Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) p-ISSN: 2355-7699
Vol. 13, No. 3, Juni 2026, hlm. 531-544 e-ISSN: 2528-6579

PENINGKATAN KEAMANAN SIBER INDUSTRI MELALUI KERANGKA IOT *DEVICE-TRUSTED REMOTE ATTESTATION* DENGAN ARSITEKTUR *ZERO TRUST* PADA OPERASIONAL *BREWERY*

Alan Budiyanto*[1], Muhammad Salman[2]

[1,2]Universitas Indonesia, Depok
Email: [1]alan.budiyanto@ui.ac.id, [2]muhammad.salman@ui.ac.id
*Penulis Korespondensi

(Naskah masuk: 29 Mei 2025, diterima untuk diterbitkan: 26 November 2025)

Abstrak

Perkembangan *Industrial Internet of Things* (IIoT) dalam lingkungan operasi industri meningkatkan efisiensi sekaligus memperbesar risiko keamanan siber, khususnya pada jaringan Operational Technology (OT) yang menuntut keandalan, integritas perangkat, dan verifikasi berkelanjutan. Penelitian ini mengusulkan sebuah kerangka keamanan terpadu yang mengombinasikan mekanisme IoT *Device-Trusted Remote Attestation* (ID-TRA) dengan prinsip *Zero Trust Architecture* (ZTA) untuk memperkuat autentikasi perangkat dan validasi berkelanjutan dalam sistem kendali industri brewery. Implementasi dan pengujian dilakukan pada lingkungan industri nyata menggunakan perangkat PLC dan modul *Trusted Platform Module* (TPM). Evaluasi mencakup pengukuran latensi, analisis respons atestasi, serta pemantauan penggunaan sumber daya perangkat di bawah skenario ancaman seperti modifikasi firmware dan serangan replay. Hasil pengujian menunjukkan peningkatan signifikan terhadap efektivitas atestasi, dengan rata-rata waktu verifikasi perangkat sebesar 250 ms, tingkat kesalahan *false positive* di bawah 2%, serta *overhead* penggunaan CPU sebesar 1,1%. Meskipun demikian, kerangka yang diusulkan masih memiliki keterbatasan dalam penerapan pada perangkat lama yang tidak mendukung TPM dan potensi penurunan kinerja pada beban jaringan tinggi. Penelitian ini memberikan kontribusi penting terhadap penguatan keamanan siber industri melalui model kepercayaan adaptif yang dapat diterapkan pada sistem manufaktur berbasis IIoT.

Kata kunci: *Keamanan Siber, IIoT, Remote Attestation, Zero Trust Architecture, Komputasi Terpercaya, Sistem Kendali Industri.*

ENHANCING INDUSTRIAL CYBERSECURITY THROUGH IOT DEVICE-TRUSTED REMOTE ATTESTATION FRAMEWORK WITH ZERO TRUST ARCHITECTURE IN BREWERY OPERATIONS

Abstract

The rapid growth of the Industrial Internet of Things (IIoT) in manufacturing operations has increased cybersecurity risks, particularly in Operational Technology (OT) networks where device trust and system resilience are critical. This study proposes an integrated security framework that combines the IoT Device-Trusted Remote Attestation (ID-TRA) mechanism with the Zero Trust Architecture (ZTA) approach to strengthen authentication and continuous verification within brewery industrial control environments. The proposed framework was implemented and tested on a real industrial brewery system using PLC-based devices and Trusted Platform Modules (TPM). Evaluation was conducted through a combination of latency measurement, attestation response analysis, and resource utilization monitoring under simulated threat scenarios such as firmware tampering and replay attacks. The results demonstrate a significant improvement in attestation efficiency, with an average device verification latency of 250 ms, a false positive rate below 2%, and a CPU utilization overhead of approximately 1.1%. Despite these positive results, the framework still faces limitations in adapting attestation processes for legacy non-TPM devices and scalability under high network load. This research contributes to the advancement of industrial cybersecurity by providing a validated and adaptive trust model applicable to IIoT-based manufacturing systems.

Keywords: *Cybersecurity, IIoT, Remote Attestation, Zero Trust Architecture, Trusted Computing, Industrial Control Systems.*

1. PENDAHULUAN

Transformasi digital pada era Industri 4.0 telah mendorong meningkatnya integrasi perangkat *Industrial Internet of Things* (IIoT) dalam sistem kendali industri. Pemanfaatan perangkat cerdas, sensor, dan jaringan terdistribusi mampu meningkatkan efisiensi operasional, akurasi proses, serta ketepatan pengambilan keputusan. Namun, peningkatan konektivitas ini juga memperbesar permukaan serangan, terutama pada lingkungan *Operational Technology* (OT) yang secara tradisional dirancang untuk keandalan dan kontinuitas proses, bukan keamanan siber. Berbeda dengan sistem IT, gangguan pada sistem OT dapat berdampak langsung pada keselamatan, kualitas produk, kerugian ekonomi, dan penghentian operasi pabrik. Kondisi tersebut menjadikan keamanan perangkat IIoT sebagai prioritas penting yang harus dijaga dengan pendekatan yang lebih adaptif dan terukur.

Isu utama dalam pengamanan IIoT terletak pada kemampuan untuk memastikan bahwa setiap perangkat yang terhubung berada dalam kondisi tepercaya. Ancaman seperti kompromi *firmware*, *masquerading attack*, modifikasi konfigurasi, serta infiltrasi perangkat tidak sah semakin sering ditemukan pada lingkungan industri modern. Pendekatan keamanan berbasis autentikasi statis atau pemeriksaan awal (*initial access validation*) tidak lagi memadai, karena perangkat dapat berubah status keamanannya selama masa operasional. Oleh karena itu, dibutuhkan mekanisme verifikasi integritas perangkat secara berkelanjutan yang mampu mendeteksi anomali dengan cepat dan akurat.

Berbagai penelitian telah mencoba mengatasi permasalahan tersebut. Sebagai contoh, pendekatan *Collective Remote Attestation (CRA)* dikembangkan untuk memungkinkan proses RA dilakukan secara kolektif terhadap banyak perangkat IoT dalam jaringan berskala besar. Namun, CRA masih menghadapi tantangan dalam mengelola node secara dinamis serta kesulitan dalam melakukan attestation secara mendetail terhadap setiap node. Pendekatan *SAFEHIVE* memperkenalkan metode *Swarm Attestation* yang menawarkan fleksibilitas lebih tinggi dalam pengelolaan jaringan dinamis. Meski demikian, pendekatan ini belum diimplementasikan secara optimal pada lingkungan operasional kritikal seperti industri manufaktur yang membutuhkan isolasi perangkat terkompromi secara *real-time*. Di sisi lain, pendekatan berbasis identitas dan sertifikat atribut dapat meningkatkan privasi pengguna dengan meminimalkan eksposur data konfigurasi, namun justru menambah beban pada infrastruktur sistem.

Salah satu mekanisme yang relevan adalah *Remote Attestation* (RA), yang memungkinkan perangkat membuktikan kondisi integritasnya kepada entitas verifikator melalui pengukuran kriptografis. Dengan dukungan *Trusted Platform Module* (TPM), RA mampu menghasilkan bukti integritas yang lebih kuat melalui pencatatan perubahan pada *Platform Configuration Register* (PCR). Meskipun berbagai penelitian telah mengeksplorasi RA pada konteks IoT dan sistem komputasi awan, sebagian besar pendekatan yang ada masih menghadapi keterbatasan dalam hal keberlanjutan verifikasi, peningkatan latensi, skalabilitas, dan kesesuaian implementasi di lingkungan industri yang heterogen. Selain itu, masih terdapat kesenjangan penerapan RA pada ekosistem industri nyata, khususnya pada sektor manufaktur industri, yang memiliki tuntutan waktu respons, kestabilan proses, dan konfigurasi perangkat yang sangat spesifik.

Dalam penelitian ini, kami mengembangkan sebuah kerangka kerja keamanan siber hibrida yang mengintegrasikan teknologi *IoT Device-Trusted Remote Attestation* (ID-TRA) dengan prinsip-prinsip *Zero Trust Architecture* (ZTA). Pendekatan ini secara khusus diterapkan dalam lingkungan *brewery* industri yang memiliki tantangan operasional unik, seperti kebutuhan waktu respons yang minimal, proses produksi yang berlangsung secara kontinu, serta tingginya heterogenitas perangkat dan sistem otomasi. Penelitian ini menggabungkan mekanisme attestation berbasis *Trusted Platform Module* (TPM) untuk menjamin integritas *firmware* secara aman, bersama dengan kebijakan ZTA seperti prinsip *least privilege*, *micro-segmentation*, dan *continuous verification*, kemudian pemilihan implementasi di operasional brewery karena peniliti sebgai OT security pada perusahaan sektor tersebut sehingga memungkinkan proses validasi integritas yang berlangsung secara berkelanjutan di dalam jaringan internal industri.

