Securing Industrial Internet of Things: A Multi-Factor Authentication Approach using PUFs and AI

[1*]Fakhrul Iqbal bin Mohd Firdaus, [2]Jasmin Khan binti Abdul Rahman, [3]Karisma Khairunnisa binti Osman, [4]Mcjoey Michael Enggat anak Johnny, [5]Muhammad Zikri bin Roslan and [6]Reema Shaheen

[1, 2, 3, 5]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia
[4]Ernst & Young Consulting Sdn. Bhd. (EY), Pusat Bandar Damansara,
Kuala Lumpur 50490, Malaysia
[6]Department of eLearning Center (ELC), Jazan University, Saudi Arabia

email: [1*]74778@siswa.unimas.my, [2]73511@siswa.unimas.my, [3]73523@siswa.unimas.my, [4]Mcjoey.Johnny@my.ey.com, [5]73641@siswa.unimas.my, [6]rima@jazanu.edu.sa

**Corresponding author*

Received: 12 July 2024 | Accepted: 28 September 2024 | Early access: 29 October 2024

Abstract - *Ensuring secure and reliable authentication is a critical challenge in the Industrial Internet of Things (IIoT) due to the vulnerability of traditional authentication methods. This paper proposes a multi-factor authentication mechanism (MFA) that combines Physical Unclonable Functions (PUFs), HMAC-SHA-256 hashing, and Artificial Intelligence (AI) to address the shortcomings of existing protocols. PUFs exploit manufacturing variations to generate unique, unclonable identifiers for each IIoT device, eliminating the need to store cryptographic keys that can be extracted through physical attacks. The proposed approach consists of a registration phase where devices generate PUF responses linked to temporary identities, and an authentication phase with mutual verification using challenge-response pairs and XOR operations. This lightweight protocol maintains high security through resistance to various attacks like replay, man-in-the-middle, and impersonation, while ensuring efficiency suitable for resource-constrained IIoT environments. AI is integrated to optimize challenge-response pair selection, perform anomaly detection, and enable adaptive authentication, enhancing the robustness and scalability of the system against evolving cyber threats. The solution effectively secures IIoT device authentication while meeting the operational requirements of industrial applications.*

Keywords: Industrial Internet of Things, Multi-Factor Authentication, Physical Unclonable Functions, Hashing, Artificial Intelligence.

1 Introduction

The Industrial Internet of Things (IIoT) is revolutionizing industries by enabling advanced automation, enhanced connectivity, and real-time data exchange among devices. This technological advancement, however, brings forth significant security challenges, particularly in ensuring secure and reliable authentication of devices and users. Traditional authentication methods, such as password-based systems and key storage mechanisms are increasingly proving to be inadequate in the face of sophisticated cyber threats and physical tampering. These methods often rely on storing secret keys in non-volatile memory, making them vulnerable to extraction and cloning through physical attacks. Additionally, the computational overhead associated with traditional cryptographic methods poses a challenge for resource-constrained IIoT devices. Therefore, there is a pressing need for a secure, efficient, and scalable authentication mechanism that can address these vulnerabilities and protect IIoT environments from unauthorized access and cyber threats.

The current landscape of cybersecurity for IIoT faces significant challenges, particularly concerning authentication protocols. One prominent issue is the vulnerability of existing protocols that lack robust authentication properties, leaving them prone to attacks and message replay, consequently jeopardizing overall security. Data transmitted through insecure channels in IIoT environments are exposed to security risks, leading to various malicious attacks on the devices.

Furthermore, widely employed authentication techniques in cloud computing environments, such as Single Sign-On (SSO) and Two-Factor Authentication (2FA), are increasingly vulnerable to sophisticated cyber-attacks. This vulnerability poses a considerable threat to Small and Medium Enterprises (SMEs), which often lack the budgetary and technical capabilities to implement advanced security measures. These enterprises require cost-effective and secure multi-factor authentication (MFA) frameworks tailored to their specific needs.

Additionally, traditional password-based authentication methods are proving insufficient for ensuring secure communication within IIoT environments. These methods are susceptible to various forms of attacks such as hacking and phishing. The critical issue at hand is the inadequacy of existing authentication mechanisms to safeguard IIoT devices against unauthorized access. There is an urgent need to develop a secure and efficient authentication protocol explicitly designed to withstand the diverse array of threats inherent in IIoT settings.

