DMODBUS: Blockchain for Network Identity Validation in Modbus Connections

Paulo Henrique Mariano, Devanir Caetano Filho, Carlos Frederico M. Cunha Cavalcanti, and Ricardo Augusto Rabelo Oliveira

***Abstract*—The Fourth Industrial Revolution, driven by the convergence of Information Technology (IT) and Operational Technology (OT), has accelerated industrial innovation while exposing legacy systems to modern cyber threats. Widely adopted protocols, such as Modbus/TCP, lack native security mechanisms and remain inherently vulnerable to exploitation. This study proposes and validates DModbus, an adaptive security layer that enhances Modbus communications by integrating blockchain technology. The architecture introduces a non-invasive gateway that utilizes a permissioned Proof of Authority (PoA) blockchain as a distributed and immutable ledger for device identities, enabling robust authentication during communication. The proposal was validated through a Proof of Concept (TRL 3) simulating a Man-in-the-Middle (MitM) attack via Address Resolution Protocol (ARP) spoofing in a Modbus TCP/IP environment. The experimental results demonstrate that DModbus detects identity spoofing attempts in real time. Performance analysis quantifies the inherent trade-off: an average latency overhead of 91.3% relative to the unprotected baseline. This overhead suggests suitability for non-critical real-time applications, such as supervisory control and data acquisition (SCADA) systems, rather than high-speed actuators, given the significant gains in security and resilience—particularly when contrasted with the severe and unpredictable degradation observed during active attacks. The main contributions are: (i) a model for securing Industry of Things (IIoT) devices using blockchain; (ii) a quantitative assessment of Proof-of-Authority (PoA)-based overhead in OT networks; and (iii) validation of decentralized identity management as a viable security layer for industrial communications.**

Link to graphical and video abstracts, and to code:
https://latamt.ieeer9.org/index.php/transactions/article/view/10703

***Index Terms*—Blockchain, Industry 4.0, Industrial Internet of Things, Cybersecurity.**

NOMENCLATURE

APT	Advanced Persistent Threat.
ARP	Address Resolution Protocol.
CPS	Cyber-physical Systems.
DMZ	Demilitarized Zone.
DModbus	Decentralized Modbus (Proposed Architecture).
DoS	Denial of Service.
DSR	Design Science Research.
HSM	Hardware Security Module.
IDS	Intrusion Detection System.
IIoT	Industrial Internet of Things.
IT	Information Technology.
MAC	Media Access Control (Address) or Message Authentication Code.
MitM	Man-in-the-Middle attack.
MQTT	Message Queuing Telemetry Transport.
OT	Operational Technology.
PKI	Public Key Infrastructure.
PLC	Programmable Logic Controller.
PoA	Proof of Authority.
PoC	Proof of Concept.
PoS	Proof of Stake.
PoW	Proof of Work.
SCADA	Supervisory Control and Data Acquisition.
SIS	Safety Instrumented System.
TLS	Transport Layer Security.
TRL	Technology Readiness Level.

The associate editor coordinating the review of this manuscript and approving it for publication was Javier Vázquez Castillo (*Corresponding author: Paulo Mariano*).

Paulo Mariano, C. F. M. C. Cavalcanti, and R. A. R. de Oliveira are with the Universidade Federal de Ouro Preto, Ouro Preto, MG, Brazil (e-mails: paulo.hm@aluno.ufop.edu.br, cfmcc@ufop.edu.br, and rabelo@ufop.edu.br).

D. Caetano Filho is with the Federation of Industries of the State of Minas Gerais, Contagem, MG, Brazil (e-mail: defilho@fiemg.com.br).

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

I. INTRODUCTION

The Fourth Industrial Revolution, or Industry 4.0, represents the strategic fusion of information technology (IT) and operational technology (OT) to optimize productivity and minimize waste. This technological convergence enables the creation of cyber-physical production environments characterized by interconnected assets, real-time operational visibility, and decision support systems driven by technologies such as the Industrial Internet of Things (IIoT), advanced robotics, and cyber-physical systems (CPS) [1].

Despite its benefits, this integration introduces new risk vectors. Cybersecurity challenges, historically confined to the IT domain, now affect OT environments, which were not originally designed to withstand modern cyber threats. Industrial systems, which often have long life cycles, frequently operate with known vulnerabilities, and targeted attacks can result in physical damage with severe consequences for operational safety. Stuxnet is a landmark example, being the first malware known to have caused large-scale physical damage. It attacked the industrial control systems of nuclear facilities, manipulating centrifuges to self-destruct. The Stuxnet [2] case demonstrated the potential for cyberattacks to cause significant physical impacts, prompting global concern and driving standardization initiatives like the ISA/IEC 62443 series [3]. Consequently, cybersecurity in industrial environments has

become a shared responsibility between IT and OT teams. The challenge lies in addressing the complex motivations and capabilities of the various malicious actors targeting these systems.

Threat actors are diverse and are commonly classified as:

- **Criminal groups (ransomware operators)** motivated by financial gain [4].
- **Government/military agencies** conducting espionage or sabotage through Advanced Persistent Threats (APTs) [5].
- **Hacktivists** driven by ideological or political agendas [6].
- **Script kiddies and opportunistic actors** exploiting public vulnerabilities.
- **Internal actors (insider threats)**, who are malicious or negligent employees with privileged access [7].

Attacks in OT environments primarily target the availability and integrity of systems through vectors such as Denial of Service (DoS) and Man-in-the-Middle (MitM) [8]. The Triton malware [9] exemplified these risks by specifically targeting Safety Instrumented Systems (SIS), aiming to disable the final layer of protection responsible for safeguarding human lives and the environment. The failure of these critical systems carries repercussions that transcend corporate financial losses, potentially leading to human casualties, ecological disasters, and significant economic disruption for society.

Despite such severe incidents, many industrial environments still rely on legacy protocols that lack native security features. Replacing this infrastructure is often unfeasible due to high costs and operational complexities [10]. This creates a critical need for retrofit solutions that can enhance the security of existing systems without requiring a complete replacement. This research addresses this need by proposing a scalable, transparent, and reproducible security solution for the IIoT.

A. Proposal and Methodology

This research proposes a blockchain-based retrofit solution architecture to address the inherent vulnerabilities of legacy industrial systems. Aligned with the Defense in Depth strategy [11], this solution adds a layer of protection to ensure the authenticity and integrity of messages in the Operational Technology (OT) environment. It utilizes a decentralized network governed by a Proof of Authority (PoA) consensus mechanism, with the Modbus TCP/IP protocol serving as the main case study.