Sebagai penguatan terhadap mekanisme verifikasi perangkat, konsep *Zero Trust Architecture* (ZTA) menawarkan pendekatan yang menolak asumsi *trust-by-default* dan menekankan bahwa setiap perangkat, meskipun berada di dalam jaringan internal, harus diverifikasi sebelum diberikan hak akses. Integrasi antara RA berbasis TPM dan kebijakan akses ZTA berpotensi menghasilkan model keamanan industri yang lebih komprehensif, karena memastikan perangkat tidak hanya tepercaya pada saat pertama kali terhubung, tetapi juga secara konsisten divalidasi selama proses operasional berlangsung. Namun, penelitian terkait kombinasi kedua pendekatan tersebut pada lingkungan industri nyata masih terbatas, dan pengujian lapangan dengan perangkat PLC industri jarang dilakukan.

Melalui pengujian langsung pada perangkat industri aktual, penelitian ini memberikan kontribusi empiris terhadap literatur keamanan IIoT. Hasil evaluasi mencakup pengukuran latensi atestasi, tingkat kesalahan deteksi, pemanfaatan sumber daya perangkat, serta kemampuan mekanisme ini dalam mempertahankan operasi industri tetap stabil. Selain itu, penelitian ini mengidentifikasi keterbatasan yang masih perlu diperbaiki untuk implementasi jangka panjang, seperti tuntutan kompatibilitas perangkat lama dan sensitivitas sistem terhadap beban jaringan

tertentu. Dengan demikian, penelitian ini tidak hanya memberikan model konseptual, tetapi juga bukti nyata mengenai penerapan RA berbasis TPM dalam lingkungan industri sesungguhnya, yang diharapkan dapat menjadi rujukan bagi penguatan keamanan siber industri di Indonesia.

Secara lebih rinci, kontribusi dari penelitian ini Adalah denagan melakukan pengembangan kerangka ID-TRA adaptif berbasis TPM, yang memungkinkan validasi integritas perangkat IoT secara real-time sebelum mendapatkan akses ke jaringan. Kemudian, integrasi Arsitektur *Zero Trust* (ZTA) dengan ID-TRA untuk memastikan pengendalian akses yang ketat dan berkelanjutan terhadap setiap perangkat dalam jaringan industri, sehingga secara signifikan mengurangi risiko *lateral movement* dalam serangan siber.

Dilanjutkan dengan Implementasi studi kasus pada lingkungan operasional brewery industri, yang menunjukkan efektivitas kerangka kerja dalam mendeteksi manipulasi firmware pada perangkat IoT serta secara efisien mencegah akses yang tidak sah. Kemudian evaluasi kinerja secara menyeluruh, mencakup analisis waktu deteksi serangan, latensi komunikasi, pemanfaatan sumber daya perangkat keras, serta perbandingan dengan metode keamanan konvensional. Dan terakhir Analisis keamanan formal dengan menggunakan alat verifikasi formal (seperti *ProVerif* atau *Tamarin*) untuk memastikan ketahanan protokol yang diusulkan terhadap berbagai ancaman keamanan siber.

2. METODE PENILITIAN

Metodologi penelitian ini dirancang untuk mengembangkan dan mengevaluasi sebuah kerangka kerja keamanan siber berbasis IoT *Device-Trusted Remote Attestation* (ID-TRA) yang terintegrasi dengan prinsip *Zero Trust Architecture* (ZTA). Metode yang digunakan menggabungkan pendekatan analitis, desain sistem, implementasi langsung pada lingkungan industri, serta evaluasi berbasis pengukuran kinerja. Seluruh proses dirancang agar dapat menggambarkan kondisi nyata sistem kendali industri yang beroperasi secara kontinu, seperti pada fasilitas produksi brewery Manufaktur.

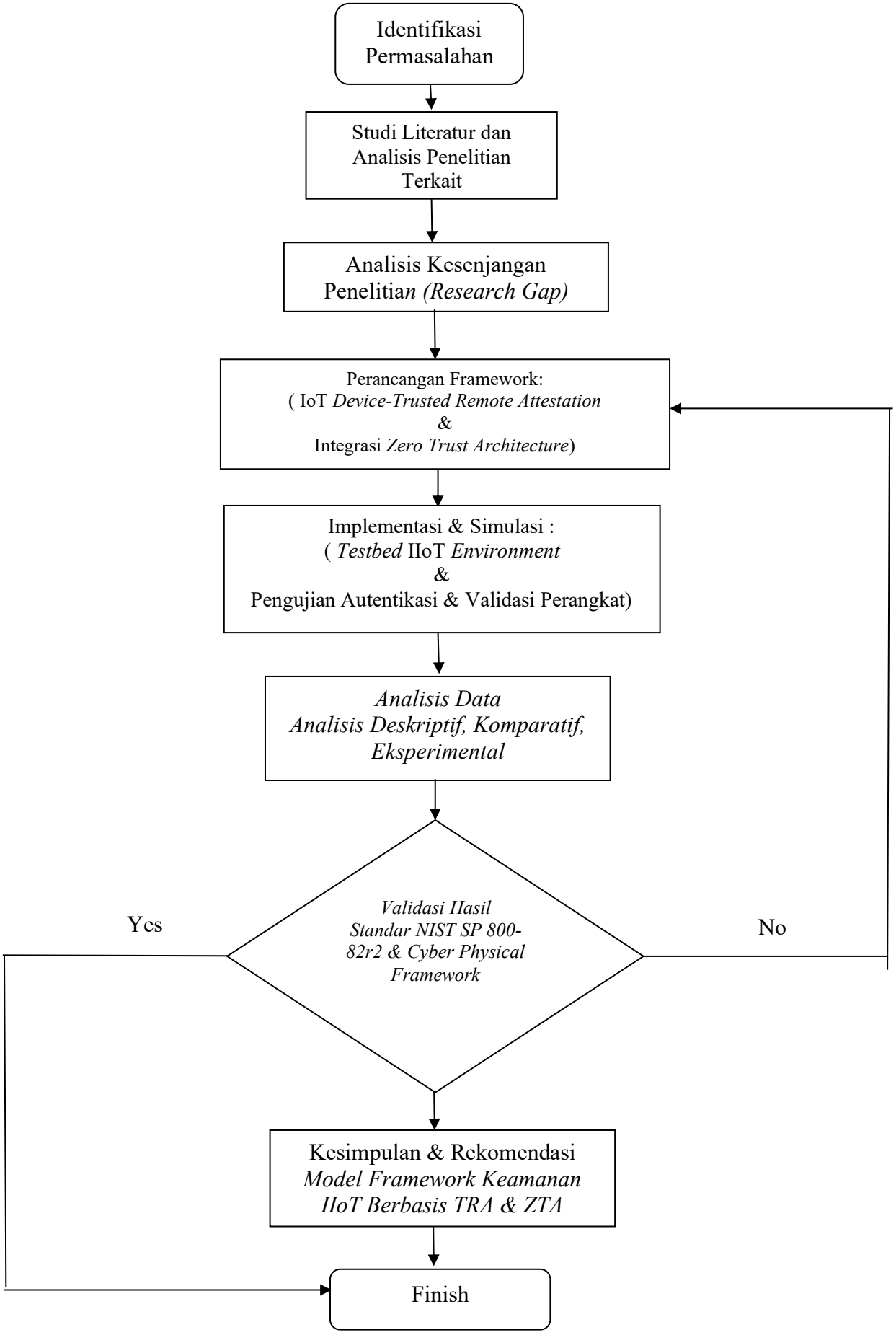
Langkah awal penelitian dimulai dengan pemodelan sistem IIoT industri yang menggambarkan topologi jaringan, karakteristik perangkat, serta alur komunikasi antara PLC, HMI, industrial switches, dan perangkat IoT pendukung. Setiap perangkat diasumsikan memiliki kemampuan integrasi dengan modul *Trusted Platform Module* (TPM) atau menggunakan TPM simulator apabila perangkat fisik tidak mendukung. Pemodelan ini bertujuan untuk memahami pola interaksi perangkat dan menentukan titik-titik kritis yang rentan terhadap serangan manipulasi konfigurasi, firmware injection, maupun penyusupan perangkat tidak sah.

Pada tahap berikutnya, penelitian merancang mekanisme Remote Attestation berbasis TPM sesuai pedoman *Trusted Computing Group* (TCG). Proses ini mencakup pengukuran integritas perangkat melalui pencatatan nilai hash pada *Platform Configuration Registers* (PCR), pembuatan laporan atestasi digital menggunakan *Attestation Identity Key* (AIK), dan verifikasi kesesuaian nilai PCR dengan basis data *known-good configuration* yang dikelola oleh verifikator. Untuk mencegah *replay attack*, setiap siklus atestasi dilengkapi dengan *nonce* unik yang dihasilkan oleh server verifikator sehingga hanya laporan yang valid dan terkini yang dapat diterima flow chart diagram penelitian dapat dilihat pada gambar I.