2 Related Works

In this paper by Xiao et al. (2023), a formal analysis of reliable MFA procedures for IIoT is explained. Furthermore, it also discusses the use of Logic of Events for formal analysis of security protocols, which focuses on MFA in IIoT. This paper highlights the weakness of protocols that fail to satisfy strong authentication properties, making them susceptible to attacks and message replay, thereby compromising security. To solve this problem, authentication properties are categorized, and the security of the MFA protocol is verified using the Logic of Events theory. Moreover, the authors explain the theoretical extension to the Logic of Events theory, to enable the formal analysis of authentication protocols. This approach shows a strong authentication property rooted in formal analysis and authentication using the Logic of Events theory (Xiao et al., 2023). However, the complexity in implementation and potential limitations in handling real-time scenarios represent the weaknesses. To evaluate the proposed solution, the authors conduct formal proofs of the improved authentication properties, analyse matching events, and verify protocol of the security requirements. This work contributes to security field by enhancing the ability to describe and analyse emerging protocols, which potentially influence the future research in IIoT industry.

Furthermore, paper by Zulkifli et al. (2023) address challenges encountered by Small and Medium Enterprises (SMEs) in adopting cloud computing, particularly concerning authentication security. SMEs often find existing authentication methods in cloud environments geared towards larger enterprises, lacking cost-effectiveness and security. The primary problem identified is the absence of a secure, yet affordable MFA framework tailored for SMEs. To address this, they propose an MFA framework incorporating various elements like Remote Desktop Authentication, Secure Socket Layer Virtual Private Network (SSL VPN), One-Time Password (OTP) via email, and Hypertext Transfer Protocol Secure (HTTPS) with SSL or Transport Layer Security (TLS). The technique offers enhanced security, cost-effectiveness through OTP email, and implementation flexibility (Muhammad Zulkifli et al., 2023). However, potential delays in receiving OTP emails and the need for SMEs' technical expertise pose weaknesses. Evaluation involves a literature review, expert consultations, and a proof of concept demonstrating OTP email authentication feasibility. Figure 1 demonstrates the proposed enhanced MFA for cloud computing for SME.

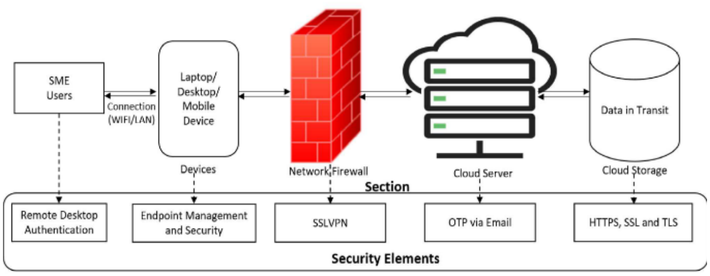

Figure 1: Proposed Multifactor Authentication Framework (Zulkifli, M.S et al., 2023)

Next, the security challenges in IIoT stem from traditional password-based authentication limitations (Li et al., 2020). Li et al. (2020) developed a protocol specifically tailored for IIoT environments. Their protocol focuses on establishing secure communication channels between devices by implementing MFA mechanisms. They utilized Oblivious Pseudo-Random Function (OPRF) to protect the confidentiality of authentication factors stored on the server side, preventing sensitive information leakage. Additionally, they introduced the Secure Remote Multi-

Factor (SRMF) protocol, which enhances the authentication and key exchange process in IIoT settings. A security analysis based on Secure Password Hash Functions (SPHF) was conducted to ensure the protocol meets the necessary security standards and can withstand prevalent online and offline attacks in IIoT environments. While enhancing communication security, potential implementation complexities and dependencies on multiple factors are acknowledged as weaknesses. Overall, Li et al. (2020) aims to provide a practical and efficient solution to address the security challenges in IIoT systems by combining MFA, OPRF, and the SRMF protocol. Evaluation metrics cover entity authentication, session key security, forward secrecy, and theoretical and experimental assessments, validating the protocol's security and performance. Future works may focus on simplifying implementation, reducing dependencies, and bolstering resistance against potential attacks, refining the protocol for broader adoption in IIoT settings. Figure 2 shows the high-level overview of how the server authenticates a user-device and establishes a session key based on multiple factors.