Methodologically, this study is applied and exploratory, following the Design Science Research (DSR) methodology to create and evaluate an innovative artifact. The project is applied because it seeks to solve the real problem of vulnerability in legacy systems, and exploratory because it investigates the technical feasibility of the solution through observation of behavior and analysis of the performance metrics of the proposed solution. The Modbus TCP protocol was chosen as the project target due to its widespread adoption and the absence of native security mechanisms in older versions. A permissioned blockchain with a Proof of Authority (PoA) consensus algorithm was selected. This choice is justified by the need for decentralization to eliminate single points of failure, combined with the computational efficiency and low latency required by the operational environment, in contrast to more expensive consensus mechanisms. The study comprises the architectural design and the implementation of a Proof of Concept (PoC) at Technology Maturity Level 3 (TRL 3) carried out in a simulated industrial automation scenario in a controlled environment.

II. Related Work

This section addresses the technologies involved in the proposed architecture and presents a literature review on the subject, aiming to establish the literary foundations and identify the applicability of the study where others have not addressed it.

A. Modernization Strategies and Legacy Protocol Security

In industrial contexts, retrofitting involves upgrading existing systems with new technological capabilities without replacing the original equipment completely. This approach is critical in environments where controllers, sensors, and machinery have life cycles measured in decades, and where production shutdowns for equipment replacement are operationally or economically prohibitive. As argued, effective retrofit [12] solutions must be non-intrusive, compatible with legacy equipment, and scalable across diverse industrial scenarios.

A primary candidate for such retrofitting is the Modbus protocol. Developed by Modicon in 1979, its simplicity and interoperability have made it a de facto standard in SCADA systems and PLCs [13]. However, its longevity is also its greatest weakness. Designed in an era when cybersecurity was not a consideration, Modbus lacks native mechanisms for encryption, authentication, or message integrity verification [14]. This exposes Modbus systems to a range of attacks, including man-in-the-middle (MitM), replay attacks, packet forgery, and malicious command injection.

The risk is amplified by the increasing exposure of industrial devices on the public internet. Search engines like Shodan and Censys make it trivial to discover equipment running Modbus TCP/IP by filtering for the default port 502 [15]. As shown in Fig. 1 Shodan example, these tools can reveal IP addresses, service banners, and geographic locations, enabling adversaries to identify and target insecure devices. This exposure directly threatens the reliability and operational continuity of industrial processes.

B. Security Paradigms: Defense-in-Depth

The defense-in-depth principle is a foundational security strategy that relies on multiple independent layers of protection. The premise is that if one layer is breached, subsequent layers will prevent the attack from succeeding. In Operational Technology (OT) environments, this strategy is implemented through network segmentation (e.g., creating a demilitarized zone (DMZ) between IT and OT networks as prescribed by ISA/IEC 62443 [3]), host-based controls, and strict access policies. This research aligns with this strategy by proposing an additional security layer within the OT zone itself.

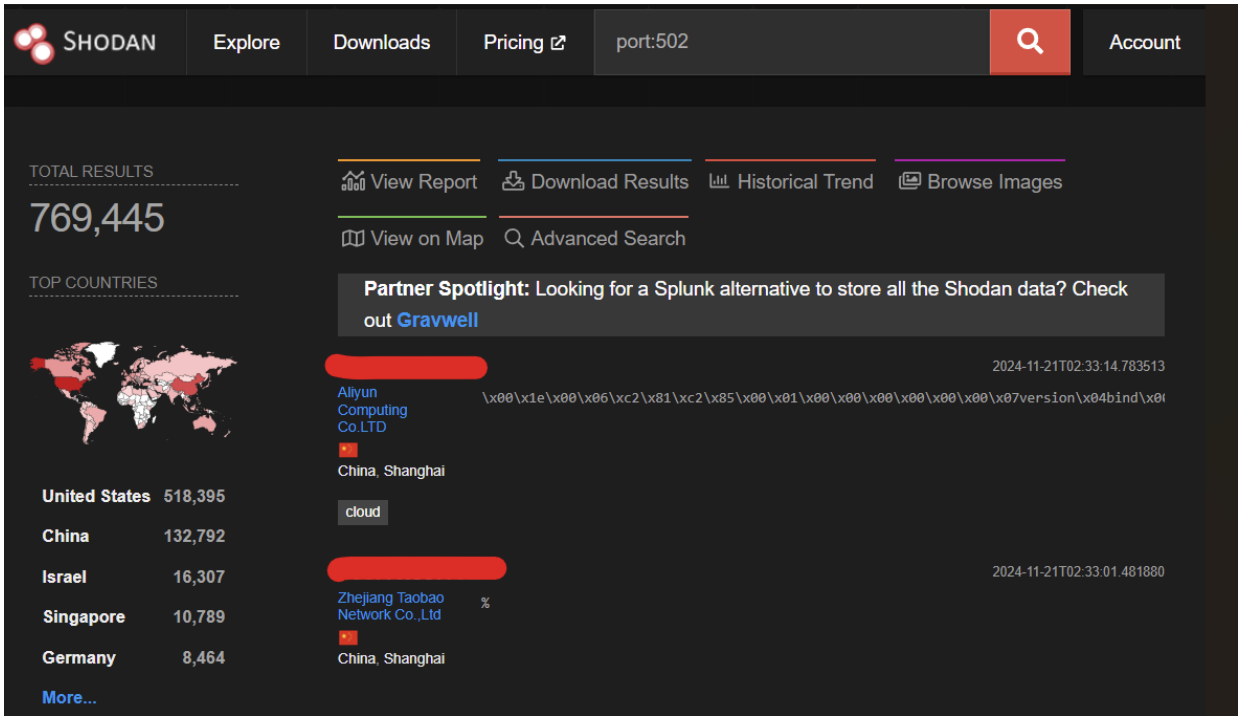


Fig. 1. Shodan search results (IP addresses omitted) with 769,445 responses.

C. Blockchain

Blockchain technology provides a decentralized mechanism for building this layer. Like a distributed and immutable ledger, it establishes trust between participants without a central authority [16]. Transactions are cryptographically linked in blocks, making retroactive tampering computationally infeasible. This trust is governed by consensus mechanisms, which are protocols that allow distributed nodes to agree on the state of the system. While public networks generally use Proof of Work (PoW) or Proof of Stake (PoS), with thousands of nodes spread across the globe, private industrial environments are better suited to Proof of Authority (PoA).

PoA relies on a set of pre-approved and trusted validators and is more commonly used in permissioned networks. This results in superior transaction speed and energy efficiency compared to other consensus mechanisms [17], are crucial factors for the low latency required in industrial applications.

As illustrated in Fig. 2, a qualitative comparison based on findings in the literature show that PoA offers the most suitable balance for industrial use cases, excelling in convergence time, confirmation latency, and energy efficiency, as previously mentioned; however, it is important to note that this performance comes from a reduction in decentralization(since the number of nodes will be proportionally smaller) and consequently a decrease in security, compared again to other consensus mechanisms. Unlike Proof-of-Work (PoW), which relies on the expenditure of computing power and energy as a source of trust, and Proof-of-Stake (PoS), where the node stakes values to guaranty its trust, security in Proof-of-Authority (PoA) resides in the reputation and knowledge of all authorized validator nodes.

