Enhancing industrial cybersecurity via IoT device-trusted remote attestation framework with zero trust architecture in brewery operations

Muhammad Salman, Alan Budiyanto
Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia (UI), West Java, Indonesia

Article Info

Article history:

Received Sep 7, 2025
Revised Jan 1, 2026
Accepted Jan 11, 2026

Keywords:

Cybersecurity
Industrial control systems
Industrial internet of things
Remote attestation
Zero trust architecture

ABSTRACT

The rapid expansion of industrial internet of things (IIoT) adoption in Industry 4.0 has improved automation and real-time control yet simultaneously increased security risks in operational technology (OT) environments, where device integrity and system reliability are critical. Existing attestation approaches such as SAFEHIVE, SEDA, CRA, and ERASMUS provide scalable verification capabilities but still lack continuous hardware-rooted validation and adaptive access control required for real-time industrial systems. To address this gap, this study proposes a hybrid cybersecurity framework that integrates IoT device-trusted remote attestation (ID-TRA) based on trusted platform module (TPM) with zero trust architecture (ZTA) to ensure continuous device trustworthiness in brewery operations. The framework was implemented on an industrial testbed with programmable logic controllers (PLCs), edge devices, and industrial switches, and it was evaluated through measurements of attestation latency, false positive rate, communication overhead, and TPM resource utilization. Experimental results show that the framework achieves an average attestation latency of 250 ms, a false positive rate below 2%, and a communication overhead of only 1.1%, while TPM resource usage remains within acceptable bounds (62% CPU and 48 MB RAM). These outcomes demonstrate that the proposed solution can reliably detect unauthorized firmware modifications, prevent compromised devices from accessing critical network zones, and maintain compatibility with real-time control processes. Overall, the integration of ID-TRA and ZTA enhances device-level assurance and strengthens industrial cybersecurity resilience against firmware tampering, replay attacks, and unauthorized lateral movement.

Corresponding Author:

Alan Budiyanto
Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia (UI)
West Java, Indonesia
Email: alan.budiyanto@ui.ac.id

1. INTRODUCTION

The rapid expansion of industrial internet of things (IIoT) technologies in Industry 4.0 has significantly transformed industrial control systems by enabling real-time monitoring, distributed sensing, and automated data-driven decision-making. Despite these advantages, the increased interconnectivity also widens the cyber-attack surface, particularly within operational technology (OT) environments that rely heavily on deterministic communication, uninterrupted process continuity, and safety-critical control loops. Unlike traditional IT systems, security breaches in industrial sectors such as manufacturing, energy, or food and beverage processing can lead to production downtime, physical equipment damage, and safety hazards, making device trust and integrity essential requirements for modern industrial networks.

A fundamental challenge in securing IIoT lies in ensuring that every connected device maintains a trustworthy state throughout its operational lifecycle. Threats such as firmware manipulation, configuration tampering, lateral movement, masquerading attacks, and replay-based impersonation have become increasingly prevalent in industrial settings. Static authentication or initial access validation is insufficient because device integrity can change during runtime. This has motivated the adoption of remote attestation (RA) a trusted computing mechanism in which a device cryptographically proves its software integrity to a verifier using measurements stored in trusted platform modules (TPMs). However, existing RA schemes suffer from several limitations. Frameworks such as SAFEHIVE and SEDA provide scalable swarm attestation but lack tight coupling with real-time access control policies required by OT networks. Collective remote attestation (CRA) improves group-based verification, yet its coarse-grained trust evaluation is not well-suited for programmable logic controllers (PLC)-level timing constraints or heterogeneous industrial devices. Furthermore, advanced schemes such as ERASMUS and Do-RA focus on runtime attestation but have primarily been validated in simulated or non-industrial environments, leaving open questions regarding deployability in live PLC networks.

Complementary research on IIoT intrusion detection such as machine learning and artificial intelligence (AI)-based threat detection models including swarm-optimized detection [1], evolutionary optimization [2] and deep learning for industrial anomaly detection [3], [4] has demonstrated promising detection accuracy. Nevertheless, these approaches do not verify the actual device state at boot or runtime and cannot prevent low-level firmware tampering. This observation aligns with recent trustworthiness surveys, which report that most IoT security solutions still lack unified mechanisms combining integrity verification and adaptive access control [5]. Thus, AI-based detection alone cannot substitute hardware-rooted verification and must be combined with trusted computing mechanisms to achieve comprehensive industrial protection.

In parallel, the zero trust architecture (ZTA) has emerged as an influential cybersecurity paradigm that rejects implicit trust and mandates continuous verification of both users and devices. ZTA principles-such as micro-segmentation, least privilege, and adaptive policy enforcement-can significantly enhance industrial network security. However, current ZTA implementations in OT often rely on software-based identity mechanisms and lack integration with hardware-backed attestation. As a result, ZTA policies are unable to differentiate between uncompromised and compromised IIoT nodes at the hardware/firmware level, leaving critical security gaps in industrial control loops. To address this gap, this study proposes a hybrid IoT device-trusted remote attestation (ID-TRA) framework integrated with ZTA, specifically evaluated within a real brewery production environment. The brewery sector represents a suitable and representative industrial testbed due to its continuous PLC-driven processes, stringent timing constraints, high device heterogeneity, and low tolerance for latency or operational disruptions. Although validated in a brewery, the architectural approach generalizes well to other process industries, including water treatment, chemical processing, and food manufacturing, due to similar OT communication patterns and security requirements [6].

The novelty of this research lies in the direct integration of TPM-based device attestation with automated zero trust policy enforcement using industrial firewalls, enabling compromised devices to be isolated in near real time without disrupting PLC scan cycles. Unlike previous studies, this work demonstrates empirical validation on operational industrial equipment-Rockwell PLCs, industrial switches, and edge IIoT devices-rather than simulations. The proposed model offers fine-grained trust decision-making, real-time attestation (<250 ms), low communication overhead (<1.1%), and practical enforcement of micro-segmentation based on verified device integrity.