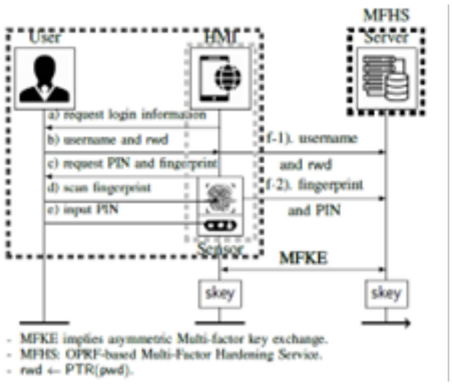

Figure2: Proposed Authentication Process (Li et al., 2020)

Khalid et al. (2021) presents the SELAMAT scheme, a MFA solution tailored for an IIoT systems in fog computing environments. Combining smart card, biometric methods, and username/password with AES-ECC encryption, it addresses communication complexity, security threats, and authentication challenges. The process involves five phases: setup, user registration, fog node registration, login, and authentication. Through this approach, SELAMAT ensures mutual authentication between edge devices and fog servers, enhancing security by preventing various attacks such as replay attacks, impersonation attacks, and man-in-the-middle attacks. Strengths include enhanced security, efficient encryption, and cost reduction, while potential weaknesses may include implementation complexity and reliance on biometric authentication. Figure 3 illustrates the system architecture of SELAMAT. Evaluation involves formal security verification, BAN logic for authentication proof, and comparisons with existing schemes regarding security, functionality, and costs.

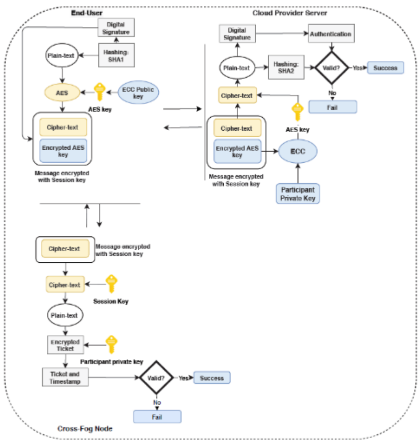

Figure 3: SELAMAT's System Architecture (Khalid et al., 2021)

Moreover, Zhang et al. (2022) analyses the use of MFA and blockchain technology to secure cross-domain device collaboration in IIoT. The technique encodes multiple variables, including hardware fingerprints, into random integers, which then converted into key materials. Each domain's dynamic accumulator is kept on the blockchain, which causes a less storage overhead (Zhang et al., 2022). The dynamic accumulator for each domain is stored on the blockchain, which reduces storage overhead. To effectively authenticate the un-linkable IDs of the IIoT devices across multiple domains, an on-chain accumulator is used. The security of the protocol is proven, and the article discusses its functionalities and features. Moreover, a significant reduction of the on-chain storage is shown through the comparison results.

Besides, Han et al. (2024) explores the security challenges inherent in IIoT systems, emphasizing the pivotal role of authentication protocols in safeguarding industrial data. They identify shortcomings in current authentication methods and propose a novel protocol aimed at bolstering security while minimizing communication and computational costs. This protocol integrates symmetric cryptography, hash functions, XOR operations, secret sharing schemes, and session-specific temporary information processing to mitigate security breaches (Han et al., 2024). Its strengths include defense against insider attacks, forward security maintenance, and rigorous analysis using the real-or-random (ROR) model for security assurance. However, potential drawbacks include moderate overhead in communication and computation and reliance on a secure channel for registration and authentication. The authors evaluate the protocol through formal security analysis, informal discussions, and comparisons with existing methods, ultimately presenting it as a promising solution for enhancing the security of IIoT applications and addressing critical vulnerabilities in industrial data protection.