Therefore, the proposed solution uses PoA not to replace existing infrastructure, but as a complementary security layer. This approach focuses on verifying the identity and integrity of communications, effectively mitigating man-in-the-middle attacks and insider threats that have already breached perimeter defenses.

D. Review of Existing Research

The challenge of securing industrial networks has been extensively studied. Following the methodology proposed by Kitchenham [18], a structured literature review was conducted using search terms such as "blockchain and Industry 4.0," "cybersecurity IoT," and "retrofit."

The previous work [19], investigated the use of blockchain as a security layer for the MQTT protocol in an IIoT environment. In this study, it was demonstrated that a permissioned blockchain could validate the origin and integrity of messages between a PLC and an edge device, effectively blocking transmissions from unauthorized sources. While that research established the foundational concept, the present study extends this model to the Modbus protocol— which is inherently less secure than MQTT— and focuses specifically on the challenges of retrofitting legacy systems.

Other researchers have explored non-blockchain solutions. [14] proposed lightweight Message Authentication Codes (MACs) to secure Modbus/TCP traffic, effectively mitigating replay and injection attacks with low latency. However, their model relies on a centralized key management infrastructure, creating a single point of failure. Similarly, Rosa et al. [20] analyzed vulnerabilities in legacy protocols and suggested solutions like intrusion detection systems (IDS), which are valuable but tend to address symptoms rather than the root causes of insecurity.

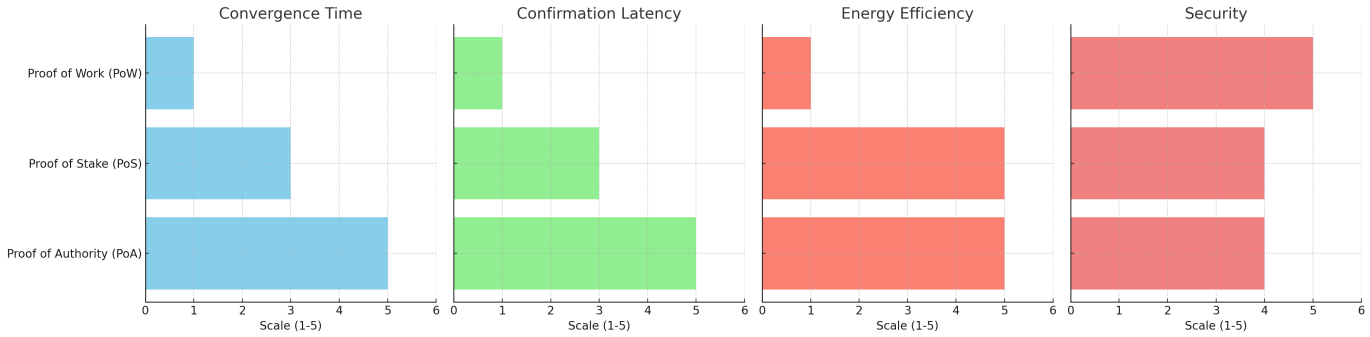


Fig. 2. A qualitative comparison of consensus algorithms based on key performance metrics for industrial environments. Higher scores indicate better performance.

Within the domain of blockchain for industrial applications, Fernández-Caramés and Fraga-Lamas [21] provided a systematic review of its potential in smart factories, highlighting challenges such as scalability and integration with resource-constrained devices. Cabrera-Gutiérrez et al. [22] proposed a hybrid architecture integrating a permissioned blockchain with hardware security modules (HSMs) to protect cryptographic keys. While highly secure, this approach adds implementation complexity and potential performance overhead. Further studies by Alajlan et al. [23] and Zhang et al. [16] have also advocated for blockchain as a trust layer for IoT data, while acknowledging the significant hurdles of scalability, transaction speed, and energy consumption.

Collectively, these studies highlight a clear need for scalable, non-intrusive security solutions for legacy protocols. This study addresses this gap by proposing a blockchain-based retrofit architecture designed explicitly for widely adopted legacy protocols, with a primary focus on Modbus TCP. Unlike centralized MAC-based approaches, the solution provides decentralized trust, and in contrast to more complex hardware-integrated systems, it focuses on software-based compatibility with a non intrusive deployment. It directly mitigates on-path attacks by ensuring message integrity and sender authenticity within the existing operational framework, thus eliminating the single point of failure associated with traditional certificate authorities, as noted in critiques of protocols like Diffie-Hellman [24].

III. Application

The architecture applicability was tested in a context representative of legacy industrial environments using Modbus TCP/IP. It is positioned as a retrofit security layer designed to integrate with existing OT network infrastructure, thereby augmenting traditional security measures like firewalls and network segmentation.

A. Experimental Scenarios

Scenarios were designed for this exploratory research. The setup used two embedded devices to emulate a sensor and a SCADA node communicating via Modbus TCP. Regular communication was established and verified using ModbusTCP-Tool.

For the attack simulation, a malicious device (Kali Linux) performed an ARP spoofing attack, positioning itself as a Man-in-the-Middle(MitM). This allowed the attacker to intercept and modify Modbus packets in transit using a Scapy-based script, a realistic compromise scenario in an unprotected OT network. The attack was monitored and confirmed using Wireshark to see the traffic network during this experiment.

1) **Baseline Communication:** A standard, legitimate Modbus TCP/IP communication between a sensor (server) and a SCADA system (client) is established to measure baseline performance (Fig. 3).

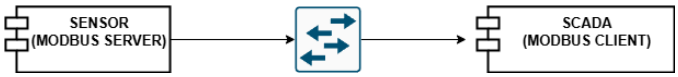


Fig. 3. Normal Modbus TCP Communication Flow.

2) **Attack Simulation:** A Man-in-the-Middle (MitM) attack is performed using ARP spoofing to intercept and modify Modbus traffic, demonstrating the protocol's vulnerability (Fig. 4).

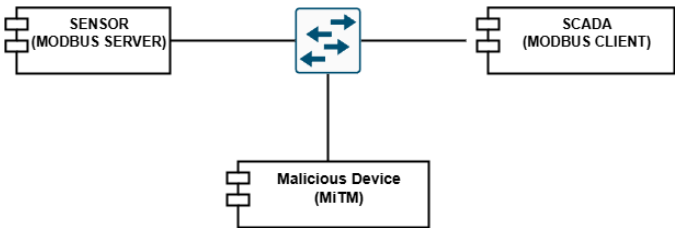


Fig. 4. Modbus TCP Communication Under a MitM Attack.

3) **Solution Implementation:** The proposed DModbus security architecture is implemented to mitigate the MitM attack by validating the origin and integrity of messages using a permissioned blockchain.

B. Blockchain Implementation

In Scenario 3, DModbus (Decentralized Modbus) was implemented, a non-invasive gateway architecture that uses a permissioned Proof of Authority (PoA) blockchain as a notary for device identities (Fig 5). For each critical device, a record containing its ID(the Unit Identifier of Modbus protocol), MAC address, and IP address is stored on the blockchain.