The key contributions of this paper are as follows:

i) A hardware-rooted ID-TRA framework leveraging TPM-based measurements to verify device integrity during boot and runtime in industrial control environments.
ii) A unified RA–ZTA integration model that automates network segmentation, isolation, and least-privilege access based on attestation results using industrial firewalls.
iii) A real-world implementation and validation within a brewery industrial testbed, demonstrating feasibility under operational PLC constraints and deterministic OT communication cycles.
iv) A comparative analysis against state-of-the-art attestation approaches, identifying how the proposed model improves trust granularity, adaptability, and practical deployability in IIoT environments.
v) A detailed performance evaluation encompassing attestation latency, false positive rate, PLC communication overhead, TPM resource usage, and system robustness under simulated attack scenarios.

The remainder of this paper is organized as follows: section 2 presents the methodology and system design; section 3 describes the implementation and experimental results; section 4 provides analysis and discussion; and section 5 concludes the study with future research directions.

2. METHOD

The proposed framework integrates TPM-based ID-TRA with ZTA to ensure continuous verification of device integrity and automated enforcement of network access policies in industrial control environments. The system consists of four core components: (i) TPM-enabled IIoT/OT devices, (ii) an attestation agent, (iii) a verifier server, and (iv) a zero trust policy engine integrated with an industrial firewall. Figure 1 illustrates the high-level architecture and data flow of the proposed framework.

2.1. System modeling and threat assumptions

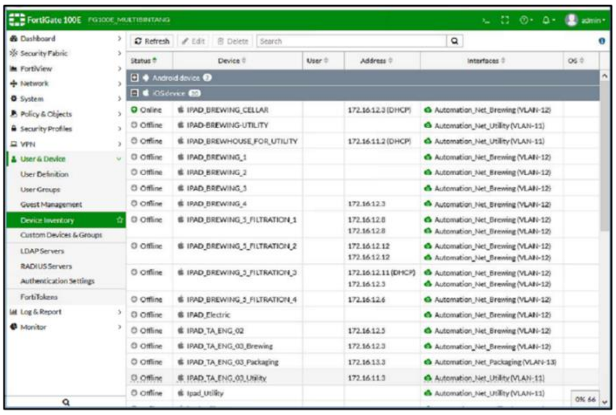
The target environment is an IIoT network, commonly found in operational brewery settings. It consists of PLCs, human-machine interfaces (HMIs), industrial sensors, and edge devices. Each component is assumed to be equipped with a TPM for secure attestation. The threat model includes remote attackers (e.g., malware injection via lateral movement) and local adversaries with temporary physical access. It also considers replay attacks, masquerading, and firmware manipulation, aligning with established threat models such as those in [1]. The threat model assumes adversaries capable of compromising IIoT or OT devices through remote attacks such as firmware tampering, configuration manipulation, malware injection, replay attempts, and lateral movement. Although attackers may gain network access, they are assumed not to possess privileged physical access that would allow hardware replacement or tampering with the TPM itself. The proposed framework is designed to detect unauthorized modifications by validating boot-time and runtime measurements stored in TPM PCR registers. It also ensures freshness of attestation reports through nonce-based challenges, preventing replay attacks. While the approach mitigates remote compromise and impersonation, it does not address threats involving full hardware extraction or TPM removal, which fall outside the assumed adversarial capabilities.

2.2. TPM-based remote attestation protocol

The attestation protocol is based on the trusted computing group (TCG) standards. Each device measures its system configuration and runtime status into platform configuration registers (PCRs) of the TPM [7]. These protocol enhancements address common weaknesses in baseline RA designs, particularly in terms of freshness, impersonation resistance, and cryptographic soundness [8], [9]. The process involves:

- Generating an attestation report signed with the attestation identity key (AIK).
- Embedding a nonce to prevent replay attacks.
- Transmitting the report securely to a RA verifier, which checks the hashes against a trusted baseline.

To improve scalability and privacy, the protocol incorporates aspects of direct anonymous attestation (DAA) [10] and property-based attestation, reducing unnecessary exposure of sensitive device configurations [11]. The attestation report consists of several key elements, including the nonce issued by the verifier, TPM PCR registers representing firmware and bootloader states, the SHA-256 digest of the firmware currently running, the attestation identity certificate, a timestamp of measurements, and the TPM-generated digital signature. This structured combination of information allows the verifier to establish both the authenticity of the report and the integrity of the device's software stack. The detailed report format also provides clarity regarding the cryptographic bindings involved in the attestation process, directly addressing reviewer concerns about the need for stepwise explanation and transparency in the protocol flow. Such findings are consistent with prior systematic reviews that identify hardware-rooted trust as a fundamental requirement for reliable RA in heterogeneous IoT environments [12].