This paper by Zou et al. (2023) discusses the design and evaluation of an efficient and robust three factor user authentication protocol in IIoT for smart factories. This paper also addresses the security and performance issues of the current existing alternatives. The problem statement stated in this research is the need for a secure authentication and a key agreement protocol to protect real-time data flow and ensure the integrity of operations in a smart factory environment. Therefore, this leads to the proposed solution, which is a three-factor authentication protocol, which uses a technique such as ProVerif tool for formal verification and heuristic analyses for the security assessment (Zou et al., 2023). The strength of the proposed solution is better performance in storage, computation costs, and communication. However, this solution shows a potential security flaw in some compared solutions. The solution is evaluated by its the network delay, the analysis functionality, the energy consumption, and semantic security proof as shown in Figure 4.

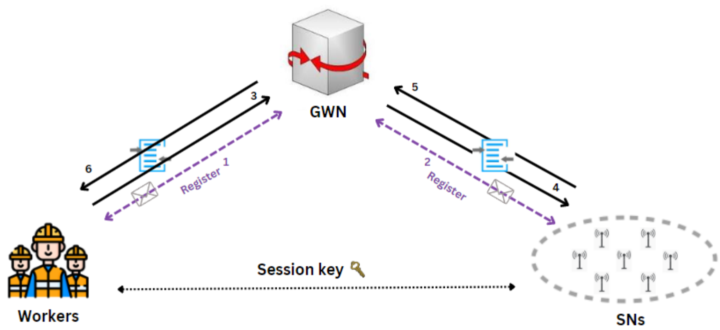

Figure 4: System model of user authentication in IIoT (Zou et al., 2023).

Next, the article by Ming et al. (2023) addresses challenges in developing a secure one-to-many Authentication and Key Agreement (AKA) scheme that allows a user to authenticate with multiple smart devices simultaneously while minimizing computational and communication costs. The scheme must address potential security vulnerabilities such as man-in-the-middle attacks, lack of perfect forward secrecy, and known session-specific temporary information attacks. Thus, the proposed scheme by Ming et al. (2023) introduces a secure one-to-many AKA system that reduces computational and communication expenses while resolving security concerns. In addition to using symmetric encryption (AES-128) and elliptic curve cryptography for session key formation, the suggested solution presents a new method that combines smart cards, passwords, and biometrics for user authentication. The system model integrates important elements such as the Key Management Center (KMC), gateway, users, and smart devices. Improved security features like mutual authentication and effective resource usage are among the advantages of the suggested method (Ming et al., 2023). On the other hand, dependence on safe implementation of cryptographic operations and key management protocols, and potential vulnerabilities in when smart devices are compromised or user credentials are exposed, are possible drawbacks. Authors assess their proposed solution through comparisons of security and functionality features with related schemes, computation cost analysis in comparison with existing AKA schemes, performance evaluation focusing on computational and communication costs, and security analysis based on the Real-or-Random (ROR) security model and simulation of potential attacks. This comprehensive evaluation ensures a thorough assessment of the proposed solution's efficacy in IIoT environments. Figure 5 illustrates the system model of one-to-many AKA scheme for IIOT.

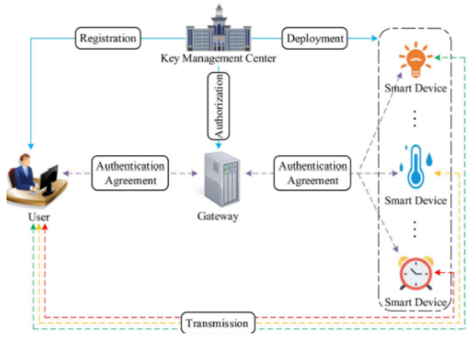

Figure 5: System Model of One-to-Many AKA Scheme for IIoT (Ming et al., 2023)

Next, Aminian Modarres & Sarbishaei (2022) propose a two-factor authentication protocol for IoT applications, leveraging PUFs and wireless fingerprints. This comprehensive protocol covers registration, authentication, data transfer, and cryptographic key management, utilizing lightweight cryptographic primitives such as one-way hash functions and XOR operations to optimize efficiency. Its strengths lie in robust mutual authentication and resilience against prevalent IoT attacks, though weaknesses include potential security risks associated with a permanent secret (IDd) and underutilization of wireless fingerprints. Evaluation encompasses informal and formal security analyses, showcasing resistance to attacks and concrete proof of strong mutual authentication through the Burrows-Abadi-Needham (BAN) logic, alongside performance metrics demonstrating improved computational efficiency compared to existing schemes. Overall, the proposed protocol offers a significant advancement in fortifying IoT environments, addressing vulnerabilities and providing enhanced security features tailored to IoT applications' unique demands.

