama dalam konteks deteksi berbasis tanda tangan), baik yang berasal dari beberapa perangkat atau ditargetkan terhadapnya.
- Modul iIRS (intelligent Intrusion Response System) memberikan informasi mengenai perangkat yang berada dalam cakupan TMS, kepentingannya, kerentanan yang ada pada

perangkat, kejadian gangguan perangkat, serta informasi topologi jaringan dan keterjangkauan.

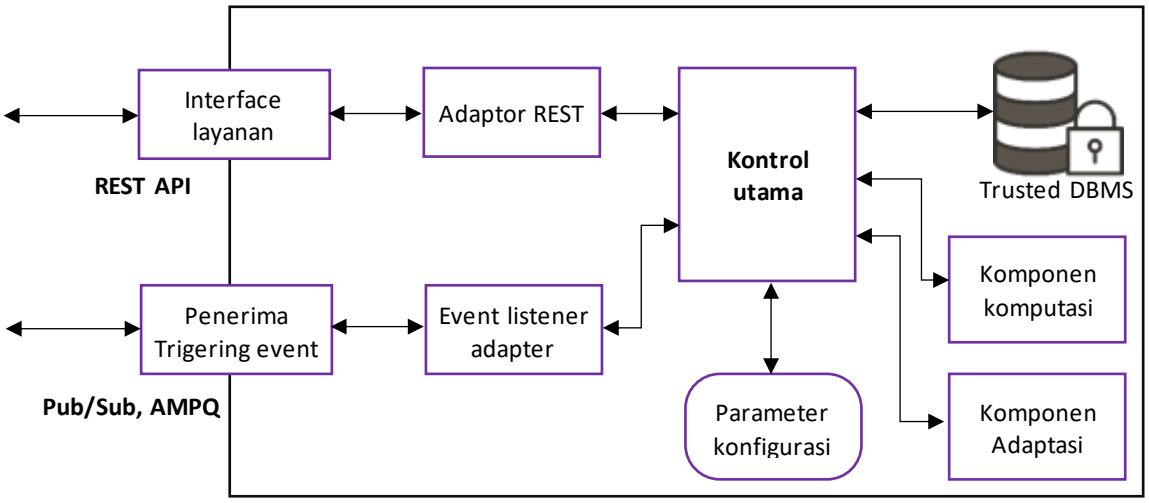
- Modul eVDB (exended Vulnerability DataBase) memberikan informasi tentang kerentanan yang terdeteksi, termasuk dampaknya, yang mendasari penilaian dampak kerentanan terhadap tingkat kepercayaan perangkat yang terkena dampak.
- Repositori profil Perangkat memberikan informasi tentang kasus-kasus ketika perangkat dihapus dari sistem dan kapan kesehatan perangkat dipulihkan setelah disusupi (yaitu malware dihapus atau versi sistem operasi/firmware yang "bersih" diinstal).
- TMS, yang bertindak sebagai entitas rekan yang tepercaya, memberikan penilaian kepercayaan yang digabungkan antara instans TMS penerima dengan estimasi kepercayaan perangkatnya sendiri, untuk mensintesis skor kepercayaan yang komprehensif.

TMS, pada gilirannya, menerbitkan informasi mengenai perubahan tingkat kepercayaan perangkat melalui bus informasi platform SIEM (komponen pub/sub yang mengirimkan jenis informasi tertentu yang dipublikasikan ke entitas yang telah mendaftarkan minat mereka untuk menerima informasi tersebut. jenis informasi), seperti digambarkan pada Gambar 8.2. Informasi ini dapat dimanfaatkan sebagai berikut:

- Operator platform SIEM dan antarmuka pengguna akhir dapat menggunakan informasi ini untuk menghasilkan peringatan, terutama dalam kasus penurunan kepercayaan yang patut dicatat.
- Mekanisme pertahanan, dan khususnya iIRS dapat mengeksploitasi informasi ini untuk menerapkan atau menonaktifkan pembatasan lalu lintas jaringan.
- Repositori Perangkat memperbarui basis datanya sendiri, menjamin konsistensi informasi dan penyebaran tingkat kepercayaan ke komponen lain yang berkepentingan.
- TMS rekan dapat menggunakan informasi ini untuk memperbarui penilaian kepercayaan mereka.



Gambar 8.2. Arus informasi keluar TMS.



Gambar 8.3. Desain tingkat tinggi TMS.

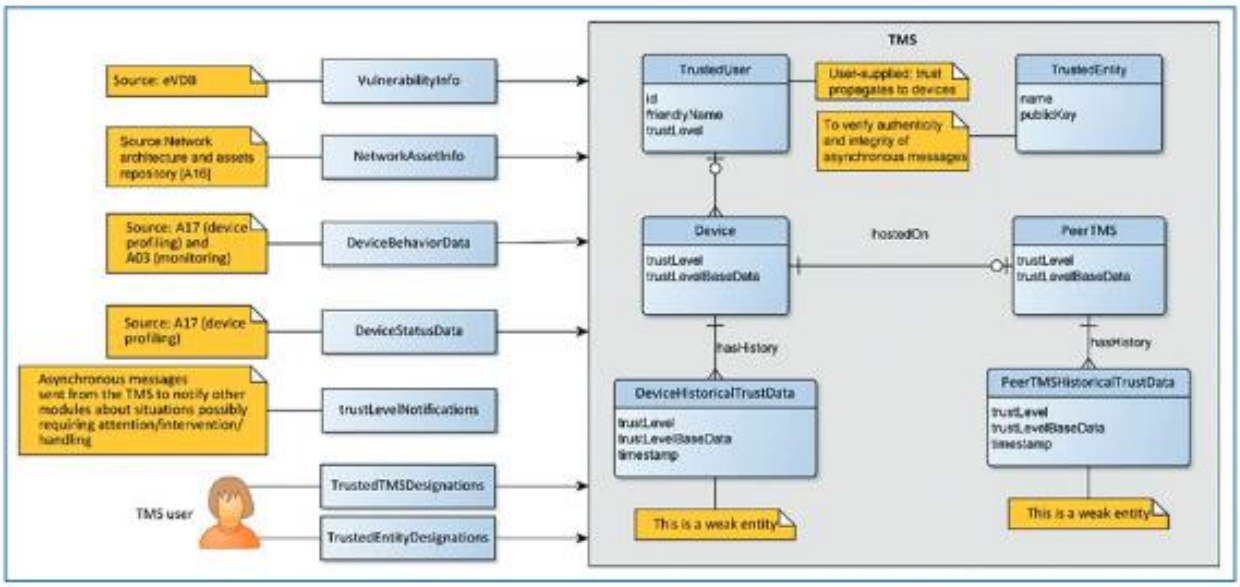
Arsitektur Aplikasi TMS

Gambar 8.3 mengilustrasikan pandangan konseptual Sistem Manajemen Kepercayaan. Arsitekturnya dirancang untuk memungkinkan pemaparan API yang koheren, memungkinkan segala aspek adaptasi diterapkan secara internal dengan mempertimbangkan semua konteks yang sesuai (ketersediaan jaringan & sumber daya, kekritisan situasi, dll.). Penerimaan informasi yang diperlukan untuk menghitung ulang skor kepercayaan dan risiko – termasuk status perangkat, perilaku, dan aspek risiko terkait sebagian besar disadap melalui pesan asinkron, melalui saluran komunikasi khusus, mengikuti paradigma pub/sub. Dengan cara ini, TMS dipisahkan dari produser acara dan pengaturan waktunya; namun, konsumsi konten melalui API juga dapat digunakan. Sebaliknya, TMS mempublikasikan peristiwa mengenai perubahan penting dalam tingkat kepercayaan dan risiko, sekaligus menawarkan informasi yang sama di bawah REST API. Adaptasi, jika diperlukan, akan didukung oleh komponen adaptasi yang akan dikembangkan dan dipelihara secara terpisah dari aspek komputasi, sehingga mendorong pemisahan kepentingan. Gambar 8.4 menggambarkan tampilan data TMS, yang menunjukkan:

a) Data disimpan secara internal dalam database TMS;
b) Pesan-pesan yang dilanggani TMS untuk memperoleh informasi yang diperlukan untuk menghitung tingkat kepercayaan dan risiko, serta sumber pesan-pesan ini, sesuai dengan arsitektur sistem SIEM secara keseluruhan;
c) Informasi yang diterima TMS langsung dari pengguna (biasanya melalui UI);
d) Pesan-pesan yang disediakan TMS ke infrastruktur komunikasi asinkron, untuk dibaca oleh komponen Siber-Trust lainnya.

TMS Peer Tepercaya dikurasi langsung oleh pengguna. Pengguna juga memberikan informasi mengenai entitas tepercaya lainnya di platform: ini berkaitan dengan modul yang menghasilkan pesan asinkron ke bus informasi, dan diharapkan digunakan oleh TMS. Setiap spesifikasi entitas tepercaya menyediakan data yang dibutuhkan TMS untuk memverifikasi keaslian dan integritas pesan yang diterima, misalnya nama rekan dan sertifikatnya. Meskipun pengguna umumnya tidak diharapkan mahir dengan data tersebut, prosedur otomatis pada pengaturan platform diharapkan dapat meringankan pengguna dari tugas mengatur informasi

ini secara manual. Jika pembaruan informasi ini diperlukan, otomatisasi, asisten konfigurasi, dan wizard juga dapat memudahkan tugas pengguna.

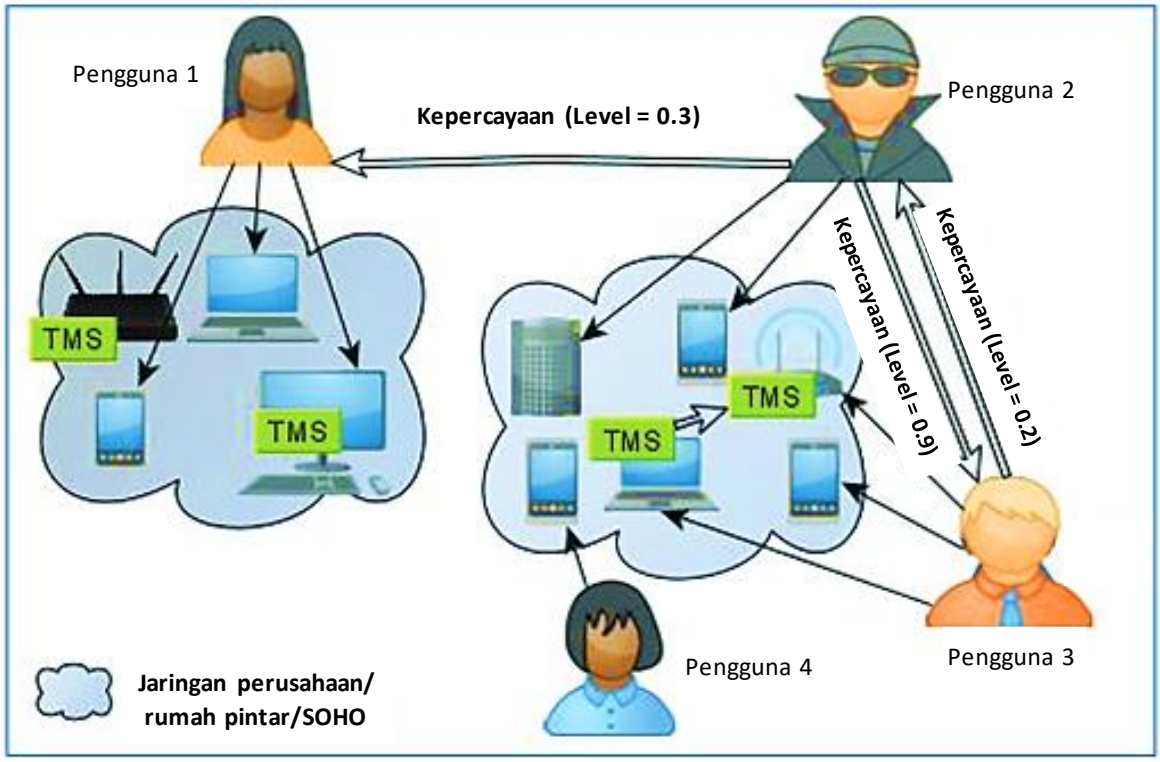


Gambar 8.4. tampilan data TMS.

Desain TMS

Pada Gambar 8.5, entitas yang terlibat dalam model kepercayaan yang diusulkan dan hubungan di antara mereka diilustrasikan. Elemen tersebut mungkin muncul dalam konteks lingkungan IoT, Smart Home, atau SOHO dan mencakup:

- Perangkat, yang berfungsi dalam lingkungan yang dipertimbangkan.
- Pengguna, yang memiliki perangkat. Satu pengguna dapat memiliki banyak perangkat. Pengguna dapat membangun hubungan kepercayaan di antara mereka, dengan hubungan ini memiliki sifat-sifat berikut (a) berbobot, (b) terarah, (c) tidak transitif dan (d) belum tentu simetris. Contoh berikut mengilustrasikan properti ini:
  - Pengguna u1 menyatakan bahwa dia mempercayai pengguna lain u2. Hal ini dilakukan dengan memberikan tingkat kepercayaan, yang menyatakan keyakinan u1 bahwa u2 tidak akan melakukan tindakan jahat terhadap u1 -atau bahkan melakukan aktivitas yang berdampak positif terhadap u1.
  - Pernyataan kepercayaan u1 terhadap u2 tidak berarti bahwa u2 juga mempercayai u1, menyatakan fakta bahwa kepercayaan tidak dapat dibalas. Namun masih ada kemungkinan bahwa u2 membuat pernyataan terpisah dan independen bahwa ia memercayai u1; pernyataan tersebut mungkin mengungkapkan tingkat kepercayaan yang berbeda dari pernyataan yang dibuat oleh u1.
  - Kepercayaan tidak transitif: jika u1 memercayai u2 dan u2 memercayai u3, tidak ada asumsi yang dibuat bahwa u1 memercayai u3. Pernyataan eksplisit oleh u1 diperlukan untuk membangun hubungan kepercayaan dengan pengguna lain dalam domain wacana.



Gambar 8.5. Entitas dalam model kepercayaan yang diusulkan dan hubungannya.

- Instance Sistem Manajemen Kepercayaan (TMS): TMS secara efektif adalah agen perangkat lunak yang melakukan perhitungan tingkat kepercayaan terhadap perangkat dalam lingkungan yang dipertimbangkan. Perhitungan nilai kepercayaan untuk suatu perangkat dilakukan dengan mempertimbangkan beberapa faktor yang dikumpulkan melalui pemantauan aktivitas dalam lingkungan atau disediakan secara eksplisit. Faktor-faktor yang dipertimbangkan adalah:
  - status perangkat: mencakup (1) informasi tentang integritas perangkat, yaitu informasi yang membuktikan keabsahan perangkat lunak/firmware/sistem operasi dan konfigurasinya, dan bukan komponen-komponen yang disebutkan di atas yang disusupi; dan (2) informasi mengenai ketahanan perangkat, yaitu jika perangkat lunak/firmware/sistem operasi/konfigurasi perangkat memiliki kerentanan yang diketahui, dan bukan jika tidak ada kerentanan yang diketahui.
  - perilaku perangkat: mencakup informasi berikut:
    1. jika perangkat dilaporkan melakukan serangan atau teridentifikasi menjadi target serangan.
    2. jika metrik pemanfaatan sumber daya perangkat mematuhi spesifikasi yang telah ditentukan sebelumnya yang menentukan perilaku normal atau menyimpang darinya. Beberapa contoh metrik ini mencakup, namun tidak terbatas pada, penggunaan jaringan, beban CPU, dan aktivitas disk. Praktisnya, setiap kelas metrik sistem yang dapat dikuantifikasi, dan metrik garis dasar mana yang dapat dibuat sehingga memungkinkan penghitungan penyimpangan dari garis dasar memenuhi syarat untuk dimasukkan ke dalam dimensi ini. Praktik serupa banyak digunakan dalam pemantauan infrastruktur, seperti Nagios dan mungkin mencakup metrik

seperti jumlah pengguna yang terhubung, jumlah disk kosong, jumlah total proses, jumlah proses yang terkait dengan beberapa contoh layanan tertentu, dll.

3. Jika perilaku perangkat sesuai dengan perilaku referensi yang telah ditentukan sebelumnya, maka akan dimasukkan ke dalam daftar putih sebagai “normal”. File spesifikasi MUD dapat memberikan informasi tersebut, namun belum diadopsi secara luas dan dukungan pabrikan kurang.

- risiko yang terkait dengan perangkat: Perangkat IoT dapat menjadi target serangan dan beberapa serangan mungkin berhasil. Kemungkinan yang menunjukkan bahwa suatu perangkat pada akhirnya akan disusupi dapat dihitung dengan mempertimbangkan informasi teknis seperti kerentanan dan jangkauannya di dalam jaringan. Grafik serangan dapat dimanfaatkan untuk tujuan ini. Tingkat dampak serangan yang berhasil terhadap organisasi/orang yang memiliki perangkat tidak selalu sama dan dapat bervariasi tergantung pada nilai yang dirasakan dari perangkat tersebut. Nilai yang dirasakan dari perangkat secara langsung terkait dengan aset yang dicakupnya (misalnya, nilai perangkat yang menampung basis data bergantung pada nilai data dalam basis data) atau dengan nilai/proses kekritisan yang menjadi tanggung jawabnya (misalnya, monitor tanda-tanda vital pada jam tangan pintar vs. monitor tanda-tanda vital yang digunakan dalam operasi jarak jauh).

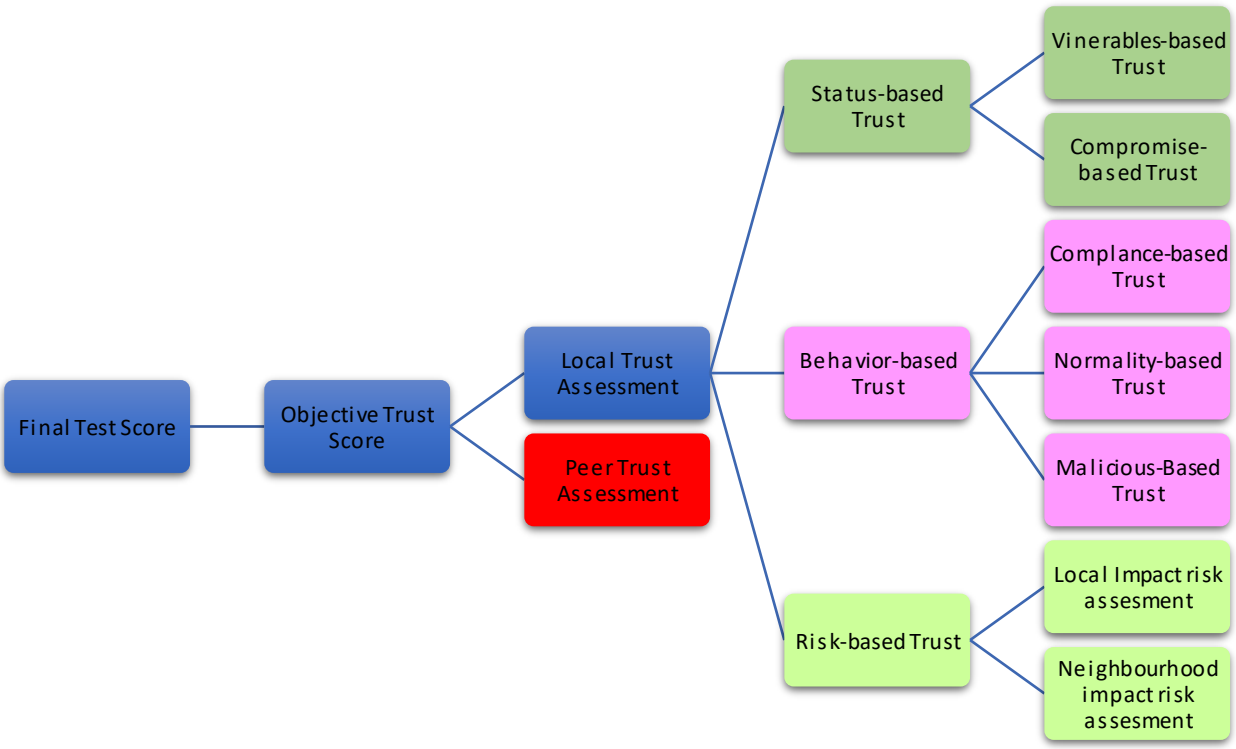
Aspek lain yang harus dipertimbangkan ketika menghitung risiko yang terkait dengan perangkat d adalah kumpulan perangkat yang dapat diakses melalui perangkat tersebut, dan apakah penyerang dapat menggunakannya sebagai benteng untuk menyerang perangkat lain, mencoba untuk mengkompromikan perangkat bernilai tinggi dalam konteks serangan multi-tahap yang lebih maju. Dalam hal ini, risiko yang terkait dengan d bergantung pada (a) probabilitas bahwa d disusupi, (b) probabilitas bahwa perangkat yang dapat dijangkau dari d disusupi dalam konteks serangan multi-tahap, dan (c) per - nilai yang diterima dari perangkat yang dapat dijangkau dari d.

Dengan mempertimbangkan hal-hal di atas, dimensi risiko terkait menggabungkan aspek-aspek yang disebutkan di atas, yaitu (i) probabilitas teknis bahwa perangkat tersebut dikompromikan dengan nilai yang dirasakan dari perangkat tersebut, dan (ii) probabilitas bahwa perangkat tersebut digunakan sebagai sebuah batu loncatan untuk menyerang perangkat lain, bersamaan dengan nilai bisnis dari aset yang terkait dengan perangkat tersebut, untuk menyatukan metrik tunggal dan komprehensif yang mengungkapkan risiko bisnis yang berlaku pada suatu perangkat.