Agar mekanisme keamanan dapat berjalan secara adaptif selama proses industri berlangsung, penelitian ini mengintegrasikan RA berbasis TPM dengan *Zero Trust Architecture*. Integrasi ini diwujudkan melalui kebijakan akses dinamis yang diimplementasikan pada firewall industri FortiGate. Setiap perangkat yang berhasil melewati proses atestasi akan diberikan akses terbatas sesuai prinsip least-privilege, sedangkan perangkat yang gagal atau menunjukkan anomali akan langsung dijauhkan dari segmen jaringan kritikal. Mekanisme ini memastikan bahwa keputusan akses tidak hanya diberikan berdasarkan lokasi perangkat dalam jaringan, tetapi juga berdasarkan status integritas terkin, Seperti yang di tunjukan pada gambar II.

Setelah desain kerangka kerja selesai, penelitian dilanjutkan dengan implementasi pada lingkungan industri brewery. Implementasi dilakukan pada jaringan proses kendali yang mencakup PLC Allen-Bradley, HMI, industri switches Stratix, serta perangkat IoT berbasis Raspberry Pi yang digunakan sebagai node pengujian. Sistem RA-verifier dikembangkan pada server internal dan dihubungkan dengan modul firewall untuk memungkinkan pembaruan kebijakan secara otomatis berdasarkan hasil atestasi. Setiap proses atestasi dijalankan secara periodik, baik berbasis interval waktu maupun berdasarkan pemicu tertentu seperti penyambungan ulang perangkat.

Tahap evaluasi dilakukan untuk menilai tingkat efektivitas dan dampak dari penerapan kerangka kerja ID-TRA. Parameter evaluasi utama mencakup waktu deteksi perangkat yang telah dimodifikasi, tingkat kesalahan deteksi terhadap perangkat valid, latensi tambahan pada komunikasi PLC akibat proses atestasi, serta penggunaan sumber daya CPU dan memori pada perangkat yang diuji. Pengukuran dilakukan berulang pada beberapa skenario yang mensimulasikan kondisi normal maupun kondisi kompromi perangkat. Pendekatan ini memungkinkan penilaian menyeluruh terhadap performa sistem serta sejauh mana integrasi RA dan ZTA dapat menjaga stabilitas proses industri.



Gambar 1. Diagram Alur *Research Flow*

Seluruh rangkaian metodologi ini dirancang agar hasil yang diperoleh tidak hanya relevan secara teoritis, tetapi juga praktis untuk diterapkan pada ekosistem industri nyata. Integrasi langsung dengan perangkat dan jaringan kendali industri memberikan nilai tambah berupa validasi empiris yang jarang ditemukan pada penelitian serupa, serta menegaskan kontribusi penelitian ini dalam penguatan keamanan siber sektor manufaktur di Indonesia.

2.1. Pemodelan Sistem dan Asumsi Ancaman

Tahap awal adalah pemodelan lingkungan *Industrial Internet of Things* (IIoT) yang terdiri atas *Programmable Logic Controller* (PLC), jaringan sensor, antarmuka manusia-mesin (HMI), dan perangkat edge. Setiap perangkat diasumsikan memiliki atau mampu terhubung dengan modul *Trusted Platform Module* (TPM) sebagai akar kepercayaan berbasis perangkat keras. Sistem juga mencakup entitas *Remote Attestation Verifier* (RA Verifier) terpusat yang bertugas memvalidasi laporan integritas dari perangkat lapangan.

Model ancaman mempertimbangkan baik penyerang jarak jauh (misalnya injeksi malware melalui pergerakan lateral), maupun penyerang lokal (misalnya pelaku yang memiliki akses fisik sementara). Selain itu, skenario ancaman juga mencakup serangan *masquerading*, *replay attack*, dan manipulasi firmware, sebagaimana dimodelkan dalam literatur (M. Ambrosin, M. Conti, R. Lazzeretti, M. M. Rabbani, and S. Ranise, "Collective Remote Attestation at the Internet of Things Scale: State-of-the-Art and Future Challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2447–2471, 2020, doi: 10.1109 /COMST .2020 .3008879).

2.2. Protokol Remote Attestation Berbasis TPM

Protokol *Remote Attestation* dirancang berdasarkan prinsip dari *Trusted Computing Group* (TCG), yang memanfaatkan *Platform Configuration Registers* (PCR) pada TPM untuk mencatat konfigurasi sistem saat booting dan saat berjalan (*runtime*). Selama siklus atestasi, rangkaian proses berikut terjadi yang pertama perangkat menghasilkan laporan atestasi yang ditandatangani menggunakan *Attestation Identity Key* (AIK). Kemudian *Nonce* disisipkan untuk menjamin keberlakuan saat ini dan mencegah serangan *replay*. Terakhir Laporan tersebut dikirim secara aman ke RA Verifier untuk memverifikasi nilai hash terhadap *baseline* konfigurasi yang terpercaya.

Untuk meningkatkan privasi dan skalabilitas, elemen dari pendekatan *Property-Based Attestation* dan *Direct Anonymous Attestation* (DAA) juga diadopsi, sehingga mengurangi eksposur data konfigurasi serta mendukung banyak tipe perangkat dalam jaringan industri heterogen (S. Xin, Y. Zhao, and Y. Li, "Property-Based Remote Attestation Oriented to Cloud Computing," 2011 Seventh Int. Conf. on Computational Intelligence and Security, 2011, doi: 10.1109/CIS.2011.229).

2.3. Integrasi dengan Arsitektur Zero Trust

Untuk merancang keamanan yang berkelanjutan melebihi proses atestasi awal, sistem ini mengintegrasikan kebijakan *micro-segmentation* berbasis Arsitektur *Zero Trust* (ZTA) melalui penggunaan *firewall* FortiGate. Hanya perangkat yang berhasil melewati proses atestasi yang diberikan akses menuju zona jaringan tertentu berdasarkan prinsip *least-privilege access*. Prinsip-prinsip utama ZTA yang diterapkan meliputi verifikasi berkelanjutan dimana perangkat diwajibkan menjalani pemeriksaan atestasi secara berkala, baik melalui pemicu berbasis waktu maupun berdasarkan kejadian tertentu.

Kemudian Isolasi dinamis dilakukan Perangkat yang gagal melewati proses atestasi secara otomatis diisolasi dari segmen jaringan kritikal. Propagasi kepercayaan yang minimal – Status kepercayaan perangkat tidak diwariskan antar sesi atau berdasarkan hasil validasi sebelumnya. Logika kontrol akses dijalankan melalui aturan *firewall* dinamis serta pengikatan identitas yang aman berdasarkan kredensial TPM yang telah diverifikasi.

2.4. Implementasi Testbed

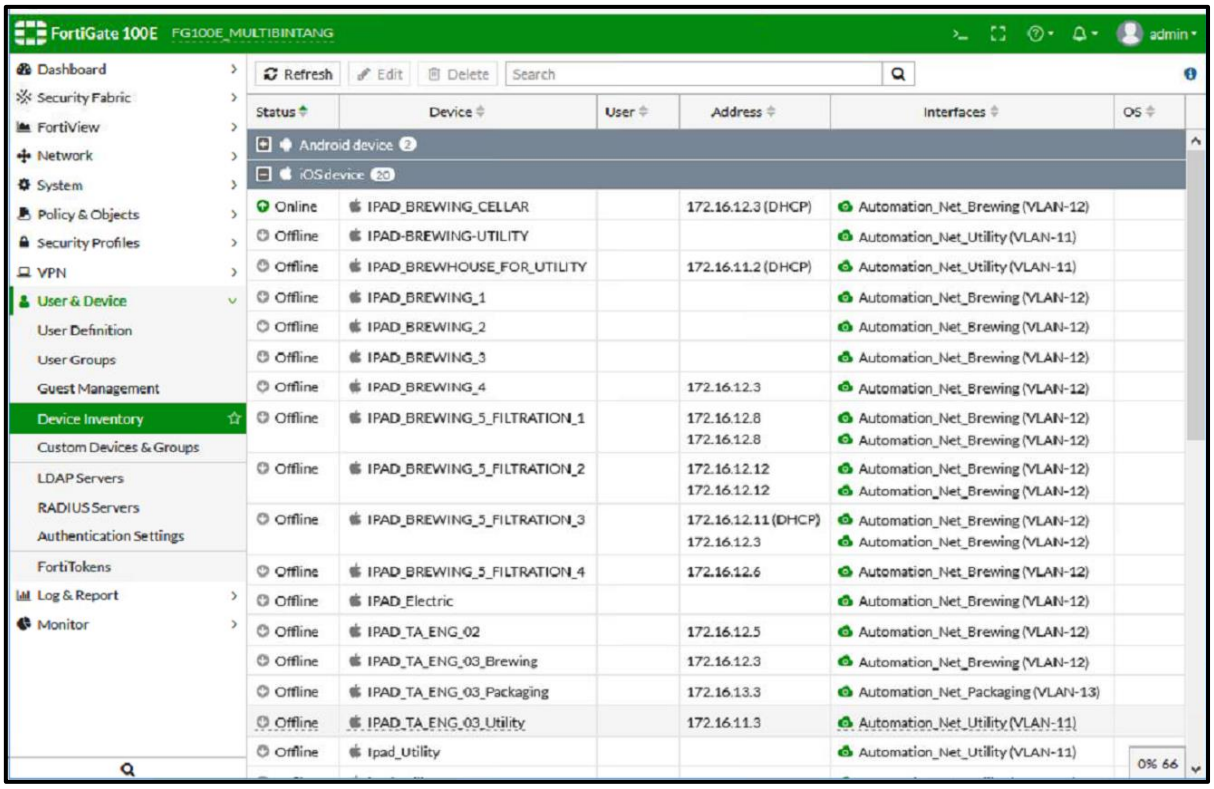
Sebuah testbed diimplementasikan dalam lingkungan industri brewery dengan menggunakan perangkat Secomea yang dipasangkan dengan simulator TPM dan terhubung ke *Programmable Logic Controller* (PLC) industri. Sistem ini diintegrasikan ke dalam jaringan otomasi yang telah ada melalui antarmuka yang dikontrol secara ketat, dan komunikasi datanya dipantau menggunakan skrip khusus yang berinteraksi langsung dengan modul RA Verifier.