Finally, the article by Xu et al. (2023) examines the privacy concerns and security in IIoT. The security issues are created when data is being transmitted over public channels. The article proposes the use of a key agreement system based on elliptic curve encryption and hash in anonymous user authentication. The suggested solution aims to protect user anonymity and enables dynamic user joining via a pseudonym tuple database on control nodes. Moreover, it includes fuzzy biometric extraction technologies to help prevent key loss and device capture assaults. A security analysis was performed by utilizing Real-Or-Random (ROR) model and Burrows-Abadi-Needham (BAN) logic. This method increases efficiency and functionality fitting choices for industrial settings, offering the promise of enhanced security and efficient data transfer for substantial benefits in the IIoT landscape. The trusted authority, user, control nodes, and smart sensor devices make up the system's four entities. Figure 6 illustrates the relationships between these entities in the network model.

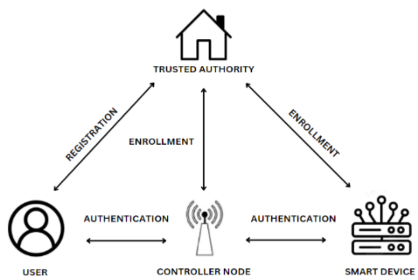

Figure 6: Three Factor Anonymous Authentication's System model (Xu et al., 2023)

In this paper, Bhatia et al. (2023), API security-critical issues are mentioned by the authors, focusing on preventing broken authentication vulnerabilities identified in the OWASP Top 10 API Security Risks of 2023. Physical Unclonable Functions (PUF) and hashing technologies are combined as the suggested method to produce a highly secure and low-complexity mutual authentication mechanism that protects privacy. The goal of this protocol is to address the shortcomings of current approaches, which often involve overly complex mathematical processes, making them impractical for modern API-based applications. The performance analysis of the proposed method demonstrates its efficiency, practicality, and enhanced security, making it an effective solution for enterprise web applications.

Furthermore, this paper by Mostafa et al. (2020) presents a robust and efficient mutual authentication protocol for IoT devices and servers using hash functions and PUFs. The proposed protocol is designed to overcome the limitations of traditional cryptographic methods, which are often too computationally intensive for powerconstrained IoT devices. By incorporating two PUFs embedded within the IoT device, the protocol ensures high security with minimal computational overhead. The authentication mechanism involves the use of Hash-Based Message Authentication Code (HMAC) computations, in particular, HMAC-SHA-256, making it lightweight and suitable for low-resource environments. Formal security analysis, including evaluations of its resistance to various cyberattacks, has demonstrated the protocol's robustness and effectiveness. The proposed method is especially relevant in scenarios where maintaining the security of web applications is critical, addressing vulnerabilities such as broken authentication. Future work involves exploring alternative hash functions, implementing proof-of-concept versions, and assessing the protocol's resilience under different attack scenarios and conditions.

This paper by Luo et al. (2022) introduces a novel authentication protocol tailored for resource-constrained devices in the IIoT. It aims to address the inefficiencies of traditional security mechanisms, which are too resource-intensive for IIoT environments. The proposed protocol utilizes PUFs to ensure secure and lightweight authentication. It operates in two main phases: the registration phase, where devices register with a backend server via a secure channel to establish unique identities, and the authentication phase, where devices authenticate with the gateway-server unit (GSU) using temporary identities and PUF-generated responses. This setup ensures mutual authentication, forward secrecy, and resilience to Denial of Service (DoS) and clone card attacks. The protocol includes a resynchronization mechanism to handle potential desynchronization caused by DoS attacks. Security properties such as user anonymity, confidentiality, and forward secrecy are maintained using secret parameters and hash functions. The protocol's robustness is further validated through formal verification using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The study concludes that this lightweight authentication protocol effectively secures IIoT devices, providing a practical solution for secure machine-to-machine communication in industrial settings while efficiently managing resource constraints.

