Jurnal Informatika & Teknologi Cerdas (JITC)
Vol. 1, No. 1, Juni 2025
ISSN 3109-7677

State of the Art: Tantangan dan Pentingnya Standarisasi Keamanan IoT dalam Berbagai Implementasi

Sutan Muhammad Sadam Awal[1*)] , Muhammad Darwis[2]
[1]Graduate School of Bioresource and Bioenvironmental Sciences, Faculty of Agriculture, Kyushu University
[2]Program Studi Teknik Informatika, Fakultas Ilmu Rekayasa, Universitas Paramadina
Email: [1]awal.muhamad.sadam.578@s.kyushu-u.ac.jp, [2]muhammad.darwis@paramadina.ac.id

Abstrak - Standarisasi keamanan data di lingkungan IoT telah menjadi isu utama dengan adopsi teknologi IoT yang cepat. Penelitian ini memberikan gambaran tentang pentingnya standarisasi keamanan informasi untuk melindungi perangkat dan data IoT. Dengan standar keamanan yang jelas dan teruji, pengembang dapat merancang perangkat IoT dengan langkah keamanan yang konsisten. Perusahaan mendapatkan benefit dari investasi keamanan. Selain itu, standardisasi juga memungkinkan interoperabilitas perangkat IoT dari vendor yang berbeda, mengurangi risiko serangan, melindungi privasi pengguna, dan meningkatkan kepercayaan pengguna terhadap teknologi IoT. Penelitian ini juga menyatakan bahwa meskipun standar keamanan IoT sudah ada, penelitian dan pengembangan masih diperlukan untuk mengatasi ancaman keamanan baru yang hadir seiring dengan kemajuan teknologi IoT.

Kata kunci: Keamanan IoT, Keamanan Siber, Perusahaan IoT, Standarisasi IoT

Abstract - Security standardization in the IoT environment has become a major issue with the rapid adoption of IoT technology. This study provides an overview of the importance of information security standardization to protect IoT devices and data. With clear and tested security standards, developers can design IoT devices with consistent security measures. Companies benefit from security investments. In addition, standardization also enables interoperability of IoT devices from different vendors, reduces the risk of attacks, protects user privacy, and increases user trust in IoT technology. The study also states that although IoT security standards exist, research and development are still needed to address new security threats that arise along with the advancement of IoT technology.

Keywords— IoT Security, Cyber Security, IoT Enterprise, IoT Standardization

I. PENDAHULUAN

Perkembangan bisnis teknologi berbasis internet of things (atau selanjutnya disebut IoT) begitu cepat sehingga dapat menimbulkan potensi kejahatan baru menggunakan dunia digital. Industri yang bergerak di bidang teknologi informasi menghadapi tantangan dalam keamanan siber berbasis IoT. Sektor ini memiliki peran vital sebagai target dalam penyerangan siber, sehingga perlu menginvestasikan keamanan infrastruktur. Di samping membawa kemudahan bagi kehidupan manusia, perangkat-perangkat ini rentan terhadap berbagai ancaman dan tantangan keamanan yang tidak hanya membuat khawatir para pengguna untuk mengadopsinya di lingkungan sensitif seperti *e-health* dan *smart home* dan lain-lain, tetapi juga menimbulkan bahaya bagi perkembangan IoT di masa mendatang [1].

Investasi keamanan merupakan sebuah kunci dalam mengupayakan kenyamanan dalam menggunakan IoT. Dengan memperkuat keamanan IoT akan mendapatkan keuntungan berupa pencegahan dari serangan siber secara masif, menghindarkan dari biaya pemulihan terdampak sangat besar, memberikan jaminan kepada pelanggan untuk terus menggunakan sistem IoT. Tentunya, untuk mencapai target keamanan IoT diperlukan standarisasi yang jelas sehingga perusahaan dapat mencapai kualifikasi keamanan siber tertentu, agar supaya dapat menjamin bahwa ini sudah aman digunakan. Berdasarkan penelitian yang dilakukan oleh Karie dkk, diketahui bahwa selama ini terdapat ketidaksesuaian standar keamanan yang diimplementasikan dalam berbagai proyek IoT, meskipun memang standar tersebut memiliki potensi untuk diterapkan [2].