Hubungan kepercayaan antara pengguna yang memiliki perangkat yang menjalankan instans TMS dan pengguna yang perangkatnya sedang dalam evaluasi kepercayaan. Aspek ini memoderasi bobot penilaian tingkat kepercayaan, sehingga penilaian tingkat kepercayaan yang bersumber dari TMS tepercaya (yaitu TMS yang dijalankan pada perangkat milik pengguna tepercaya) diperhitungkan dengan lebih kuat, sedangkan pentingnya penilaian kepercayaan yang bersumber dari TMS yang tidak tepercaya (yaitu TMS yang berjalan pada perangkat milik pengguna yang tidak dikenal atau memiliki kepercayaan rendah) dilemahkan.

Penilaian kepercayaan secara keseluruhan dibentuk oleh contoh TMS dengan mensintesis tiga dimensi kepercayaan: (i) berbasis status, (ii) berbasis perilaku, dan (iii) kepercayaan berbasis risiko terkait. Selain itu, hubungan kepercayaan dapat dibangun antar instance TMS, sama seperti hubungan kepercayaan dibangun antar pengguna. Mirip dengan kasus hubungan kepercayaan pengguna-ke-pengguna, hubungan kepercayaan TMS-ke-TMS bersifat (a) berbobot, (b) terarah, (c) non-transitif, dan (d) tidak harus simetris. Hubungan kepercayaan antara instans TMS secara eksplisit disediakan oleh pengguna yang memiliki perangkat tempat instans TMS dijalankan. Setelah hubungan kepercayaan yang menyatakan bahwa instans TMS T1 memercayai instans TMS T2 terjalin, T1 akan mengambil sumber penilaian kepercayaan untuk perangkat dari TMS T2, dan mempertimbangkannya saat menghitung tingkat kepercayaan masing-masing perangkat.

Terakhir, pengguna diperbolehkan untuk mengatur secara eksplisit tingkat kepercayaan perangkat yang mereka miliki, mengesampingkan perhitungan yang dilakukan oleh TMS. Ketentuan ini diakomodasi untuk menangani false-positif terutama yang terkait dengan serangan jaringan (serangan ditandai oleh modul yang relevan namun tidak benar-benar dilakukan), anomali jaringan (misalnya lalu lintas berlebih terdeteksi namun hal ini disebabkan oleh pencadangan yang dilakukan pengguna atau pembaruan perangkat lunak/firmware) dan penyusupan (misalnya beberapa perangkat lunak pada perangkat salah diklasifikasikan sebagai malware). TMS akan mampu memberikan tingkat kepercayaan perangkat yang dihitung secara otomatis dan eksplisit, sehingga aplikasi yang relevan akan dapat mendeteksi perangkat yang memiliki perbedaan besar dan terus memberikan informasi kepada pengguna tentang penyimpangan tersebut, meningkatkan kesadaran dan memfasilitasi intervensi, sebagai diperlukan.



Gambar 8.6. Dimensi dan aspek komposisi skor kepercayaan.

Berdasarkan uraian di atas, TMS menyusun skor kepercayaan secara hierarkis, seperti digambarkan pada Gambar 8.6, dengan pandangan holistik terhadap penilaian kepercayaan. Untuk melakukan komposisi ini, TMS memerlukan jenis informasi yang berbeda untuk setiap perangkat. TMS beroperasi dalam konteks luas c dan mendapatkan informasi yang diperlukan dari modul platform SIEM lainnya.

8.5 KESIMPULAN

Dalam bab ini, kami menyajikan pendekatan komputasi kepercayaan di Internet of Things, yang menggabungkan aspek perilaku, status perangkat, dan risiko terkait ke dalam skor kepercayaan komprehensif, yang dapat dikonsultasikan untuk mewujudkan kontrol akses berbasis kepercayaan. Pendekatan yang diusulkan juga mempertimbangkan hubungan kepemilikan perangkat dan hubungan kepercayaan pemilik-ke-pemilik, yang digunakan dalam proses komputasi kepercayaan.

Parameter yang berbeda dari proses komputasi manajemen kepercayaan dapat dikonfigurasi dan disesuaikan; khususnya, pendekatan yang berbeda-beda dapat digunakan untuk menghitung skor kepercayaan keseluruhan berdasarkan skor parsial dan spesifik dimensi; penurunan kepercayaan dapat dipengaruhi oleh penuaan, yaitu dampaknya dapat berkurang seiring berjalannya waktu, atau mungkin tetap berlaku sampai akar permasalahannya diketahui telah teratasi; Data SIEM mungkin dikaitkan dengan tingkat kepercayaan, dan tingkat ini dapat dipertimbangkan dalam penghitungan skor kepercayaan secara keseluruhan. Semua parameter ini bergantung pada konteks tertentu di mana TMS beroperasi. Pekerjaan kami di masa depan mencakup studi mendalam dan analisis aspek-aspek ini; selain itu, arsitektur TMS yang diusulkan akan dievaluasi, untuk mengukur kinerjanya secara keseluruhan, serta ketahanannya terhadap serangan spesifik yang diluncurkan terhadap jaringan IoT.

BAB 9
PROSES EVALUASI KEPERCAYAAN DUNIA MAYA

Lingkungan Internet of Things (IoT) terus berubah, dibentuk oleh kebutuhan teknis dan sosial. Kemajuan IoT yang pesat dan peningkatan jumlah data yang saling terhubung antara layanan dan infrastruktur yang berpotensi menimbulkan ancaman terhadap dunia maya, merupakan dimulainya konseptualisasi proyek Siber-Trust. Siber-Trust melakukan penelitian ekstensif di bidang di mana IoT diterapkan secara luas. Struktur proyek antara lain diandalkan dengan mempertimbangkan kebutuhan pemangku kepentingan, sehingga hasil yang dihasilkan proyek realistis berdasarkan kebutuhan pengguna akhir.

Dalam konteks ini, rencana evaluasi dirancang untuk menilai operasi platform. Dalam bab ini disajikan metodologi validasi, verifikasi dan evaluasi yang diikuti Siber-Trust selama fase percontohan pertama siklus hidup proyek. Proses Evaluasi Siber-Trust berisi informasi tentang bagaimana mitra teknis akan memvalidasi komponen teknis berdasarkan spesifikasi sistem dan metode yang tepat di mana pengguna akhir akan mengevaluasi semua fungsi platform. Tujuan validasi, verifikasi dan evaluasi sejalan dengan tujuan proyek. Bab ini juga dipandu oleh hasil proyek yang terkait dengan (a) skenario kasus penggunaan, (b) arsitektur Siber-Trust, (c) persyaratan pengguna akhir, dan d) integrasi sistem secara keseluruhan.

9.1 PENDAHULUAN

Validasi, verifikasi, dan evaluasi adalah metode yang ada di bawah payung yang sama dari keseluruhan Proses Evaluasi. Karena evaluasi adalah tahap akhir di mana keseluruhan “produk” dinilai oleh pengguna aktual atau potensial, kami menyebut keseluruhan proses dengan nama ini. Dalam banyak kasus, masing-masing metode ini tertanam satu sama lain, namun dalam tahapan yang berbeda. Mulai sekarang, demi kesederhanaan, ketika kita ingin menunjukkan prosedur penilaian secara keseluruhan, kita akan mengacu pada Proses Evaluasi yang mencakup ketiga metode tersebut di atas sebagai tiga tahapan berbeda yang terkandung di dalamnya.

Secara keseluruhan, metodologi validasi menilai apakah produk yang dibangun berdasarkan kriteria (persyaratan) yang diberikan oleh pengguna akhir menjawab pertanyaan “Apakah sistem yang dikembangkan ini melakukan apa yang dimaksudkan?”, verifikasi apakah sistem menjalankan fungsi tertentu berdasarkan pada spesifikasi sistem yang menjawab pertanyaan “Apakah kita membangun produk yang tepat?”, dan evaluasi mengacu pada apakah platform yang dikembangkan secara keseluruhan telah memenuhi kebutuhan yang diinginkan.

Metode validasi, verifikasi dan evaluasi telah dirumuskan dan diterapkan oleh berbagai perusahaan, perusahaan, serta proyek. Banyak kerangka kerja multi-level telah dikembangkan untuk menilai berbagai produk, termasuk objek dan metodologi. Ruang lingkupnya antara lain adalah untuk memastikan kualitas, meningkatkan kinerja produk dan berdasarkan hasil yang diperoleh (jika evaluasi berkelanjutan) untuk menentukan langkah selanjutnya. Kerangka

kerja proses evaluasi yang canggih telah diidentifikasi di bawah ini, yang membuktikan bahwa kerangka kerja yang digunakan untuk membangun metodologi penilaian Siber-Trust adalah metodologi yang dapat diperluas dan disesuaikan.

9.2 KEADAAN PENGETAHUAN

Proses Evaluasi Umum

Pada subbagian ini diperkenalkan proses evaluasi umum yang menjadi dasar metodologi Siber-Trust. Kerangka ini digunakan secara luas untuk mengevaluasi produk akhir dan terdiri dari prosedur langkah demi langkah yang spesifik.

1. Dimulai dengan menetapkan kerangka (misalnya, konteks, tujuan, kasus penggunaan, persyaratan, dll.)
2. Rancang sistemnya.
3. Mendefinisikan kelompok evaluasi, tujuan evaluasi, strategi evaluasi dll.
4. Menyiapkan dan melaksanakan uji coba untuk mengevaluasi "produk".
5. Hasil evaluasi dan penilaian

Berdasarkan Langkah 5 evaluasi dianggap berhasil atau tidak. Untuk tujuan perbaikan, ketika iterasi evaluasi pertama selesai, Langkah 5 dapat memberikan umpan balik pada Langkah 3 yang melanjutkan proses hingga akhir fase iterasi kedua dan seterusnya. Langkah-langkah yang hampir sama digunakan dalam penilaian dilakukan pada jenis "produk" yang berbeda. Dengan demikian, kesimpulan yang diambil adalah bahwa metodologi evaluasi digunakan apapun jenis objek evaluasinya. Kerangka Evaluasi Siber-Trust dijelaskan pada Sub bab 9.3.

Kerangka Evaluasi yang Diimplementasikan

Innovate Uk adalah lembaga pendanaan nasional yang berinvestasi dalam ilmu pengetahuan dan penelitian di Inggris yang telah menerapkan kerangka evaluasi untuk memahami secara obyektif bagaimana suatu kebijakan atau tindakan lain ditegakkan dan apa konsekuensinya. Badan ini mengevaluasi kegiatan investasi mereka terhadap tiga (3) bidang dengan melakukan (a) evaluasi proses, (b) evaluasi dampak dan (c) evaluasi ekonomi. Kerangka tersebut mengikuti alur melingkar yang memungkinkan evaluasi lingkaran pertama mempunyai dampak total dengan memberikan umpan balik pada lingkaran kedua dan memodifikasi dasar pemikiran lingkaran baru yang akan dimulai (lingkaran kedua).

Kerangka Evaluasi Strategi Keamanan Siber Nasional (NCSS), menargetkan untuk menyempurnakan pedoman kebijakan keamanan siber, dengan menilai sistem dan memberikan perbaikan pada strategi yang telah ditetapkan. Terdiri dari 4 Tahap, dimulai dari tahap awal (a) mengembangkan strategi, (b) melaksanakan strategi, (c) mengevaluasi strategi, dan berakhir pada (d) mempertahankan strategi. Untuk keperluan evaluasi, telah ditetapkan serangkaian tujuan evaluasi yang berkaitan dengan setiap tahapan evaluasi. Institut Standar dan Teknologi Nasional (NIST) telah mendistribusikan Kerangka Keamanan Siber (CSF) untuk mengembangkan pendekatan standar terhadap penilaian keamanan siber untuk semua sektor infrastruktur penting negara. CSF dapat disesuaikan dengan berbagai teknologi, tahapan siklus hidup, perusahaan. Tahapan proses kerja secara umum adalah (a) menentukan ruang lingkup dan prioritas (b) orientasi (c) membuat profil saat ini (d) penilaian risiko (e) membuat profil

target (f) mengidentifikasi, mengevaluasi, dan memprioritaskan kesenjangan, (g) melaksanakan rencana aksi.

PDCA (Plan-Do-Check-Act) adalah pendekatan empat tahap yang berulang untuk terus meningkatkan proses, produk atau layanan, dan untuk menyelesaikan masalah. Hal ini melibatkan pengujian solusi yang mungkin dilakukan secara sistematis, menilai hasilnya, dan menerapkan solusi yang terbukti berhasil. Kerangka kerja PDCA/PDSA efektif di berbagai organisasi. Ini dapat digunakan untuk meningkatkan proses atau produk apa pun dengan membaginya menjadi langkah atau tahapan yang lebih kecil dan berupaya untuk meningkatkan masing-masing proses atau tahapan tersebut.

9.3 KERANGKA EVALUASI SIBER-TRUST

Siber-Trust sejak awal proyek menetapkan dasar kerangka evaluasi dengan memperkenalkan hasil yang terkait dengan skenario kasus penggunaan, kebutuhan pengguna akhir, arsitektur platform, dan spesifikasi alat yang memerlukan elemen inti untuk mendukung proses evaluasi. Namun, proses evaluasi sebenarnya dimulai setelah fase integrasi pertama, hingga mencapai titik di mana platform konkrit telah dibuat, dan dapat digunakan sebagai percontohan selama fase evaluasi.

Sebelum evaluasi melalui uji coba dimulai, materi evaluasi disintesis dan didistribusikan kepada pengguna akhir. Selain itu, 7 langkah yang dijelaskan pada Gambar 9.1 dianalisis di dalam bab ini.

Konteks

Konteks evaluasi siber -Trust dibangun untuk mencapai dua (2) tujuan. Yang pertama adalah untuk meyakinkan pengguna tentang fitur dan penawaran platform, dan yang terakhir adalah untuk mengukur dampak solusi agar dapat diterapkan pada komunitas pengguna akhir (lihat Bagian 9.4). Konsorsium pertama-tama harus memvalidasi apakah solusi yang dikembangkan memenuhi kriteria penerimaan pengguna akhir, mencapai ambang batas yang tepat untuk setiap komponen (misalnya, tingkat deteksi serangan siber pada tingkat perangkat dan jaringan, dll.).

siber Trust bertujuan untuk memajukan lingkungan dengan lingkungan yang aman di mana warga negara Eropa merasa terlindungi, memiliki rasa otonomi, dan merasa aman dalam konteks keamanan kerangka digital. Oleh karena itu, proyek ini tidak hanya bertujuan untuk memperkuat teknologi terkini di berbagai domain keamanan siber. siber-Trust akan menggunakan operasi intelijen, identifikasi, dan mekanisme mitigasi ancaman siber yang canggih untuk menyelesaikan tantangan dalam mengamankan lingkungan perangkat IoT.

Gambar 9.1. Proses Evaluasi Siber-Trust di dalam struktur proyek

Tujuan

Sejumlah tujuan strategis ditetapkan untuk memastikan keberhasilan implementasi percontohan, pengujian, dan proses evaluasi. Dimulai dengan penerapan uji coba Proof of Concept (PoC) pertama, disertai dengan analisis hasil yang dikumpulkan, sistem operasional yang menyediakan semua layanan yang diharapkan dikembangkan. Melanjutkan proses uji coba, yang merupakan bagian penting dari prioritas. Platform ini akan diuji secara menyeluruh untuk mencapai tujuan tertentu, seperti mendeteksi serangan siberspesifik pada tingkat perangkat dan jaringan (misalnya, kerentanan zero-day), memantau dan mengembangkan kerangka kerja untuk penilaian dan remediasi kerentanan berkelanjutan yang efisien, meningkatkan IoT ketahanan jaringan terhadap jenis serangan tertentu (misalnya DDoS), dan yang terakhir, memberikan intelijen ancaman tingkat lanjut.

Selain itu, keamanan, keandalan, efisiensi, interoperabilitas, dan skalabilitas merupakan tujuan evaluasi penting yang berkontribusi terhadap keberhasilan evaluasi dan proses pengujian percontohan. Hasilnya, platform keamanan siber akan jauh melampaui

kondisi keamanan siber saat ini, dan mengantarkan era baru bagi arsitektur keamanan siber generasi berikutnya.

Tim Asesor

Kelompok pengguna akhir yang terlibat dalam proses evaluasi adalah Pemilik Rumah Pintar (SHO), Penyedia Layanan Internet (ISP), dan Badan Penegakan Hukum (LEA). Tiga (3) kelompok mengevaluasi platform Siber-Trust melalui tiga (3) Antarmuka Pengguna (UI) berbeda yang disesuaikan. Ada UI tambahan yang didedikasikan untuk Administrator ICT untuk pengguna ISP juga. Setiap kelompok pemangku kepentingan akan mengakses fungsi komponen yang berbeda-beda, karena setiap UI dirancang semata-mata untuk memenuhi kebutuhan sehari-hari para pemangku kepentingan, seperti yang digambarkan pada Tabel 9.1.

Kebutuhan tingkat tinggi Pengguna Akhir

Tabel 9.1. Tujuan utama di balik tuntutan para pemangku kepentingan.

Pengguna akhir	**Target**
Smart Home Owners (SHOs)	• Menjaga Perangkat dan Infrastruktur Rumah Pintar ◦ Memantau status kesehatan aset rumah pintar, tingkat risiko. ◦ Mendeteksi perilaku lalu lintas yang tidak normal dan memberi tahu kerentanan kecil atau kritis atau kemungkinan serangan. ◦ Memperingatkan SHO akan serangan siber pada tingkat perangkat dan jaringan. ◦ Memperbarui perangkat, pengaturan keamanan infrastruktur.
Internet Service Providers (ISPs)	• Melindungi Pelanggan ◦ Memantau infrastruktur jaringan pelanggan ◦ Memberikan informasi penting kepada LEA ketika diminta oleh pelanggan mereka.
Administrator (Admin)	• Orkestrasi tingkat tinggi pada akun ISP UI.
Law Enforcement Agencies (LEAs)	• Meningkatkan Rantai Pengawasan • Mengurangi waktu yang diperlukan untuk bertukar informasi, yang mungkin berisi bukti forensik, mengenai serangan dunia maya antara LEA dan Penyedia Layanan Internet

Metodologi persyaratan Pengguna Akhir

Ekstraksi kebutuhan pengguna akhir berasal dari analisis penelitian dan agregasi permintaan pengguna. Empat sumber digunakan untuk menentukan persyaratan platform. Tindakan yang dilakukan terhadap sumber-sumber tersebut adalah:

- Analisis solusi industri yang ada dan aktivitas penelitian-domain pengetahuan
- Analisis kasus penggunaan Siber-Trust
- Penyelenggaraan lokakarya khusus dengan kelompok pengguna akhir
- Pembuatan Kuesioner yang ditargetkan (total 5 Kuesioner)

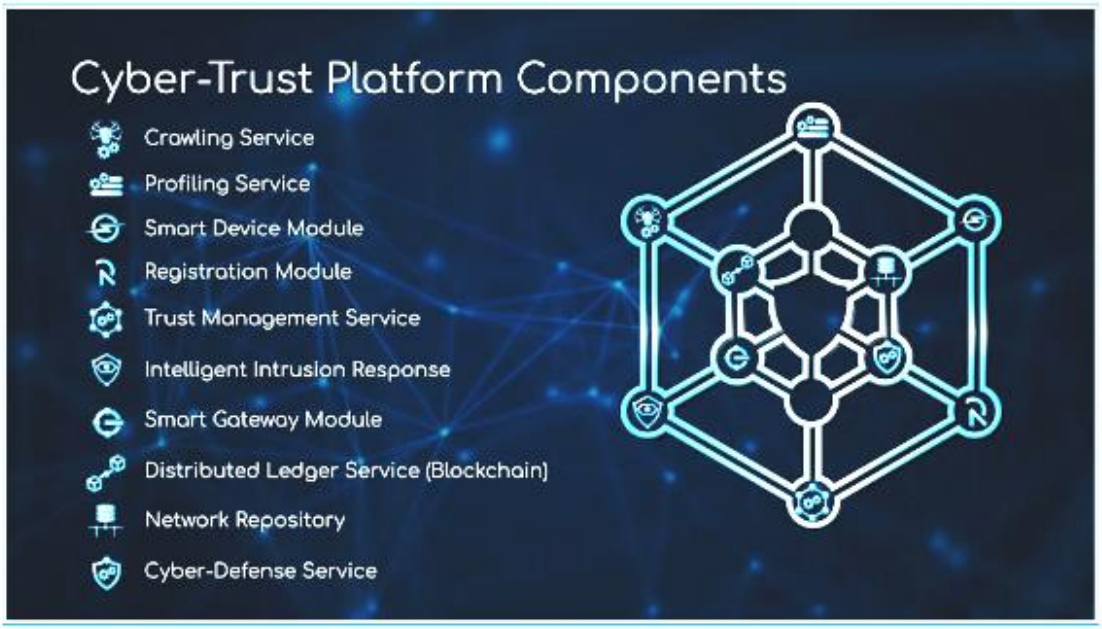
Metodologinya diuraikan pada Gambar 9.2. Persyaratan pengguna akhir dibagi menjadi kategori fungsional dan non-fungsional berdasarkan konten setiap persyaratan, dan kemudian diprioritaskan menggunakan metodologi MoSCoW.

Gambar 9.2. Metodologi ekstraksi pengguna akhir.

Komponen Siber-Trust

Siber-Trust berisi berbagai komponen yang dirancang untuk mencapai cakupan proyek. Peran dan tanggung jawab komponen awalnya dijelaskan melalui dokumentasi arsitektur dan kemudian didefinisikan ulang menjadi hasil teknis, disesuaikan dengan kebutuhan arsitektur dan operasional alat.

Beberapa komponen Siber-Trust, yang disajikan pada Gambar 9.3, digunakan dalam sistem backend dan tidak tersedia untuk pengguna. Dengan demikian, komponen-komponen tersebut tidak dievaluasi oleh pemangku kepentingan. Satu-satunya komponen yang dinilai adalah komponen dengan antarmuka pengguna grafis.



Gambar 9.3. Komponen Siber-Trust (Gambar digunakan dari video diseminasi Siber-Trust).

Tabel 9.2. Distribusi kemampuan antar komponen.