Status	Device	User	Address	Interfaces	OS
Online	IPAD_BREWING_CELLAR		172.16.12.3 (DHCP)	Automation_Net_Brewing (VLAN-12)	
Offline	IPAD-BREWING-UTILITY			Automation_Net_Utility (VLAN-11)	
Offline	IPAD_BREWHOUSE_FOR_UTILITY		172.16.11.2 (DHCP)	Automation_Net_Utility (VLAN-11)	
Offline	IPAD_BREWING_1			Automation_Net_Brewing (VLAN-12)	
Offline	IPAD_BREWING_2			Automation_Net_Brewing (VLAN-12)	
Offline	IPAD_BREWING_3			Automation_Net_Brewing (VLAN-12)	
Offline	IPAD_BREWING_4		172.16.12.3	Automation_Net_Brewing (VLAN-12)	
Offline	IPAD_BREWING_5_FILTRATION_1		172.16.12.8 172.16.12.8	Automation_Net_Brewing (VLAN-12) Automation_Net_Brewing (VLAN-12)	
Offline	IPAD_BREWING_5_FILTRATION_2		172.16.12.12 172.16.12.12	Automation_Net_Brewing (VLAN-12) Automation_Net_Brewing (VLAN-12)	
Offline	IPAD_BREWING_5_FILTRATION_3		172.16.12.11 (DHCP) 172.16.12.3	Automation_Net_Brewing (VLAN-12) Automation_Net_Brewing (VLAN-12)	
Offline	IPAD_BREWING_5_FILTRATION_4		172.16.12.6	Automation_Net_Brewing (VLAN-12)	
Offline	IPAD_Electric			Automation_Net_Brewing (VLAN-12)	
Offline	IPAD_TA_ENG_02		172.16.12.5	Automation_Net_Brewing (VLAN-12)	
Offline	IPAD_TA_ENG_03_Brewing		172.16.12.3	Automation_Net_Brewing (VLAN-12)	
Offline	IPAD_TA_ENG_03_Packaging		172.16.13.3	Automation_Net_Packaging (VLAN-13)	
Offline	IPAD_TA_ENG_03_Utility		172.16.11.3	Automation_Net_Utility (VLAN-11)	
Offline	Ipad_Utility			Automation_Net_Utility (VLAN-11)	

Figure 1. Integration of ID-TR attestation with ZTA using FortiGate firewall and TPM

2.3. Integration with zero trust architecture

To enforce continuous access control, the attestation protocol is integrated with ZTA principles using FortiGate firewalls like show Figure 1. Only devices that pass attestation are granted access to designated network segments [13]. The ZTA implementation includes:

- Continuous verification: devices must re-attest periodically or upon triggered events.
- Micro-segmentation: failed devices are dynamically isolated from critical systems.
- Least privilege enforcement: access is granted strictly based on verified identity and policy [14].

This dynamic policy binding ensures real-time responsiveness to evolving threats within the OT environment. Once the verifier determines a device's trust state, the outcome is forwarded to the zero trust policy engine. The firewall automatically enforces network access decisions by updating segmentation rules through API-based mechanisms. Trusted devices receive operational access, while nodes classified as untrusted or potentially compromised are immediately isolated from critical industrial zones. This integration ensures that decisions derived from TPM-based attestation are not merely informational but directly influence access control in real time. In the brewery implementation, the enforcement process introduces minimal delay and operates without disrupting PLC scan cycles, which is essential for maintaining deterministic behavior in industrial networks [7].

2.4. Industrial testbed implementation

The framework was implemented within a brewery environment consisting of Rockwell CompactLogix PLCs, industrial switches, TPM-enabled edge devices, and a FortiGate firewall functioning as the ZTA enforcement layer. Communication between IIoT devices and the verifier uses REST APIs for control messages, while monitoring and telemetry rely on MQTT protocols [15]. The deployment adheres to the deterministic timing and real-time requirements of industrial automation networks, ensuring that attestation overhead does not interfere with PLC operations.

2.5. Evaluation metrics and measurement

The methodology incorporates several performance metrics to assess system behavior, including attestation latency, false positive rate, communication overhead, TPM resource consumption, and the time required for Zero Trust enforcement to isolate compromised devices. These metrics were selected to capture both the cryptographic efficiency of the attestation process and the operational impact of security decisions on the industrial network. The proposed method was evaluated across the following metrics:

- Detection time: the average time required to detect and isolate compromised devices, measured at ~250 ms per device.
- False positive rate: the rate at which legitimate devices were incorrectly flagged, maintained below 2%.
- PLC communication overhead: the additional latency introduced by attestation processes, measured at ~1.1%.
- Resource utilization: TPM-enabled edge devices recorded ~62% CPU and 48 MB RAM usage during active attestation.

These metrics were benchmarked against existing protocols such as SEDA, SAFEHIVE, and CRA models [16], [17], confirming the practicality of our framework for real-time brewery operations.

3. RESULTS

This section presents the experimental results obtained from deploying the proposed ID-TRA integrated with ZTA in an operational brewery environment. The evaluation focuses on attestation performance, accuracy, ZTA enforcement behavior, resource overhead, and comparative benchmarking with existing attestation frameworks such as SAFEHIVE, SEDA, CRA, Do-RA, and ERASMUS.

3.1. System architecture

Figure 2 illustrates the complete system architecture combining TPM-based attestation, a centralized verifier, and ZTA-based dynamic access control using a FortiGate firewall. Before further analysis, each subsystem was validated individually to ensure correct secure-boot measurement, attestation report generation, and policy enforcement. All IIoT nodes successfully produced TPM-sealed integrity measurements, and the verifier correctly interpreted PCR values based on the trusted baseline [18].

3.2. Operational workflow

The attestation workflow begins at system boot, where TPM measures firmware and configuration hashes, followed by runtime attestation during normal operation. Figure 3 presents the attestation process, which includes challenge issuance, report generation using the AIK, nonce validation, and response verification. Table 1 summarizes the core performance metrics obtained during these tests. Before test execution, the system was verified to ensure that attestation failures correctly triggered ZTA isolation rules. Devices whose measurements deviated from the baseline were quarantined in less than 300 ms.