Penelitian ini akan menyoroti standarisasi protokol keamanan IoT yang mengacu kepada jurnal penelitian terkait keamanan IoT. Data umumnya ditelaah melalui studi literatur agar dapat mengorientasikan informasi yang lebih akurat dan efisien. Studi literatur adalah kegiatan yang berkaitan dengan metode pengumpulan data perpustakaan, membaca dan menyimpan bahan penelitian, serta mengolahnya. Selanjutnya, hasil dari penelitian ini berupa pengumpulan data dengan konteks standarisasi keamanan IoT yang bisa dihubungkan dengan dunia pekerjaan secara nyata, agar menjadi acuan perusahaan menerapkan standar keamanan berbasis IoT.

Penelitian ini penting untuk dilaksanakan mengingat saat ini pengembangan teknologi berbasis IoT sedang ramai digalakkan dan diprediksi akan terus menjadi trend teknologi dalam beberapa dekade kedepan. Perkembangan teknologi IoT perlu untuk diperhatikan keamanannya karena dampaknya dapat bersinggungan langsung dengan

 ISSN 3109-7677

keberadaan manusia sebagai penggunanya. Standarisasi keamanan IoT pada akhirnya akan menjadi salah satu poin penting untuk mengurangi resiko dan kesalahan. Dengan demikian, langka untuk memajukan peradaban dengan berbagai solusi canggih berbasis IoT dapat tercapai dan sangat berguna bagi kehidupan.

II. LITERATURE STUDY

A. Keamanan IoT

Keamanan merupakan salah satu bagian terpenting sekaligus tantangan dalam sebuah penerapan IoT. IoT adalah sistem yang kompleks. Iot tidak hanya terlibat sebagai entitas data, mesin, RFID, sensor dan lain-lain, tetapi juga mencakup berbagai perangkat dengan kemampuan komunikasi dan pemrosesan data. Karena banyaknya entitas dan data yang terlibat, IoT menghadirkan risiko keamanan yang dapat mengancam dan merugikan konsumen. Risiko keamanan dapat mempengaruhi kualitas dari IoT itu sendiri. Menurut Roman, dkk. [3] bentuk kejahatan siber terdiri dari:

1. *Eavesdropping*, serangan pasif yang dilakukan di berbagai saluran komunikasi dengan tujuan mengekstraksi data dari arus informasi.
2. *Node Capture*, penyerang mengekstrak data dari node atau infrastruktur lain dengan kemampuan penyimpanan data.
3. Perusakan objek-objek IoT dalam bentuk fisik.
4. *Denial of Service*, serangan yang mengakibatkan pihak yang resmi tidak bisa mengakses layanan.

B. Keamanan Siber

Keamanan siber adalah perlindungan komputer, jaringan, perangkat lunak, sistem kritis, dan data terhadap potensi ancaman digital. Perusahaan memiliki tanggung jawab untuk melindungi data untuk menjaga kepercayaan pelanggan dan mematuhi peraturan. Berdasarkan laporan *National Cyber Security Index* (NCSI) terbaru, tingkat keamanan siber Indonesia menempati peringkat ke-84 dengan skor 38,96. NCSI menggunakan 12 indikator dalam laporannya, mulai dari pengembangan kebijakan keamanan siber atas perlindungan data pribadi hingga memerangi kejahatan siber [4]. Laporan NCSI menunjukkan bahwa tingkat keamanan siber Indonesia masih relatif rendah dibandingkan negara lain. [5] Langkah-langkah keamanan siber memberikan pertahanan dari serangan siber dan memberikan manfaat sebagai berikut, antara lain:

1. Mencegah atau mengurangi biaya pelanggaran
2. Memelihara kepatuhan terhadap peraturan
3. Mengurangi ancaman siber yang terus berkembang.