Komponen & layanan C-T	Deteksi	Perlindungan	Mitigasi	Penyimpanan Dan Berbagi
Layanan Perayapan	X			
Layanan Profil				X
Modul Perangkat Cerdas	X	X		
Modul Pendaftaran				X

Layanan Manajemen Kepercayaan	X	X	X	
Respons Intrusi Yang Cerdas	X		X	
Modul Gerbang Cerdas	X		X	
Teknologi Buku Besar Terdistribusi				X
Repositori Jaringan	X			
Layanan Pertahanan Siber	X		X	

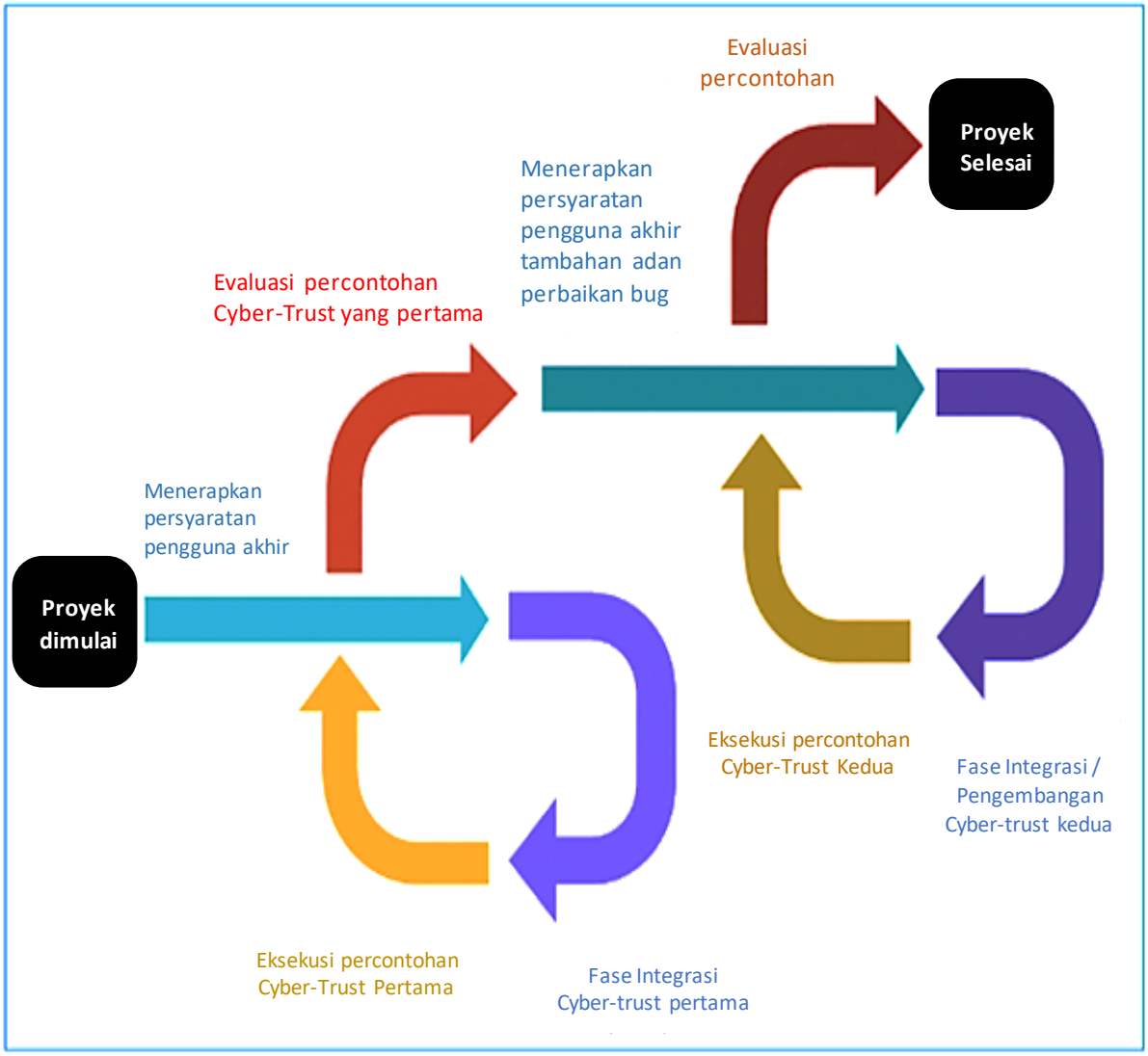
Pada Tabel 9.2 komponen diklasifikasikan berdasarkan kemampuannya. Berikut analisis deskriptif alat berdasarkan kemampuannya:

- Layanan Perayapan bertanggung jawab untuk mendeteksi halaman web dan situs web terkait keamanan mengenai ancaman sibersecara cerdas untuk mengidentifikasi ancaman yang muncul, perangkat eksploitasi, dan kerentanan zero-day.
- Layanan Profiling menyimpan informasi dan profil secara terpusat yang terhubung ke perangkat Siber-Trust dan mendeteksi korelasi informasi perangkat yang ada dengan data yang baru diperoleh dari repositori dan sumber aman lainnya.
- Modul Perangkat Cerdas berjalan di perangkat dan memberi tahu pengguna tentang status kesehatan perangkat mereka (seperti deteksi kerentanan, pembaruan firmware, dll.). Pengguna akan diberi tahu melalui saluran peringatan, seperti pesan aplikasi seluler.
- Modul Registrasi memberikan kemampuan registrasi ke berbagai aktor, seperti pengguna dan organisasi termasuk Smart Home Owners (SHOs), Internet Service Providers (ISPs), Law Enforcement Agencies (LEAs).
- Layanan Manajemen Kepercayaan mengumpulkan tindakan/perilaku dan kerentanan perangkat IoT dan meresponsnya dengan meningkatkan atau menurunkan kepercayaan.
- Respons Intrusi Cerdas yang berjalan pada gateway jaringan di lokasi pengguna yang menyediakan pemantauan berkelanjutan terhadap status keamanan Rumah Pintar dan perhitungan kemungkinan tindakan mitigasi terhadap serangan siberyang canggih.
- Modul Smart Gateway adalah komponen yang berjalan pada gateway jaringan dan menggunakan teknik Machine Learning untuk mengidentifikasi anomali jaringan.
- Layanan Buku Besar Terdistribusi (Blockchain) pada dasarnya terkait dengan penyimpanan integritas dan peningkatan kemampuan berbagi melalui blockchain. Beberapa operasi utama adalah penyimpanan data yang berkaitan dengan bukti forensik, validasi transaksi, konsensus, dll.
- Repositori Jaringan adalah seperangkat alat yang digunakan untuk mengumpulkan, mengelola, dan menyimpan informasi tentang arsitektur jaringan termasuk topologi dan pertahanan keamanan.
- Layanan Pertahanan Siber menangani pendeteksian dan mitigasi serangan siber pada jaringan

Tahap Integrasi

Siber-Trust memerlukan dua (2) fase integrasi dalam siklus hidupnya, saat ini fase pertama telah berhasil dicapai. Pentingnya hal ini berasal dari fakta bahwa komponen Siber-

Trust melalui fase ini (a) menjadi berfungsi dan (b) saling berhubungan sebagai satu sistem terpadu. Tiga tes berturut-turut dimasukkan ke dalam metodologi Integrasi yang lengkap. Pengujian tersebut adalah (a) Pengujian Fungsional, (b) Rencana Uji Stres (termasuk Uji Beban dan Stres, Dimensi Pemanfaatan Sumber Daya) dan (c) Rencana Uji Penetrasi. Integrasi sistem dan pengujian fungsional secara keseluruhan difokuskan pada alur kerja (Kasus Penggunaan), dan tujuannya adalah untuk memastikan bahwa pesan komponen dikirimkan dengan benar dan komponen Siber-Trust berkomunikasi dengan baik. Setiap alur kerja telah dianalisis dengan hubungan komunikasi antara berbagai komponen yang diidentifikasi. Versi pertama dari platform terintegrasi digunakan pada tahap percontohan pertama.



Gambar 9.4. Rencana keseluruhan pengembangan dan evaluasi Siber-Trust.

Proses Percontohan dan Evaluasi

Seperti yang ditunjukkan pada Gambar 9.4, proses evaluasi dilaksanakan dalam dua (2) siklus pengembangan Siber-Trust atau "sprint" yang berulang. Siber-Trust menangkap dan mengimplementasikan kebutuhan pengguna akhir pada sprint pertama, kemudian dilanjutkan dengan implementasi sistem sebelum tahap percontohan pertama. Sebelum dimulainya

"musim semi" kedua dan selama durasinya, komentar yang dikumpulkan selama uji coba pertama akan diterapkan. Tujuan dari struktur ini adalah agar pengguna akhir menerima produk yang mereka inginkan dan mendapatkan manfaat dari penggunaannya.

Uji Coba Percontohan

Uji coba menyadari keduanya secara sinkron dan asinkron. Pengujian sinkron dilakukan secara real-time dalam uji coba percontohan melalui serangkaian sesi evaluasi sistem yang memanfaatkan slot khusus enam (6) jam. Pengujian asinkron dilakukan dari jarak jauh, sesuai kecepatan evaluator, sepanjang periode percontohan pertama (pertama). Kedua metode pengujian ini memungkinkan pengguna akhir untuk menjalankan platform dan mendapatkan pengalaman dari platform tersebut sekaligus memberikan umpan balik dan komentar yang berharga untuk tahap evaluasi kedua. Selama kedua metode pengujian, hak asasi manusia, kepatuhan GDPR (679/2016) dan peraturan privasi elektronik diterapkan pada semua kasus percontohan untuk semua pengujian yang dilakukan.

Skenario Percontohan

Ketika platform dijalankan secara sinkron dan asinkron, skrip juga dibuat untuk kedua tujuan pengujian. Untuk jenis prosedur sebelumnya, satu (1) skenario percontohan terkonsolidasi dengan banyak kasus uji telah dibuat. Dalam skenario tersebut semua evaluator dapat berpartisipasi. Selama uji coba langsung, skenario serangan nyata dibuat, sehingga pengguna akhir terbiasa menangani serangan siber. Untuk jenis prosedur yang terakhir, empat (4) skenario percontohan berorientasi pengguna dengan beberapa kasus uji dibangun dan didistribusikan kepada pengguna akhir sehingga memberi mereka kesempatan untuk mengeksekusi semua kasus uji sebelum atau sesudah pengujian langsung. Melalui skenario tersebut, pengguna dapat meninjau kembali fitur dan aturan yang diterapkan pada platform (divisualisasikan melalui UI).

Verifikasi Fungsionalitas

Siber-Trust telah membuat rencana Verifikasi Fungsionalitas yang mencakup semua tindakan yang sesuai untuk memverifikasi fungsi proyek, sebagaimana ditentukan oleh kelompok pengguna akhir proyek. Persyaratan fungsional dan non-fungsional dimasukkan dalam Daftar Fungsionalitas. Daftar Fungsi dapat direvisi dan dilengkapi dengan status verifikasi (Tercapai, Tidak Tercapai, Sebagian, dan Dimodifikasi). Karena persyaratan pengguna akhir diubah menjadi spesifikasi sistem pada tahun awal proyek, status verifikasi persyaratan pengguna akhir memberikan jawaban atas pertanyaan "Apakah sistem yang dikembangkan ini melakukan apa yang dimaksudkan?".

Validasi Komponen (KPI)

Indikator Kinerja Utama (KPI) memvalidasi sistem dan komponen berdasarkan metrik numerik. Mitra teknis dan pengguna akhir dimungkinkan untuk memvalidasi platform dan memvalidasi komponen platform dan KPI berorientasi percontohan. Dalam sudut pandang yang lebih sederhana, validasi adalah prosedur yang memungkinkan untuk menjawab pertanyaan "Apakah kita membuat produk yang tepat?". KPI produk Siber-Trust diukur secara konstan selama fase percontohan dan integrasi. Baru-baru ini dan dibandingkan dengan fase integrasi terakhir, pengukuran menunjukkan bahwa nilai KPI meningkat tajam (dengan

sebagian kecil nilai konstan), yang menunjukkan bahwa kualitas kinerja produk terus meningkat.

Kuesioner Kegunaan

Sebuah kuesioner utama dikembangkan dalam pengertian Siber-Trust. Kuesioner ini berisi pertanyaan-pertanyaan tertutup dengan skala Likert, dan tata letaknya difokuskan pada dua bidang utama: kepuasan platform dan efisiensi serta efektivitas operasi platform. Di kedua zona kuesioner, kerangka kuesioner dan pertanyaan disesuaikan dengan masing-masing target audiens pengguna akhir.

Kuesioner SiberTrust didasarkan pada metodologi System Usability Scale [8] (SUS) dan Technology Acceptance Model (TAM). SUS adalah alat yang andal untuk menghitung kegunaan. Jawabannya terdiri dari lima dan tiga pilihan skala likert untuk masing-masing responden mulai dari sangat setuju hingga sangat tidak setuju. Di TAM, ada dua faktor utama yang mempengaruhi keputusan pengguna tentang bagaimana dan kapan menggunakan teknologi. Kedua faktor tersebut adalah (a) persepsi kegunaan dan (b) persepsi kemudahan penggunaan. Keputusan pengguna akhir untuk menggunakan pendekatan yang dirancang dipengaruhi oleh kepribadian individu terhadap penggunaan metode tertentu. Sikap seseorang terhadap penggunaan suatu alat dipengaruhi oleh persepsi kegunaan dan kemudahan penggunaannya. Kedua metodologi yang disebutkan di atas ditampilkan dalam SiberTrust, Kemudahan Penggunaan yang Diukur dan manfaat yang dirasakan untuk memberikan analisis yang konsisten dan koheren.

9.4 DAMPAK EVALUASI

Selain kriteria kemanjuran dan kinerja, aksesibilitas sistem berbasis web kini menjadi lebih penting karena kepuasan pengguna yang merupakan salah satu faktor penentu yang kuat. Literatur akademis telah menyelidiki masalah kegunaan platform berbasis web. Penelitian sebelumnya telah menawarkan wawasan berharga mengenai kinerja platform berbasis web. Analisis sistematis diperlukan untuk menganalisis pekerjaan yang dilakukan dalam lingkungan keamanan siber, membandingkan temuan yang dikumpulkan, mengidentifikasi target topik dan tantangan yang masih belum terselesaikan, dan mendiskusikan topik penelitian masa depan yang mungkin dilakukan.

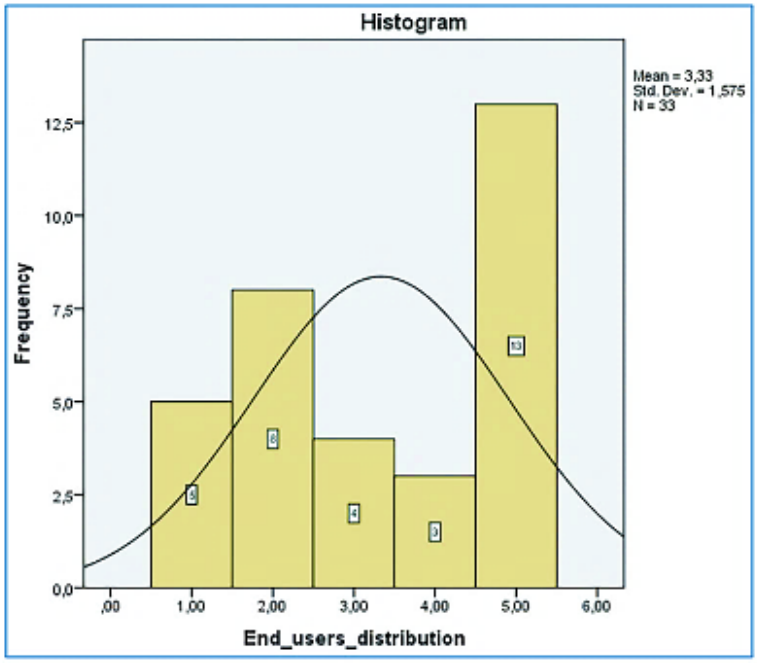
Tabel 9.3. Statistik distribusi pengguna akhir.

DISTRIBUSI PENGGUNA AKHIR				
	Persen Frekuensi		Presentase Yang Valid	Persen Kumulatif
LEAS yang valid	5	15,2	15,2	15,2
ISP	8	24,2	24,2	39,4
ISP dalam Lokakarya 3D	4	12,1	12,1	51,5
Admin	3	9,1	9,1	60,6
SOHOS	13	39,4	39,4	100,0
Total	33	100,00	100,00	

Selain hal-hal di atas, penilaian dampak sering kali digunakan untuk menentukan apakah suatu platform telah sepenuhnya terintegrasi. Hal ini juga digunakan untuk mengatasi masalah desain produk, seperti menentukan solusi mana di antara alternatif yang dianggap paling menjanjikan oleh platform. Tahap percontohan kedua diselesaikan oleh kelompok pengguna akhir Siber-Trust (Tabel 9.3), dan hasil kuesioner yang menganalisis dampak terhadap komunitas pengguna akhir diberikan di bawah ini.

Diagram di atas menggambarkan distribusi pengguna akhir. Gambar tersebut juga menggambarkan distribusi normal. Apa yang diberikan adalah adil mengingat distribusi pengguna akhir SiberTrust dan antarmuka jaringan yang tersedia (Gambar 9.5).

Tujuan dari konsorsium SiberTrust adalah untuk melihat apakah tanggapan yang diberikan konsisten dan dapat dipercaya. Alfa Cronbach (atau koefisien alfa) dirancang oleh Lee Cronbach untuk menilai konsistensi survei skala Likert dengan beberapa pertanyaan. Peringkat konsistensi total suatu ukuran ditentukan oleh koefisien keandalan, yang berkisar antara 0 hingga 1. Dengan rata-rata konsistensi internal 0,968, pengguna akhir menilai keandalan 96,8% dengan platform CT.



Gambar 9.5. Grafik distribusi pengguna akhir.

Alfa Cronbach	Konsisten Internal
a≤ 0,9	Bagus sekali
0,9 > a ≥ 0,8	Bagus
0,8 > a ≥ 0,7	Dapat diterima
0,7 > a ≥ 0,6	Dipertanyakan
0,6 > a ≥ 0,5	Miskin
0,5 > sebuah	Tidak dapat diterima

Gambar 9.6. Interpretasi alfa Cronbach.

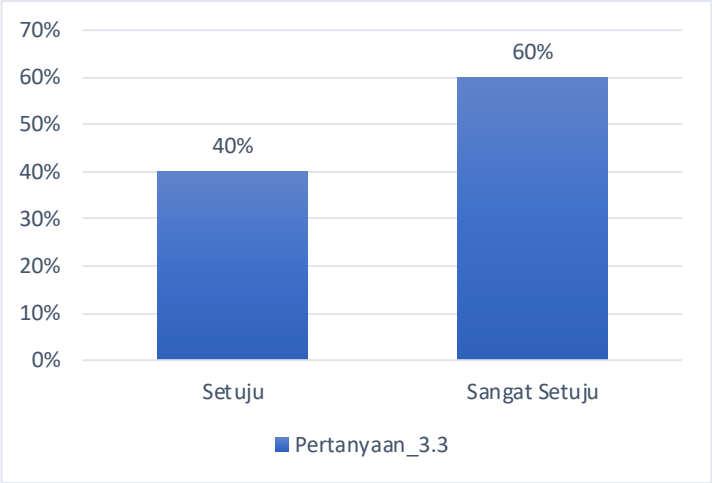
SEWA		
Alfa Cronbach	Alfa Cronbach Berdasarkan item Standar	N item
.963	.973	22

ISP		
Alfa Cronbach	Alfa Cronbach Berdasarkan item Standar	N item
.972	.946	23

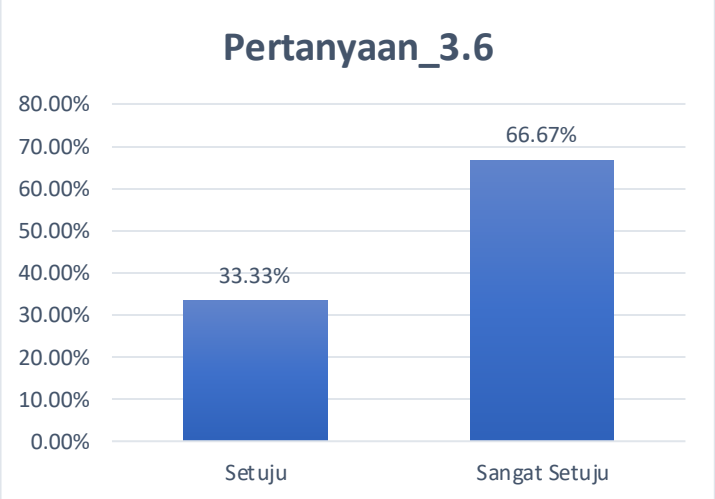
ADMIN		
Alfa Cronbach	Alfa Cronbach Berdasarkan item Standar	N item
.991	1.000	15

SOHOS		
Alfa Cronbach	Alfa Cronbach Berdasarkan item Standar	N item
.949	.951	25

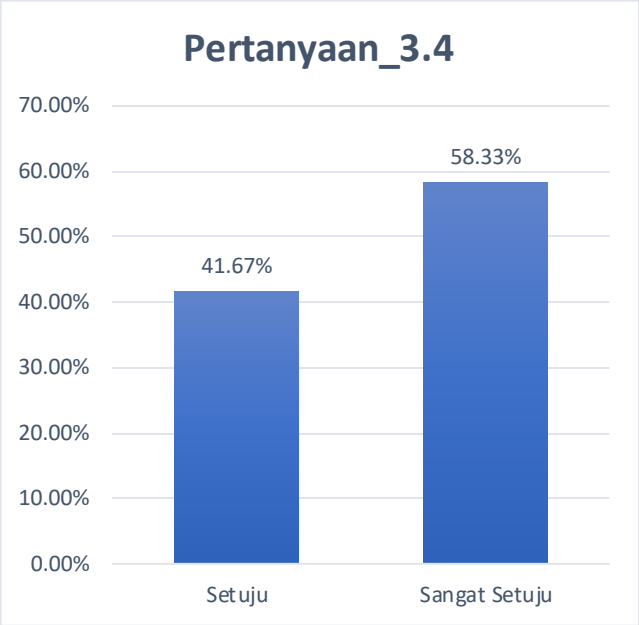
Gambar 9.7. Hasil alfa Cronbach seperti yang ditunjukkan oleh empat kelompok pengguna akhir yang berbeda.