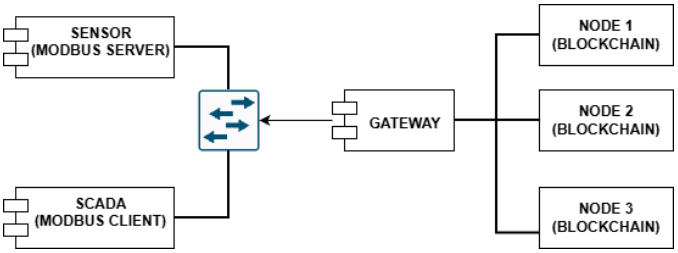


Fig. 5. Blockchain applied to Modbus, design of DModbus.

The gateway validates communications by:

1) The gateway queries its local synchronized copy of the blockchain ledger for the trusted data associated with a source IP.
2) Checking its local ARP table for the MAC address currently using that IP.
3) Comparing the data A mismatch triggers a security alert, indicating a potential ARP spoofing attack.

By anchoring trust in an immutable cryptographic record, DModbus establishes a "Zero Trust" security perimeter. The solution uses SHA-256 to create the hash of new blocks and a PoA consensus mechanism. The consensus threshold is formalized in Equation (1), where T defines the quorum required to achieve the transaction objective within the decentralized ledger. In this architecture, N represents the total population of validator nodes in the permissioned environment. By enforcing a strict majority ($T > N/2$), the system implements a Byzantine Fault Tolerance mechanism adapted for identity management [25]. This configuration ensures that the integrity of the ledger is maintained as long as the number of honest nodes exceeds the number of Byzantine (malicious or faulty) participants.

$$T = \left\lfloor \frac{N}{2} \right\rfloor + 1 \tag{1}$$

Consequently, the ledger remains immutable against identity spoofing attempts, since a successful subversion would require the coordinated compromise of the majority of decentralized validators—a scenario that significantly increases the computational and operational barriers for internal or external adversaries. The proof of concept was realized with 3 validators, a transaction requires 2 approvals to be valid [25], as per Equation (1).

Fig. 6 illustrates a sample block from the blockchain template used in the prototype. It showcases the data structure where device identity records are stored immutably. Each record links essential identifiers such as the device ID(Modbus TCP ID Field), its canonical IP address, and its physical MAC address. Additionally, each entry includes a timestamp and the identifier of the validating node ("validator") that confirmed the transaction. This distributed ledger serves as the authoritative source of truth against which the gateway performs identity validation during network communications.

Fig. 7 displays the real-time output log from the DModbus gateway during uninterrupted communication. The log demonstrates the successful validation process for multiple Modbus packets detected on the network. For each packet, the gateway

Fig. 6. Data Registers on the Blockchain Template.

```
--- Modbus Packet Detected: 172.25.10.52 ->
    172.25.10.70 ---
Verifying Source IP: 172.25.10.52
-> Trusted MAC (Blockchain): d0-94-66-e2-8e-93
-> Local Network MAC (ARP Table): d0-94-66-e2-8e-93
[STATUS] OK: Sender identity is valid.

--- Modbus Packet Detected: 172.25.10.52 ->
    172.25.10.70 ---
Verifying Source IP: 172.25.10.52
-> Trusted MAC (Blockchain): d0-94-66-e2-8e-93
-> Local Network MAC (ARP Table): d0-94-66-e2-8e-93
[STATUS] OK: Sender identity is valid.

--- Modbus Packet Detected: 172.25.10.70 ->
    172.25.10.52 ---
Verifying Source IP: 172.25.10.70
-> Trusted MAC (Blockchain): 08-00-27-16-04-f0
-> Local Network MAC (ARP Table): 08-00-27-16-04-f0
[STATUS] OK: Sender identity is valid.

--- Modbus Packet Detected: 172.25.10.52 ->
    172.25.10.70 ---
Verifying Source IP: 172.25.10.52
-> Trusted MAC (Blockchain): d0-94-66-e2-8e-93
-> Local Network MAC (ARP Table): d0-94-66-e2-8e-93
[STATUS] OK: Sender identity is valid.
```

Fig. 7. Real-time gateway output during normal operation, showing successful identity validation.

verifies the source IP, retrieves the trusted MAC address associated with that IP from the blockchain ("Trusted MAC (Blockchain)"), and compares it with the MAC address found in the local ARP table ("Local Network MAC (ARP Table)"). As shown in the output, the MAC addresses consistently match, leading the gateway to confirm the sender's identity as valid ([STATUS] OK: Sender identity is valid).

Conversely, Fig. 8 captures the gateway's output during the simulated Man-in-the-Middle attack scenario. Due to the ongoing ARP spoofing, the MAC address associated with the legitimate sender's IP in the local ARP table ("Local Network MAC (ARP Table)") now corresponds to the MAC address of the attacker's device. The gateway detects this critical mismatch when comparing it against the trusted MAC address registered on the blockchain ("Trusted MAC (Blockchain)"). This discrepancy immediately triggers a security alert message ("[ALERT!] ATTACK DETECTED! [...]"), demonstrating the DModbus system's effectiveness in identifying the identity spoofing attempt in real time. A prototype was implemented in Go (blockchain) and Python (gateway). Regular communication was successfully registered. During the Man in The Middle Attack(MitM attack), the system correctly identified the data mismatch and generated an alert (Fig. 8).

```
--- Modbus Packet Detected: 172.25.10.52 ->
    172.25.10.70 ---
Verifying Source IP: 172.25.10.52
-> Trusted MAC (Blockchain): d0-94-66-e2-8e-93
-> Local Network MAC (ARP Table): 08-00-27-d1-f8-5d
[ALERT!] ATTACK DETECTED! Sender MAC address in
    local network does not match the blockchain!

--- Modbus Packet Detected: 172.25.10.52 ->
    172.25.10.70 ---
Verifying Source IP: 172.25.10.52
-> Trusted MAC (Blockchain): d0-94-66-e2-8e-93
-> Local Network MAC (ARP Table): 08-00-27-d1-f8-5d
[ALERT!] ATTACK DETECTED! Sender MAC address in
    local network does not match the blockchain!
```

Fig. 8. Gateway security alert triggered during a Man-in-the-Middle (MitM) attack.

IV. Results and Discussion

For any security solution to be viable in an Operational Technology (OT) environment, the trade-off between security gains and performance overhead—primarily in terms of latency—is paramount. Having established the experimental methodology, this section presents the quantitative performance evaluation of the proposed DModbus solution. This analysis provides a quantitative assessment of the communication overhead introduced by the blockchain security layer, to evaluate whether this approach can secure legacy Modbus/TCP networks without critically compromising the performance required for industrial operations.