C. Standarisasi Keamanan IoT

Standar keamanan untuk perangkat IoT yang dikeluarkan oleh organisasi terkemuka dan diakui secara luas untuk melindungi perangkat IoT, data pengguna, dan masalah terkait. Saat ini jumlahnya sedikit dan tidak tersedia secara luas, hanya diatur di wilayah tertentu. Di negara bagian California, Amerika Serikat misalnya, memberlakukan undang-undang perdata California, yang memiliki bagian terpisah tentang keamanan wajib perangkat IoT. Hukum California adalah salah satu dari sedikit hukum di dunia yang secara hukum mengatur privasi dan keamanan perangkat IoT. Salah satu standar yang digunakan misalnya adalah Institut Nasional Standar dan Teknologi (NIST), yang merilis buku putih berjudul Kriteria Keamanan Dasar untuk Perangkat IoT Konsumen. NIST memiliki kerangka kerja untuk memudahkan perusahaan dalam mencapai target standarisasi keamanan. Metode NIST dapat digunakan untuk mengidentifikasi lalu lintas serangan pada jaringan IoT dan menggunakan hasilnya sebagai bukti digital yang resmi dalam bentuk laporan. Selain itu, masih terdapat beberapa standar yang mengatur mengenai jaringan dan teknologi IoT, meskipun terbatas di negara dan wilayah tertentu saja [6].

III. METODE PENELITIAN

Penelitian ini menggunakan pendekatan studi literatur, yang dilakukan dengan mengumpulkan dan menganalisis berbagai referensi dari penelitian-penelitian sebelumnya. Data yang diperoleh kemudian diintegrasikan untuk menghasilkan kesimpulan yang komprehensif. Dalam penelitian ini, teknik analisis data yang digunakan adalah metode analisis isi, yang memungkinkan penarikan kesimpulan yang valid dan pengecekan kembali terhadap konteksnya. Proses analisis dimulai dengan mengidentifikasi hasil penelitian yang paling penting, esensial, dan relevan. Selanjutnya, penelitian diurutkan berdasarkan tahun publikasi, dimulai dari yang paling terbaru, kemudian bergerak mundur ke tahun-tahun sebelumnya. Peneliti kemudian membaca ringkasan dari setiap penelitian yang relevan untuk menilai kesesuaian topik yang dibahas dengan fokus penelitian ini. Pada tahap finalisasi, perhatian diberikan pada bagian-bagian yang penting dan relevan dengan masalah penelitian.

IV. HASIL DAN DISKUSI

Seperti yang telah dijelaskan, bahwa penelitian ini dengan mengemukakan studi literatur. Oleh karena itu, langkah selanjutnya yang penulis lakukan setelah mengidentifikasi kebutuhan pada penelitian ini adalah mulai melakukan literature studi. Berbagai penelitian yang memiliki topik kajian sama sebelumnya, penulis kumpulkan dan telaah kemudian penulis rangkum satu sama lain. Rangkuman hasil studi tersebut seperti pada TABEL 1.