Gambar 9.8. Persentase evaluator menjawab pertanyaan "Saya merasa mudah mempelajari cara bernavigasi dalam platform Siber-Trust".



Gambar 9.9. Persentase pengguna menjawab pertanyaan "Saya merasa sangat percaya diri dalam menyelesaikan semua pekerjaan saya menggunakan platform Siber-Trust".



Gambar 9.10. Saya berhasil mengakses dan mengambil semua informasi yang diperlukan.

Mayoritas jawaban terhadap kuesioner evaluasi menunjukkan bahwa kemudahan penggunaan platform meningkat dengan cepat. Dengan skor keramahan pengguna sebesar 62%, CT tampaknya merupakan platform yang ramah pengguna. Selain itu, dalam hal navigasi dan masalah yang memakan waktu, pengguna akhir merasa nyaman dan sesuai dengan kebutuhan mereka.

Gambar 9.11. Persentase pengguna menjawab pertanyaan "Dalam 2D-UI: Saat saya masuk ke sistem, saya menggunakan aturan minimal 3 klik untuk mengakses informasi terkait serangan siber".

Gambar 9.12. Persentase pengguna menjawab pertanyaan "Saya membayangkan sebagian besar pengguna akhir akan setuju bahwa Siber-Trust diperlukan untuk melindungi perangkat IoT mereka dari serangan siberyang berbahaya".

CT tampaknya merupakan platform yang dapat beradaptasi dengan beragam kebutuhan pengguna akhir, dengan skor rata-rata 60%. "Saya merasa cukup percaya diri dalam menyelesaikan semua pekerjaan saya dengan menggunakan platform Siber-Trust," kata 67 persen responden yang disurvei sebagai jawaban atas pertanyaan tersebut. Data ini menunjukkan seberapa relevan pengguna akhir menilai "kemudahan penggunaan" platform SiberTrust. Dan yang terakhir, 58 persen mengindikasikan bahwa mereka mampu mengakses dan mendapatkan semua informasi yang mereka perlukan, yang menunjukkan manfaat platform tersebut.

Gambar 9.13. Saya tidak mengalami gangguan apa pun (misalnya sakit) selama interaksi 3D.

Gambar 9.14. Saya berhasil menavigasi dan melihat semua informasi ID CVE tertentu.

Dalam hal kemanjuran dan efisiensi platform, 100 persen audiens pengguna akhir percaya bahwa antarmuka pengguna (UI) Siber-Trust mengikuti aturan tiga klik untuk memperoleh informasi mengenai serangan siber. Selain itu, 46% pengguna akhir komunitas Siber-Trust sangat setuju bahwa Siber-Trust sangat penting untuk melindungi perangkat IoT mereka dari serangan siberyang berbahaya. Terakhir, jika mengacu pada komponen 3D SiberTrust, 100 persen pengguna mengatakan mereka tidak merasakan gangguan apa pun (seperti sakit) selama interaksi 3D serta hanya menavigasi dan melihat semua informasi dari ID CVE tertentu.

9.5 KESIMPULAN

Singkatnya, pengumpulan dan analisis data dari kegiatan percontohan mengungkapkan tingkat kepuasan para pemangku kepentingan dan tingkat kinerja sistem. Lebih khusus lagi, keterkaitan tugas-tugas proyek (berisi kasus penggunaan, kebutuhan pengguna, hasil akhir yang canggih, dan deskripsi alat) sejak awal, memungkinkan Siber-Trust mencatat kebutuhan para pemangku kepentingan serta bidang penerapannya. - tion dari platform. Desain metodologi evaluasi dibuat berdasarkan standar yang diketahui (SUS, TAM), disesuaikan dengan ruang lingkup proyek, dan materi evaluasi dirancang untuk menilai kemajuan teknologi Siber-Trust. Selain itu, komentar-komentar selama tahap percontohan akhirnya mengarah pada modifikasi drastis atau peningkatan elemen evaluasi. Oleh karena itu, Proses Evaluasi Siber-Trust sangat penting tidak hanya untuk mengumpulkan informasi dan mengevaluasi uji coba, namun juga untuk memberikan umpan balik mengenai fitur-fitur dalam antarmuka pengguna grafis (GUI) dan prosedur apa yang perlu ditingkatkan. Hasil yang diperoleh melalui platform SiberTrust akan mengarah pada kemajuan solusi revolusioner yang meningkatkan visibilitas komersial dan kelayakan produk dengan tingkat kesiapan teknis tinggi yang menawarkan solusi komprehensif terhadap masalah keamanan siber.

BAB 10
UJI COBA RUMAH PINTAR (SMART HOME) UNTUK BISNIS

Pada sub bab 10.1, pentingnya pengujian ini, baik dari sudut pandang pemasaran dan eksploitasi untuk berbagai jenis organisasi; mereka akan mendapat manfaat dari eksploitasi hasil dan informasi relevan, yang timbul dari penggunaan dan pemanfaatan platform tersebut. Pada sub bab 10.2, kami menyajikan persyaratan, baik teknis maupun non-teknis serta interkonektivitas berbagai teknologi heterogen yang ada. Pada sub bab 10.3, hasil utama disajikan dan berikut beberapa pembahasannya. sub bab 10.4 didedikasikan untuk eksploitasi hasil, dampaknya terhadap potensi bisnis dan kemungkinan perluasan.

10.1 PENDAHULUAN

Saat ini, produksi besar-besaran perangkat pintar yang terjangkau, mudah diakses dan digunakan, dikombinasikan dengan peningkatan dan perbaikan jangkauan jaringan telekomunikasi telah menyebabkan munculnya apa yang disebut SoHos. Selain itu, kompleksitas ekstrem, terkait dengan fakta bahwa data, jaringan yang hidup berdampingan (seringkali beberapa jenis jaringan), dikirimkan dari beberapa jaringan, yang berada di tempat yang sama, keberadaan protokol yang berbeda secara berdampingan, seperti 4G, 5G, Wi-Fi , dll. serta kebutuhan akan komunikasi mesin-ke-mesin yang berkelanjutan dan protokol terkait (misalnya Bluetooth) merupakan indikasi tingkat kompleksitas yang ada. Untuk mencapai tujuan ini, masalah keamanan dan privasi, yang timbul akibat adanya protokol yang berbeda dan fakta bahwa data yang sama dikirimkan melalui protokol yang berbeda dan pada saat yang sama terekspos ke internet, menyebabkan peningkatan kompleksitas lebih lanjut.

Popularitas SoHo dan penerapannya oleh semakin banyak orang di seluruh dunia semakin meningkat, baik di lingkungan non-komersial maupun komersial. Terbukti, ada entitas, seperti organisasi, perusahaan, dan badan, yang termasuk dalam kategori terakhir, yang dapat memperoleh manfaat besar dari hasil yang dihasilkan, kesimpulan yang diambil, dan pembelajaran, setelah melakukan penelitian tentang SoHos. Entitas-entitas ini termasuk, namun tidak terbatas pada kategori utama berikut:

- Teknologi Informasi dan Komunikasi (TIK)
- Organisasi penelitian yang melakukan dan/atau tertarik melakukan uji coba
- Organisasi/perusahaan keamanan
- Organisasi/perusahaan teknologi mana pun yang fokus atau aktif di bidang teknologi, layanan, dan/atau perangkat pintar terkait SoHo

Oleh karena itu, setelah berkontribusi aktif di bidang teknologi keamanan, pengaturan testbed, secara umum; dan setelah melakukan penelitian di lapangan yang sedang dipertimbangkan melalui partisipasi aktif KEMEA dalam uji coba dan pelaksanaan proyek percontohan “Siber-Trust (CT)”, kontribusi OTE/Cosmote dalam uji coba, dan kontribusi CGI dalam eksploitasi dan penyerapan pasar, kami berada dalam posisi yang sangat baik untuk menyajikan dan berbagi hasil dan spesifikasi yang berharga, berdasarkan eksperimen yang berhasil dilakukan dalam konteks “Siber-Trust”. Hasil-hasil yang dapat dieksploitasi dari

“Siber-Trust” sebagian besar berada dalam lingkup solusi, strategi, dan bidang bisnis, keuangan, teknologi, dan penelitian yang potensial dari segi bisnis dan eksploitasi.

Sekarang, kita lanjutkan dengan spesifikasi, baik teknis maupun non-teknis, yang diperlukan dalam proses pengaturan tempat pengujian, interkonektivitasnya, teknologi heterogen yang berbeda-beda yang ada serta beberapa alat, persyaratan, dan detail penting.

10.2 SPESIFIKASI PENGUJIAN SIBER-TRUST

Pertama-tama, testbed telah disiapkan dengan bantuan teknologi virtualisasi yang berbeda dan secara intrinsik heterogen, baik itu:

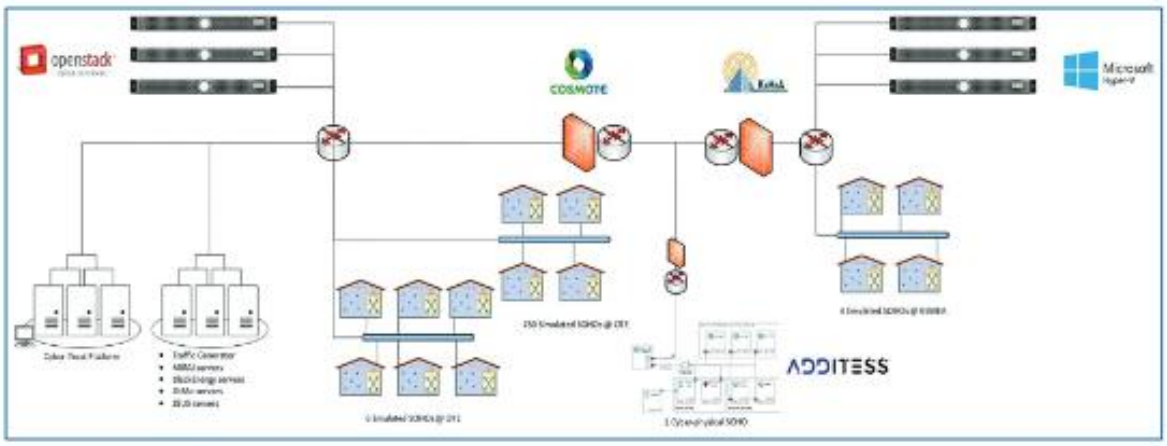
- Microsoft Hyper-V: yang diinstal di lokasi KEMEA dan telah digunakan untuk menyiapkan testbed KEMEA dan Mesin Virtual (VM) terkait; ini tidak berbasis cloud.
- OpenStack: yang merupakan perangkat lunak cloud sumber terbuka; itu diinstal di lokasi OTE dan telah digunakan untuk mengatur SoHoVM OTE
- Beragam Sistem Operasi yang digunakan untuk siber-fisik

Uji coba ini tidak hanya mencakup SoHos tetapi juga platform Siber-Trust, Server Komando dan Kontrol untuk serangan Mirai, Black Energy, ZEUS, dan ZitMo.

Jadi, masing-masing teknologi yang disebutkan di atas harus:

- saling berhubungan
- dibuat untuk bekerja terus menerus, dalam waktu nyata (atau setidaknya kadang-kadang terus menerus), dan
- tersinkronisasi dan mampu berinteraksi dengan pengguna senyata mungkin, sehingga mampu meniru fungsi dan karakteristik rumah pintar dan/atau jaringan rumah pintar di dunia nyata

Tidak dapat disangkal, testbed ini, yang representasi grafisnya ditunjukkan pada Gambar 10.1, benar-benar kompleks dari sudut pandang infrastruktur serta dari sudut pandang konektivitas dan fungsionalitas. Namun demikian, tingginya tingkat kompleksitas ini tidak hanya dapat dibenarkan, namun hal ini juga diperlukan. Signifikansi kompleksitasnya terletak pada kenyataan bahwa sistem dunia nyata benar-benar kompleks dan melibatkan beragam teknologi berbeda yang hidup berdampingan, sehingga kompleksitas yang mendasari pengujian dianggap perlu, jika simulasi dibuat serealistis mungkin. Oleh karena itu, dengan mempertimbangkan berbagai teknologi yang ada di dunia nyata (seperti Bluetooth, 4G/5G, Wifi, inframerah, apalagi perbedaan arsitektur, versi, dan implementasinya), sumber daya yang diperlukan, dan biaya teknologi yang sebenarnya -dunia pengujian, banyaknya waktu yang dihabiskan untuk menyiapkan pengujian kompleks kami dan kesulitan yang terlibat dapat dibenarkan.



Gambar 10.1. Representasi grafis dari pengujian kepercayaan siber.

Struktur, komponen dan karakteristik dasar serta sumber daya dari setiap simulasi SoHoof yang kami uji ditunjukkan pada Gambar 10.2, di bawah ini:

S0H0	A05/TMS	A13/IRE	A13/IRG	A04/A16	MTSPL	Ubuntu	WINXP	Win7	Win7SP2	A12/SDA	Android	Bbox#1	Bbox#2	TOTAL	VCPU	VRAM (GB)	VHDO(GB)
SOHO1	1	1	1	1	1		1	1		1	1	1	1	11/7	20	66	352
SOHO2	1	1	1	1	1				1	1	1	1	1	11/6	18	58	320
SOHO3	1	1	1	1		1		1		1	1	1	1	11/6	18	58	320
SOHO4	1	1	1	1		1			1	1	1	1	1	11/6	18	58	320
SOHO5	1	1	1	1	1	1			1	1			1	11/5	20	64	336
SOHO6	1	1	1	1	1	1				1	1		1	11/6	28	56	304
SOHO7	1	1	1	1	1	1		1		1	1		1	11/6	24	70	390
SOHO8	1	1	1	1	1	1		1		1			1	11/6	22	72	416
SOHO9	1	1	1	1		1	1		1	1	1	1	1	11/6	24	72	406
SOHO10	1	1	1	1		1	1		1	1			1	11/6	22	74	432
TOTAL SUMBER DAYA YANG DIALOKASIKAN UNTUK RUMAH PINTAR															202	652	3708

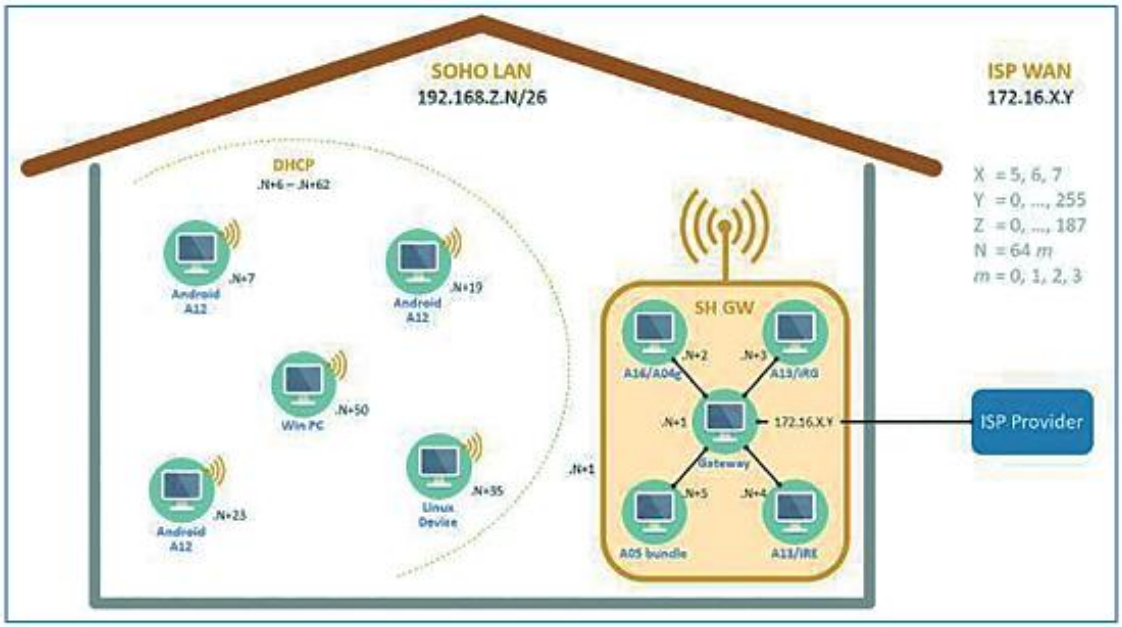
Gambar 10.2. Komponen mesin virtual dari testbed biasa.

10.3 INTERKONEKTIVITAS MELALUI PROSES ROUTERING AD-HOC

Interkonektivitas di antara jaringan heterogen telah dicapai melalui proses routering yang disesuaikan, dengan tabel perutean IP yang ditentukan pengguna, yang menyimulasikan paparan alamat IP dari penyedia serta proses perutean di dalam negeri, bisnis, dan jaringan. jaringan industri, yang menjadi tuan rumah SoHos. Emulator router adalah UbuntuVM yang mengimplementasikan proses perutean. Bersama dengan generator lalu lintas, yang merupakan UbuntuVM lain, yang bertanggung jawab atas pembuatan lalu lintas jaringan. Selain itu, untuk memastikan koneksi terjalin dengan aman, sertifikat khusus yang diperlukan telah diterbitkan dan dipasang di setiap SoHo; perangkat lunak sumber terbuka OpenVPN telah digunakan untuk membuat koneksi aman melalui Secure Sockets Layer (SSL) dan juga layanan ssh standar di Ubuntu. Dalam kasus Sistem Operasi yang berbeda, alat OpenSSH telah digunakan untuk tujuan yang sama.

Komponen SoHo Kepercayaan Dunia Maya

Oleh karena itu, representasi grafis dari SoHoto yang kami terapkan beserta koneksi dan interaktivitasnya dengan Penyedia Layanan Internet (ISP) serta jaringan eksternal atau internal (misalnya WAN, LAN, dll.) disajikan pada Gambar 10.3 di bawah.



Gambar 10.3. Ekosistem rumah pintar (SoHo) yang diterapkan.

10.4 METODOLOGI YANG DI GUNAKAN

Mengingat pengujian yang dipertimbangkan terletak pada infrastruktur yang berbeda, konversi hard disk virtual ke format yang diinginkan, kompilasi silang, dan tugas pembangunan memainkan peran penting dalam menegakkan dan menjaga kompatibilitas di berbagai lingkungan. Selain itu, penetapan prosedur pengujian/verifikasi yang berkelanjutan, memastikan kelangsungan tempat pengujian yang berinteraksi, merupakan hal yang sangat penting.

Mengenai konversi antara berbagai format disk virtual, seperti VDI (Oracle Virtualbox, openstack), VMDK (Oracle Virtualbox, produk VMWare, QEMU, Parallels Desktop for Mac, openstack), VHD (Hyper-V, Oracle Virtualbox, openstack) , VHDX (Hyper-V, openstack), format file gambar Parallels version2 HDD (Oracle Virtualbox), qcow2 (openstack, QEMU), mentah (hanya untuk menyebutkan beberapa yang banyak digunakan), alat sumber terbuka telah digunakan. Alat-alat ini termasuk qemu-img , alat baris perintah VBoxManage serta Star-Wind V2V Converter.

Selain itu, beberapa jenis eksperimen telah dilakukan, termasuk serangan siber, pencatatan serangan, dan peringatan tingkat keparahan telah dihasilkan dan disajikan secara grafis melalui Antarmuka Pengguna Grafis (GUI), yang dibuat dan diatur dalam Proyek yang sama. untuk menjembatani Interaksi Manusia-Komputer (HCI); yaitu antarmuka platform.