Several other researchers have also contributed to end-to-end security mechanisms even with the assistance of the counter partners i.e. universities or industries, for broaden implications in future works section. This research article can act as a guideline for future young researchers in end-to-end security measures in 6th generation networks. This improved work (proposed solution) for the given problem statement is adopted from papers by Bhatia et al. (2023), Mostafa et al. (2020), and Luo et al. (2022), which act as a benchmark for this research article.

3 Proposed Solutions

PUFs play a crucial role in boosting security for IoT devices, especially in MFA. PUFs are hardware-based security primitives that exploit the inherent and uncontrollable manufacturing variations in electronic circuits to generate unique identifiers or responses. These identifiers are known as Challenge-Response Pairs (CRPs), where each challenge input results in a distinct response output, as depicted in Figure 7.

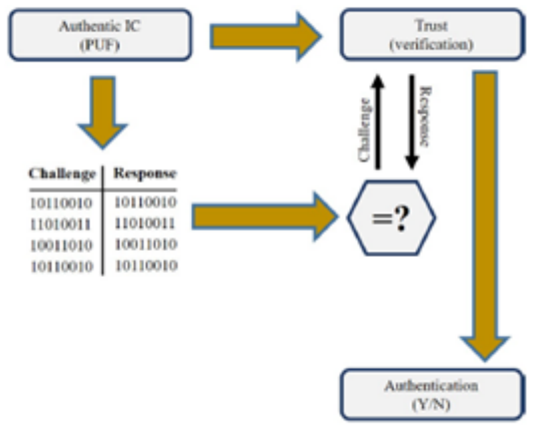

Figure 7: Authentication process of Physical Unclonable Function (PUFs) chip (Asif et al., 2020)

These identifiers are nearly impossible to replicate or clone due to the small differences created during the manufacturing process, ensuring each device has a specific and individual identifier (Bhatia et al., 2023). The functional relationship between the challenge and response in PUFs resembles that of a random function, deriving its unpredictability from the variance in manufacturing processes. This characteristic makes it exceedingly difficult, if not practically impossible, to predict the response to a specific challenge or to replicate the PUF's behavior in hardware or software. This unique characteristic of PUFs provides a strong advantage for verifying the authenticity and integrity of devices.

Traditional authentication methods often depend on storing secret keys in the non-volatile memory of IoT devices, which can be risky if an attacker gains physical access. PUFs address this vulnerability by dynamically generating device-specific secret keys, thus eliminating the need to store cryptographic keys on the device. This dynamic key generation ensures that even if someone physically tampers with the device, the cryptographic identity remains secure, making PUFs highly resistant to a wide range of attacks, including physical tampering and cloning (Mostafa et al., 2020).

In the proposed authentication mechanism, PUFs are combined with HMAC-SHA-256 to enhance security further. HMAC-SHA-256 helps establish secure session keys and supports secure data communication once authentication is successful. This hashing algorithm ensures message integrity by functioning as a one-way process that verifies the authenticity of messages. Each IoT device undergoes a registration phase with a backend server through a secure channel, where it generates a unique response using its PUF in response to a challenge from the server. This response is stored for future authentication. During the authentication phase, devices use temporary identities and generate PUF-based responses combined with XOR operations to communicate with the Gateway-Server Unit (GSU). The GSU verifies these responses using the stored data from the registration phase, ensuring mutual authentication and forward secrecy (Luo et al., 2022). The combination of PUFs and HMAC-SHA-256 makes each authentication attempt unique, effectively protecting against replay and relay attacks. The challenge-response mechanism of PUFs adds another layer of security, ensuring that the authentication process cannot be easily duplicated or intercepted (Mostafa et al., 2020).

PUFs also offer a lightweight and efficient alternative to traditional encryption methods, which is particularly beneficial for IoT applications with limited resources. By generating cryptographic keys on-the-fly, PUFs eliminate the need for key storage and management, thereby enhancing security without adding significant computational or storage overhead. This efficiency makes PUFs an ideal solution for IoT devices that have limited space and power, ensuring that security measures do not compromise device performance (Mostafa et al., 2020). Moreover, PUF-based authentication mechanisms ensure that sensitive data is never stored in the device's memory, which enhances resilience against physical tampering. The unique responses generated by PUFs during each authentication attempt prevent attackers from cloning or replicating the device's cryptographic identity. This capability is vital for maintaining the security of devices in potentially hostile environments where physical attacks are a real threat (Mostafa et al., 2020).