 ISSN 3109-7677

TABEL 1. Studi Literatur

Penelitian	***Permasalahan***	***Topik Keamanan***	***Tantangan***	***Kesimpulan***
A Review of Security Standards and Frameworks for IoT-Based Smart Environments	Menemukan standar keamanan dan kerangka kerja penilaian yang paling memenuhi persyaratan keamanan serta menilai secara komprehensif dan memaparkan postur keamanan lingkungan pintar berbasis IoT	Menggunakan metode taksonomi untuk mendaftarkan langkah-langkah standarisasi keamanan IoT	Banyaknya produsen perangkat IoT tidak memasukkan desain keamanan dan menggunakan berbagai protokol terbaik sehingga membuat konfigurasi kompleks di lingkungan cerdas berbasis IoT.	Keamanan lingkungan pintar berbasis IoT sulit dikembangkan dan diterapkan karena kombinasi tantangan yang ada. Untuk mengatasi ini, makalah ini membahas berbagai standar keamanan, termasuk 80 standar ISO/IEC, 32 standar ETSI, dan 37 kerangka kerja keamanan konvensional yang mencakup 7 publikasi khusus NIST dalam teknik keamanan.
ANT-Centric IoT Security Reference Architecture—Security-by-Design for Satellite-Enabled Smart Cities	Memahami masalah keamanan sistem IoT yang kompleks, dan mengusulkan arsitektur referensi keamanan untuk menilai risiko keamanan dan menangani persyaratan keamanan	Keamanan *ANT Centric* bertujuan melindungi aktivitas kritis dan menerapkan keamanan end-to-end dengan menggunakan konsep mikro-perimeter untuk menghindari asumsi keamanan pada jaringan fisik yang mendasarinya.	1. Kompleksitas sistem IoT dalam hal jumlah perangkat yang terhubung dan persyaratan komunikasi dan pemrosesan yang luas. 2. Peningkatan paparan serangan fisik karena penempatan di lapangan.	IoV meningkatkan navigasi, keselamatan, dan manajemen lalu lintas. SAGIN menjadi infrastruktur ideal untuk menghubungkan IoV dan mendukung kota pintar.
Reviewing IoT Security via Logic Bugs in IoT Platforms and Systems	Kompleksitas (*platform* dan sistem IoT) justru meningkat dalam hal interaksi antara dunia fisik dan dunia maya. Kompleksitas yang meningkat dapat menghasilkan kerentanan baru.	Sistem model, dan skenario serangan perangkat IoT secara umum (*Hardware, Cloud)*	Lebih Banyak Entitas yang Terlibat. Dibandingkan dengan sistem komputasi tradisional, ada lebih banyak entitas yang terlibat	Pabrikan perangkat IoT harus menyadari bahwa perangkat IoT tidak lagi beroperasi sebagai sistem individual. Mereka harus lebih memperhatikan bahaya logika yang terlibat dalam komunikasi perpustakaan.
Arm PSA-Certified IoT Chip Security: A Case Study	Menganalisis keamanan chip IoT yang telah memperoleh sertifikasi *Arm Platform Security Architecture* (PSA) Level 2.	Sertifikasi *Arm Platform Security Architecture* (PSA) Level 2.	Mengevaluasi kebocoran fisik pada chip target dan menganalisis kebisingan dalam jejak elektromagnetik yang dikumpulkan. Mereka juga melakukan simulasi serangan saluran samping EM dengan skenario yang sesuai dengan dunia nyata sebanyak mungkin.	Menganalisis chip keamanan yang telah lulus sertifikasi *Arm's PSA Level 2.* Penulis berhasil memulihkan setengah dari byte kunci enkripsi AES di chip keamanan dengan menggunakan analisis saluran samping EM.
A Network-Aware Internet-Wide Scan for Security Maximization of IPv6-Enabled WLAN IoT Devices	WLAN IoT, seperti IEEE 802.11ah (*WiFi-HaLow*), rentan terhadap ancaman keamanan karena sumber daya yang terbatas, membatasi penggunaan perlindungan dan protokol keamanan.	Aktivasi IPv6 WLAN di Perangkat IoT	Dampak pemindaian tingkat pada skor temporal melibatkan perbaikan, kepercayaan laporan, dan kematangan kode. Metrik lingkungan mencerminkan pengaruh pada keamanan perangkat melalui modifikasi lingkungan keamanan seperti CONF, INT, AVA, dan persyaratan terkait.	Peneliti mengamati bahwa kecepatan pemindaian yang optimal memberikan keamanan yang tinggi sambil memastikan QoS. Namun, pendekatan ini mempertimbangkan perspektif admin detik, yang tidak dapat mengontrol parameter jaringan.
A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security	Sifat lintas sektoral dan multidisiplin sistem IoT menyebabkan tantangan keamanan baru. Langkah-langkah keamanan tradisional tidak efektif untuk melindungi perangkat IoT dan mengatasi kerentanan yang ada.	Taksonomi ML/DL Metode untuk keamanan IoT	Tantangan utama dalam ML dan DL adalah memperoleh set data pelatihan berkualitas tinggi yang mencakup berbagai jenis serangan.	ML dan DL untuk keamanan IoT saling terkait dan saling berinteraksi. Integrasi sinergis ML, DL, dan *blockchain* meningkatkan keamanan dalam sistem IoT.
Blockchain mechanisms for IoT security	Penelitian ini menyoroti beberapa lingkungan IoT di mana BCM memainkan peran penting, sementara pada saat yang sama	Mekanisme *Blockhain*	Teknologi IoT/CPS relatif baru dan belum sepenuhnya dipahami seperti sistem TI tradisional. Belum ada standar komprehensif untuk	Keuntungan menggunakan blockchain adalah bahwa mereka dapat bekerja di lapisan bawah model komunikasi serta di lapisan