A. Performance Analysis

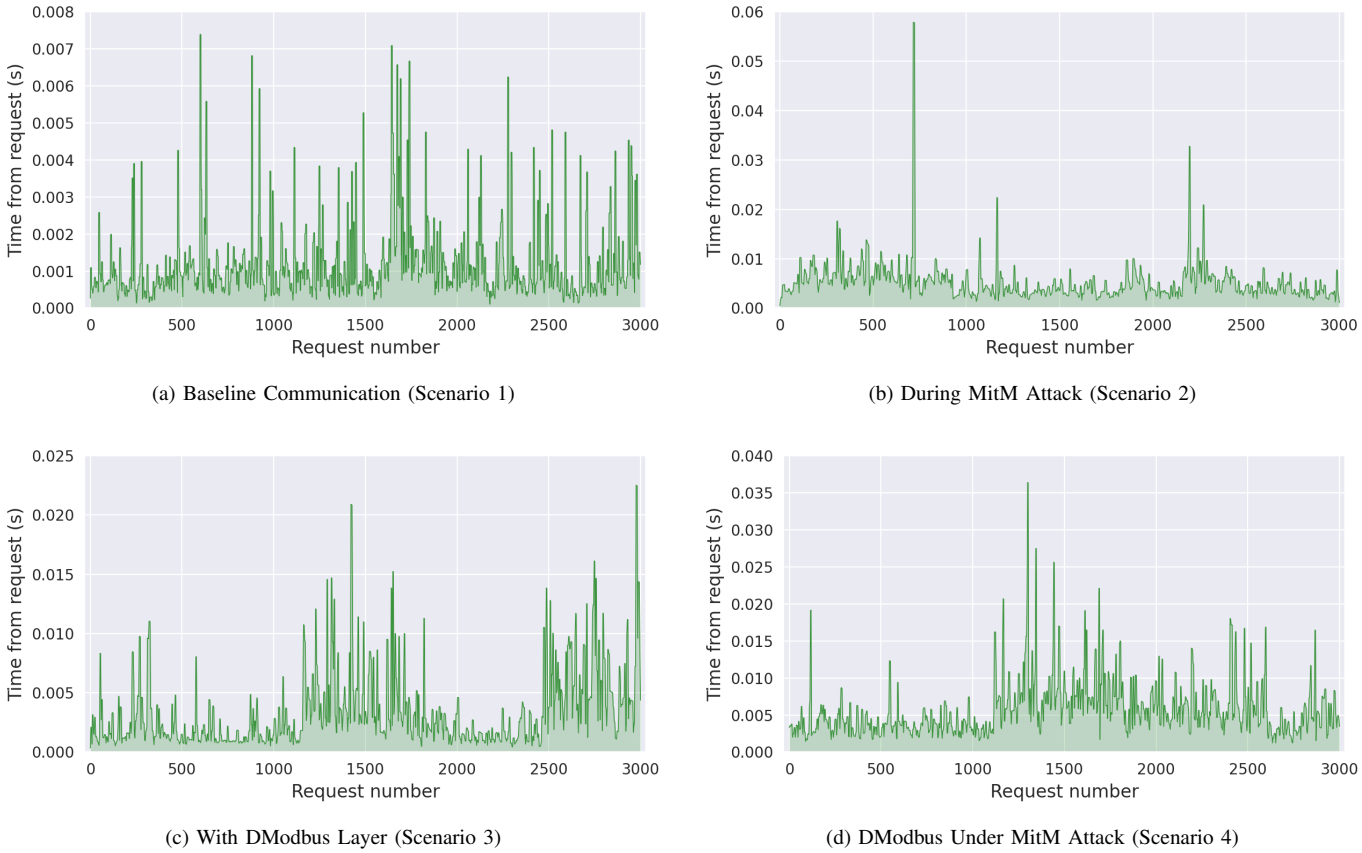
It was quantify the Modbus/TCP communication latency under three conditions: regular operation, during a MitM attack and with the DModbus security layer. A fourth scenario was also analyzed, in which the DModbus security layer remained active during a Man-in-the-Middle (MitM) attack:

- Scenario 1: Baseline Communication: The baseline network performance was established by capturing 3,007 samples of a standard Modbus/TCP communication. The statistical results (Table I) show a mean latency of 0.700 ms, indicating stable communication with occasional peaks (Fig. 9a).
- Scenario 2: Impact of a MitM Attack: The MitM attack dramatically increased the mean latency to 2.406 ms (Table I), demonstrating severe performance degradation and high instability (Fig. 9b).
- Scenario 3: Performance with DModbus: The DModbus security layer introduced a performance overhead, resulting in a mean latency of 1.339 ms an increase of approximately 91.3% compared to the baseline (Table I). Although higher, this latency was more stable and predictable than during the attack.
- Supplementary Analysis: DModbus Under Attack: When the DModbus solution was active during a MitM attack, the mean latency was 2.643 ms (Table I). Despite the instability caused by the ongoing attack, communication remained functional, demonstrating the solution's resilience.

B. Discussion

The DModbus security layer introduces a 91% latency overhead. This represents a controlled trade-off compared to the severe and unpredictable performance degradation caused by an active attack. The choice of a Proof of Authority (PoA) consensus mechanism within the study's objectives was specifically motivated by the need to minimize this latency, offering a faster alternative for more computationally intensive blockchain architectures. Fig. 10 presents a comparative boxplot analysis of Modbus/TCP communication latency across the four experimental scenarios. Scenario 1 (baseline) exhibits the lowest and most consistent latency, with a median of 0.508 ms and a mean (represented by 'X') of 0.700 ms, confirming stable and unprotected communication. Scenario 2 (MitM attack) reveals a drastic increase in both median latency (1.830 ms) and dispersion. While the boxplot's visual scale is focused on the distribution of the majority of samples to maintain clarity, with outliers represented up to 7 ms, the actual peak latency reached an extreme value of 57.830 ms (see Table I), reflecting the severe and unpredictable degradation caused by active ARP spoofing.In Scenario 3 (DModbus active, no attack), the median latency (0.776 ms) and mean (1.339 ms) are higher than the baseline—consistent with the 91.3% overhead. The proximity between the median and the mean in this scenario, compared to the attack scenario, highlights the solution's stability. Finally, Scenario 4 (DModbus active under MitM attack) show a dispersion comparable to Scenario 2 due to the ongoing attack, but the presence of a stable mean (2.643 ms) demonstrates that the system remains operational while successfully triggering real-time security alerts.