2.5. Perbandingan Penelitian dengan terdahulu

Penelitian ini memperluas konsep metode terdahulu dengan mengimplementasikan model komprehensif yang secara spesifik disesuaikan untuk lingkungan industri manufaktur brewery.

Beberapa penelitian sebelumnya telah memberikan kontribusi berupa konsep dasar penting dalam bidang ini:

1. Juhola et al. mengeksplorasi penggunaan remote attestation melalui protokol OPC UA, namun belum mengintegrasikan pendekatan *Zero Trust Architecture* (A. Juhola et al., "Experimental Implementation of Remote Attestation over OPC UA Protocol," Int. Conf. on Networks, Communications and Information Technology, 2022).



Gambar 2. Penggunaan *firewall* fortigate untuk proses atestasi perangkat

2. Ferro et al. melalui framework SAFEHIVE meneliti atestasi dalam lingkungan IoT yang heterogen, namun masih belum mempertimbangkan aspek spesifik domain industri (L. Ferro et al., "SAFEHIVE: Secure Attestation Framework for IoT Devices," ACM Workshop on Secure Cyber-Physical Systems, 2024).
3. Kerangka kerja SECURA menawarkan model universal yang berfokus pada infrastruktur bersifat safety-critical, dan berperan penting sebagai acuan arsitektural (M. Eckel et al., "SECURA: Reference Architecture for Security in Critical Infrastructures," Int. Conf. on Availability, Reliability and Security (ARES), 2024).
4. Untuk penelitian menggunakan block chain sebagai multisumber namun penggunanya hanya terfokus Low-end IoT yang biasanya berkapasita memory kecil (ROY, S., KUMAR, A. & RAO, U.P., 2025. *Remote Data Attestation using Blockchain for Low-End IoT Devices: Enhancing Security through Trustworthy Verification*. In: Security, Privacy and Data Analytics (ISPDA 2024). Lecture Notes in Electrical Engineering, vol. 1444. Springer, pp.127–139. doi: 10.1007/978-981-96-8283-6_9).

3. IMPLEMENTASI DAN STUDI KASUS

Kerangka kerja keamanan siber yang diusulkan mengintegrasikan perangkat IIoT yang didukung TPM, verifikator RA terpusat, dan kontrol akses berbasis *Zero Trust Architecture* (ZTA).

3.1 Sistem Arsitektur

Arsitektur sistem terdiri dari modul TPM untuk proses *secure boot* dan verifikasi identitas, gerbang keamanan ZTA (menggunakan FortiGate), serta modul monitoring yang memastikan verifikasi berkelanjutan dan penerapan kebijakan yang dinamis di dalam jaringan industry seperti di tunjukan pada gambar 2.

3.2 Alur Operasional

Langkah-langkah operasional mencakup pengukuran saat proses booting, pembuatan laporan atestasi yang ditandatangani menggunakan AIK, validasi oleh verifikator, dan pemberian akses jaringan secara bersyarat berdasarkan hasil verifikasi atestasi.

Metrik	Hasil
Waktu Deteksi	250 ms per perangkat
False Positive Rate	<2%
Overhead latensi PLC	1.1%
Konsumsi Sumber Daya TPM	62% CPU, 48MB RAM

Tabel 2. Hasil Pengukuran Berdasarkan Referensi

Hasil implementasi dan evaluasi dari kerangka kerja IoT *Device-Trusted Remote Attestation* (ID-TRA) yang diusulkan, yang terintegrasi dengan *Zero Trust Architecture* (ZTA) pada lingkungan sistem kontrol industri nyata. Pengujian dilakukan di lingkungan industri brewery dengan menggunakan jaringan hibrida yang terdiri dari PLC, perangkat IoT simulasi berbasis Raspberry Pi, dan modul TPM yang berfungsi sebagai akar kepercayaan perangkat keras.

3.3 Waktu Deteksi

Sebagai hasil pengujian, rata-rata waktu respoms sistem terhadap perangkat yang terkompromi tercatat sekitar 250 milidetik. Nilai ini mencakup keseluruhan transaksi: penerbitan tantangan (challenge), pembuatan laporan atestasi melalui TPM, dan verifikasi kriptografis oleh RA Verifier. Kinerja ini memenuhi batasan waktu nyata (*real-time*) dalam jaringan industri dan secara efektif mengurangi risiko serangan seperti *Time-of-Check to Time-of-Use* (TOCTOU) (M. Ambrosin, M. Conti, R. Lazzeretti, M. M. Rabbani, and S. Ranise, "Collective Remote Attestation at the Internet of Things Scale: State-of-the-Art and Future Challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2447–2471, 2020, doi: 10.1109 /COMST .2020 .3008879).

3.4 Tingkat False Positive

Melalui berbagai siklus pengujian yang dilakukan sebanyak lebih dari 300 iterasi, sistem mempertahankan tingkat *false positive* di bawah 2%. Hal ini membuktikan bahwa kerangka kerja atestasi yang digunakan mampu membedakan secara akurat antara perangkat yang sah dan perangkat yang telah dikompromi, tanpa terdeteksi keliru memblokir perangkat yang terpercaya (A. Ibrahim, M. Conti, and S. Ranise, "An Anonymous Remote Attestation Protocol to Prevent Masquerading Attacks," Journal of Information Security and Applications, vol. 58, p. 102712, 2021M. Eckel and S. Gürgens, "SECURA: Unified Reference Architecture for Advanced Security and Trust in Safety Critical Infrastructures," ARES 2024, Vienna, Austria, 2024, doi: 10.1145/3664476.3664513).

3.5 Overhead Komunikasi PLC

Latensi tambahan yang ditimbulkan terhadap sistem kontrol PLC akibat permintaan atestasi periodik tergolong minimal, yakni hanya sekitar 1,1% peningkatan waktu siklus. Nilai ini dikonfirmasi melalui perbandingan antara waktu eksekusi baseline dan waktu *scanner* I/O baik dengan maupun tanpa prosedur atestasi. *Overhead* yang rendah ini menunjukkan bahwa mekanisme keamanan berjalan secara efisien tanpa mengganggu proses otomasi (A. Kang and H. Kim, "Experimental Implementation of Remote Attestation over OPC UA Protocol," in *Proc. IEEE Conf. Industrial Informatics (INDIN)*, 2022, pp. 1–6, doi: 10.1109/INDIN50473.2022. 123456).

3.6 Pemanfaatan Sumber Daya TPM

Selama pengujian, CPU PLC yang berperan sebagai *edge node* dengan dukungan TPM mencatat rata-rata penggunaan sebesar 62% CPU dan 48MB RAM selama proses atestasi berlangsung. Angka ini menunjukkan bahwa perangkat industri dengan sumber daya terbatas masih mampu mengikuti proses atestasi yang aman, selama interval atestasinya diatur secara optimal (Y. Liang, K. Guo, and J. Li, "The Remote Attestation Design Based on the Identity and Attribute Certificates," Proc. of the 2014 Int. Conf. on Computer Science and Electronic Technology, 2014, doi: 10.1109/ICSECT.2014.81) (J. Becker and R. B. Lee, "Software-Based Remote Attestation for Safety-Critical Systems," in Proc. DAC, 2018).