 ISSN 3109-7677

	menunjukkan bahwa BCM hanyalah bagian dari solusi Keamanan IoT (IoTSec).		arsitektur, jaringan, dan keamanan yang telah dikembangkan, distabilkan, diadopsi, atau diterapkan. Standarisasi akan memfasilitasi kesederhanaan dan integrasi sistem (termasuk keamanan) dari berbagai vendor terbaik.	aplikasi, sehingga memungkinkan penggunaan sinergis mekanisme lintas lapisan dan domain ekosistem IoT.
Security of IoT Systems: Design Challenges and Opportunities	Memberikan dorongan untuk pengembangan teknik keamanan IoT *Computer-aided design* (CAD). Kita mulai dengan menyajikan survei singkat tentang tantangan dan peluang IoT dengan penekanan pada masalah keamanan	*IoT Security Desiderata* dan *Public physical unclonable function* (PUF)	Dua kendala utama untuk perangkat IoT adalah energi dan keamanan. Kedua kendala tersebut dapat diatasi dengan baik menggunakan teknik CAD	Teknik CAD intensif pengoptimalan ditambah dengan pemodelan akurat tradisional mereka secara alami cocok untuk mengaktifkan desain yang sangat optimal perangkat IoT
IoT Security : ZWave and Thread	Penelitian ini membahas tantangan keamanan untuk sistem IoT. Fitur keamanan sistem IoT tersebar di banyakZ bagian protokol IoT dan membahas berbagai jenis serangan pada sistem IoT dan cara protokol menanganinya	*Zwave* dan *Thread*	- Autentikasi: Verifikasi kredensial perangkat sebelum akses sumber daya PAN. - Kerahasiaan: Enkripsi data untuk melindungi isi pesan. - Otorisasi: Perangkat yang telah dikonfirmasi memiliki izin dan hak akses untuk mengakses sumber daya PAN.	*Z-Wave* dapat beradaptasi dan bertahan dari perubahan teknologi. *Thread* masih baru, sehingga sulit menemukan produk dengan logo *Thread* di pasaran. Waktu akan menentukan bagaimana *Thread* berkembang seiring berjalannya waktu.
Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures	IoT biasanya memiliki arsitektur tiga lapisan yang terdiri dari lapisan Persepsi, Jaringan, dan Aplikasi. Sejumlah prinsip keamanan harus diterapkan pada setiap lapisan untuk mencapai realisasi IoT yang aman.	3 Layar arsitektur IoT: Aplikasi, Jaringan dan Persepsi	Tantangan teknologi biasanya terkait dengan teknologi nirkabel, skalabilitas, energi, dan sifat terdistribusi, sedangkan tantangan keamanan memerlukan kemampuan untuk memastikan keamanan dengan otentikasi, kerahasiaan, keamanan *end-to-end*, integritas, dll.	Kerangka IoT rentan terhadap serangan di semua lapisan, dan banyak tantangan dan persyaratan keamanan perlu diatasi. otentikasi dan protokol kontrol akses, tetapi dengan kemajuan teknologi seperti IPv6 dan 5G, integrasi protokol jaringan baru menjadi penting untuk mencapai topologi IoT yang dinamis.