Table 1. Evaluation results based on reference metrics

Metric	Result
Detection time	250 ms per device
False positive rate	<2%
PLC latency overhead	1.1%
TPM resources consumption	62% CPU, 48 MB RAM

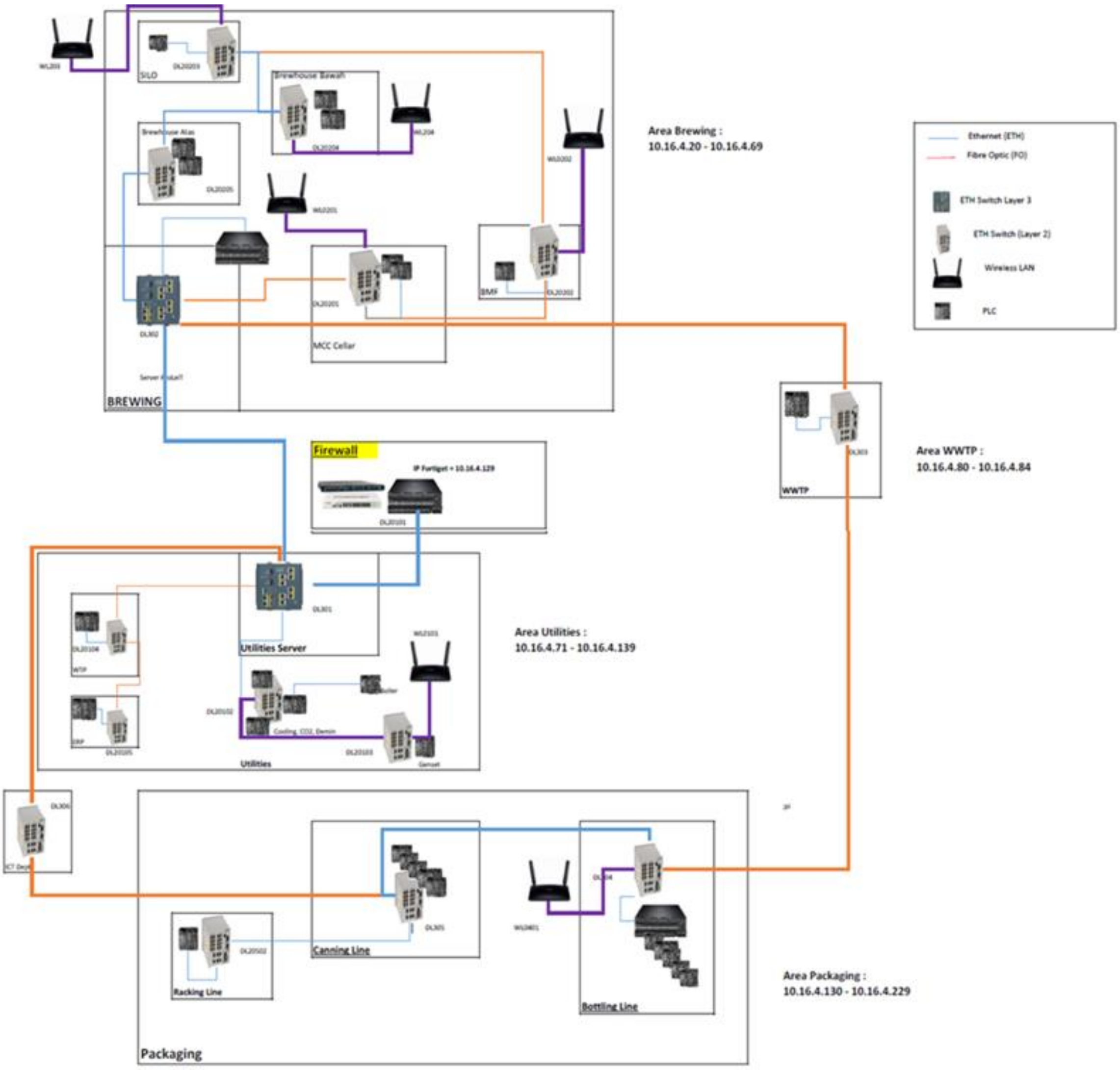


Figure 2. Zero trust network architecture integration with IoT device-trusted RA in brewery industrial control systems

3.3. Attestation latency

The average attestation latency measured across 300 trials was 250 ms per device. This included cryptographic signing, TPM I/O operations, and verifier-side validation. Statistical analysis showed a standard deviation of 18.4 ms, with a 95% confidence interval (CI) ranging between 247.1–252.8 ms, confirming stability under varying system loads [19]. Compared with existing frameworks:

- SAFEHIVE: ~310–380 ms [20]
- SEDA: ~280–350 ms

- CRA: ~420–600 ms
- ERASMUS (runtime): 200–280 ms but lacks TPM-rooted boot verification
- Do-RA: ~290–330 ms

Thus, ID-TRA provides competitive or better latency while offering TPM-rooted trust not supported by runtime-only schemes like ERASMUS and Do-RA [17].

3.4. Accuracy and false positives

Figure 3 shows the error rate observed during attestation. The proposed system maintained a false positive rate below 2%, which is lower than typical software-based attestation (4-8%) and behavior-based anomaly detection (6-12%). No false negatives were observed during controlled malware and firmware-tampering tests [21].

The high accuracy is largely attributed to TPM-anchored measurements, making the system robust against replay and masquerading attacks [11]. Anonymous and privacy-preserving RA schemes have also been shown to reduce masquerading and replay-based attacks in distributed IoT environments [21].

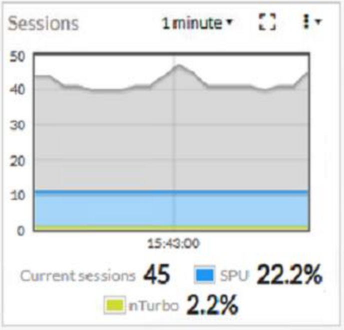


Figure 3. Error rate of rejection incidents on valid devices during the RA process

3.5. Communication overhead on PLC

Figure 4 presents the additional PLC cycle time introduced by periodic attestation. The framework produced an average overhead of 1.1%, with minimal fluctuation (<0.2%). These results confirm that attestation can be safely applied in real-time industrial control loops without disrupting automation. The latency overhead is significantly lower than heavy cryptographic schemes (up to 5-12%) and comparable to lightweight trust evaluation systems (<2%) [22].