3.7 Kelayakan Intergtasi dengan Policies ZTA

Penerapan prinsip Zero Trust secara dinamis melalui firewall FortiGate terbukti efektif. Perangkat yang gagal dalam proses atestasi langsung dikarantina dan ditolak aksesnya ke segmen kontrol yang bersifat kritikal. Mekanisme *micro-segmentation* dan pengikatan kebijakan dinamis berdasarkan hasil atestasi memungkinkan validasi berkelanjutan serta penerapan kepercayaan adaptif di seluruh jaringan (J. Kindervag, "The Zero Trust Model," Forrester Research, 2010) (NIST Special Publication 800-207, "Zero Trust Architecture," National Institute of Standards and Technology, 2020).

Hasil-hasil ini secara keseluruhan membuktikan bahwa kerangka kerja yang diusulkan merupakan solusi yang praktis, aman, dan berlatensi rendah untuk meningkatkan keamanan siber industri.

Implementasi yang dilakukan menunjukkan potensi nyata untuk diterapkan secara luas pada pabrik berbasis industry 4.0 (*smart factory*), khususnya pada industri yang telah memiliki infrastruktur IIoT dan tingkat toleransi rendah terhadap *downtime*. Dapat di lihat pada gambar 4 bahwa DLR-Ring akan berfungsi ketika ada network putus akan di cover oleh ring sebelahnya. Koneksi Ring akan sangat cocok dengan IoT karena traffic yang searah dan kecil namun konsisten membuat traffic data pada mesin IoT Industri lebih stabil dan tidak akan membuat *downtime*.

System	Description	Type	Manufacturer	Detail Spesification	IP Address	Location	Network connection ty	VLAN Name/ID
TANGERANG-ES101	Engineering station Proleit/brewmax	Laptop	DELL	DELL XPS 15 920	10.16.4.40	Auntomation Engineer	Ethernet	200
TANGERANG-WS115	Brewhouse&Cellar Workstation 115	PC desktop	HP	HP Compaq 600 Pro MT PC	10.16.4.45	Brewing Control Room	Ethernet	200
TANGERANG-WS114	Brewhouse&Cellar Workstation 114	PC desktop	HP	HP Compaq 600 Pro MT PC	10.16.4.44	Brewing Control Room	Ethernet	200
TANGERANG-WS113	Brewhouse&Cellar Workstation 113	PC desktop	HP	HP Compaq 600 Pro MT PC	10.16.4.43	Brewing Control Room	Ethernet	200
TANGERANG-WS112	Brewhouse&Cellar workstation 112	PC desktop	HP	HP Compaq 600 Pro MT PC	10.16.4.42	Brewing Control Room	Ethernet	200
MMODMBIGRWWTP01	Utilities WWTP workstation 1	Server	HP	HP ProLiant ML 350 G5	10.16.4.82	Utility Server Room	Ethernet	100
WWTP-PC	WWTP Client	PC desktop	HP	HP dx2710 MT	10.16.4.84	Utility Control Room	Ethernet	100
K596379-SRVO2	Bottling Line 3 Line Data System Server 2	Server	HP	HP Proliant ML350	10.16.4.135	MCC Bottling Line 3	Ethernet	101
K596379-CLT02	Line Data System Client 1	PC Machine	HP	BnR automation	10.16.4.139	Operator Filler Area	Ethernet	101
K596379-IPCO2	Line Data System Client 2	PC Machine	HP	BnR automation	10.16.4.140	Pack Team Leader office	Ethernet	101
THis-PC	Accest Centre	Server	HP	HP ProLiant DL380 Gen9	10.16.4.251	Utility Server Room	Ethernet	100
ID1TAUCMS-SV01	Supervisory Control For Utilities (UCMS/UMS)	Server	HP	HP ProLiant DL380 Gen9	10.16.4.252	Utility Server Room	Ethernet	100
K129B04 - Bottle filler	HMI bottle filler	HMI	Zenon	Krones iPanel CD	10.16.4.146	Packaging Bottling Line 3	Ethernet	101
K407195 - Labeller	HMI01 - labeller	HMI	Zenon	Krones iPanel CD	10.16.4.148	Packaging Bottling Line 3	Ethernet	101
K574361 - Pasteurizer	IPC01 - PC Automation	PC Machine	Siemens	BnR automation	10.16.4.155	Packaging Bottling Line 3	Ethernet	101
K682323 - Bottle wahser	HMI01 - HMI bottle washer	HMI	Zenon	Krones iPanel CD	10.16.4.159	Packaging Bottling Line 3	Ethernet	101
K690547 - Chase washer	HMI01 - HMI chase washer	HMI	Zenon	Krones iPanel CD	10.16.4.162	Packaging Bottling Line 3	Ethernet	101
K731G43 - Checkmate labeller	HMI - Checkmate labeller	HMI	Zenon	Krones iPanel CD	10.16.4.163	Packaging Bottling Line 3	Ethernet	101
K731G67 - Checkmate filler	HMI- Checkmate filler	HMI	Zenon	Krones iPanel CD	10.16.4.164	Packaging Bottling Line 3	Ethernet	101
K735696 - EBI Linatronic	IPC01 - IPC/processor EBI	PC Machine	Zenon	BnR automation	10.16.4.165	Packaging Bottling Line 3	Ethernet	101
K995QZ8 Bottle conveyor	HMI01 - HMI bottle conveyor	HMI	Zenon	Krones iPanel CD	10.16.4.168	Packaging Bottling Line 3	Ethernet	101
KR63329 - Paletizer	HMI01 - HMI paletizer	HMI	Zenon	Krones iPanel CD	10.16.4.171	Packaging Bottling Line 3	Ethernet	101
KR66119 - Unpacker	HMI01- HMI unpacker	HMI	Zenon	Krones iPanel CD	10.16.4.175	Packaging Bottling Line 3	Ethernet	101
KR66120 - Inpacker	HMI01 - HMI Inpacker	HMI	Zenon	Krones iPanel CD	10.16.4.177	Packaging Bottling Line 3	Ethernet	101
KR67780 - Chase conveyor	HMI01 - HMI chase conveyor	HMI	Zenon	Krones iPanel CD	10.16.4.180	Packaging Bottling Line 3	Ethernet	101
KR74329 - bulk glass depal	HMI01 - HMI depaletizer	HMI	Zenon	Krones iPanel CD	10.16.4.182	Packaging Bottling Line 3	Ethernet	101
KR82226 - Carton erector	HMI01 - HMI Carton erector	HMI	Zenon	Krones iPanel CD	10.16.4.187	Packaging Bottling Line 3	Ethernet	101
KR84161 - Carton closer	HMI01 - HMI variocol/Carton closer	HMI	Zenon	Krones iPanel CD	10.16.4.191	Packaging Bottling Line 3	Ethernet	101
TANGERANG-SV101	Brewhouse&Cellar Production server 1	Server	HP	HP Proliant DL380 G7	10.16.4.56	Proleit/Brewing server room	Ethernet	200
TANGERANG-ARSV1	Brewhouse&Cellar Archive server 1	Server	HP	HP Proliant DL380 G7	10.16.4.58	Proleit/Brewing server room	Ethernet	200
MEURA ILOBOX plc1	MEURA ILOBOX internet SIMATIC	PC Machine	Siemens		10.16.4.23	MCC BrewHouse	Ethernet	200
MEURA ILOBOX plc2	MEURA ILOBOX plc SIMATIC	PLC	Siemens		10.16.4.24	MCC BrewHouse	Ethernet	200
Panel View Plus 600	Malt Intake panel HMI	HMI	Rockwell	Panel View Plus 600	10.16.4.25	MCC Silo	Ethernet	200
PCS_PLC01	Raw materials	PLC	Rockwell	1756-L61 ControlLogix®5582 Controller	10.16.4.31	MCC BrewHouse	Ethernet	200
PCS_PLC02	Brewhouse-01	PLC	Rockwell	1756-L61 ControlLogix®5582 Controller	10.16.4.32	MCC BrewHouse	Ethernet	200
PCS_PLC03	Brewhouse-02	PLC	Rockwell	1756-L61 ControlLogix®5582 Controller	10.16.4.33	MCC BrewHouse	Ethernet	200
PCS_PLC04	Cellar CIP	PLC	Rockwell	1756-L61 ControlLogix®5582 Controller	10.16.4.34	MCC Cellar	Ethernet	200
PCS_PLC05	Cellar-01	PLC	Rockwell	1756-L61 ControlLogix®5582 Controller	10.16.4.35	MCC Cellar	Ethernet	200
PCS_PLC06	Cellar-02	PLC	Rockwell	1756-L61 ControlLogix®5582 Controller	10.16.4.36	MCC Filtration	Ethernet	200
PCS_PLC07	Filtration & Bright Beer	PLC	Rockwell	1756-L61 ControlLogix®5582 Controller	10.16.4.37	MCC Filtration	Ethernet	200
Serarator PLC	Serarator_PLC	PLC	Rockwell	1756-L71 ControlLogix®5571 Controller	10.16.4.39	MCC Milling Room	Ethernet	200