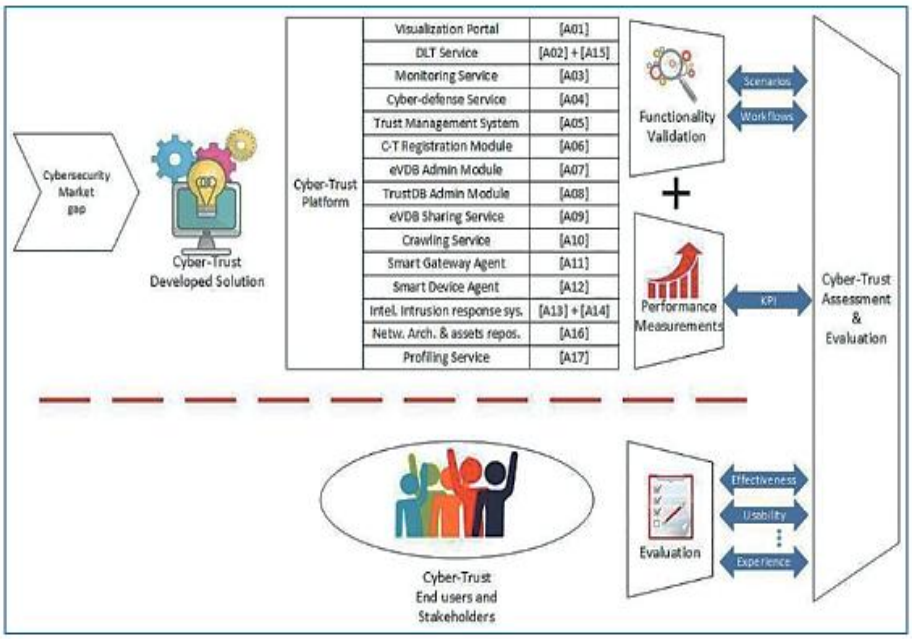
10.5 HASIL & PEMBAHASAN

Sekarang, kami menyajikan hasil yang dihasilkan. Fungsionalitas testbed telah terbukti sangat baik. Lebih khusus lagi, tahapan penilaian Siber-Trust, evaluasi, integrasi, pengujian, pelaksanaan percontohan dan analisis hasil bersama dengan hasil yang sesuai (yaitu hasil

verifikasi fungsionalitas, hasil evaluasi, hasil pengukuran kinerja, dll.) telah tersedia hingga saat ini. Ini termasuk:

i. Integrasi sistem dan hasil pengujian fungsional secara keseluruhan: Platform Siber-Trust didasarkan pada arsitektur berorientasi layanan yang digerakkan oleh peristiwa dan digabungkan secara longgar yang menerapkan pendekatan publikasi/berlangganan, didukung oleh komunikasi komponen langsung melalui antarmuka RESTful.
ii. Hasil Pengujian Kinerja: Pengujian beban dan tegangan telah dilakukan dan Indikator Kinerja Utama (KPI) yang sesuai telah ditetapkan dan dievaluasi. Pengujian tersebut mencakup pengujian regresi, pengujian konektivitas dan aksesibilitas layanan, pengujian beban dan tekanan, dll.
iii. Hasil evaluasi pengguna akhir : Proses evaluasi mencakup berbagai metode yang digunakan untuk menilai materi evaluasi. Hal ini juga menyajikan materi evaluasi (misalnya manual, kuesioner, skenario uji kasus, persyaratan, KPI, dll. Secara lebih rinci, jenis pengujian sinkron dan asinkron digunakan untuk mengevaluasi platform secara keseluruhan dan layanannya. Sinkronisasi pengujian kronus dilakukan secara bersamaan dalam serangkaian sesi evaluasi sistem menggunakan slot khusus berdurasi tiga jam (3), dengan keterlibatan berbagai pemangku kepentingan. Pengujian asinkron dilakukan sesuai kecepatan evaluator, dari jarak jauh. Demo pelatihan terhadap pengguna akhir juga telah dilakukan. Pada kedua metode pengujian, persyaratan fungsional diverifikasi oleh kelompok pengguna akhir terkait dan persyaratan non-fungsional diverifikasi baik dari mitra teknis maupun evaluator. Selain itu, uji kegunaan memeriksa efisiensi, efektivitas, kepuasan, kemudahan penggunaan dan kegunaan dibagikan.
iv. Pengujian penetrasi dan hasilnya (untuk diekstraksi/dipublikasikan): Ini akan
    - menentukan tingkat keamanan minimum;
    - mencakup pengujian penetrasi pada tingkat aplikasi;
    - dikaitkan dengan manajemen sesi, otentikasi, kontrol akses;
    - mempertimbangkan kompleksitas kata sandi, pengelolaan pengguna, edit/pulihkan kata sandi, port terbuka, proksi terbalik, dll;
    - mencakup praktik terbaik yang disebutkan, berdasarkan: OWASP, ASVF, ISO27001
    - menggabungkan peninjauan kode komponen yang menggunakan cara otomatis.

Semua hasil yang disebutkan di atas melampaui konteks saat ini; misalnya, pada bidang ilmiah termasuk e-privasi, GDPR, etika, dll. Gambaran umum prosedur Evaluasi dan Penilaian disajikan pada Gambar 10.4 di bawah.



Gambar 10.4. Prosedur evaluasi dan penilaian.

10.6 EKSPLOITASI HASIL & DAMPAK TERHADAP BISNIS

Hasil-hasil yang disebutkan di atas dapat dimanfaatkan secara besar-besaran, pertama-tama oleh anggota konsorsium proyek Siber-Trust, oleh organisasi, perusahaan, dan pihak berwenang, yang terlibat dalam bidang-bidang berikut atau serupa:

- TIK
- Penelitian dengan uji coba
- (Informasi keamanan
- Kejahatan Dunia Maya
- Solusi/perangkat/elektronik/peralatan rumah pintar
- Perangkat pintar

Selain itu, eksploitasi terhadap hasil-hasilnya melampaui kategori-kategori yang disebutkan di atas. Lebih khusus lagi, berdasarkan hasil yang dikumpulkan, diproses, dan pasca-pemrosesan setelah melakukan simulasi serangan siber dan uji coba terkait serta terkait, entitas yang berkepentingan dapat memanfaatkan sepenuhnya diantaranya dalam konteks berikut:

1. Simulasi serangan siber dan prediksi dampaknya terhadap bisnis. Simulasi berikutnya berdasarkan beberapa skenario dengan dan tanpa (kemungkinan) komponen yang terkena dampak dan evaluasi dampak terhadap bisnis bersama dengan skenario pemulihan bencana dan optimalisasi (adopsi skenario/skenario optimal. Optimasi dinamis dimungkinkan.
2. Selangkah lebih dekat ke (co-)simulation-in-the-loop berdampingan dengan aktivitas bisnis dunia nyata.
3. Pengujian dan pengerasan proses, komponen, peningkatan komponen pertahanan diri dan keamanan siber, peningkatan strategi failover.
4. Peningkatan perangkat, peralatan, perangkat lunak rumah pintar yang ada.
5. Perangkat, peralatan, perangkat lunak rumah pintar baru

6. Peningkatan interkonektivitas antara rumah pintar (smart home) dan perangkat rumah pintar (smart home) yang heterogen (secara teknologi).
7. Mengembangkan strategi untuk menjembatani dan mengatasi komponen/dan atau perangkat cerdas yang berbeda dan saat ini tidak kompatibel, termasuk namun tidak terbatas pada komponen yang memiliki komponen agnostik dan/atau kode sumber tertutup.

10.7 KESIMPULAN

Dalam buku ini, kami telah menyajikan hasil simulasi dan pengujian platform SoHo kami, potensi eksploitasinya di beberapa bidang, terutama dari sudut pandang bisnis serta dampaknya terhadap bisnis dan perluasan. Kami juga telah menganalisis tantangan-tantangan yang dihadapi, sejauh menyangkut kompleksitasnya, baik dalam hal interkonektivitas teknologi dan protokol yang secara inheren berbeda, meskipun teknologi dan protokol saling berinteraksi dan bekerja sama. Untuk mencapai tujuan ini, kami juga telah mempresentasikan metodologi yang berhasil kami adopsi, proses perutean khusus untuk memastikan interkonektivitas serta kerja sama antar komponen yang lancar dan tidak terputus. Terakhir, namun tidak kalah pentingnya, kami telah membahas penerapan penerapan kami secara luas dan membenarkan kebutuhan untuk menyiapkan pengujian yang kompleks, heterogen, dan menuntut sumber daya menuju realisasi lingkungan simulasi yang realistis dan hampir seperti dunia nyata.

BAB 11
REALITAS KEAMANAN DIGITAL

Organisasi saat ini memerlukan ketangkasan dan inovasi untuk menghadirkan pengalaman digital yang lancar kapan saja, di mana saja. Sebagai tanggapannya, ekosistem pelanggan, karyawan, dan pemasok menjadi lebih kompleks, terhubung, dan terbuka. Pada saat yang sama, risiko dan ancaman dunia maya semakin cepat dan kompleks.

Untuk mengatasi tantangan-tantangan ini, perusahaan memerlukan pendekatan keamanan siber yang seimbang dan proaktif. Hal ini mencakup pengelolaan identitas dan akses digital manusia dan non-manusia, melindungi teknologi informasi dan operasional, mengamankan lingkungan multi-cloud, menjaga beban kerja otomatisasi dan kecerdasan buatan, serta mematuhi peraturan yang semakin meningkat.

Realitas keamanan digital untuk lingkungan kerja modern saat ini telah teruji dan terbukti. Kami menghadirkan akselerator dalam bentuk model kedewasaan, arsitektur referensi, pengetahuan teknis, keahlian lintas domain, metode manajemen risiko, dan pembelajaran klien untuk mempercepat dan memberdayakan bisnis Anda. Dengan Layanan dan Akselerator Keamanan Siber CGI, Anda dapat meningkatkan ketangkasan dan inovasi sekaligus memastikan manajemen risiko siber yang holistik. Dalam bab ini, kami membahas realitas keamanan digital dan apa artinya bagi keamanan siber, serta bagaimana CGI membantu kliennya mengamankan operasi mereka yang terhubung.

11.1 REALITAS KEAMANAN DIGITAL SAAT INI DAN KEAMANAN SIBER

Perusahaan terus berkembang untuk memberikan nilai kepada pelanggan, masyarakat, karyawan, dan pemegang saham dengan cepat sebagai respons terhadap kebutuhan yang berubah dengan cepat. Teknologi, sumber data, dan koneksi baru memungkinkan evolusi ini, termasuk lingkungan multi-cloud, komputasi edge, otomatisasi, kecerdasan buatan (AI), Internet of Things, 5G, layanan mikro, perangkat, dan antarmuka pemrograman aplikasi (Lebah). Namun, pelaku ancaman siber memanfaatkan kemajuan yang sama untuk menciptakan lanskap risiko yang semakin canggih dan dinamis. Perlombaan senjata keamanan siber semakin meningkat. Perusahaan juga memperluas ekosistem pemasok dan basis pelanggan mereka. Banyak di antara mereka yang terlibat dalam merger, akuisisi, divestasi, dan reorganisasi, serta semakin banyak tenaga kerja hibrida (manusia dan non-manusia) yang bekerja hampir di mana saja.

SENANG MENDENGARNYA

Semakin pentingnya keamanan siber:

- Keamanan siber adalah prioritas bisnis yang paling sering disebutkan
- 64% mengatakan mengamankan platform cloud adalah prioritas utama keamanan siber bagi organisasi mereka
- 25% mengatakan mereka tidak tahu apakah mereka memiliki mekanisme untuk menemukan lokasi pemrosesan dan penyimpanan aset data utama

Pelanggaran terkait identitas yang dapat dicegah:

- 79% organisasi pernah mengalami pelanggaran keamanan terkait identitas dalam dua tahun terakhir, dan …
- 99% yakin pelanggaran terkait identitas mereka dapat dicegah.

Masa depan adalah dunia hibrida:

- Pada tahun 2025, akan ada 55,7 miliar perangkat yang terhubung di seluruh dunia, 75% di antaranya akan terhubung ke platform IoT.
- Pada tahun 2023, 75% negara G2000 berkomitmen untuk memberikan kesetaraan teknis pada angkatan kerja yang bersifat hybrid, bukan berdasarkan keadaan, sehingga memungkinkan mereka untuk bekerja sama secara terpisah dan secara real-time.

Merger dan akuisisi semakin meningkat:

- Sejak tahun 2000, lebih dari 790.000 transaksi M&A telah diumumkan di seluruh dunia dengan nilai yang diketahui lebih dari Rp. 570 triliun.

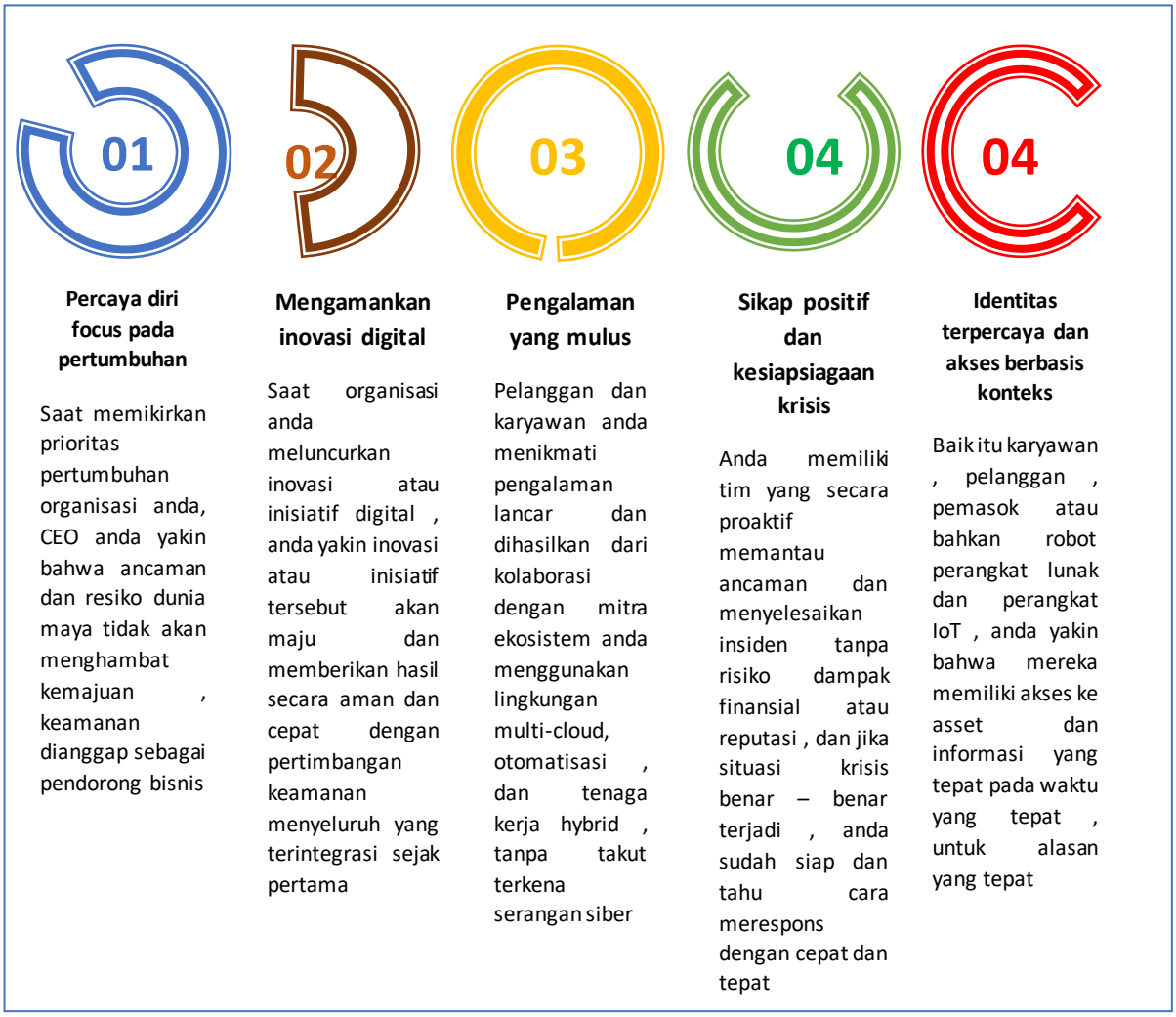
11.2 MELINDUNGI BISNIS TANPA MENGHAMBAT INOVASI DAN KECEPATAN

Dalam realitas digital ini, para eksekutif memiliki prioritas utama:

- Memungkinkan inovasi dan kolaborasi dengan cepat: Organisasi-organisasi saat ini melampaui batas-batas perusahaan tradisional hingga ke ekosistem eksternal—begitu juga dengan keamanan. Pendekatan modern di seluruh rangkaian operasi keamanan memungkinkan terciptanya, pengoperasian, dan evolusi ekosistem yang fleksibel, efisien, dan kolaboratif dengan aman, serta memastikan pengalaman yang lancar.
- Mengurangi eksposur risiko dan mengelola risiko secara efektif: Pendekatan manajemen risiko berbasis wawasan menggunakan data yang kaya untuk mengidentifikasi dan mengelola risiko secara holistik di seluruh perusahaan hampir secara real-time, sehingga memungkinkan mitigasi risiko yang proaktif dan komprehensif serta respons yang cepat terhadap ancaman. Hal ini mencakup pengelolaan identitas digital manusia dan non-manusia serta akses amannya, pemantauan dan respons ancaman tingkat lanjut, dan sebagainya.
- Meningkatkan kepatuhan terhadap peraturan: Data ada di mana-mana dan mendorong inovasi, peluang pendapatan baru, pengalaman pengguna yang lebih baik, dan operasi yang optimal. Memastikan akses yang tepat terhadap data ini sangat penting untuk mematuhi peraturan yang semakin ketat.
- Mengadopsi sikap proaktif melalui kesadaran situasional secara real-time: Hal penting dalam operasi keamanan modern adalah memiliki proses, keterampilan, dan teknologi yang tepat. Teknologi-teknologi ini mencakup analitik tingkat lanjut, kecerdasan buatan, pembelajaran mesin, otomatisasi dan orkestrasi alur kerja keamanan siber, serta visualisasi real-time dari lanskap kerentanan dan ancaman Anda.
- Bersiap dan merespons secara efektif ketika krisis terjadi: Seiring dengan meningkatnya volume dan kompleksitas ancaman dan risiko dunia maya, organisasi modern bersiap

menghadapi situasi krisis dan siap merespons secara efektif, sambil menangkap pembelajaran.

Seperti apa kesuksesannya? Pada Gambar 11.1 jawabannya diberikan dengan rincian dan penjelasan.



Gambar 11.1. Seperti apa kesuksesannya?

11.3 LAYANAN PENASIHAT KEAMANAN SIBER CGI

Kami menyoroti delapan layanan konsultasi utama untuk membantu klien mencapai pendekatan seimbang terhadap keamanan siber dalam realitas digital baru yang kompleks dan terhubung ini.

Layanan IAM Digital

Variasi, volume dan kecepatan identitas manusia dan non-manusia (atau silikon) (misalnya, sensor Internet of Things, perangkat, perangkat lunak, kecerdasan buatan, layanan mikro, dan antarmuka pemrograman aplikasi) dan kebutuhan aksesnya semakin meningkat. secara dramatis. Dengan Layanan Penasihat IAM Digital kami, Anda dapat mencapai ketangkasan dan inovasi sekaligus menjaga identitas digital dan akses mereka ke sistem dan data penting tetap aman dan tanpa hambatan. Layanan kami berkisar dari strategi dan pengembangan peta jalan tata kelola dan administrasi identitas (IGA), hingga layanan

konsultasi IGA khusus untuk kelas baru silikon dan identitas eksternal, hingga desain model operasi IAM, hingga federasi dan integrasi IAM di seluruh perusahaan dan ekosistem Anda.

Saran Operasi Multi-Cloud yang Aman

Lingkungan hibrid dan multi-cloud menjadi hal yang normal dan baru, sehingga menciptakan lingkungan keamanan yang kompleks. Pakar kami dapat memberi saran kepada Anda tentang cara mengintegrasikan layanan cloud dengan aman ke dalam lanskap TI Anda. Kami memulai dengan penilaian kematangan dan eksposur risiko, lalu merancang cetak biru untuk membangun model operasi yang mengamankan operasi Anda di dunia hybrid. Kami mempercepat proses ini dengan menghadirkan kontrol yang telah ditentukan sebelumnya untuk Amazon Web Services, Microsoft Azure, dan Google Cloud, serta model kematangan dan arsitektur referensi.

Saran Otomasi Aman

Kita tahu bahwa otomatisasi adalah faktor utama yang memungkinkan terjadinya efisiensi biaya dan operasional, serta peningkatan pengalaman pelanggan. Banyak perusahaan berupaya mengotomatiskan tugas dan menggunakan kecerdasan buatan untuk mendorong otomatisasi tersebut, dan kami dapat membantu Anda melakukannya dengan aman. Melalui layanan konsultasi ini, kami menilai kematangan otomatisasi Anda, termasuk aspek keamanan, menggunakan model kematangan kami. Kami juga menilai titik permasalahan, mengidentifikasi masalah privasi data dalam proses (misalnya, panggilan keamanan dalam proses SDM), dan membuat katalog sistem target Anda.

Nasihat Manajemen Risiko Digital

Dunia digital hadir dengan risiko-risiko baru—mulai dari ancaman yang berkembang, sistem dan teknologi yang saling terhubung, lingkungan kerja dan TI yang hybrid dan tanpa perimeter, hingga peraturan data dan privasi yang kompleks. Hal ini memerlukan manajemen risiko yang lebih dinamis, lancar dan berkesinambungan, kesiapsiagaan terhadap krisis, dan respons yang cepat. Para ahli kami dapat membantu Anda mengelola risiko secara efektif, sekaligus memastikan Anda terus memberikan hasil bisnis dengan cepat. Layanan kami mencakup program manajemen risiko terintegrasi, visualisasi dinamis risiko perusahaan, penilaian privasi dan kepatuhan, ketahanan rantai pasokan dan manajemen risiko, kesiapsiagaan krisis keamanan siber, dan dukungan respons krisis.

Saran Modernisasi Operasi Keamanan Digital

Pendekatan operasi keamanan pada dekade terakhir atau bahkan lima tahun terakhir (misalnya pra-cloud, pra-smartphone, pra-kecerdasan buatan (AI), pra-bot, pra-Internet of Things/teknologi operasional) sudah tidak dapat dijalankan lagi. Tuntutan digital saat ini memerlukan perubahan mendasar dalam operasi keamanan, baik secara evolusioner maupun transformatif. Melalui layanan konsultasi kami, kami menilai kondisi kemampuan Anda saat ini dalam hal peralatan, proses, dan talenta. Hal ini termasuk mengevaluasi cakupan lingkungan Anda, sumber data, konektivitas, logging dan aliran peristiwa, analisis mendalam dan AI, pemrosesan insiden, intelijen ancaman, orkestrasi dan otomatisasi, kemampuan berburu, dan desain. Kami melaporkan temuan kami dan bersama-sama mengembangkan strategi dan peta jalan modernisasi dengan inisiatif praktis yang diprioritaskan (misalnya, re-platforming, pendampingan, dan peningkatan keterampilan/pelatihan). Kami juga

menawarkan layanan konsultasi hybrid "milik sendiri vs. beli" dan membantu Anda dalam mengembangkan kasus bisnis strategis pendukung.

Privasi Keamanan Siber berdasarkan Kerangka Desain

Akses yang lebih mudah ke platform pengembangan berarti lebih banyak pengembangan yang dilakukan di luar departemen TI (misalnya, pengembang warga dan TI bayangan). Perusahaan semakin mencari konektivitas dan interoperabilitas sistem dan layanan yang lebih besar dalam rantai pasokan mereka untuk meningkatkan efisiensi, kolaborasi, dan pengalaman pengguna. Peraturan dan pelanggaran data dan privasi mempunyai konsekuensi yang semakin mahal. Semua faktor ini memperkuat fakta bahwa memasukkan keamanan siber dan privasi ke dalam setiap proyek jauh lebih efisien dan efektif dibandingkan hanya mengelolanya begitu saja. Tim keamanan dan privasi harus menetapkan solusi standar dan siap pakai untuk semua proyek TI dan bisnis. Pakar kami dapat membantu Anda dalam membangun kerangka kerja untuk mencapai tingkat kesiapan dan penggunaan kembali ini. Setelah melakukan analisis menyeluruh terhadap lanskap Anda saat ini, kami merekomendasikan langkah-langkah khusus untuk mengisi kesenjangan, termasuk saran dan dukungan peralatan.