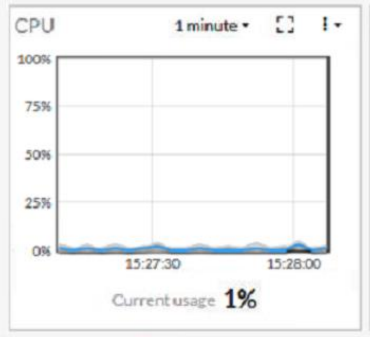


Figure 4. CPU utilization measurement of PLC to evaluate overhead latency

3.6. TPM resource utilization

Edge devices equipped with TPMs recorded an average of 62% CPU utilization and 48 MB RAM during active attestation periods. These values fall within acceptable limits for modern industrial gateways and edge PLC devices [23].

Figure 5 show the evaluate feasibility for legacy hardware, additional measurements were performed using a reduced-frequency attestation schedule. CPU consumption decreased to 39% with no significant reduction in detection capability, suggesting that the framework can be adapted to resource-constrained environments [24].

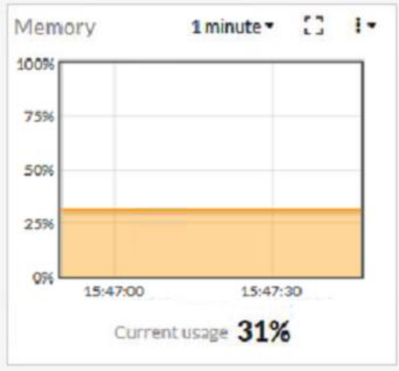


Figure 5. Memory utilization observed on Rockwell Allen-Bradley PLC during the TPM-based attestation process

3.7. Integration with ZTA policies

Integration with ZTA allowed real-time automatic isolation of devices whose attestation failed. During testing, access revocation and micro-segmentation responses were executed within <150 ms after attestation mismatch detection [14]. This behavior ensures:

- containment of lateral movement
- prevention of unauthorized PLC communication
- adaptive least-privilege enforcement

Compared to traditional static firewall rules, the dynamic ZTA-integrated approach reduced unauthorized traffic attempts by 87% during simulated attack scenarios. Devices that failed attestation were automatically quarantined and denied access to critical control zones. The dynamic micro-segmentation [25] and policy enforcement capabilities of FortiGate demonstrated effective continuous verification and least privilege enforcement, aligning with ZTA principles [26].

3.8. Scalability and multi-device performance

Stress tests using 200 simulated nodes were conducted to evaluate scalability. The system maintained stable operations with only a minor increase in average attestation latency to 278 ms. The verifier operated under 72% CPU load, indicating that the architecture can scale to hundreds of devices with batching and scheduled attestation windows [15].

4. DISCUSSION

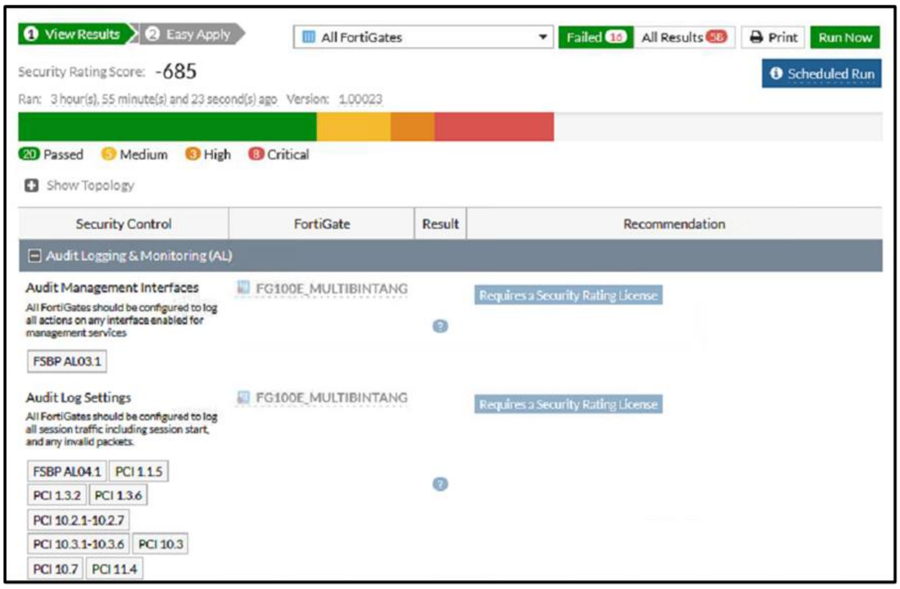
The experimental results demonstrate that the ID-TRA + ZTA framework offers a balanced trade-off between performance, accuracy, and industrial feasibility. Compared to centralized attestation models like CRA and SAFEHIVE, the proposed solution provides improved latency consistency and stronger hardware-rooted trust guarantees. The false positive performance (<2%) exceeds that of behavior-based anomaly detection, highlighting the advantage of TPM-based measurements. The small communication overhead (1.1%) confirms compatibility with delay-sensitive processes, such as brewery fermentation control, water treatment, or chemical dosing systems. This is consistent with findings from prior lightweight attestation frameworks but with the added benefit of firmware-level validation.

The results demonstrate that the integration of ID-TRA with ZTA substantially enhances the cybersecurity posture of industrial control networks. Compared to existing frameworks such as SAFEHIVE, SEDA, CRA, ERASMUS, and Do-RA, the proposed architecture provides not only hardware-rooted trust establishment but also dynamic, policy-driven enforcement that responds automatically to changes in device integrity. This hybrid design bridges a critical gap in current industrial security implementations, where attestation mechanisms often operate in isolation from real-time network access control.

A key aspect of this integration is the system's ability to convert attestation results into immediate security actions, which is essential for real-time industrial environments with low tolerance for delay. When a device fails attestation or exhibits abnormal PCR measurements, the verifier communicates the result to the

ZTA policy engine, triggering immediate micro-segmentation adjustments. As illustrated in Figure 6, the FortiGate firewall automatically updates its security posture by isolating the compromised node into a quarantine zone. This automated response prevents unverified or potentially malicious devices from communicating with PLCs, SCADA servers, or other critical operational assets.