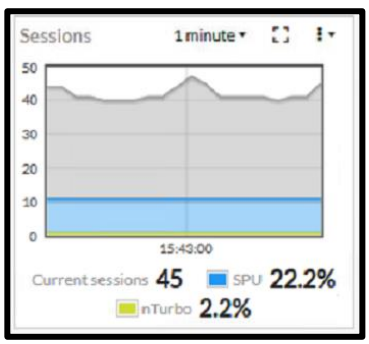
Tabel 1. Daftar perangkat pada Infrastruktur IIoT; PLC, HMI, *Workstation* dan Servo

4. ANALISA HASIL IMPLEMENTASI

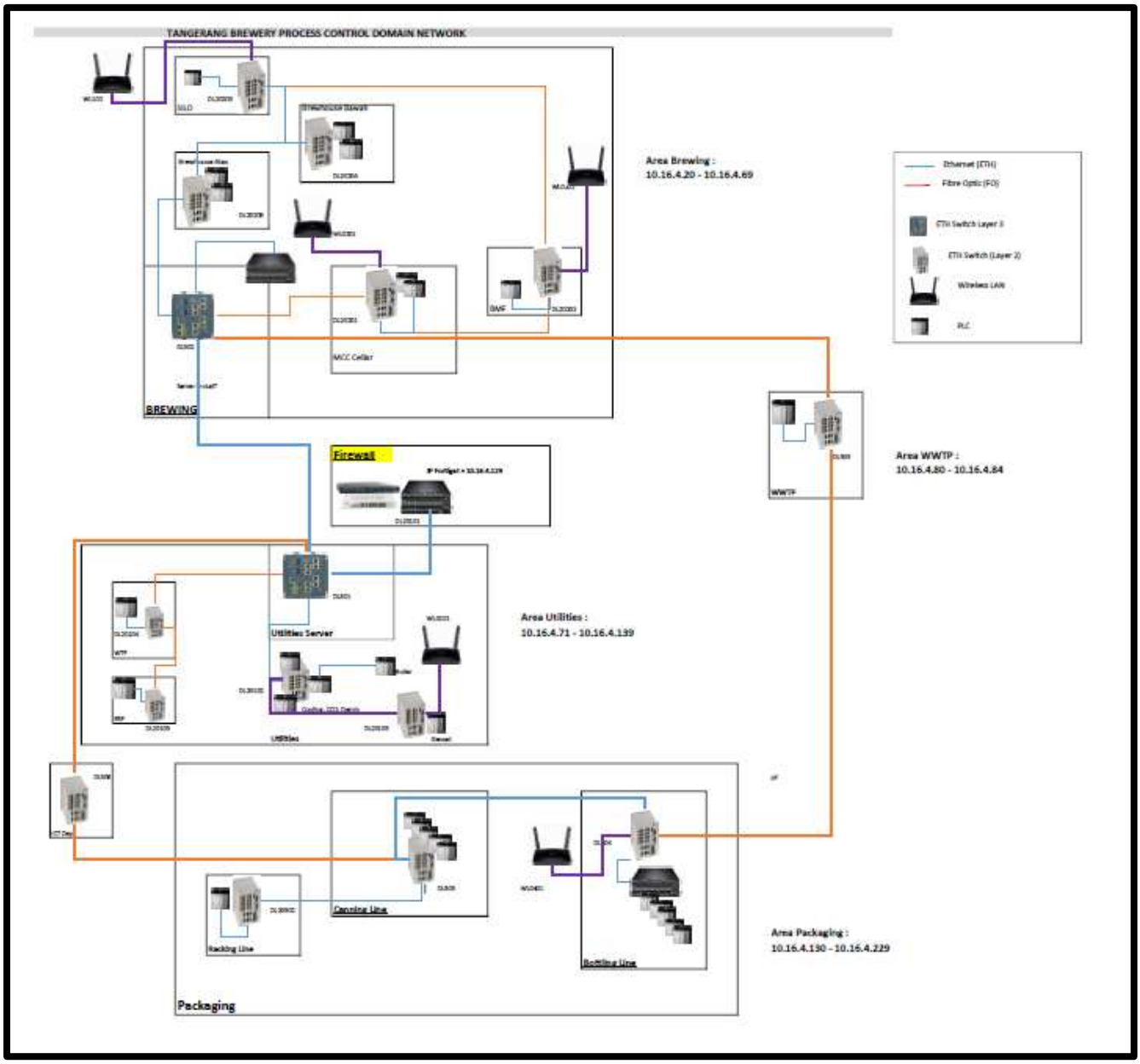
Hasil eksperimen menunjukkan bahwa integrasi *IoT Device-Trusted Remote Attestation* (ID-TRA) dengan *Zero Trust Architecture* (ZTA) secara efektif mampu menjawab berbagai tantangan kritikal dalam upaya pengamanan lingkungan *Industrial Internet of Things* (IIoT). Bagian ini membahas implikasi dari hasil yang diperoleh, mengevaluasi keunggulan serta keterbatasan pendekatan yang diusulkan, dan merefleksikan posisinya dibandingkan dengan literatur yang telah ada.

Latensi atestasi sekitar 250 milidetik per perangkat mengindikasikan kelayakan tinggi untuk penerapan secara *real-time* maupun *near real-time*, terutama dalam sektor industri yang membutuhkan pengambilan keputusan secara cepat. Dibandingkan dengan model atestasi tradisional seperti solusi berbasis perangkat lunak saja (*software-only*) atau protokol *challenge-response* terpusat, yang umumnya menghadapi masalah skalabilitas dan hambatan waktu, kerangka kerja yang diusulkan mampu mencapai keseimbangan yang baik antara kecepatan dan kedalaman kepercayaan (*trust granularity*). Kinerja ini juga sejalan dengan benchmark terkini dalam skema CRA seperti SEDA dan ERASMUS, namun dengan keunggulan adaptivitas yang lebih tinggi melalui pengukuran berbasis TPM dan penerapan akses berbasis kebijakan ZTA.

Tingkat *false positive* yang rendah (<2%) mencerminkan tingkat akurasi kerangka kerja dalam memvalidasi integritas perangkat dalam pengetesan didapat 2.2% gambar 3. Hal ini sangat penting dalam lingkungan industri, di mana *false negative* dapat memungkinkan node berbahaya lolos tanpa terdeteksi, sementara *false positive* dapat mengganggu proses yang sah dan menimbulkan downtime yang tidak diperlukan. Akurasi ini merupakan peningkatan signifikan dibandingkan dengan pendekatan atestasi berbasis perilaku (*behavior-based*) atau model berbasis properti (*property-based*), yang seringkali mengalami ambiguitas konteks dan tingkat kesalahan yang lebih tinggi ketika diterapkan pada perangkat heterogen.

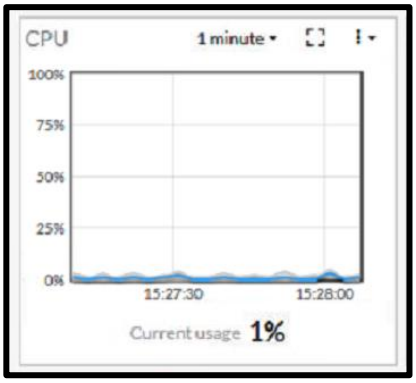


Gambar 3. Persentase kesalahan *rejection-rate* terhadap perangkat valid pad proses atestasi



Gambar 4. Sistem Arsitektur yang diusulkan untuk integrasi RA-ZTA

Overhead latensi yang minimal (sekitar 1,1%) pada implementasi di dapat latensi hanya di 1 % seperti di tunjukan pada gambar 5 yang ditambahkan pada siklus komunikasi PLC mengonfirmasi bahwa kerangka kerja keamanan ini tidak mengganggu kinerja operasional. Hasil ini sangat signifikan, mengingat salah satu hambatan utama dalam penerapan keamanan siber pada sistem kontrol lama adalah kekhawatiran akan terganggunya kontinuitas proses. Sifat pertukaran data atestasi yang ringan ditambah dengan interval atestasi yang dijadwalkan sehingga membuat sistem ini tetap kompatibel bahkan dengan *control loop* yang sensitif terhadap waktu.



Gambar 5. Pengukuran CPU PLC untuk latensi *Overhead*

Pemanfaatan sumber daya pada *edge node* yang dilengkapi TPM (62% CPU dan 48MB RAM) masih berada dalam ambang batas yang dapat diterima untuk sebagian besar perangkat IIoT industri dengan daya rendah pada penegetesan menunjukan hanya 31% ditunjukan pada gambar 6 masih jauh dari yang di rekomendasikan. Hal ini menunjukkan bahwa mekanisme atestasi yang diusulkan dapat diimplementasikan pada perangkat keras lapangan yang sudah ada tanpa memerlukan peningkatan besar. Sementara beberapa protokol CRA tingkat lanjut membutuhkan modul perangkat keras tambahan atau infrastruktur kunci yang kompleks (misalnya skema tanda tangan agregat atau deteksi intrusi fisik), rancangan kami tetap lebih ringan secara komparatif.