Desain Pusat Layanan Keamanan

Organisasi digital semakin memerlukan akses fleksibel terhadap keterampilan baru, retensi pengetahuan penting, dan otomatisasi untuk memastikan kelangsungan dan ketahanan bisnis. Kami dapat bekerja sama dengan Anda untuk merancang pusat layanan keamanan yang memenuhi kebutuhan modern, menstandardisasi praktik, dan memberikan tingkat keahlian yang tepat. Kami memulai dengan memahami layanan yang diperlukan, lalu membuat katalog layanan, merancang cara melibatkan pusat layanan, dan menetapkan proses perbaikan berkelanjutan.

Desain Model Operasi Keamanan

Saat Anda memulai inisiatif digital, struktur organisasi baru, atau merger, akuisisi atau divestasi, atau pemisahan, model operasi target keamanan (TOM) Anda harus disesuaikan untuk memastikan semua proses dan infrastruktur mencerminkan perubahan ini. Para ahli kami bekerja bersama Anda untuk merancang dan mengimplementasikan TOM Anda dengan menilai keadaan Anda sebagaimana adanya, mengidentifikasi kelemahan dan kesenjangan, merancang model baru (termasuk proses dan tata kelola), dan mendapatkan persetujuan dan penerimaan. Kami menggunakan templat yang telah terbukti dan praktik terbaik untuk mempercepat proses.

11.4 BROKER KONTROL AKSES UNTUK ASET DIGITAL IOT INDUSTRI

Untuk program besar berskala nasional yang melibatkan peluncuran jutaan aset digital industri IoT, CGI merancang, membangun, mengimplementasikan, menghosting, menjalankan, dan mendukung layanan data yang merupakan inti dari program ini. Layanan konsultasi IAM kami, bersama dengan layanan keamanan, memungkinkan perusahaan mengakses informasi guna meningkatkan layanan dan pengalaman pelanggan mereka. Layanan IAM ini sangat penting untuk menjaga kepercayaan konsumen yang mendasari program dan peluncuran secara nasional.

Solusi kami menyediakan layanan komunikasi dengan ketersediaan tinggi dan ketahanan tinggi sesuai dengan spesifikasi dan menyediakan fungsi kontrol akses yang secara kriptografis memvalidasi semua permintaan akses dan memverifikasi hak akses terhadap data pendaftaran IoT. Ini juga mencakup layanan penyedia identitas gabungan (IDP) di seluruh industri, yang menerapkan autentikasi dua faktor gabungan untuk karyawan pihak industri, penegasan peran dan hak istimewa menggunakan SAML, dan manajemen layanan mandiri oleh administrator pihak industri. Selain itu, layanan IDP juga mencakup pengelolaan staf istimewa yang efektif, pengelolaan risiko sesuai dengan ISO 27005, dan pemberian layanan keamanan terkait.

Pindah Ke Cloud Dengan Aman Dan Andal

Ketika sebuah perusahaan kedirgantaraan dan pertahanan besar berupaya menerapkan strategi migrasi cloud publiknya, keamanan data dan keandalan layanan merupakan hal yang sangat penting. Berdasarkan pengalaman signifikan kami dalam manajemen vendor pihak ketiga, serta pengelolaan lingkungan cloud dan risiko terkait, klien melibatkan kami untuk membantu menegosiasikan aspek manajemen keamanan kontrak cloud publiknya.

Hal ini termasuk mengembangkan lampiran keamanan standar dan klausul kontrak, menganalisis praktik keamanan penyedia cloud, mengadakan lokakarya negosiasi, dan memberikan penilaian risiko sisa. Untuk lampiran keamanan yang disesuaikan, kami menetapkan kriteria untuk memilih persyaratan keamanan yang berlaku berdasarkan jenis layanan dan peningkatan proses yang diidentifikasi. Selain menyelesaikan negosiasi, klien kini memiliki serangkaian persyaratan standar dan proses terdokumentasi untuk mendukung pengadaan di masa depan yang mencakup keterlibatan awal tim keamanan.

Inovasi, Kolaborasi, Kreasi Bersama, Eksperimen, Dan Pembuatan Prototipe Dengan Mitra Dan Klien

Kami berinvestasi dalam kolaborasi, inovasi, pertukaran pengetahuan dengan para ahli yang diakui secara internasional di bidang keamanan siber dengan tujuan untuk meningkatkan pengetahuan, keterampilan, layanan, dan pendekatan keamanan siber kami. Contohnya adalah proyek penelitian dan inovasi kemitraan Eropa Horizon 2020, Siber-Trust, di mana CGI bersama dengan 8 mitra lainnya dari 7 negara Eropa bekerja sama untuk mengembangkan inovasi ekosistem intelijen, deteksi, dan mitigasi ancaman siberyang canggih. Kami juga merupakan kontributor tetap dalam berbagai forum inovasi mengenai topik keamanan siber yang melibatkan klien dan mitra kami.

11.5 KEAMANAN SIBER YANG SEIMBANG DAN PROAKTIF

Kami memahami bahwa tanpa keamanan siber dan perlindungan privasi yang tepat, Anda akan menghadapi risiko dan hambatan yang terus berkembang dalam berinovasi dan berkolaborasi secara efektif. Oleh karena itu, tujuan kami sederhana. Kami ingin membantu Anda beroperasi dan bertransformasi dengan cepat dan percaya diri—saat ini dan di masa depan.

Dengan pengalaman selama 45 tahun dalam mengamankan sistem bisnis penting di berbagai industri secara global, pendekatan keamanan siber kami untuk lingkungan kerja modern saat ini telah teruji dan terbukti. Berkat pengalaman ini, kami menghadirkan akselerator dalam bentuk model kedewasaan, arsitektur referensi, pengetahuan teknis, keahlian lintas domain, metode manajemen risiko, dan pembelajaran klien untuk mempercepat dan memberdayakan bisnis Anda.

Dengan terus mengikuti perkembangan teknologi, ekosistem, dan ancaman yang berubah dengan cepat, konsultan kami bekerja sama dengan Anda untuk memahami lingkungan dan kebutuhan Anda. Kami membantu Anda mencapai keseimbangan yang tepat antara ketangkasan bisnis dan kemampuan pencegahan, pertahanan, deteksi, dan respons yang efektif.

BAB 12
KEAMANAN DAN PRIVASI PADA DIGITAL TWINS

Istilah Digital Twins merupakan salah satu topik penting dalam dunia digitalisasi yang semakin penting di berbagai bidang industri. Ada banyak perdebatan yang mengeksplorasi semakin pentingnya digital twins, termasuk kemungkinan bahwa mereka akan mengambil kendali atas manusia, atau kesulitan untuk berinteraksi dengan digital twins, pengguna akhir dari digital twins, dampaknya terhadap masyarakat dan keberlanjutan serta menjadikan dunia ini tempat yang lebih baik, dan yang tak kalah pentingnya, aspek keamanan dan privasi di Digital Twins. Bab ini akan mengeksplorasi keamanan dan privasi di Digital Twins berdasarkan presentasi penulis G. Sargsyan yang diberikan pada acara "Digital Twin a Promising Thing?" pada tanggal 29 Oktober 2020 di Amsterdam, yang disiarkan secara global dan diselenggarakan serta diselenggarakan oleh Amsterdam University of Applied Sciences bekerja sama dengan Digital Society School. Dalam acara ini penulis berbagi pandangannya tentang digital twins untuk berbagai industri, risiko, privasi, keamanan, dan pertimbangan etis dengan memperkenalkan contoh-contoh praktis, yang diperkenalkan dalam bab ini. Rekomendasi bagaimana mengelola risiko, masalah keamanan dan privasi juga ditawarkan dan didemonstrasikan dalam bab ini.

12.1 PENDAHULUAN

Kembar digital adalah replika virtual perangkat fisik yang menggabungkan ilmu data dan TI dapat digunakan untuk menjalankan simulasi sebelum perangkat sebenarnya dibuat dan diterapkan. Mereka juga mengubah cara teknologi seperti IoT, AI, dan analitik dioptimalkan. Kembaran digital (digital twins) menjadi suatu keharusan dalam bisnis, mencakup seluruh siklus hidup suatu aset dan membentuk landasan bagi produk dan layanan yang terhubung. Meskipun istilah "kembaran digital" pertama kali diciptakan pada tahun 2002, konsepnya sendiri sudah ada sejak lama. Pada tahun 1970 NASA memelopori gagasan bekerja dengan model digital sistem dunia nyata selama misi Apollo. Mampu membuat simulasi yang akurat, berdasarkan data dunia nyata, memainkan peran penting dalam membantu NASA membawa astronotnya kembali ke Bumi dengan selamat setelah kegagalan peralatan di Apollo 13.

Saat ini, kembaran digital (digital twins) menjadi suatu keharusan dalam bisnis, mencakup seluruh siklus hidup suatu aset dan membentuk landasan bagi produk dan layanan yang terhubung. Perusahaan yang gagal merespons akan tertinggal.

Ada banyak sekali riset pasar yang dilakukan mengenai topik Digital Twin. Sebagai contoh, fakta-fakta dan angka-angka terpilih diperkenalkan dari riset pasar. Menurut laporan MarketsAndMarkets, pasar kembar digital diperkirakan akan tumbuh dari Rp.3,1 miliar pada tahun 2010 menjadi Rp.48,2 miliar pada tahun 2026 dengan CAGR sebesar 58% dari tahun 2020 hingga 2026 dengan beberapa pengguna terbesar adalah layanan kesehatan dan pertahanan. Gartner berpendapat bahwa pada tahun 2021, setengah dari perusahaan industri

besar akan menggunakan digital twins, sehingga organisasi-organisasi tersebut memperoleh peningkatan efektivitas sebesar 10%. Dengan jumlah perangkat yang terhubung diperkirakan akan tumbuh menjadi 42 miliar pada tahun 2025, menurut kelompok riset IDC, kita dengan cepat memasuki era "hiper-data". Masing-masing perangkat tersebut memancarkan aliran data secara konstan, memungkinkan kita membangun cloud digital yang secara metaforis akan mengelilingi planet kita. Dengan menggunakan jargon tersebut, kita dapat menciptakan "kembaran digital" di dunia nyata. Berdasarkan laporan tersebut, jelas bahwa digital twins akan mengubah dunia dan dunia usaha harus tetap relevan agar tidak kehilangan peluang yang ada.

12.2 SMART CITY

Bayangkan tantangan yang terkait dengan pemindahan kota. Inilah kenyataan yang dihadapi kota paling utara di Swedia, kota pertambangan Kiruna. Untuk melanjutkan pertumbuhan pertambangan yang aman sebuah industri yang penting bagi perekonomian dan budaya kota Kiruna dan 18.000 penduduknya pindah ke 3 kilometer ke arah timur. Sementara rumah-rumah baru dan pusat kota baru sedang dibangun, beberapa bangunan paling bersejarah di Kiruna, seperti Gereja Kiruna, yang dikenal sebagai salah satu bangunan kayu paling populer dan indah di Swedia, akan dipindahkan secara fisik ke pusat kota baru.

Untuk memungkinkan relokasi kota terbesar di dunia, Kiruna memerlukan pendekatan inovatif, dan pengelola kota mendirikan Kiruna Sustainability Center (KSC) untuk mengembangkan dan menguji ide-ide baru untuk solusi berkelanjutan. KSC menyatukan ekosistem pemerintah kota, pakar industri, peneliti, universitas, dan masyarakat dalam upaya mendorong inovasi yang lebih besar dan peluang bisnis baru. Selama fase awal relokasi Kiruna, CGI membantu kota Kiruna merancang konsep inovatif yang disebut Kota Tersembunyi yang menggunakan augmented reality Microsoft HoloLens yang dikombinasikan dengan peralatan dan data sistem informasi geografis (GIS) untuk memetakan dan memvisualisasikan infrastruktur bawah tanah secara digital. Proyek ini memelopori penggunaan HoloLens di luar ruangan, yang dirancang untuk digunakan di dalam ruangan. Bagi Kiruna, Kota Tersembunyi memberikan gambaran bawah tanah yang akurat sebelum memulai perbaikan infrastruktur.

Hidden City adalah finalis kategori "ide inovatif" di World Smart City Awards 2018 dan finalis penghargaan "inovator terbaik" di penghargaan bisnis Kiruna City. Kiruna dan CGI juga telah ditampilkan oleh Microsoft dalam kisah pelanggannya: "Memindahkan kota dengan bantuan Microsoft HoloLens.

Transportasi: Kereta Api

Meskipun ada investasi besar di jalur Betuweroute dan jalur kereta api pelabuhan, volume barang di jalur kereta api Belanda pada dasarnya stabil selama sekitar 15 tahun, sementara moda transportasi pedalaman lainnya untuk barang (truk & tongkang) terus bertambah (sumber: CBS). Mengejutkan ketika keberlanjutan menjadi semakin penting. Oleh karena itu, Kementerian Infrastruktur dan Pengelolaan Air di Belanda telah menyatakan ambisinya bahwa angkutan barang dengan kereta api akan meningkat dua kali lipat pada tahun 2030.

Untuk manajemen proses bisnis yang lebih baik dan efisien, CGI membantu ProRail mengembangkan pengujian dan memperkenalkan inovasi termasuk menciptakan Digital Twin. Kembaran digital ini adalah dasar sistem informasi yang kami gunakan untuk mengontrol proses inti ProRail. Dunia operator jaringan ProRail ada di luar sana dan banyak hal yang terjadi di sana. Jaringan melakukan semua jenis tugas di tempat berbeda pada waktu yang sama. Pengukuran memberikan informasi digital yang dikumpulkan, dimurnikan, dimodelkan, dan digabungkan. Kembar Digital dihasilkan dari informasi tersebut, yang sebenarnya merupakan representasi digital dari dunia nyata. Tapi ini lebih dari itu. Digital Twin juga mewakili objek yang direncanakan/dirancang dan sudah lenyap. Dengan demikian mencakup seluruh siklus hidup struktur objek dan manajemen informasi terkait. Selain itu, penggunaan jaringan merupakan bagian dari dunia 5D ProRail. 5D merupakan kombinasi informasi terikat lokasi 3D dengan registrasi waktu dan tingkat detail produk. Hal ini pada gilirannya berfungsi sebagai dasar bagi sistem informasi yang digunakan ProRail untuk mengelola proses intinya.

Dirgantara dan Pertahanan

Aerodinamika jet tempur sangatlah rumit sehingga simulasi komputer dengan cepat mencapai batasnya. Akibatnya BAE (Brithish Airpospace) menciptakan model cetak 3-D untuk uji terowongan angin supersonik guna menyempurnakan bentuk pesawat. Konsep kembar digital akan digunakan untuk merancang pengujian dan mendukung setiap sistem dan struktur untuk Tempest, yang dijadwalkan untuk memasuki layanan aktif pada tahun 2035. Masih dalam tahap konsep, Tempest akan menjadi salah satu dari yang keenam yang pertama. pesawat tempur generasi (6G) dan dirancang untuk melengkapi kapal tempur saat ini. Pesawat ini akan memiliki kecerdasan buatan (AI) yang dapat dikonfigurasi dan komunikasi yang diperkeras secara siber yang memungkinkan pesawat bertindak sebagai pusat komando dan kendali terbang, dengan pilot bertindak lebih sebagai pejabat eksekutif dibandingkan sebagai dogfighter. Dengan mengambil pendekatan digital sepenuhnya, mereka juga mengubah cara kerja organisasi. Sistem BAE mencapai apa yang biasanya memakan waktu beberapa bulan dalam beberapa hari. Hasilnya mereka bekerja lebih cepat untuk masa depan yang memicu pikiran terbuka dan inovasi.

12.3 RISIKO, KEAMANAN, PRIVASI DAN ETIKA

Dengan semua hal yang dibahas di atas, ada unsur risiko yang terlibat. Sekarang mari kita lihat potensi risiko dan tantangan yang dapat dihadapi oleh digital twin dari perspektif keamanan dan privasi. Kekhawatiran yang jelas adalah keamanan, privasi, pengawasan dan etika yang perlu ditangani sebelum sistem ini diterapkan. Penerapan konsep kembaran digital yang lebih luas menimbulkan tantangan etika dan tantangan teknis. Perusahaan biasanya memiliki aset yang mereka gunakan di pabriknya. Setelah Anda menjual produk fisik kepada pelanggan, siapa yang memiliki hak atas kembaran digitalnya? Kekhawatiran terhadap privasi dan potensi penyalahgunaan data sudah meluas di dunia e-commerce dan media sosial. Kini konsumen mengajukan pertanyaan yang sama mengenai semakin banyaknya produk yang terhubung dalam kehidupan mereka. Para pendukung hak konsumen sudah mengajukan

pertanyaan tentang penggunaan mainan terhubung yang mengumpulkan data tentang perilaku dan preferensi penggunanya, misalnya.

Implikasi etis, privasi dan sosial dari Digital Twins adalah dimensi lain yang penting dan perlu mendapat perhatian. Sejauh ini spekulasi mengenai ketentuan etika, privasi, dan hukum untuk mengatur pengembangan dan penggunaan Kembar Digital didasarkan pada konsep kembaran fisik dan digital yang tetap merupakan entitas terpisah, seperti yang disarankan oleh istilah "kembaran" itu sendiri. Tanggung jawab, etika, kesopanan, moralitas tidak hanya akan mengalami kebangkitan, tetapi hal-hal tersebut juga perlu diberi makna yang sangat penting, karena ini adalah masalah data dan transparansi.

12.4 DIGITAL TWINS SEBAGAI STRATEGI KEAMANAN SIBER

Pendekatan keamanan dan privasi berdasarkan desain menjadi sebuah norma di lingkungan digital yang kompleks saat ini. Dengan mengoperasionalkan keamanan dan privasi berdasarkan pendekatan desain, keamanan dapat menjadi faktor penting yang memungkinkan kepercayaan dalam pengoperasian produk dan aset menggunakan digital twins. Kembaran digital dapat menjadi pendorong penuh komunikasi dan kolaborasi di seluruh rangkaian digital organisasi, dengan kata lain hal ini dapat menjadi kerangka kerja untuk menyatukan dan mengatur data di seluruh siklus hidup suatu produk. Hal ini dapat terjadi hanya jika kebijakan dan teknologi keamanan yang dipilih dan tepat diterapkan dan dipelihara untuk menjaga dan memelihara kepercayaan digital. Para peserta dapat berkolaborasi dan mengoperasikan produk, aset, dan proses dengan aman melalui digital twins, hanya dalam ekosistem yang terautentikasi dan tepercaya.

Seperti halnya strategi keamanan digital lainnya, pembaruan teknologi dan kebijakan secara konsisten sangatlah penting agar organisasi dapat tetap selangkah lebih maju dari penjahat dunia maya, dan mengamankan berbagai titik akhir produk, aset, dan proses akan memerlukan pendekatan yang kompleks, berlapis-lapis, dan terdistribusi. keamanan.

Bagi organisasi yang ingin membuat atau meningkatkan inisiatif, proyek, atau program kembaran digitalnya, dan untuk memastikan keberhasilan transformasi digitalnya secara umum, mereka dapat mengandalkan tim keamanan. Kini tim keamanan mempunyai peluang untuk memposisikan diri sebagai penggerak bisnis yang mendorong inovasi dan hasil bisnis. Dengan demikian, tim keamanan dapat menjadi penjamin kepercayaan digital, dengan menerapkan keamanan sesuai desain ke dalam inisiatif kembar digital, namun juga di seluruh budaya, praktik, proses, dan platform organisasi.

Penyertaan seluruh ekosistem dan rantai pasok secara aman ke dalam kembaran digital akan menjadi hal yang sangat penting, karena semua mitra harus menjadi bagian dari model ini agar dapat berfungsi dengan baik. Meskipun keterlibatan dan kolaborasi semua pemangku kepentingan mempunyai tantangannya masing-masing, penting bagi semua pihak untuk berkolaborasi secara efektif agar mampu mengelola risiko keamanan dan privasi serta berhasil.

DAFTAR PUSTAKA

"Cyber-Trust," Cyber-Trust, 2019.https://cyber-trust.eu/(accessed Mar. 24, 2021). Sagan, "Hilbert's Space-Filling Curve," 1994.

"Dionaea," Nepenthes Development Team, 2011.http://dionaea.carnivore.it/ (accessed Mar. 28, 2021).

"KDD Cup 1999 Data," University of California, Irvine, 1999.http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html(accessed Mar. 26, 2021). "NSL-KDD dataset," University of new brunswock, 2019.https://www.unb.ca/cic/datasets/nsl.html(accessed Mar. 26, 2021).

A. Arabsorkhi, M. Sayad Haghighi, and R. Ghorbanloo, "A conceptual trust model for the Internet of Things interactions," in 2016 8th Interna- tional Symposium on Telecommunications (IST), Sep. 2016, pp. 89–93, doi: 10.1109/ISTEL.2016.7881789.

A. Coladangelo, "Smart contracts meet quantum cryptography," arXiv preprint arXiv:1902.05214, 2019.

A. de Melo e Silva, J.J.C. Gondim, R. de Oliveira Albuquerque, and L.J. García- Villalba. A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence. Future Internet, 2020, 12(6):108, doi: 10.3390/fi12060108

A. J. H. Witwit and A. K. Idrees, "A Comprehensive Review for RPL Routing Protocol in Low Power and Lossy Networks," 2018, pp. 50–66.

A. Shameli-Sendi and M. Dagenais, "ORCEF: Online response cost evalua- tion framework for intrusion response system," Journal of Network and Com- puter Applications, vol. 55, pp. 89–107, 2015.

A. Verma and V. Ranga, "Machine learning based intrusion detection systems for IoT applications," Wirel. Pers. Commun., vol. 111, no. 4, pp. 2287–2310, 2020.

A. Verma and V. Ranga, "Machine learning based intrusion detection systems for IoT applications," Wirel. Pers. Commun., vol. 111, no. 4, pp. 2287–2310, 2020.