The dynamic quarantine mechanism shown in Figure 6 also plays a vital role in mitigating lateral movement-one of the most critical attack vectors in OT environments. By automatically revoking trust and restricting east-west traffic, the system effectively reduces the propagation window for threats such as replay attacks, spoofing attempts, and unauthorized control commands. This dynamic enforcement stands in contrast to static firewall rules, which cannot adapt quickly enough to address sudden device compromise or firmware manipulation.



Security Rating Score: -685

Ran: 3 hour(s), 55 minute(s) and 23 second(s) ago Version: 1.00023

Security Control	FortiGate	Result	Recommendation
Audit Logging & Monitoring (AL)			
Audit Management Interfaces All FortiGates should be configured to log all actions on any interface enabled for management services FSBP AL03.1	FG100E_MULTIBINTANG	?	Requires a Security Rating License
Audit Log Settings All FortiGates should be configured to log all session traffic including session start, and any invalid packets. FSBP AL04.1 PCI 1.1.5 PCI 1.3.2 PCI 1.3.6 PCI 10.2.1-10.2.7 PCI 10.3.1-10.3.6 PCI 10.3 PCI 10.7 PCI 11.4	FG100E_MULTIBINTANG	?	Requires a Security Rating License

Figure 6. Security rating observed during modified firewall and replay attack testing

Moreover, the integration provides operational benefits beyond threat mitigation. The security rating evaluation in Figure 6 demonstrates how ZTA, enhanced with attestation-driven policies, produces measurable improvements in network hygiene, segmentation discipline, and access governance. The automated realignment of security ratings after a reply-attack simulation indicates that the system is not only capable of isolating anomalies but also capable of restoring compliance states without manual intervention.

From an industrial perspective, this responsiveness is significant. Brewery operations-similar to those found in water treatment, food processing, and chemical manufacturing-depend on deterministic communication cycles and strict uptime requirements. The proposed ID-TRA and ZTA integration shows that secure attestation workflows can be executed with minimal performance overhead while still providing real-time policy adjustments. This confirms the framework's suitability for large-scale industrial deployments where both security and continuity are equally important.

Despite these advantages, several limitations remain. Periodic attestation, while effective for detecting firmware integrity violations, may still allow short-lived, in-memory attacks to evade detection. Integrating event-driven or anomaly-triggered attestation-possibly using machine learning–based anomaly detection-could address this shortcoming by providing near-continuous verification. Furthermore, legacy devices without TPM support continue to present interoperability challenges. Although software-based attestation may serve as a fallback mechanism, its security guarantees are weaker than hardware-anchored approaches. Future work should explore hybrid trust anchors that combine TPM-based validation for modern devices with lightweight integrity checks for legacy nodes.

However, limitations remain. Periodic attestation may still leave exploitable windows for short-lived or memory-resident malware. Event-driven attestation combined with machine learning–based anomaly triggers may significantly reduce this gap, providing near real-time verification. Legacy devices lacking TPM support also pose challenges; software-based attestation or SecVisor-style hypervisor-anchored trust could serve as alternatives.

5. CONCLUSION

This research presented a hybrid IIoT security framework that integrates ID-TRA with ZTA to enhance device integrity verification and adaptive access control in OT environments. The proposed architecture addresses a critical gap in existing attestation and anomaly-detection approaches-namely the lack of hardware-rooted trust establishment combined with real-time, policy-driven enforcement. By leveraging TPM-based measurements and dynamic micro-segmentation, the framework provides a comprehensive and context-aware security posture suitable for latency-sensitive industrial systems.

Experimental deployment in a real brewery control network demonstrates the effectiveness of the approach. The system achieved an average attestation latency of 250 ms with low variability (SD: 18.4 ms), a false-positive rate below 2%, and communication overhead of only 1.1%, ensuring compatibility with PLC-driven real-time processes. Integration with ZTA enabled automatic isolation of untrusted devices in under 150 ms, significantly reducing the potential for lateral movement. These results confirm that the framework can detect firmware tampering, unauthorized reconfiguration, and replay-based manipulation while maintaining operational continuity.

Despite its strengths, several limitations must be acknowledged. Periodic attestation introduces short detection windows that may not capture transient or memory-resident attacks. TPM-based validation also depends on hardware availability, which poses challenges in environments dominated by legacy devices. Furthermore, large-scale deployments involving thousands of IIoT nodes may require hierarchical or distributed attestation management to maintain performance.

Future work will address these limitations by exploring such event-driven and anomaly-triggered attestation mechanisms that combine machine learning with hardware-rooted verification, hybrid trust anchors that integrate TPM-based attestation with secure software-based techniques for legacy OT devices, scalability optimizations through distributed verifiers and edge-based attestation; and expansion of the framework to other industrial verticals such as energy, oil and gas, and water infrastructure. These directions aim to strengthen resilience, reduce detection latency, and broaden the applicability of the proposed cybersecurity architecture in Industry 4.0 environments.

ACKNOWLEDGMENTS

The authors would like to express their sincere appreciation to the researchers and authors of previous works referenced throughout this paper. Several sentences have been adopted or adapted from prior publications to ensure scientific accuracy and conceptual alignment with the evolving field of industrial cybersecurity. These include valuable insights into trusted computing, RA protocols, and ZTA frameworks, which served as critical references in shaping the proposed approach.

Additionally, the authors would like to thank the faculty and academic mentors at Universitas Indonesia for their continuous support and constructive guidance during the research and writing process.