 ISSN 3109-7677

Berdasarkan TABEL 1, selanjutnya penulis mulai menganalisis topik standar keamanan IoT yang terdapat pada masing-masing penelitian. Langkah ini dilakukan untuk melihat kesamaan dan inti dari masing-masing objektif penelitian tersebut. Kompleksitas *platform* dan sistem IoT semakin meningkat di dunia siber dan nyata maka akan semakin menghasilkan kerentanan yang baru. Kendala utama untuk perangkat IoT adalah energi dan keamanan [7]. Kerangka IoT rentan terhadap serangan di setiap lapisan jaringan dan sistem [8], karenanya ada banyak tantangan dan persyaratan keamanan yang perlu ditangani. Persyaratan untuk mengamankan perangkat IoT sangat kompleks, karena berbagai teknologi, mulai dari perangkat fisik dan komunikasi nirkabel hingga arsitektur seluler dan komputasi awan, harus diamankan dan diintegrasikan dengan teknologi lainnya. Karena standar keamanan dan kerangka kerja dapat diterapkan di domain IoT sangat berbeda dari yang digunakan di domain non-IoT, diperlukan standar keamanan yang efektif dan dengan kerangka kerja berbasis IoT. Semua tantangan ini membuat pengembangan, penerapan, pemantauan, dan pemeliharaan keamanan lingkungan cerdas berbasis IoT menjadi jauh lebih sulit [2].

Lebih jauh, dari 80 standar keamanan ISO/IEC, 32 standar ETSI, dan 37 kerangka kerja keamanan konvensional yang berbeda, termasuk 7 publikasi desain keamanan khusus NIST. Proses peninjauan menemukan bahwa standar keamanan dan kerangka kerja evaluasi akan secara langsung menangani persyaratan keamanan berbasis IoT [2]. Taksonomi mencakup kemungkinan solusi untuk tantangan yang teridentifikasi. Arsitektur referensi keamanan *ANT-centric* sebagai salah satu fokus pada tiga perspektif arsitektur dalam mempelajari sistem IoT yaitu perangkat, internet dan semantik [9]. *ANT-centric* bisa direkomendasikan untuk perangkat IoT dan sudah diterapkan di penelitian kendaraan internet (IoV). Sedangkan untuk spesifik perangkat *chip* IoT, *sertifikasi Arm's PSA Level 2* termasuk aman dibandingkan chip keamanan lain yang beredar di pasar. Meskipun, tetap memiliki risiko kebocoran informasi kunci yang sudah dienkripsi karena sertifikasi PSA level 2 hanya persyaratan dasar. Sertifikasi PSA Level 3 lebih baik karena memungkinkan jaminan keamanan yang lebih ketat. Namun, hanya dua chip yang memperoleh sertifikasi Level 3, dan sebagian besar *chip* yang ada belum mendapatkan sertifikasi tersebut [10].

Kemajuan dalam *machine learning* dan *data mining* telah memungkinkan pengembangan berbagai metode analitik yang kuat yang dapat digunakan untuk meningkatkan keamanan IoT [11]. *Blockchain* tidak terbatas peruntukkannya untuk uang digital, namun bisa diterapkan di integrasi aplikasi data IoT yang ditransasikan ruang lingkup jaringan *multi-tier* yang besar maupun arsip sistem [12]. Teknik *computer-aided design* (CAD) intensif dan optimal yang digabungkan dengan pemodelan akurat tradisional, secara alami cocok untuk memungkinkan desain perangkat IoT yang sangat aman. *Z-wave* lebih aman karena *Z-wave* mendapatkan kerangka keamanan S2 [13]. Kerangka kerja keamanan S2, didasarkan pada AES-128 untuk tautan data dan ECDH untuk pertukaran kunci [14]. Thread masih sangat baru sehingga sulit untuk menemukan produk apa pun di pasaran [15].