A. Vetterl and R. Clayton, "Honware: A virtual honeypot framework for cap- turing CPE and IoT zero days," in 2019 APWG Symposium on Electronic Crime Research (eCrime), 2019, pp. 1–13.

Apollo 13 mission report, Manned Spacecraft Center, Sept 1970https://sma.nasa.gov/SignificantIncidents/assets/apollo-13-mission-report.pdf.

B. Das, A. Holcomb, M. Mosca and G. C. Pereira, "PQ-Fabric: A Permis- sioned Blockchain Secure from Both Classical and Quantum Attacks," arXiv preprint arXiv:2010.06571, 2020.

B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in 2016 8th IEEE Interna- tional Conference on Communication Software and Networks (ICCSN), 2016, pp. 581–585.

B. Jovanovi c´, “Internet of Things statistics for 2021 – Taking Things Apart,” DataPort, 2021.https://dataprot.net/statistics/iot-statistics/(accessed Jun. 03, 2021).

B. Roy and H. Cheung, “A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural network,” in 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), 2018, pp. 1–6.

B. Sotirios, K. Nicholas, L. Konstantinos and S. Stavros, “On the Security of Permissioned Blockchain Solutions for IoT Applications,” 2020 6th IEEE Conference on Network Softwarization (NetSoft), pp. 465–472, 2020.

Bernstein, M. Schneider, P. Schwabe and Z. Wilcox-O’Hearn, “SPHINCS: practical stateless hash-based signatures,” Annual international conference on the theory and applications of cryptographic techniques, pp. 368–397, 2015.

C. A. Ardagna, E. Damiani, S. De Capitani di Vimercati, S. Foresti, and P. Samarati, “Trust Management,” in Security, Privacy, and Trust in Modern Data Management, Springer, 2007, pp. 103–117.

C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, “DDoS in the IoT: Mirai and other botnets,” Computer, vol. 50, pp. 80–84, 1, 2017.

C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and other botnets,” Computer (Long. Beach. Calif)., 2017, doi: 10.1109/MC.2017.201.

C. L. Corritore, B. Kracher, and S. Wiedenbeck, “On-line trust: concepts, evolving themes, a model,” Int. J. Hum. Comput. Stud., vol. 58, no. 6, pp. 737– 758, Jun. 2003, doi: 10.1016/S1071-5819(03)00041-7.

C. Lei, D. Ma and H. Zhang, “Optimal Strategy Selection for Moving Target Defense Based on Markov Game,” IEEE Access, vol. 5, pp. 156–169, 2017.

C. Lei, H.-Q. Zhang, T. Jinglei, Y.-C. Zhang and X.-H. Liu, “Moving Tar- get Defense Techniques: A Survey,” Security and Communication Networks, vol. 2018, pp. 1–25, 7, 2018.

C. V. L. Mendoza and J. H. Kleinschmidt, “Mitigating On-Off Attacks in the Internet of Things Using a Distributed Trust Management Scheme,” Int. J. Distrib. Sens. Networks, vol. 11, no. 11, p. 859731, Nov. 2015, doi: 10.1155/2015/859731.

C. Vassilakis et al., “Cyber-Trust Project D2.1: Threat landscape: trends and methods,” 2018.

C. Wagner, A. Dulaunoy, G. Wagener, A. Iklody. MISP: The Design and Imple- mentation of a Collaborative Threat Intelligence Sharing Platform. In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, Vienna, Austria, 24–28 October 2016; ACM: New York, NY, USA; pp. 49–56.

C. Yin, Y. Zhu, J. Fei, and X. He, “A deep learning approach for intrusion detection using recurrent neural networks,” Ieee Access, vol. 5, pp. 21954– 21961, 2017.

CGI Case Study – “Using augmented reality and precision data to enable the future smart city” 2017–2018”,https://www.cgi.com/en/case-studies/kiruna-sweden-augmented-reality-smart-future-city.

CGI Cybersecurity Advisory Services,https://www.cgi.com/en/cybersecurity/cyber-advisory-services

CGI, Risk and Cost Driven Architecture Methodology (RCDA) – CGI regis- tered IP 2012 (NL and corp).

CGI, Voice of our Clients 2021 –https://www.cgi.com/en/voice-of-our-clients [2]IDSA,Identity Security: A Work in Progress – Identity Defined SecurityAlliance(idsalliance.org)

CNIL, Privacy Impact Assessment (PIA), available at:https://www.cnil.fr/en/ privacy-impact-assessment-pia Kloza Dariusz and others, Data Protection Impact Assessment in the European Union: Developing a Template for a Report from the Assessment Process (2020) 52, available at:https://osf.io/preprints/lawarxiv/7qrfp/

Cyber-Trust Project –https://cyber-trust.eu/– Advanced Cyber-Threat Intel- ligence, Detection and Mitigation in Trusted IoT, EU H2020 project grant agreement no. 78669

Cyber-Trust Project –https://cyber-trust.eu/– Advanced Cyber-Threat Intel- ligence, Detection and Mitigation in Trusted IoT, EU H2020 project grant agreement no. 78669.

Cyber-Trust Project –https://cyber-trust.eu/– Advanced Cyber-Threat Intel- ligence, Detection and Mitigation in Trusted IoT, EU H2020 project grant agreement no. 78669

Cyber-Trust, “The ever-evolving IoT landscape: Blessing or Curse?,” October 2020. [Online]. Available:https://cyber-trust.eu/2020/10/12/the-ever-evolving-iot-landscape-blessing-or-curse/.Innovate UK, “Innovate Uk_ Evaluation Framework,” 2018.

D. B. Davis, “ISTR 2019: Cyber Criminals Ramp Up Attacks on Trusted Software and Supply Chains,” ISTR 24, 2019.https://symantec-enterprise- blogs.security.com/blogs/expert-perspectives/istr-2019-cyber-criminals-ram p-attacks-trusted-software-and-supply-chains(accessed Jun. 04, 2021).

D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, “TRM-IoT: A trust management model based on fuzzy reputation for internet of things,” Comput. Sci. Inf. Syst., vol. 8, no. 4, pp. 1207–1228, 2011, doi: 10.2298/CSIS110303056C.

D. D. Level, “D2 . 1 Threat landscape?: trends and methods,” no. 2018, p. 250, 2020.

D. Goodin, “Record-breaking DDoS Reportedly Delivered by >145k

D. R. E. Lear, R. Droms, “Manufacturer Usage Description Specification,” 2019.https://datatracker.ietf .org/doc/html/rf c8520(accessed Jun. 16, 2021).

D. R. E. Lear, R. Droms, “Manufacturer Usage Description Specification,” 2018.https://tools.ietf .org/html/draf t-ietf -opsawg-mud-25(accessed Apr. 13, 2020).

D. Sikeridis, P. Kampanakis and M. Devetsikiotis, “Post-Quantum Authen- tication in TLS 1.3: A Performance Study.,” IACR Cryptol. ePrint Arch., vol. 2020, p. 71, 2020.

Digital Society School events – Webinar –https://digitalsocietyschool.org/e vent/digital-twin-a-promising-thing-webinar/Amsterdam Oct 29, 2020.

E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, “A Supervised Intrusion Detection System for Smart Home IoT Devices,” IEEE Internet Things J., 2019, doi: 10.1109/JIOT.2019.2926365.

E. Miehling, M. Rasouli and D. Teneketzis, “A POMDP Approach to the Dynamic Defense of Large-Scale Cyber Networks,” IEEE Transactions on Information Forensics and Security, vol. 13, pp. 2490–2505, 2018.

E. Miehling, M. Rasouli and D. Teneketzis, “Optimal Defense Policies for Partially Observable Spreading Processes on Bayesian Attack Graphs,” in Pro- ceedings of the Second ACM Workshop on Moving Target Defense, New York, NY, USA, 2015.

E.R. Poort, H. van Vliet, “RCDA: Architecting as a risk- and cost management discipline” Journal of Software and Systems, Selected Papersfrom 2011 Joint Working IEEE/IFIP Conference on Software Architecture (WICSA 2011), Vol- ume 85, Issue 9, September 2012, pp 1995–2013https://www.sciencedirect. com/science/article/abs/pii/S0164121212000994 Open Group Certified Architect – http://www.opengroup.org/openca/cert/

ENISA, “An evaluation framework for Cyber Security Strategies,” ENISA, 2014.

Enisa, “ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected,” 2021. [Online]. Avail- able:https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2 020.

Enisa, “Security and Resilience of Smart Home Environments,” 2015. [Online]. Available:https://www.enisa.europa.eu/publications/security- resilience-good-practices/at_download/fullReport.

Enisa, “Threat Landscape for Smart Home and Media Convergence,” 2015. [Online]. Available:https://www.enisa.europa.eu/publications/threat-landsc ape-for-smart-home-and-media-convergence.

F. Bao and I.-R. Chen, “Dynamic trust management for internet of things applications,” in Proceedings of the 2012 international workshop on Self-aware internet of things – Self-IoT ’12, 2012, p. 1, doi: 10.1145/2378023.2378025.

F. Bao, I.-R. Chen, and J. Guo, “Scalable, adaptive and survivable trust man- agement for community of interest based Internet of Things systems,” in 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), Mar. 2013, pp. 1–7, doi: 10.1109/ISADS.2013.6513398.

F. Chen, Z. Liu, Y. Long, Z. Liu and N. Ding, “Secure scheme against compro- mised hash in proof-of-work blockchain,” International Conference on Network and System Security, pp. 1–15, 2018.

F. Gómez Mármol and G. Martínez Pérez, “Providing trust in wireless sensor networks using a bio-inspired technique,” Telecommun. Syst., vol. 46, no. 2, pp. 163–180, Feb. 2011, doi: 10.1007/s11235-010-9281-7.

F. Medjek, D. Tandjaoui, I. Romdhani, and N. Djedjig, “A Trust-Based Intru- sion Detection System for Mobile RPL Based Networks,” in 2017 IEEE Inter- national Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Comput- ing (CPSCom) and IEEE Smart Data (SmartData), Jun. 2017, pp. 735–742, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.113.

G. Bendiab et al., “Network-level attacks: methods and results” Deliverable (D6.7) of Cyber-Trust 2021.

G. Bendiab, B. Saridou, L. Barlow, N. Savage, S. Shiaeles, “IoT Security Frameworks and Countermeasures,” in IoT Security Frameworks and Coun- termeasures, 1st Editio., N. K. Stavros Shiaeles, Ed. Boca Raton: CRC Press, 2021, p. 51.

G. Bendiab, S. Shiaeles “D6.1 State-of-the-art on profiling, detection and mit- igation,” 2019. [Online]. Available:https://cyber-trust.eu/.

G. Bendiab, S. Shiaeles, A. Alruban, and N. Kolokotronis, “IoT malware net- work traffic classification using visual representation and deep learning,” in Proceedings of the 2020 IEEE Conference on Network Softwarization: Bridg- ing the Gap Between AI and Network Softwarization, NetSoft 2020, 2020, doi: 10.1109/NetSoft48620.2020.9165381.

G. Bendiab, S. Shiaeles, A. Alruban, and N. Kolokotronis, “IoT malware net- work traffic classification using visual representation and deep learning,” in Proceedings of the 2020 IEEE Conference on Network Softwarization: Bridg- ing the Gap Between AI and Network Softwarization, NetSoft 2020, 2020, doi: 10.1109/NetSoft48620.2020.9165381.

G. Boulougaris et al., “Device-level attacks: proposed solutions” Deliverable (D6.6) of Cyber-trust 2021.

G. Sargsyan et al., “Final Exploitation and Technology Implementation Plan” Deliverable (D9.10) of Cyber-Trust 2021.

G. Sargsyan, R. Binnenjijk (CGI) et al., “Rapid Prototype Evaluation Results and Assessment” Deliverable (D4.2) of Cyber-Trust 2019

Gartner, Prepare for the Impact of Digital Twins, 2017https://www.gartner. com/smarterwithgartner/prepare-for-the-impact-of-digital-twins.

GDC – Global Defense Corp – “BEA Systems Developed Digital Twin and 3D Printing Techniques for Tempest fighter” August 21, 2020.

Gkotsopoulou, O. and Quinn, P. (eds), D3.1 Regulatory framework analysis, August 2018, available at:https://cyber-trust.eu/wp-content/uploads/2020/0 2/D3.1.pdf

Gkotsopoulou, O. and Quinn, P. (eds), D3.2 Legal analysis of the use of evidence material, October 2018, available at:https://cyber-trust.eu/wp-content/uplo ads/2020/02/D3.2.pdf

Gkotsopoulou, O. and Quinn, P. (eds), D3.3 Legal and ethical recommendations, October 2018, available at:https://cyber-trust.eu/wp-content/uploads/2020/02/D3.3.pdf

H. Artail, H. Safa, M. Sraj, I. Kuwatly, and Z. Al-Masri, “A hybrid honeypot framework for improving intrusion detection systems in protecting organiza- tional networks,” Comput. Secur., 2006, doi: 10.1016/j.cose.2006.02.009.

H. Binsalleeh, “On the analysis of the Zeus botnet crimeware toolkit,” in PST 2010:2010 8th International Conference on Privacy, 2010.

H. Lin and N. W. Bergmann, “IoT privacy and security challenges for smart home environments,” Inf., 2016, doi: 10.3390/info7030044.

H. Lin and N. W. Bergmann, “IoT privacy and security challenges for smart home environments,” Inf., 2016, doi: 10.3390/info7030044.

H. Maleki, S. Valizadeh, W. Koch, A. Bestavros and M. van Dijk, “Markov Modeling of Moving Target Defense Games,” in Proceedings of the 2016 ACM Workshop on Moving Target Defense, New York, NY, USA, 2016.

H. Moonen – “Digital Twins zijn cruciaal bouwblok voor toekomst railgoed-erenvervoer”https://www.cgi.com/sites/default/files/2021-03/clm_ed._5_digital_twins_zijn_cruciaal_bouwblok_voor_toekomst_railgoederenvervoe r.pdfCLM No1 Vervoer March 2021.

H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” in Proceedings - 2012 International Conference on Computer Sci- ence and Electronics Engineering, ICCSEE 2012, 2012, doi: 10.1109/ICC- SEE.2012.373.

H. Taylor, “What Are Cyber Threats and What to Do About Them,” preypro- ject.com, 2021.https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/(accessed Mar. 22, 2021).

Hacked Cameras,” Ars Technica, 29 September 2016. [Online]. Available: https://arstechnica.com/information-technology/2016/09/botnet-of-145k- cameras-reportedly-deliver-internets-biggest-ddos-ever/. [Accessed 9 June 2021].

I. A. I. D. Stewart, A. Zamyatin, S. Werner, M. Torshizi and W. J. Knotten- belt, “Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack,” Royal Society open science, vol. 5, no. 6, p. 180410, 2018.

I. Baptista, S. Shiaeles, and N. Kolokotronis, “A novel malware detection system based on machine learning and binary visualization,” in 2019 IEEE International Conference on Communications Workshops, ICC Workshops 2019 – Proceedings, 2019, doi: 10.1109/ICCW.2019.8757060.

I. Baptista, S. Shiaeles, and N. Kolokotronis, “A novel malware detection system based on machine learning and binary visualization,” in 2019 IEEE International Conference on Communications Workshops, ICC Workshops 2019 – Proceedings, 2019, doi: 10.1109/ICCW.2019.8757060.

I. Kuwatly, M. Sraj, Z. Al Masri, and H. Artail, “A dynamic honeypot design for intrusion detection,” in The IEEE/ACS International Conference onPer- vasive Services, 2004. ICPS 2004. Proceedings., Jul. 2004, pp. 95–104, doi: 10.1109/PERSER.2004.1356776.

I.-R. Chen, F. Bao, and J. Guo, “Trust-Based Service Management for Social Internet of Things Systems,” IEEE Trans. Dependable Secur. Comput., vol. 13, no. 6, pp. 684–696, Nov. 2016, doi: 10.1109/TDSC.2015.2420552.

I.-R. Chen, J. Guo, and F. Bao, “Trust Management for SOA-Based IoT and Its Application to Service Composition,” IEEE Trans. Serv. Comput., vol. 9, no. 3, pp. 482–495, May 2016, doi: 10.1109/TSC.2014.2365797.

IDC research, “The birth of ‘digital twins’ will transform our world”,https: //www.ft.com/content/22158d06-3b5e-11ea-b232-000f4477f bcaJanuary 2020.

IDC,The Future Enterprise: The Next Normal Priorities Driving Technology Investments, October 2020, andFutureScape_2021_Cloud Institute for Mergers, Acquisitions and Alliances (IMAA),https://imaa-institu te.org/mergers-and-acquisitions-statistics/

Investopedia, “PDCA Cycle,” August 2020. [Online]. Available:https://www. investopedia.com/terms/p/pdca-cycle.asp.

J. Bach, “Good Enough Quality: Beyond the Buzzwords,” IEEE Computer, 1997.

J. Buchmann and E. A. H. A. Dahmen, “XMSS-a practical forward secure sig- nature scheme based on minimal security assumptions,” International Work- shop on Post-Quantum Cryptography, pp. 117–129, 2011.

J. D. Guarnizo et al., “Siphon: Towards scalable high-interaction physical hon- eypots,” in Proceedings of the 3rd ACM Workshop on Cyber-Physical System Secu- rity, 2017, pp. 57–68.

J. Guo, I.-R. Chen, and J. J. P. Tsai, “A survey of trust computation models for service management in internet of things systems,” Comput. Commun., vol. 97, pp. 1–14, Jan. 2017, doi: 10.1016/j.comcom.2016.10.012.

J. Kim, J. Kim, H. L. T. Thu, and H. Kim, “Long short term memory recur- rent neural network classifier for intrusion detection,” in 2016 International Conference on Platform Technology and Service (PlatCon), 2016, pp. 1–5.

J. Preece and J. Easton, “Towards encrypting industrial data on public dis- tributed networks,” 2018 IEEE International Conference on Big Data (Big Data), pp. 4540–4544, 2018.

J. R. C. Nurse, S. Creese, and D. De Roure, “Security Risk Assessment in Internet of Things Systems,” IT Prof., vol. 19, no. 5, pp. 20–26, 2017, doi: 10.1109/MITP.2017.3680959.

J. R. Lewis, “Computer System Usability Questionnaire,” [Online]. Available: https://garyperlman.com/quest/quest.cgi.

J. Roux, E. Alata, G. Auriol, V. Nicomette, and M. Kaâniche, “Toward an intrusion detection approach for IoT based on radio communications profil- ing,” in 2017 13th European dependable computing conference (EDCC), 2017, pp. 147–150.

J. Yuan and X. Li, “A Reliable and Lightweight Trust Computing Mech- anism for IoT Edge Devices Based on Multi-Source Feedback Infor- mation Fusion,” IEEE Access, vol. 6, pp. 23626–23638, 2018, doi: 10.1109/ACCESS.2018.2831898.

J.A. Biega, K.P. Gummadi, I. Mele, D. Milchevski, C. Tryfonopoulos, G. Weikum. R-Susceptibility: An IR-Centric Approach to Assessing Privacy Risks for Users in Online Communities. In Proceedings of the 39th International ACM SIGIR Conference on Research and Development in Information Retrieval, Pisa, Italy, 17–21 July 2016, SIGIR ’16. pp. 365–374

J.-H. Cho, D. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. Moore, D. S. Kim, H. Lim and F. Nelson, “Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense,” IEEE Communications Surveys & Tutori- als, vol. PP, pp. 1–1, 1, 2020.

Joint Technical Committee ISO/IEC JTC 1, “International standard NEN- ISO/IEC 27001: Information technology – Security techniques – Informa- tion security management systems – Requirements,” 2013.

K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albu- querque, “Internet of Things: A survey on machine learning-based intrusion detection approaches,” Comput. Networks, vol. 151, pp. 147–157, 2019.

K. Chalkias, “Blockchained post-quantum signatures,” Cryptology ePrint Archive: Report 2018/658, 2018.

K. Govindan and P. Mohapatra, “Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey,” IEEE Commun. Surv. Tutorials, vol. 14, no. 2, pp. 279–298, 2012, doi: 10.1109/SURV.2011.042711.00083.

K. Irwin and T. Yu, “Preventing attribute information leakage in auto- mated trust negotiation,” in Proceedings of the 12th ACM conference on Computer and communications security – CCS ’05, 2005, p. 36, doi: 10.1145/1102120.1102128.

K. S. Kiran, R. N. K. Devisetty, N. P. Kalyan, K. Mukundini, and R. Karthi, “Building a Intrusion Detection System for IoT Environment using Machine Learning Techniques,” Procedia Comput. Sci., vol. 171, pp. 2372–2379, 2020.

K. Vieira, L. Barbosa, A.S. da Silva, J. Freire, E. Moura. Finding seeds to bootstrap focused crawlers. World Wide Web 2016, 19, 449–474, doi: 10.1007/s11280-015-0331-7

L. and J. P. and M. M. Chen, “https://www.intel.com/content/dam/www/public/us/en/ai/documents/stamina-scalable-deep-learning-whitepaper.pdf,” 2020.https://www.intel.com/content/dam/www/public/us/en/ai/documents/stamina-scalable-deep-learning-whitepaper.pdf(accessed Jun. 21, 2021).

L. Barlow, G. Bendiab, S. Shiaeles, and N. Savage, “A Novel Approach to Detect Phishing Attacks using Binary Visualisation and Machine Learning,” in 2020 IEEE World Congress on Services (SERVICES), 2020, pp. 177–182.

Li Xiong and Ling Liu, “PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities,” IEEE Trans. Knowl. Data Eng., vol. 16, no. 07, pp. 843–857, Jul. 2004, doi: 10.1109/TKDE.2004.1318566.

M. A. Hakim, H. Aksu, A. S. Uluagac, and K. Akkaya, “U-pot: A honeypot framework for upnp-based iot devices,” in 2018 IEEE 37th International Per- formance Computing and Communications Conference (IPCCC), 2018, pp. 1–8.

M. Ahmed, A. N. Mahmood, and J. Hu, “A survey of network anomaly detec- tion techniques,” J. Netw. Comput. Appl., vol. 60, pp. 19–31, 2016.