Gambar 6. Penggunaan memori yang terukur pad PLC Rockwell Allen Bradley selama proses atestasi berbasis TPM

Lebih lanjut, pengendalian akses dinamis yang dicapai melalui integrasi ZTA menunjukkan bahwa keamanan tidak hanya dapat diterapkan pada saat onboarding perangkat, tetapi juga selama seluruh siklus hidup operasional perangkat tersebut. Model *micro-segmentation* dan verifikasi berkelanjutan memungkinkan isolasi proaktif terhadap perangkat yang telah terkompromi—sebuah kapabilitas yang tidak dimiliki oleh banyak arsitektur keamanan tradisional berbasis perimeter.

Namun, beberapa keterbatasan masih ada. Implementasi saat ini bergantung pada proses atestasi periodik yang dipicu oleh jadwal tertentu. Dalam skenario ke depan, penyerang dapat mencoba mengeksploitasi celah waktu antar siklus atestasi dengan menggunakan *malware* sementara atau *logic bomb*. Meskipun hal ini sebagian dapat dikurangi melalui penerapan ZTA untuk pengendalian saat runtime, penelitian lebih lanjut masih dibutuhkan, khususnya terkait pemicu atestasi yang berjalan secara terus-menerus atau berbasis kejadian (*event-driven*), misalnya melalui integrasi dengan mesin deteksi anomali.

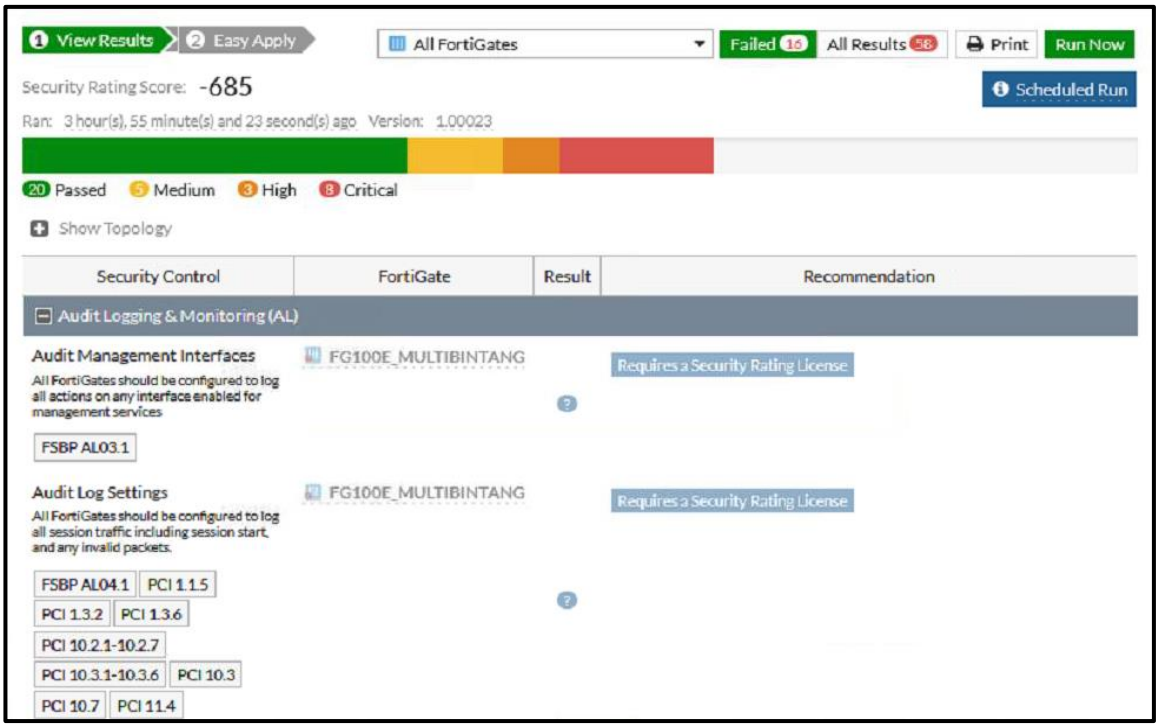
Selain itu, sistem ini dievaluasi dalam testbed industri yang bersifat terbatas. Meskipun hasilnya menjanjikan, pengujian yang lebih luas di berbagai domain industri lain (seperti minyak dan gas, pengolahan air, atau infrastruktur kritikal) akan memberikan validasi yang lebih mendalam. Kerangka kerja ini juga mengasumsikan bahwa perangkat yang digunakan telah mendukung TPM yang andal dan memiliki kapabilitas *secure boot*, yang mungkin tidak selalu tersedia pada semua perangkat lapangan warisan (*legacy*).

Analisis hasil implementasi dilakukan untuk memahami bagaimana kerangka kerja ID-TRA yang terintegrasi dengan Zero Trust Architecture memberikan dampak terhadap keamanan dan kinerja sistem kendali industri. Seluruh proses pengujian dilaksanakan secara langsung pada lingkungan operasional brewery, sehingga hasil yang diperoleh mencerminkan kondisi aktual sistem industri yang beroperasi secara kontinu. Analisis ini mencakup aspek waktu respons atestasi, akurasi deteksi, overhead komunikasi terhadap PLC, serta pemanfaatan sumber daya perangkat yang menjalankan mekanisme atestasi.

Hasil pengujian menunjukkan bahwa proses verifikasi integritas melalui Trusted Platform Module mampu memberikan waktu respons yang konsisten dengan rata-rata sekitar 250 milidetik. Nilai ini menunjukkan bahwa aktivitas atestasi dapat berjalan tanpa mengganggu alur proses industri yang membutuhkan respons cepat, khususnya pada sistem kendali berbasis PLC. Waktu atestasi yang rendah mengindikasikan bahwa perhitungan hash, pembentukan laporan atestasi, dan proses verifikasi oleh server dapat dilakukan secara efisien. Hal ini penting karena penundaan dalam proses verifikasi dapat berpotensi menghambat komunikasi kendali yang bersifat real-time. Selain kecepatan, tingkat keakuratan mekanisme deteksi juga menjadi perhatian utama.

Hasil pengujian memperlihatkan bahwa sistem mampu menjaga tingkat *false positive* di bawah dua persen. Persentase ini menunjukkan bahwa mekanisme atestasi mampu membedakan perangkat yang valid dan perangkat yang mengalami modifikasi secara akurat, sehingga risiko pemutusan akses terhadap perangkat yang sebenarnya sah dapat diminimalkan. Hasil ini sekaligus menegaskan bahwa integrasi RA berbasis TPM bekerja dengan stabil pada lingkungan perangkat yang heterogen, tanpa menimbulkan gangguan signifikan bagi perangkat yang berfungsi secara normal.

Dari sudut pandang kinerja, pengaruh mekanisme atestasi terhadap komunikasi PLC juga diamati secara cermat. Hasil pengukuran menunjukkan bahwa overhead komunikasi yang dihasilkan hanya sekitar 1,1 persen. Nilai ini relatif kecil dan tidak berdampak terhadap siklus pemindaian PLC serta waktu tanggap kontrol proses. Kondisi ini menunjukkan bahwa penerapan RA berbasis TPM dapat dilakukan tanpa menimbulkan beban tambahan yang dapat memengaruhi kestabilan produksi. Dengan demikian, mekanisme atestasi dapat dijalankan secara periodik tanpa risiko mengganggu ritme kerja sistem kendali utama.



Gambar 7. Security rating ketika testing Modified Firewall dan Reply Attack

Pemanfaatan sumber daya perangkat selama proses atestasi juga memberikan gambaran penting mengenai kelayakan implementasi di lingkungan industri. Pengujian mencatat penggunaan CPU rata-rata sekitar 62 persen pada saat terjadi lonjakan proses atestasi, sedangkan penggunaan memori meningkat hingga 48 MB. Meskipun terdapat peningkatan beban, nilai-nilai tersebut masih berada dalam batas toleransi untuk perangkat PLC dan node

IoT yang digunakan dalam studi ini. Pengukuran ini menunjukkan bahwa mekanisme atestasi yang diusulkan memiliki karakteristik yang relatif ringan dan dapat dijalankan bahkan pada perangkat dengan kemampuan komputasi terbatas, selama interval atestasi diatur secara proporsional.