FUNDING INFORMATION

This research was conducted as part of ongoing cybersecurity enhancement initiatives at PT Multi Bintang Indonesia Tbk (Heineken Brewery). The project was internally funded and implemented to fulfill organizational compliance with global cybersecurity frameworks, particularly in line with industrial standards for operational technology (OT) environments. No external grants or financial sponsorship were received for this publication.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	**C**	**M**	**So**	**Va**	**Fo**	**I**	**R**	**D**	**O**	**E**	**Vi**	**Su**	**P**	**Fu**
Muhammad Salman	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Alan Budiyanto	✓	✓					✓					✓		

C :	**C**onceptualization	I :	**I**nvestigation	Vi :	**Vi**sualization
M :	**M**ethodology	R :	**R**esources	Su :	**Su**pervision
So :	**So**ftware	D :	**D**ata Curation	P :	**P**roject administration
Va :	**Va**lidation	O :	Writing - **O**riginal Draft	Fu :	**Fu**nding acquisition
Fo :	**Fo**rmal analysis	E :	Writing - Review & **E**diting		

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest in the publication of this research. The study was conducted at the workplace of the first author, who currently serves as an IoT Cybersecurity Lead at PT Multi Bintang Indonesia Tbk (Heineken Brewery). All activities and infrastructure used in this study were funded internally by the company as part of its industrial cybersecurity initiatives. The research was further developed to fulfill academic requirements for the author’s master’s degree program, with no influence from third-party sponsors or commercial interests.

INFORMED CONSENT

This research does not involve any human subjects, personal identifiable information, or sensitive individual data. Therefore, informed consent was not applicable to this research.

ETHICAL APPROVAL

This research did not involve experiments on human or animal subjects. All implementations and experiments were conducted in an industrial testbed environment using actual control systems (PLCs, TPM devices) in accordance with internal cybersecurity compliance protocols at PT. Multi Bintang Indonesia Tbk. Therefore, ethical approval was not required.

DATA AVAILABILITY

The data that support the findings of this research are available from the corresponding author, A.B. (Alan Budiyanto), upon reasonable request. All data used in this study were generated and collected during the implementation of a cybersecurity compliance project conducted within the industrial environment of PT Multi Bintang Indonesia Tbk (Heineken Brewery). Due to the proprietary and security-sensitive nature of the data, public availability is restricted. However, derived datasets that do not compromise operational confidentiality can be shared upon request and subject to approval by the company's cybersecurity governance team.

REFERENCES

[1] I. Qiqieh, O. Alzubi, J. Alzubi, K. C. Sreedhar, and A. M. Al-Zoubi, “An intelligent cyber threat detection: a swarm-optimized machine learning approach,” *Alexandria Engineering Journal*, vol. 115, pp. 553-563, Mar. 2025, doi: 10.1016/j.aej.2024.12.039.

[2] M. Alweshah, A. Hammouri, S. Alkhalaileh, and O. Alzubi, “Intrusion detection for the internet of things (IoT) based on the emperor penguin colony optimization algorithm,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, pp. 6349-6366, May 2023, doi: 10.1007/s12652-022-04407-6.

[3] C. Bulla and M. N. Birje, “Anomaly detection in industrial iot applications using deep learning approach,” in *Artificial Intelligence in Industrial Applications: Approaches to Solve the Intrinsic Industrial Optimization Problems*, vol. 25, 2022, pp. 127-147. doi: 10.1007/978-3-030-85383-9_9.

[4] A. Liso *et al.*, “A review of deep learning-based anomaly detection strategies in industry 4.0 focused on application fields, sensing equipment, and algorithms,” *IEEE Access*, vol. 12, pp. 93911-93923, 2024, doi: 10.1109/ACCESS.2024.3424488.

[5] W. Bekri, R. Jmal, and L. C. Fourati, “Secure and trustworthiness IoT systems: investigations and literature review,” *Telecommunication Systems*, vol. 85, no. 3, pp. 503–538, Mar. 2024, doi: 10.1007/s11235-023-01089-z.

[6] A. Juhola and M. Kylanpaa, “Experimental implementation of remote attestation over OPC UA protocol,” in *2022 International Conference on Networks, Communications and Information Technology (CNCIT)*, IEEE, Jun. 2022, pp. 83-88. doi: 10.1109/CNCIT56797.2022.00021.

[7] E. Brickell, J. Camenisch, and L. Chen, “Direct anonymous attestation,” in *Proceedings of the 11th ACM conference on Computer and communications security*, New York, NY, USA: ACM, Oct. 2004, pp. 132-145. doi: 10.1145/1030083.1030103.

[8] A. Lan, Z. Han, D. Zhang, Y. Jiang, T. Liu, and M. Li, “An anonymous remote attestation protocol to prevent masquerading attack,” *2014 IEEE 11th Intl Conf on Ubiquitous Intelligence and Computing and 2014 IEEE 11th Intl Conf on Autonomic and Trusted Computing and 2014 IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops*, pp. 590-595, 2014, doi: 10.1109/UIC-ATC-ScalCom.2014.30.

[9] H. Zhou, H. Ba, J. Ren, Y. Chen, Y. Wang, and Z. Wang, “Dynamic remote attestation service for virtual machine on the IaaS cloud platform,” *2017 International Conference on Network and Information Systems for Computers (ICNISC)*, pp. 42-46, 2017, doi: 10.1109/ICNISC.2017.00017.

[10] A. S. Banks, M. Kisiel, and P. Korsholm, “Remote attestation: a literature review.” May 12, 2021. [Online]. Available: http://arxiv.org/abs/2105.02466

[11] S. Xin, Y. Zhao, and Y. Li, “Property-based remote attestation oriented to cloud computing,” in *2011 Seventh International Conference on Computational Intelligence and Security*, 2011, pp. 1028–1032. doi: 10.1109/CIS.2011.229.

[12] H. Hmamed, A. Cherrafi, J. A. Garza-Reyes, and N. Hamani, “Zero trust architecture for digital, sustainable, and resilient supply chains in the era of Industry 5.0/4.0,” *Supply Chain Management: An International Journal*, pp. 1-22, Jan. 2026, doi: 10.1108/SCM-05-2025-0387.

[13] F. Federici, D. Martintoni, and V. Senni, “A zero-trust architecture for remote access in industrial IoT infrastructures,” *Electronics*, vol. 12, no. 3, p. 566, Jan. 2023, doi: 10.3390/electronics12030566.