M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis and et al., “Under- standing the Mirai Botnet,” in 26th USENIX Security Symposium (USENIX Security ’17), 2017.

M. Blaze, J. Ioannidis, and A. D. Keromytis, “Experience with the KeyNote Trust Management System: Applications and Future Directions,” 2003, pp. 284–300.

M. C. Semmouni, A. Nitaj and M. Belkasmi, “Bitcoin Security with Post Quantum Cryptography,” Networked Systems, pp. 281–288, 2019.

M. Cukier, “Study: Hackers Attack Every 39 Seconds,” University of Maryland, 2021.https://eng.umd.edu/news/story/study-hackers-attack-every-39-secon ds(accessed Mar. 10, 2021).

M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, “Deep learning- based intrusion detection for iot networks,” in 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), 2019, pp. 256– 25609.

M. Grieves, Florida Institute of Technology, Digital Twins Presentation, Conference 2002 University of Michigan, Society of Manufacturing Engi- neers conference in Troy, Michigan.

M. Hildebrandt, “Defining profiling: A new type of knowledge?,” Profiling Eur. Citiz. Cross-Disciplinary Perspect., pp. 17–45, 2008, doi: 10.1007/978-1- 4020-6914-7_2.

M. Nitti, R. Girau, and L. Atzori, “Trustworthiness Management in the Social Internet of Things,” IEEE Trans. Knowl. Data Eng., vol. 26, no. 5, pp. 1253– 1266, May 2014, doi: 10.1109/TKDE.2013.105.

M. Safaei Pour, E. Bou-Harb, K. Varma, N. Neshenko, D. A. Pados, and K. K. R. Choo, “Comprehending the IoT cyber threat landscape: A data dimension- ality reduction technique to infer and characterize Internet-scale IoT probing campaigns,” Digit. Investig., 2019, doi: 10.1016/j.diin.2019.01.014.

M. Sato and S. Matsuo, “Long-term public blockchain: Resilience against compromise of underlying cryptography,” 2017 26th International Conference on Computer Communication and Networks (ICCCN), pp. 1–8, 2017.

M. Theoharidou, A. Mylonas, and D. Gritzalis, “A Risk Assessment Method for Smartphones,” 2012, pp. 443–456.

M. Wang, J. Santillan, and F. Kuipers, “ThingPot: an interactive Internet-of- Things honeypot,” arXiv Prepr. arXiv1807.04114, 2018.

M. Zaman and C.-H. Lung, “Evaluation of machine learning techniques for network intrusion detection,” in NOMS 2018–2018 IEEE/IFIP Network Operations and Management Symposium, 2018, pp. 1–5.

MarketsAndMarkets Report 2019 (176 pages) “Digital Twin Market by Tech- nology, Type (Product, Process, and System), Application (predictive main- tenance), Industry (Aerospace & Defense, Automotive & Transportation, Healthcare), and Geography – Global Forecast to 2026”.

Microsoft, CGI – “Moving a city with the help of Microsoft HoloLens” https: //www.youtube.com/watch?v=1wq7ZQMUy-k.

N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Net- work Intrusion Detection for IoT Security Based on Learning Techniques,” IEEE Commun. Surv. Tutorials, vol. 21, no. 3, pp. 2671–2701, 2019, doi: 10.1109/COMST.2019.2896380.

N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Net- work Intrusion Detection for IoT Security Based on Learning Techniques,” IEEE Commun. Surv. Tutorials, vol. 21, no. 3, pp. 2671–2701, 2019, doi: 10.1109/COMST.2019.2896380.

N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, “New trust metric for the RPL routing protocol,” in 2017 8th International Conference on Infor- mation and Communication Systems (ICICS), Apr. 2017, pp. 328–335, doi: 10.1109/IACS.2017.7921993.

N. F. Haq, A. R. Onik, M. A. K. Hridoy, M. Rafni, F. M. Shah, and D. M. Farid, “Application of machine learning approaches in intrusion detec- tion system: a survey,” IJARAI-International J. Adv. Res. Artif. Intell., vol. 4, no. 3, pp. 9–18, 2015.

N. Kolokotronis et al., “Cyber-Trust Project D5.1 State-of-the-art on proac- tive technologies,” 2019.

N. Kolokotronis, S. Brotsis, G. Germanos, C. Vassilakis and S. Shiaeles, “On Blockchain Architectures for Trust-Based Collaborative Intrusion Detection,” 2019 IEEE World Congress on Services (SERVICES), pp. 21–28, 2019.

N. Poolsappasit, R. Dewri and I. Ray, “Dynamic Security Risk Management Using Bayesian Attack Graphs,” IEEE Transactions on Dependable and Secure Computing, vol. 9, pp. 61–74, 2012.

N. Poolsappasit, R. Dewri, and I. Ray, “Dynamic Security Risk Manage- ment Using Bayesian Attack Graphs,” IEEE Trans. Dependable Secur. Comput., vol. 9, no. 1, pp. 61–74, Jan. 2012, doi: 10.1109/TDSC.2011.34.

N. Provos and others, “A Virtual Honeypot Framework.,” in USENIX Security Symposium, 2004, vol. 173, no. 2004, pp. 1–14.

N. Sakellion, “Post-quantum cryptography in blockhain technologies,” Cyprus, 2020.

N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A deep learning approach to network intrusion detection,” IEEE Trans. Emerg. Top. Comput. Intell., vol. 2, no. 1, pp. 41–50, 2018.

Nexusguard.com, “Distributed Denial of Service (DDoS) Threat Report Q4 2016,” 2016. [Online]. Available:https://www.nexusguard.com/hubfs/Nexusguard_DDoS_Threat_Report_Q4_2016_EN.pdf.

NIST Information Technology/Software and Systems Division, “Methodology Overview,” NIST, May 2017. [Online]. Available:https://www.nist.gov/itl/ssd/sof tware-quality-group/computer-forensics-tool-testing-program-cftt/cftt- general-0.

O. Sheyner, J. Haines, S. Jha, R. Lippmann and J. M. Wing, “Automated generation and analysis of attack graphs,” in Proceedings 2002 IEEE Symposium on Security and Privacy, 2002.

OpenVPNhttps://openvpn.net/ [3]https://linux.die.net/man/1/qemu-img

OWASP, “Internet of Things (IoT) Top 10 2018,” OWASP Internet of Things Project, 2018.https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10(accessed Sep. 20, 2020).

P. A. Bonatti and P. Samarati, “A uniform framework for regulating service access and information release on the Web,” J. Comput. Secur., vol. 10, no. 3, pp. 241–271, Jul. 2002, doi: 10.3233/JCS-2002-10303.

P. Baecher, M. Koetter, T. Holz, M. Dornseif, and F. Freiling, “The nepenthes platform: An efficient approach to collect malware,” in International Workshop on Recent Advances in Intrusion Detection, 2006, pp. 165–184.

P. J. Hanson, L. Truax, and D. D. Saranchak, “IOT honeynet for military deception and indications and warnings,” in Autonomous Systems: Sensors, Vehicles, Security, and the Internet of Everything, 2018, vol. 10643, p. 106431A.

P. Koloveas, T. Chantzios, C. Tryfonopoulos, S. Skiadopoulos. A crawler archi- tecture for harvesting the clear, social, and dark web for IoT-related cyber-threat intelligence. In 2019 IEEE World Congress on Services (SERVICES), 2642, 3–8. IEEE, 2019

P. Koloveas, T. Chantzios, S. Alevizopoulou, S. Skiadopoulos, C. Tryfonopou- los. INTIME: A Machine Learning-Based Framework for Gathering and Leverag- ing Web Data to Cyber-Threat Intelligence. Electronics 2021, 1, 5, March 2021, doi: 10.3390/electronics1010005

P. Madani and N. Vlajic, “Robustness of deep autoencoder in intrusion detection under adversarial contamination,” in Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security, 2018, pp. 1–8.

P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad, “A fuzzy approach to trust based access control in internet of things,” in Wireless VITAE 2013, Jun. 2013, pp. 1–5, doi: 10.1109/VITAE.2013.6617083.

P. Quinn, O. Gkotsopoulou (Vrij Universiteit Brussels), “Legal Issues, Data protection and Privacy” – Work Pachage in Cyber-Trust, 2018–2021, “Legal and Ethical Recommendations” Deliverable (D3.3) of Cyber-Trust 2018, “Cyber- Trust Impact Assessment” – 1, 2 Deliverables D3.4 and D3.5, 2020–2021.

P. Van Huong, D. V. Hung, and others, “Intrusion detection in IoT systems based on deep learning using convolutional neural network,” in 2019 6th NAFOSTED Conference on Information and Computer Science (NICS), 2019, pp. 448–453.

R. Binnendijk, G Sargsyan (CGI) et al.: “Architecture and Design Specifications: Initial” Cyber-Trust project Deliverable (D4.1) of Cyber-Trust 2019.

R. C. Mayer, J. H. Davis, and F. D. Schoorman, “An Integrative Model of Organizational Trust,” Acad. Manag. Rev., vol. 20, no. 3, p. 709, Jul. 1995, doi: 10.2307/258792.

R. C. Merkle, “A certified digital signature,” Conference on the Theory and Application of Cryptology, pp. 218–238, 1989.

R. Doshi, N. Apthorpe, and N. Feamster, “Machine learning ddos detection for consumer internet of things devices,” in 2018 IEEE Security and Privacy Workshops (SPW), 2018, pp. 29–35.

R. Ismail and A. Josang, “The Beta Reputation System,” in Proceedings of the BLED 2002 Conference, 2002, [Online]. Available:https://aisel.aisnet.org/b led2002/41.

R. Samrin and D. Vasumathi, “Review on anomaly based network intrusion detection system,” in International Conference on Electrical, Electronics, Com- munication Computer Technologies and Optimization Techniques, ICEECCOT 2017, 2018, doi: 10.1109/ICEECCOT.2017.8284655.

R. Shen, H. Xiang, X. Zhang, B. Cai and T. Xiang, “Application and Imple- mentation of Multivariate Public Key Cryptosystem in Blockchain (Short Paper),” International Conference on Collaborative Computing: Networking, Applications and Worksharing, pp. 419–428, 2019.

R. Shire, S. Shiaeles, K. Bendiab, B. Ghita, and N. Kolokotronis, “Malware Squid: A Novel IoT Malware Traffic Analysis Framework Using Convolutional Neural Network and Binary Visualisation,” in Lecture Notes in Computer Sci- ence (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019, doi: 10.1007/978-3-030-30859-9_6.

R. Shire, S. Shiaeles, K. Bendiab, B. Ghita, and N. Kolokotronis, “Malware Squid: A Novel IoT Malware Traffic Analysis Framework Using Convolutional Neural Network and Binary Visualisation,” in Lecture Notes in Computer Sci- ence (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019, doi: 10.1007/978-3-030-30859-9_6.

R. Vinayakumar, K. P. Soman, and P. Poornachandran, “Applying convo- lutional neural network for network intrusion detection,” in 2017 Interna- tional Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 1222–1228.

R. Vinayakumar, K. P. Soman, and P. Poornachandran, “Evaluation of recur- rent neural network and its variants for intrusion detection system (IDS),” Int. J. Inf. Syst. Model. Des., vol. 8, no. 3, pp. 43–63, 2017.

R. Vishwakarma and A. K. Jain, “A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks,” in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1019–1024.

R. Voute – “CGI helpt ProRail bij ontwikkelen, testen en invoeren van inno- vaties”, Grond, Weg, waterbouw, September 3, 2020https://www.gww-bo uw.nl/artikel/cgi-helpt-prorail-bij-ontwikkelen-testen-en-invoeren-van-inn ovaties/.

R. Zhuang, S. A. DeLoach and X. Ou, “Towards a Theory of Moving Target Defense,” in Proceedings of the First ACM Workshop on Moving Target Defense, New York, NY, USA, 2014.

S. A. Kumar, T. Vealey, and H. Srivastava, “Security in internet of things: Challenges, solutions and future directions,” in Proceedings of the Annual Hawaii International Conference on System Sciences, 2016, doi: 10.1109/HICSS.2016.714.

S. A. Kumar, T. Vealey, and H. Srivastava, “Security in internet of things: Challenges, solutions and future directions,” in Proceedings of the Annual Hawaii International Conference on System Sciences, 2016, doi: 10.1109/HICSS.2016.714.

S. A. Zonouz, H. Khurana, W. H. Sanders and T. M. Yardley, “RRE: A game- theoretic intrusion Response and Recovery Engine,” in 2009 IEEE/IFIP Inter- national Conference on Dependable Systems Networks, 2009.

S. B. Ambati and D. Vidyarthi, “A Brief Study and Comparison of, Open Source Intrusion Detection System Tools,” Int. J. Adv. Comput. Eng. Netw., no. 110, pp. 2320–2106, 2013, [Online]. Available:http://www.iraj.in/jour nal/journal_file/journal_pdf/3-27-139087836726-32.pdf.

S. Bhatt, P. K. Manadhata, and L. Zomlot, “The Operational Role of Secu- rity Information and Event Management Systems,” IEEE Secur. Priv., vol. 12, no. 5, pp. 35–41, Sep. 2014, doi: 10.1109/MSP.2014.103.

S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis and S. Shiaeles, “On the suitability of blockchain platforms for IoT applications: Architectures, secu- rity, privacy, and performance,” Computer Networks, p. 108005, March 2021.

S. Brotsis, N. Kolokotronis, K. Limniotis, S. Shiaeles, D. Kavallieros and E. Bellini, “Blockchain Solutions for Forensic Evidence Preservation in IoT Envi- ronments,” IEEE Conference on Network Softwarization (NetSoft), pp. 110– 114, 2019.

S. Bruce, “Academic: Attack Trees - Schneier on Security,” 1999. [Online]. Available:https://www.schneier.com/academic/archives/1999/12/attack_tree s.html.

S. Cuomo, S. Naldini et al. (Mathema) “UI mock-ups evaluation, assessment and validation” Deliverable (D4.3) of Cyber-Trust, 2019

S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “The Eigentrust algo- rithm for reputation management in P2P networks,” in Proceedings of the twelfth international conference on World Wide Web – WWW ’03, 2003, p. 640, doi: 10.1145/775152.775242.

S. Dowling, M. Schukat, and H. Melvin, “A ZigBee honeypot to assess IoT cyberattack behaviour,” in 2017 28th Irish signals and systems conference (ISSC), 2017, pp. 1–6.

S. Gamage and J. Samarabandu, “Deep learning methods in network intrusion detection: A survey and an objective comparison,” J. Netw. Comput. Appl., vol. 169, p. 102767, 2020.

S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, “Intrusion detec- tion systems in the Internet of things: A comprehensive investigation,” Com- put. Networks, vol. 160, pp. 165–191, 2019.

S. K. Prajapati, S. Changder, and A. Sarkar, “Trust Management Model for Cloud Computing Environment,” arXiv.org, Apr. 2013, [Online]. Available: https://arxiv.org/abs/1304.5313.

S. Namal, H. Gamaarachchi, G. MyoungLee, and T.-W. Um, “Autonomic trust management in cloud-based and highly dynamic IoT applications,” in 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015), Dec. 2015, pp. 1–8, doi: 10.1109/Kaleidoscope.2015.7383635.

S. Rakitin, “Software Veriication and Validation for Practitioners and Man- agers,” Artech House, 2001.

S. S. G. Bendiab, B. Saridou, L. Barlow, N. Savage, “IoT Security Frameworks and Countermeasures,” in IoT Security Frameworks and Countermeasures, 1st Editio., N. K. Stavros Shiaeles, Ed. Boca Raton: CRC Press, 2021, p. 51.

S. Sengupta, A. Chowdhary, A. Sabur, D. Huang, A. Alshamrani and S. Kamb- hampati, “A Survey of Moving Target Defenses for Network Security,” CoRR, vol. abs/1905.00964, 2019.

S. Suhail, R. Hussain, A. Khan and C. S. Hong, “On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions,” IEEE Internet of Things Journal, 2020.

S. Yeldi et al., “Enhancing network intrusion detection system with honey- pot,” in TENCON 2003. Conference on Convergent Technologies for Asia-Pacific Region, 2003, vol. 4, pp. 1521–1526.

T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, “Deep recurrent neural network for intrusion detection in sdn-based networks,” in 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), 2018, pp. 202–206.

T. Chantzios, P. Koloveas, S. Skiadopoulos, N. Kolokotronis, C. Tryfonopoulos, V. Bilali, D. Kavallieros. The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform. Proceedings of the 8th International Conference on Data Sci- ence, Technology and Applications, DATA 2019, Prague, Czech Republic, July 26–28, 2019, 369–376, doi: 10.5220/0007978103690376

T. G. Tan, P. Szalachowski and J. Zhou, “SoK: Challenges of Post-Quantum Digital Signing in Real-world Applications”.eprint.iacr.

T. Luo, Z. Xu, X. Jin, Y. Jia, and X. Ouyang, “Iotcandyjar: Towards an intelligent-interaction honeypot for iot devices,” Black Hat, pp. 1–11, 2017.

T. M. Fernández-Caramès and P. Fraga-Lamas, “Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum com- puting attacks,” IEEE Access, vol. 8, pp. 21091–21116, 2020.

T. Mikolov, I. Sutskever, K. Chen, G. Corrado, J. Dean. Distributed Represen- tations of Words and Phrases and Their Compositionality. Proceedings of the 26th International Conference on Neural Information Processing Systems, NIPS, 2013, 2, 3111–3119

T. Toth and C. Kruegel, “Evaluating the impact of automated intrusion response mechanisms,” in 18th Annual Computer Security Applications Con- ference, 2002. Proceedings, 2002.

U. D. Gandhi, P. M. Kumar, R. Varatharajan, G. Manogaran, R. Sundarasekar, and S. Kadu, “HIoTPOT: surveillance on IoT devices against recent threats,” Wirel. Pers. Commun., vol. 103, no. 2, pp. 1179–1194, 2018.

UserSense, “Technology Acceptance Model (TAM model),” [Online]. Avail-able:https://www.usersense.at/analysing-usability-testing/technology-accept ance-model.

V. G. Bilali et al., “Platform’s 1st evaluation report” Deliverable (D8.3) of Cyber-Trust 2021.

V. G. Bilali et al., “Platfrom’s 2nd evaluation report” Deliverable (D8.5) of Cyber-Trust 2021.

V. Sharma, J. Kim, S. Kwon, I. You, K. Lee and K. Yim, “A framework for mitigating zero-day attacks in IoT,” ArXiv, vol. abs/1804.05549, 2018.

W. Yin, Q. Wen, W. Li, H. Zhang and Z. Jin, “An anti-quantum transaction authentication approach in blockchain,” IEEE Access, vol. 6, pp. 5393–5401, 2018.

W. Zhang, B. Zhang, Y. Zhou, H. He, and Z. Ding, “An IoT Honeynet Based on Multiport Honeypots for Capturing IoT Attacks,” IEEE Internet Things J., vol. 7, no. 5, pp. 3991–3999, 2019.

X. Ou, S. Govindavajhala and A. W. Appel, “MulVAL: A Logic-based Net- work Security Analyzer,” in 14th USENIX Security Symposium (USENIX Secu- rity 05), Baltimore, 2005.

X. Ou, W. F. Boyer, and M. A. McQueen, “A scalable approach to attack graph generation,” in Proceedings of the 13th ACM conference on Com- puter and communications security – CCS ’06, 2006, pp. 336–345, doi: 10.1145/1180405.1180446.

X. Wu and F. Li, “A multi-domain trust management model for supporting RFID applications of IoT,” PLoS One, vol. 12, no. 7, p. e0181124, Jul. 2017, doi: 10.1371/journal.pone.0181124.

Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, “Trust manage- ment system design for the Internet of Things: A context-aware and multi- service approach,” Comput. Secur., vol. 39, pp. 351–365, Nov. 2013, doi: 10.1016/j.cose.2013.09.001.

Y. Liu, S. Liu, and X. Zhao, “Intrusion detection algorithm based on con- volutional neural network,” DEStech Trans. Eng. Technol. Res., no. iceta, 2017.

Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, “IoTPOT: Analysing the rise of IoT compromises,” in 9th USENIX Workshop on Offensive Technologies (WOOT 15), 2015.

Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things,” IEEE Internet Things J., 2017, doi: 10.1109/JIOT.2017.2694844.

Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu and Y.-X. Yang, “A secure cryptocurrency scheme based on post-quantum blockchain,” IEEE Access, vol. 6, pp. 27205–27213, 2018.

Z. A. Khan, J. Ullrich, A. G. Voyiatzis, and P. Herrmann, “A Trust-based Resilient Routing Mechanism for the Internet of Things,” in Proceedings of the 12th International Conference on Availability, Reliability and Security – ARES ’17, 2017, pp. 1–6, doi: 10.1145/3098954.3098963.

TEKNOLOGI KEAMANAN SIBER
(Cyber Security)

oleh:
Dr. Joseph Teguh Santoso, S.Kom, M.Kom

BIODATA PENULIS

Dr. Joseph Teguh Santoso, S.Kom, M.Kom adalah Rektor dari Universitas Sains & Teknologi Komputer (Universitas STEKOM) Semarang yang memiliki banyak pengalaman praktis dalam bidang *e-commerce*sejak Tahun 2002. Beliau mempunyai 3 (tiga) toko *Official Online Store* di China untuk merek Sepeda Raleigh, dengan omzet tahunan pada Tahun 2019 mencapai lebih dari Rp. 35 Milyar rupiah dan terus meningkat. Dr. Joseph T.S memiliki lisensi tunggal sepeda merek "Raleigh" untuk penjualan *Online* di seluruh China. Di samping itu beliau juga memiliki pabrik sepeda dan sepeda listrik merek "Fengjiu", yaitu Pabrik Sepeda Listrik yang masih tergolong kecil di China. Pengalaman beliau malang melintang di dunia *online store* di China seperti Alibaba, Tmall, Taobao, JD, Aliexpress sangat membantu mahasiswa untuk memiliki pengalaman teknis dan praktis untuk membuka toko *online* bersama beliau.

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-8120-71-0 (PDF)
9 786238 120710