Although data indicate that this overhead may be prohibitive for complex real-time control processes requiring microsecond-level response, DModbus becomes more suitable for supervisory, control, and monitoring applications, where the legitimacy of data sources is prioritized over minimum latency. Furthermore, communication time in Modbus/TCP networks is inherently non-deterministic, with the literature reporting values for supervisory systems frequently exceeding 100 ms (e.g., web-based SCADA latency of 156 ms) [26]. Therefore, the additional delay introduced by the proposed approach remains insignificant when compared to the natural variability and application timeouts of Modbus communication reported in the literature. It is also important to note that since the lifecycle of machines and equipment in industrial environments is long and changes are infrequent (occurring mainly during topology changes), the blockchain infrastructure will not need to perform write procedures on the consensus network at all times, which is more costly, thus not imposing a continuous overload on the operational cycle. Similarly, the nodes that make up the network would not be overloaded with data, In the experimental setup, each device entry in the ledger has a footprint of approximately 250 to 300 bytes. This total is derived from essential device identifiers(ID, IP, MAC, and timestamp (80 bytes)), combined with block metadata (including a 64-byte SHA-256 hash, index, validation timestamp, and validator ID (120 bytes)). The identification of industrial assets in communication in this study is based on IP, MAC, and



(a) Baseline Communication (Scenario 1)

(b) During MitM Attack (Scenario 2)

(c) With DModbus Layer (Scenario 3)

(d) DModbus Under MitM Attack (Scenario 4)

Fig. 9. Temporal evolution of communication latency across the four experimental scenarios.

TABLE I
COMPARATIVE LATENCY STATISTICS ACROSS EXPERIMENTAL SCENARIOS

Metric (ms)	**Scenario 1** (Baseline)	**Scenario 2** (MitM Attack)	**Scenario 3** (DModbus)	**Scenario 4** (DModbus + MitM)
Mean	0.700	2.406	1.339	2.643
Median	0.508	1.830	0.776	1.890
Standard Deviation	0.639	2.274	1.799	2.479
Minimum	0.258	0.273	0.258	0.267
Maximum	7.386	57.830	22.497	36.393
Total Samples	**3007**	**3007**	**3007**	**3007**

Modbus Identified Field (ID) addresses, which are known to be weak identifiers from a cryptographic point of view. However, this choice reflects the real limitations of low-power, older industrial devices, such as simple sensors and legacy controllers, which typically lack the computational resources, secure hardware modules, or firmware resources needed to support certificates, asymmetric keys, or hardware-based identities. In these limited scenarios, common in OT networks, ID/IP/MAC-based identification remains a viable mechanism to complement other defense strategies. The official Modbus TCP security model, based on Transport Layer Security (TLS) and X.509 certificates, was launched in 2018(the original Modbus TCP was launched in 1999). The TLS approach offers robust end-to-end confidentiality for the payload through a Public Key Infrastructure (PKI). Based on this, a secondary experiment was conducted using the same DModbus standards to simulate industrial communication over the Modbus TCP TLS protocol, aiming to verify communication latency in this experimental scenario and compare the results with the reference scenario and with DModbus, in order to collect quantitative data from different solutions. It was used a virtual machine representing a server (sensor) providing data to a client (simulating a PLC). Data traffic was captured using Wireshark, with 3007 samples collected, according to previous experiments results described in Table I . Modbus TLS recorded an average latency of 1.408 ms compared to scenario 1 (baseline) of 0.700 ms, representing an increase of approximately 101% in response time, compared to a 91% increase for DModbus relative to baseline. The standard deviation of Modbus TLS was 1.5111 ms, which is lower than that of scenario 3 (DModbus) of 1.7990 ms, indicating a smaller dispersion around the mean in this experiment, compared to DModbus. Table II summarizes these data. Although Modbus TLS is based on open standards, its practical adoption in industrial environments often involves additional costs related to hardware upgrades, licensing, and Public Key Infrastructure (PKI) management. The practical

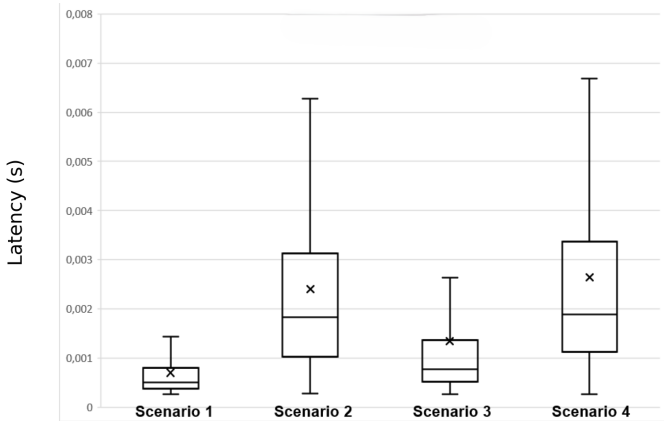


Fig. 10. Latency Analysis - Outliers exceeding 1.5 times the interquartile range are omitted from the whisker extension for greater visual clarity; the full range of observed values is presented in Table I.

TABLE II
COMPARATIVE LATENCY STATISTICS(BASELINE), DMODBUS AND MODBUS TLS.

Metric (ms)	Baseline	DModbus	Modbus TLS
Mean	0.700	1.339	1.408
Median	0.508	0.776	0.889
Standard Deviation	0.639	1.799	1.511
Minimum	0.258	0.258	0.269
Maximum	7.386	22.497	18.482
Total Samples	**3007**	**3007**	**3007**

implications of adopting the official Modbus TLS security model, instead of the proposed architecture, lie primarily in the disparity of computational requirements and the complexity of infrastructure management. While Modbus TLS demands a Public Key Infrastructure (PKI) for managing the X.509 certificate lifecycle, which can pose logistical challenges in industrial environments, DModbus uses a decentralized layer for notarization and identity management. The process of storing certificates and cryptographic validations on devices with low computing power can make TLS implementation impractical on legacy programmable logic controllers (PLCs), whose hardware was not designed for the continuous processing of intensive security protocols [14]. DModbus presents itself as a non-intrusive alternative aimed at industrial retrofitting [12]. By shifting the trust logic to the Blockchain network, the architecture enables endpoint protection without the need for firmware modifications or increased local processing load, mitigating the single point of failure inherent in centralized certification authorities and delegating the security validation burden of industrial devices to the decentralized network. The architecture proposed here, therefore emerges not as an absolute replacement, but as a viable alternative where technical constraints preclude other solutions, and can also act as a complementary security layer under a defense-in-depth strategy [11].

The identity validation process at the gateway follows a complexity of $O(1)$, as it involves a local lookup against the synchronized state of the ledger, ensuring that the per-packet overhead does not scale with the network size. On the other hand, the consensus latency for registering new devices follows a complexity of $O(N)$, where N is the number of validator nodes. This is because the PoA mechanism requires a majority of T nodes (Equation 1) to exchange messages and reach agreement. Therefore, while adding more nodes increases the system's resilience and security, it introduces a predictable, linear increase in the time required for administrative state updates, but not in the continuous monitoring of established Modbus flows.