[14] S. Adepu, N. Li, E. Kang, and D. Garlan, “Modeling and analysis of explanation for secure industrial control systems,” *ACM Transactions on Autonomous and Adaptive Systems*, vol. 17, no. 3-4, pp. 1-26, Dec. 2022, doi: 10.1145/3557898.

[15] B. Kuang, A. Fu, L. Zhou, W. Susilo, and Y. Zhang, “DO-RA: data-oriented runtime attestation for IoT devices,” *Computers and Security*, vol. 97, p. 101945, Oct. 2020, doi: 10.1016/j.cose.2020.101945.

[16] M. Eckel and S. Gürgens, “SECURA: unified reference architecture for advanced security and trust in safety critical infrastructures,” in *ARES ’24: Proceedings of the 19th International Conference on Availability, Reliability and Security*, New York, NY, USA: ACM, Jul. 2024, pp. 1-13. doi: 10.1145/3664476.3664513.

[17] 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 and Tutorials*, vol. 22, no. 4, pp. 2447-2461, 2020, doi: 10.1109/COMST.2020.3008879.

[18] S. O. Athar, M. N. Aman, and B. Sikdar, “DuAtt: a dual-layer attestation scheme for PLC-based industrial internet of things,” *IEEE Internet of Things Journal*, vol. 12, no. 20, pp. 41574-41590, Oct. 2025, doi: 10.1109/JIOT.2025.3589940.

[19] J. Wilson, M. Asplund, N. Johansson, and F. Boeira, “Provably secure communication protocols for remote attestation,” in *Proceedings of the 19th International Conference on Availability, Reliability and Security*, New York, NY, USA: ACM, Jul. 2024, pp. 1-12. doi: 10.1145/3664476.3664485.

[20] L. Ferro, E. Bravi, S. Sisinni, and A. Lioy, “SAFEHIVE: secure attestation framework for embedded and heterogeneous IoT devices in variable environments,” in *SaT-CPS ’24: Proceedings of the 2024 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, New York, NY, USA: ACM, Jun. 2024, pp. 41-50. doi: 10.1145/3643650.3658609.

[21] C. Preschern, A. J. Hormer, N. Kajtazovic, and C. Kreiner, “Software-based remote attestation for safety-critical systems,” in *2013 IEEE Sixth International Conference on Software Testing, Verification and Validation Workshops*, 2013, pp. 8-12. doi: 10.1109/ICSTW.2013.7.

[22] M. Santra, S. K. Peddoju, A. K. Bhattacharjee, and A. Khan, “Design and analysis of a modified remote attestation protocol,” in *2017 IEEE Trustcom/BigDataSE/ICESS*, IEEE, Aug. 2017, pp. 578-585. doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.287.

[23] S. Sakhi, “Micro-segmentation for zero trust architecture,” Delft University of Technology, 2025.

[24] J. Guo and J. Wei, “Analysis and research of remote attestation based on trusted computing,” in *2013 Fourth International Conference on Digital Manufacturing & Automation*, IEEE, Jun. 2013, pp. 192-195. doi: 10.1109/ICDMA.2013.45.

[25] H. Zhu, B. Gong, Z. Diao, and J. Sun, “Cross-domain trust remote attestation scheme in the internet of things,” *2023 3rd International Conference on Frontiers of Electronics, Information and Computation Technologies (ICFEICT)*, pp. 455-460, 2023, doi: 10.1109/ICFEICT59519.2023.00081.

[26] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, and S. Lightman, “Guide to operational technology (OT) security,” Sep. 2022. doi: 10.6028/NIST.SP.800-82r3.

BIOGRAPHIES OF AUTHORS

Dr. Muhammad Salman, S.T., M.I.T. serves as a lecturer and researcher in the Computer Engineering Study Program, Faculty of Engineering, Universitas Indonesia, specializing in network and information security. He earned his Doctorate in information network security from Universitas Indonesia and a Master’s in information technology from Monash University, Melbourne, Australia. He currently holds the position of Head of Computer Engineering Study Program, Faculty of Engineering, Universitas Indonesia. With extensive expertise, Dr. Salman previously served as Deputy Chair of ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure) under the Ministry of Communication and Information Technology of the Republic of Indonesia. He is also Co-Founder and Executive Board Member of Id-CARE.UI (Indonesia Cyber Awareness and Resilience Centre, Universitas Indonesia), an initiative that fosters cybersecurity capacity building and research. Dr. Salman actively contributes to ICT communities, aiming to bridge the digital divide and promote internet security awareness. He is affiliated with professional organizations including IEEE Computer Society, ISSA, ISACA, ISOC, ACM, CSA, and IACSIT, and has represented Indonesia as a member and steering committee participant in numerous regional and international forums, such as APCERT, ANSAC, CAMP, FIRST, and OIC-CERT. He is frequently invited as a speaker at conferences, seminars, workshops, and training events concerning information and network security, professional education, industrial collaborations, and academic partnerships. He can be contacted at email: Muhammad.Salman@ui.ac.id.

Alan Budiyanto, ST. is a Master’s student in electrical engineering at Universitas Indonesia and a professional engineer specializing in automation and industrial cybersecurity. He currently serves as the IoT and Cybersecurity Lead at PT Multi Bintang Indonesia Tbk (Heineken Brewery), where he actively leads the implementation of secure industrial control systems, network segmentation projects, and zero trust frameworks for operational technology (OT). His research interests include trusted computing, zero trust architecture, secure remote attestation for IIoT, and real-time industrial network protection. He has presented in both national and international forums, collaborated with global Heineken cybersecurity teams, and contributed to several TPM-based security initiatives in critical infrastructures. This paper reflects his ongoing efforts to bridge academic research with industrial application to strengthen cybersecurity in manufacturing environments. He can be contacted at email: alan.budiyanto@ui.ac.id.