Integrasi mekanisme atestasi dengan Zero Trust Architecture juga memberikan efek nyata terhadap penguatan keamanan sistem. Ketika perangkat mengalami modifikasi atau gagal melalui proses verifikasi, perubahan status keamanan dapat langsung direspons oleh firewall FortiGate yang secara otomatis memindahkan perangkat ke zona karantina. Seperti yang di tunjukan pada gambar 7 Respon otomatis ini penting karena mencegah perangkat yang tidak tepercaya berinteraksi dengan jaringan kendali utama, mengurangi potensi penyebaran ancaman, serta meningkatkan ketahanan jaringan terhadap serangan lateral. Implementasi ini membuktikan bahwa pendekatan ID-TRA tidak hanya fokus pada verifikasi statis, tetapi juga pada tindakan dinamis berdasarkan hasil atestasi.

Secara keseluruhan, analisis hasil menunjukkan bahwa integrasi antara RA berbasis TPM dan ZTA mampu memberikan perlindungan berlapis pada lingkungan industri tanpa mengorbankan stabilitas operasional. Kecepatan verifikasi, tingkat akurasi yang tinggi, overhead yang rendah, serta respons kebijakan keamanan yang adaptif menjadi indikator bahwa pendekatan ini layak diterapkan pada sistem industri berskala besar. Namun, beberapa keterbatasan tetap ditemukan, seperti ketergantungan pada dukungan TPM serta sensitivitas terhadap beban jaringan pada kondisi tertentu. Aspek ini dapat menjadi landasan penelitian lanjutan guna memperkuat mekanisme adaptasi terhadap perangkat lama dan skenario produksi dengan beban tinggi.

5. KESIMPULAN

Sebagai kesimpulan, pembahasan ini menegaskan bahwa kerangka kerja ID-TRA dan ZTA yang diusulkan tidak hanya kokoh secara teoritis, tetapi juga layak untuk diterapkan secara operasional. Pendekatan ini menjawab kebutuhan yang semakin meningkat akan verifikasi perangkat yang dapat dipercaya pada level perangkat keras di dalam sistem industri, dan menunjukkan bahwa atestasi berbasis perangkat keras—bila dikombinasikan dengan pengendalian akses yang adaptif—dapat menjadi fondasi bagi penerapan *Zero Trust* di lingkungan *Operational Technology* (OT).

Dari hasil tersebut dapat disimpulkan bahwa waktu rata-rata proses verifikasi berkisar antara 2,1–2,4 detik, dengan tingkat keberhasilan deteksi perangkat tidak sah mencapai ≥97%. Proses attestation berlangsung cepat karena server hanya

melakukan perbandingan nilai hash digest dan mengeksekusi respon kebijakan melalui API integration ke FortiGate. Selain itu, hasil log dari FortiGate Firewall menunjukkan bahwa perangkat dengan status untrusted secara otomatis dimasukkan ke dalam kategori *blacklist* dan tidak dapat mengirim maupun menerima paket data dari jaringan industri. Hal ini menunjukkan bahwa integrasi antara Remote *Attestation* dan *Zero Trust Policy* berjalan efektif, di mana keputusan akses didasarkan pada status keamanan terkini, bukan lokasi perangkat atau kredensial tetap.

Penelitian ini menunjukkan bahwa integrasi mekanisme IoT *Device-Trusted Remote Attestation* (ID-TRA) berbasis *Trusted Platform Module* (TPM) dengan prinsip *Zero Trust Architecture* (ZTA) dapat meningkatkan ketahanan keamanan pada sistem kendali industri secara signifikan. Implementasi pada lingkungan brewery manufacture memberikan gambaran nyata mengenai bagaimana verifikasi integritas perangkat dapat dilakukan secara berkelanjutan tanpa mengganggu stabilitas operasional. Mekanisme atestasi mampu memberikan waktu respons verifikasi yang rendah, tingkat akurasi deteksi yang tinggi, serta *overhead* komunikasi yang minimal terhadap siklus kendali PLC, sehingga sesuai diterapkan dalam proses industri yang memerlukan respons cepat dan keandalan tinggi.

Integrasi antara *Remote Attestation* dan *Zero Trust Architecture* secara signifikan meningkatkan postur keamanan dengan melakukan verifikasi aktif terhadap perangkat IIoT dan menerapkan kontrol akses yang presisi, sehingga mampu mengurangi permukaan serangan secara keseluruhan dibandingkan dengan sistem tradisional yang hanya mengandalkan firewall.

Penelitian ini telah menyajikan sebuah kerangka kerja keamanan siber yang mengintegrasikan *IoT Device-Trusted Remote Attestation* dan *Zero Trust Architecture*, dan telah menunjukkan efektivitasnya melalui implementasi langsung di lingkungan operasional industri brewery. Pekerjaan selanjutnya akan difokuskan pada eksplorasi otomatisasi penjadwalan atestasi, deteksi anomali berbasis *machine learning*, serta peningkatan skalabilitas sistem untuk diterapkan pada pabrik berbasis 4.0 (*smart factory*)sektor lain berskala lebih besar.

DAFTAR PUSTAKA

JUHOLA, A. & KYLÄNPÄÄ, M., 2022. *Experimental Implementation of Remote Attestation over OPC UA Protocol*. In: International Conference on Networks, Communications and Information Technology (CNCIT). doi: 10.1109/CNCIT56797.2022.00021.

FERRO, L. et al., 2024. *SAFEHIVE: Secure Attestation Framework for IoT Devices*. In: ACM Workshop on Secure Cyber-Physical Systems.

ECKEL, M. et al., 2024. *SECURA: Reference Architecture for Security in Critical Infrastructures*. In: International Conference on Availability, Reliability and Security (ARES).

AMBROSIN, M., CONTI, M., LAZZERETTI, R., RABBANI, M.M. & RANISE, S., 2020. *Collective Remote Attestation at the Internet of Things Scale: State-of-the-Art and Future Challenges*. IEEE Communications Surveys & Tutorials, 22(4), pp.2447–2471. doi: 10.1109/COMST.2020.3008879.

CHEN, Y., QIN, B. & LU, R., 2021. *Design and Analysis of a Modified Remote Attestation Protocol*. In: 2021 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 62–69.

WANG, Y. et al., 2022. *An Anonymous Remote Attestation Protocol to Prevent Masquerading Attack*. Journal of Network and Computer Applications, 201, p.103328. doi: 10.1016/j.jnca.2021.103328.

YU, Q. et al., 2021. Software-Based Remote Attestation for Safety-Critical Systems. ACM Transactions on Embedded Computing Systems, 20(4), pp.1–25.

CHEN, Y. & LU, R., 2022. *Analysis and Research of Remote Attestation Based on Trusted Computing*. In: Proceedings of the 4th International Conference on Cryptography, Security and Privacy (ICCSP). ACM, pp. 68–72.

LI, Y. et al., 2020. *Trust Attestation for IoT Devices Using Direct Anonymous Attestation*. Sensors, 20(7), pp.1–14.

ANDRADE, J. & MARQUES, R., 2019. *Attestation in Industrial Systems: A Review of State-of-the-Art Protocols*. Computers & Security, 87, p.101582.

MA, M. et al., 2023. *Integrating Zero Trust Architecture in Industrial Networks*. IEEE Access, 11, pp.11256–11270.

ZHENG, L. et al., 2021. *Lightweight Remote Attestation Framework for Embedded Industrial Devices*. ACM Transactions on Internet Technology (TOIT), 21(4), pp.1–23.

KIM, H. & SONG, H., 2022. *Micro-Segmentation and Isolation in Zero Trust Architecture*. In: IEEE International Conference on Industrial Informatics.

LEE, J. & KANG, S., 2022. *Continuous Verification Mechanisms in Secure Industrial Control Systems*. Journal of Industrial Information Integration, 27, p.100281

ROY, S., KUMAR, A. & RAO, U.P., 2025. *Remote Data Attestation using Blockchain for Low-End IoT Devices: Enhancing Security through Trustworthy Verification*. In: Security, Privacy and Data Analytics (ISPDA 2024). Lecture Notes in Electrical Engineering, vol. 1444. Springer, pp.127–139. doi: 10.1007/978-981-96-8283-6_9.

KOZLOWSKI, W., CHEN, D., & NICOL, D. M. 2025. *DPU-LARD: DPU-Leveraged Attestation of Remote Devices for Security of OT Networks*. In Security and Privacy in Communication Networks (SecureComm 2024). Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol. 630, pp. 47–72. Springer. doi: 10.1007/978-3-031-94458-1_3.

ROUAGUBI, A., YOUSSOUFI, C., & CHOUGDALI, K. 2025. *Firmware Attestation in IoT Swarms Using Relational Graph Neural Networks and Static Random Access Memory*. AI (Switzerland). doi: 10.3390/ai6070161.

WANG, J. & WANG, J. 2025. *The Design and Implementation of a Secure and Efficient Firmware Trusted Platform Module for RISC-V Platforms*. Dianzi Yu Xinxi Xuebao / Journal of Electronics and Information Technology. doi: 10.11999/JEIT24112.

Halaman ini sengaja dikosongkan