A deliberate limitation of the proposed architecture concerns the automation of identity revocation. Although DModbus enables the identification of compromised or anomalous credentials through the blockchain, automatic revocation and immediate traffic blocking have not been implemented to prioritize system availability and operational continuity. In critical industrial environments, the automated blocking of a resource can result in unforeseen process stoppages, the financial and physical security risks of which, in certain scenarios, outweigh the risks of a monitored intrusion. Therefore, DModbus acts as a notarization and alerting layer, designed to operate non-intrusively in the production process. The architecture can be coupled with other solutions, such as Security Information and Event Management (SIEM) systems and monitoring dashboards, allowing for a human approach. In this configuration, the detection of an irregularity in the blockchain generates an alert so that the operations team can make an informed decision about isolating the device, ensuring that cybersecurity does not compromise the determinism and stability of the industrial process.

V. CONCLUSION

This research proposed and investigated the application of a decentralized architecture using blockchain technology as a security layer to increase the resilience of legacy industrial automation networks, targeting the Modbus/TCP protocol and observing the principles of retrofitting. This was achieved through the development of a proof of concept using DModbus, a solution capable of guaranteeing the origin of data in an environment susceptible to "Man-in-the-Middle" attacks.

The proof of concept demonstrated the viability of the proposed approach in a laboratory environment. Experimental results confirmed that, while standard Modbus/TCP communication is vulnerable and suffers severe performance degradation under an ARP Spoofing attack, the network alert generated by DModbus helps to maintain communication integrity by successfully detecting data manipulation.

The primary trade-off identified was the performance overhead, resulting in a mean latency increase of 91.3% compared to the baseline. This finding leads to the conclusion that the solution, in its current form, is best suited for OT applications that do not operate under hard real-time constraints and where data integrity and auditability are prioritized over minimal latency, such like industrial monitoring systems. This study contributes an architectural model and a practical validation, demonstrating that legacy protocols can be hardened against cyberattacks using a distributed ledger system.

A. Limitations and Future Work

This study was limited to validating the Modbus/TCP solution in a controlled laboratory environment. The observed latency is an inherent cost of cryptographic processing, making the solution more suitable for systems where integrity takes precedence over strict real-time requirements. The threat used was based on ARP Spoofing Attacks; the scope of the solution is to ensure that only devices notarized on the blockchain can participate in the network, and it was not tested for other types of existing cyberattacks. Regarding the threat model, DModbus validates the sender's identity, but not the internal state of the device or the content of the transmitted packet. Consequently, a compromised device (acting as part of a botnet, for example) that retains valid credentials falls outside the scope of this specific validation layer. This limitation reinforces the need for a defense-in-depth strategy, where DModbus operates in conjunction with behavioral analysis tools to cover both identity spoofing and internal threats. This study sought the logical validation of the architecture in a controlled environment. The absence of physical variables such as electromagnetic noise is a recognized limitation of the emulation stage. Future work will focus on validating the solution in a high-fidelity test environment with physical PLCs to analyze scalability, potential electromagnetic interference, and performance optimization, thus advancing the architecture to a maturity level of TRL 5 (Technology Readiness Level). It's also planned to extend the proposed architecture in DModbus to other industrial protocols, such as PROFINET and OPC UA, and integrate it into a Public Key Infrastructure (PKI), where the blockchain would serve as a decentralized Certificate Authority. Finally, migrating the prototype to an enterprise-level framework, will allow for a robust comparative evaluation of commercial solutions (such as Multichain, Hyperledge Fabric, etc) and how they can integrate with Security Information and Event Management ecosystems. These steps are essential to advance the solution's Technology Readiness Level toward practical architecture for protecting critical infrastructure.

ACKNOWLEDGMENTS

The authors declare that no funding was received for the conduct of this research. AI-assisted tools were used in the preparation of this manuscript as follows: (i) Gemini (Google) was used for grammar and language editing; and (ii) Consensus (consensus.app) was used as an AI-assisted academic search tool to support the literature review process. All scientific content, methodology, experimental design, results, and conclusions are exclusively the work of the authors.

REFERENCES

[1] J. W. Veile, D. Kiel, J. M. Müller, and K.-I. Voigt, "Lessons learned from industry 4.0 implementation in the german manufacturing industry," *Journal of Manufacturing Technology Management*, vol. 31, no. 5, pp. 977–997, 2020. doi: 10.1108/JMTM-08-2018-0270. [Online]. Available: https://doi.org/10.1108/JMTM-08-2018-0270

[2] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011. doi: 10.1109/MSP.2011.67. [Online]. Available: https://doi.org/10.1109/MSP.2011.67

[3] I. Cindrić, M. Jurčević, and T. Hadjina, "Mapping of industrial iot to iec 62443 standards," *Sensors*, vol. 25, no. 3, p. 728, 2025. doi: 10.3390/s25030728. [Online]. Available: https://doi.org/10.3390/s25030728

[4] J. Martin and C. Whelan, "Ransomware through the lens of state crime: Conceptualizing ransomware groups as cyber proxies, pirates, and privateers," *State Crime Journal*, vol. 12, no. 1, pp. 4–28, 2023. doi: 10.13169/statecrime.12.1.0004. [Online]. Available: https://doi.org/10.13169/statecrime.12.1.0004

[5] A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, "Survey of publicly available reports on advanced persistent threat actors," *Computers & Security*, vol. 72, pp. 26–59, 2018. doi: 10.1016/j.cose.2017.08.005. [Online]. Available: https://doi.org/10.1016/j.cose.2017.08.005

[6] T. J. Holt, J. D. Freilich, and S. M. Chermak, "Exploring the subculture of ideologically motivated cyber-attackers," *Journal of Contemporary Criminal Justice*, vol. 33, no. 3, pp. 212–233, 2017. doi: 10.1177/1043986217699100. [Online]. Available: https://doi.org/10.1177/1043986217699100

[7] A. Moneva and R. Leukfeldt, "Insider threats among dutch smes: Nature and extent of incidents, and cyber security measures," *Journal of Criminology*, vol. 56, no. 4, pp. 416–440, 2023. doi: 10.1177/26338076231161842. [Online]. Available: https://doi.org/10.1177/26338076231161842

[8] M. Bhole, T. Sauter, and W. Kastner, "Enhancing industrial cybersecurity: Insights from analyzing threat groups and strategies in operational technology environments," *IEEE Open Journal of the Industrial Electronics Society*, vol. 6, pp. 145–157, 2025. doi: 10.1109/OJIES.2025.3527585. [Online]. Available: https://doi.org/10.1109/OJIES.2025.3527585

[9] M. Geiger, J. Bauer, M. Masuch, and J. Franke, "An analysis of black energy 3, crashoverride, and trisis, three malware approaches targeting operational technology systems," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1, 2020. doi: 10.1109/ETFA46521.2020.9212128 pp. 1537–1543. [Online]. Available: https://doi.org/10.1109/etfa46521.2020.9212128

[10] L. L. Dhirani, E. Armstrong, and T. Newe, "Industrial iot, cyber threats, and standards landscape: Evaluation and roadmap," *Sensors*, vol. 21, no. 11, p. 3901, 2021. doi: 10.3390/s21113901. [Online]. Available: https://doi.org/10.3390/s21113901