V. KESIMPULAN

Berdasarkan identifikasi dari literatur yang relevansi, 9 (sembilan) dari 10 (sepuluh) jurnal membahas tujuan utama dari standarisasi keamanan IoT. Pengumpulan data terfokus kepada beragam standarisasi dan kerangka kerja keamanan yang digunakan. Standarisasi keamanan data IoT sangat penting untuk melindungi data yang dikirimkan oleh perangkat IoT dan jaringan IoT. Standarisasi keamanan yang jelas memungkinkan pengembang merancang perangkat IoT dengan tindakan keamanan yang konsisten dan teruji. Membantu mengurangi risiko serangan dan melindungi privasi pengguna. Hal ini berbanding lurus dengan perusahaan meningkatkan kepercayaan pengguna menggunakan sistem IoT. Investasi keamanan sesuai standar menghasilkan biaya yang lebih layak dihabiskan dibanding biaya pemulihan. Meskipun standar keamanan data IoT sudah ada, melibatkan berbagai pihak dalam proses standarisasi penelitian dan pengembangan harus terus dilakukan untuk memerangi ancaman keamanan baru yang hadir dengan perkembangan teknologi IoT.

1. REFERENSI

[1] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," IEEE Internet Things J, vol. 7, no. 10, pp. 10250–10276, 2020, doi: 10.1109/JIOT.2020.2997651.

[2] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," IEEE Access, vol. 9, pp. 121975–121995, 2021, doi: 10.1109/ACCESS.2021.3109886.

[3] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2019, doi: 10.1016/j.comnet.2012.12.018.

[4] Zen Munawar and Novianti Indah Putri, "Keamanan IoT Dengan Deep Learning dan Teknologi Big Data," Tematik, vol. 7, no. 2, pp. 161–185, 2020, doi: 10.38204/tematik.v7i2.479.

[5] A. Haryanto and S. M. Sutra, "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020," Global Political Studies Journal, vol. 7, no. 1, pp. 56–69, 2023, doi: 10.34010/gpsjournal.v7i1.8141.

[6] L. Arsada and H. Pembahasan, "Penerapan Metode NIST untuk Analisis Serangan Denial of Service (DOS) pada Perangkat Internet of Things (IoT)," Jurnal Ilmiah Komputasi, vol. 20, no. 2, pp. 275–281, 2021, doi: 10.32409/jikstik.20.2.2724.

[7] W. Zhou et al., "Reviewing IoT Security via Logic Bugs in IoT Platforms and Systems," IEEE Internet Things J, vol. 8, no. 14, pp. 11621–11639, 2021, doi: 10.1109/JIOT.2021.3059457.

[8] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015, pp. 336–341, 2016, doi: 10.1109/ICITST.2015.7412116.

[9] D. Lammert, "The connection between the sustainability impacts of software products and the role of software engineers," ACM International Conference Proceeding Series, pp. 294–299, 2021, doi: 10.1145/3463274.3463346.

[10] F. Chen, D. Luo, J. Li, V. C. M. Leung, S. Li, and J. Fan, "Arm PSA-Certified IoT Chip Security: A Case Study," Tsinghua Sci Technol, vol. 28, no. 2, pp. 244–257, 2023, doi: 10.26599/TST.2021.9010094.

[11] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," IEEE Communications Surveys

 ISSN 3109-7677

and Tutorials, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2988293.

[12] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," Internet of Things (Netherlands), vol. 1–2, pp. 1–13, 2018, doi: 10.1016/j.iot.2018.05.002.

[13] J. Shepard, "New Security Requirements for All Z-Wave Certified IoT Devices," eepower.com.

[14] Silicon Lab, "Introduction to Z-Wave SmartStart," 2017.

[15] I. Unwala, Z. Taqvi, and J. Lu, "IoT security: ZWave and thread," IEEE Green Technologies Conference, vol. 2018-April, pp. 176–182, 2018, doi: 10.1109/GreenTech.2018.00040.