[11] Y. Xu, J. Yang, Z. Zhou, X. Shi, J. Wang, and J. Zhang, "Extending defense-in-depth to multi-domain networks," in *Proceedings of the 2024 8th International Conference on Electronic Information Technology and Computer Engineering (EITCE)*. New York, NY, USA: ACM, 2024. doi: 10.1145/3711129.3711254 pp. 1–5. [Online]. Available: https://doi.org/10.1145/3711129.3711254

[12] T. Lins and R. A. R. Oliveira, "Cyber-physical production systems retrofitting in context of industry 4.0," *Computers & Industrial Engineering*, vol. 139, p. 106193, 2020. doi: 10.1016/j.cie.2019.106193. [Online]. Available: https://doi.org/10.1016/j.cie.2019.106193

[13] S. Figueroa, J. Añorga, and S. Arrizabalaga, "A role-based access control model in modbus scada systems. a centralized model approach," *Sensors*, vol. 19, no. 20, p. 4455, 2019. doi: 10.3390/s19204455. [Online]. Available: https://doi.org/10.3390/s19204455

[14] F. Katulić, D. Sumina, S. Groš, and I. Erceg, "Protecting modbus/tcp-based industrial automation and control systems using message authentication codes," *IEEE Access*, vol. 11, pp. 47 007–47 023, 2023. doi: 10.1109/ACCESS.2023.3275443. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3275443

[15] Y. Chen, X. Lian, D. Yu, S. Lv, S. Hao, and Y. Ma, "Exploring shodan from the perspective of industrial control systems," *IEEE Access*, vol. 8, pp. 75 359–75 369, 2020. doi: 10.1109/ACCESS.2020.2988691. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.2988691

[16] Z. Zhang, L. Huang, R. Tang, T. Peng, L. Guo, and X. Xiang, "Industrial blockchain of things: A solution for trustless industrial data sharing and beyond," in *2020 IEEE 16th International Conference on Automation Science and Engineering (CASE)*, 2020. doi: 10.1109/CASE48305.2020.9216817 pp. 1187–1192. [Online]. Available: https://doi.org/10.1109/CASE48305.2020.9216817

[17] S. M. Alrubei, E. Ball, and J. Rigelsford, "Securing iot-blockchain applications through honesty-based distributed proof of authority consensus algorithm," in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2021. doi: 10.1109/CyberSA52016.2021.9478257 pp. 1–7. [Online]. Available: https://doi.org/10.1109/CyberSA52016.2021.9478257

[18] B. Kitchenham, P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – a systematic literature review," *Information and Software Technology*,

vol. 51, no. 1, pp. 7–15, 2009. doi: 10.1016/j.infsof.2008.09.009. [Online]. Available: https://doi.org/10.1016/j.infsof.2008.09.009

[19] P. Mariano, C. Garrocho, C. Cavalcanti, and R. Oliveira, "Blockchain applied to security in industrial internet of things devices," in *Proceedings of the 26th International Conference on Enterprise Information Systems - Volume 1: ICEIS*, INSTICC. SciTePress, 2024. doi: 10.5220/0012692500003690 pp. 345–353. [Online]. Available: https://doi.org/10.5220/0012692500003690

[20] L. Rosa, M. Freitas, S. Mazo, E. Monteiro, T. Cruz, and P. Simões, "A comprehensive security analysis of a scada protocol: From osint to mitigation," *IEEE Access*, vol. 7, pp. 42 156–42 168, 2019. doi: 10.1109/ACCESS.2019.2906926. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2906926

[21] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories," *IEEE Access*, vol. 7, pp. 45 201–45 218, 2019. doi: 10.1109/ACCESS.2019.2908780. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2908780

[22] A. J. Cabrera-Gutiérrez, E. Castillo, A. Escobar-Molero, J. A. Álvarez-Bermejo, D. P. Morales, and L. Parrilla, "Integration of hardware security modules and permissioned blockchain in industrial iot networks," *IEEE Access*, vol. 10, pp. 114 331–114 345, 2022. doi: 10.1109/ACCESS.2022.3217815. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3217815

[23] R. Alajlan, N. Alhumam, and M. Frikha, "Cybersecurity for blockchain-based iot systems: A review," *Applied Sciences*, vol. 13, no. 13, p. 7432, 2023. doi: 10.3390/app13137432. [Online]. Available: https://doi.org/10.3390/app13137432

[24] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976. doi: 10.1109/TIT.1976.1055638. [Online]. Available: https://doi.org/10.1109/TIT.1976.1055638

[25] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982. doi: 10.1145/357172.357176. [Online]. Available: https://doi.org/10.1145/357172.357176

[26] R. Villamar, P. Proaño, A. Cuenca Sánchez, J. Tipan, R. Pillajo, and A. Quito Carrión, "An open-source web-based approach to industrial supervision and data acquisition in the context of industry 4.0," *Engineering Proceedings*, vol. 115, no. 1, p. 23, 2025. doi: 10.3390/engproc2025115023. [Online]. Available: https://doi.org/10.3390/engproc2025115023

Paulo Henrique Mariano is a Master's student in Computer Science at the Federal University of Ouro Preto(UFOP), with postgraduate specializations in Cyber Security (FIAP) and Software Engineering (PUC Minas). He works as a Software Engineer at the Federation of Industries of the State of Minas Gerais (FIEMG) and a Software Development instructor, with experience in software development, cyber-physical system integration, and information security.

Devanir Caetano Filho is a Postgraduate student in Smart Factory at SENAI-SP College and a Control and Automation Engineer. He works as a Technology Analyst III at the FIEMG System and Technical Leader of the SENAI Center 4.0 team in Automation and Systems Integration for Industry 4.0 projects. He is also a Professor in postgraduate programs at SENAI-MG College. He has experience in industrial automation, instrumentation, process control, and IT–OT integration. Specialist in industrial networks, IoT, and MES/ERP/PIMS systems.

Carlos Frederico M. C. Cavalcanti is a Professor in the Computing Department at the Federal University of Ouro Preto (UFOP), Brazil, and coordinator of KryptoLab – Cryptography and Network Security Laboratory. He holds a Ph.D. in Computer Science from the Federal University of Minas Gerais (UFMG), including a doctoral research period at the University of Surrey, United Kingdom, and previous degrees in Computer Science from the University of Campinas (UNICAMP) and Electrical and Electronic Engineering from the Pontifical Catholic University of Minas Gerais (PUC-MG). His current work focuses on applied cryptography, blockchain-based security, Industry 4.0, tokenization, decentralized identity, IoT, cyber-physical systems, and secure industrial protocols such as Modbus.

Ricardo Augusto Rabelo de Oliveira received his Ph.D. degree in Computer Science from the Federal University of Minas Gerais in 2008. Nowadays, he is an Associate Professor in the Computing Department at the Federal University of Ouro Preto. Has experience in Computer Science, acting on the following subjects: Wavelets, Neural Networks, 5G, VANT, and Wearables.