Using PUFs in MFA frameworks for IoT devices significantly boosts overall security. By leveraging the physical differences in each device for unique identification, PUFs ensure the integrity and confidentiality of data exchanges, even in resource-constrained environments (Luo et al., 2022). The reliability and unpredictability of PUFs make them a strong defense against sophisticated cyber threats common in IoT environments, such as man-in-the-middle attacks, insider attacks, and impersonation attacks. PUFs also offer notable advantages in terms of reliability and uniqueness, which are critical for verifying the authenticity of IoT devices and users. Using PUFs in the authentication process helps create secure communication channels and verify device and user identities without relying solely on traditional methods like passwords or smart cards. This adds an extra layer of security to the authentication process, making it more robust against sophisticated cyber threats (Luo et al., 2022).

While PUFs provide a strong foundation for secure authentication, integrating Artificial Intelligence (AI) can further enhance the robustness and efficiency of this system. AI algorithms can optimize the selection of CRPs used in PUFs. By learning patterns and predicting the most effective CRPs, AI ensures robust authentication while minimizing the risk of replay attacks. AI can continuously monitor the authentication process and detect anomalies. For instance, if an unusual pattern of access requests is detected, AI can flag potential security breaches and trigger additional verification steps. AI can also analyze contextual data (e.g., location, time of access, user behavior) to dynamically adjust the authentication requirements. For example, accessing an IoT device from an unusual location might prompt the system to require additional verification steps. Furthermore, AI and machine learning techniques can be used to improve the reliability and robustness of PUFs by compensating for environmental variations and aging effects that might affect the PUF's performance over time. AI can dynamically adjust cryptographic parameters and CRPs to ensure enhanced forward secrecy and mutual authentication, adapting to potential threats in real-time.

Integrating AI with PUFs that combined with HMAC-SHA-256 for MFA in IoT devices provides a sophisticated and secure approach to protecting these devices. This combination leverages the unique properties of PUFs and the intelligent capabilities of AI, resulting in a robust, adaptable, and scalable security solution. By optimizing challenge-response pairs, detecting anomalies, and adapting to contextual data, AI enhances the security provided by PUFs, ensuring that IoT devices remain secure even in the face of evolving cyber threats.

4 Analysis Discussion

4.1 Descriptive Analysis

The proposed MFA mechanism addresses several critical issues identified in the current landscape of IIoT security. By leveraging PUFs and HMAC-SHA-256, the solution effectively mitigates vulnerabilities associated with traditional authentication protocols, particularly those relying on stored secret keys. In traditional systems, secret keys stored in non-volatile memory are prone to extraction and cloning through physical tampering. PUFs, on the other hand, generate unique device-specific keys dynamically based on the inherent physical characteristics of each device, thereby making it exceedingly difficult for attackers to replicate or extract these keys. This dynamic key generation significantly enhances the robustness of the authentication process against physical tampering and unauthorized access. The protocol includes two phases: registration phase and authentication phase.

i. Registration Phase

   In the initial registration phase, each IoT device engages in secure communication with the backend server. The server issues a unique challenge to the device, which then generates a corresponding response using its PUF. This response is sent back to the server and stored securely for future reference. This phase ensures that the server has a unique, device-specific identifier that can be used to authenticate the device in subsequent interactions.

ii. Authentication Phase

   The authentication phase is designed to be both secure and efficient. When an IoT device at-tempts to authenticate with the gateway-server unit (GSU), it uses a temporary identity to initiate the process. The GSU responds with a new challenge. The device, leveraging its PUF, generates a response that is combined with the temporary identity using XOR operations. This response is transmitted to the GSU, which verifies it against the stored data from the registration phase. This method ensures mutual authentication, where both the device and the server validate each other's identities, thus preventing impersonation attacks.

   Moreover, the proposed mechanism is particularly suitable for resource-constrained IIOT devices. Traditional cryptographic methods often impose substantial computational and storage overhead, which can be detrimental to the performance of devices with limited resources. The integration of PUFs with HMAC-SHA-256 ensures a lightweight and efficient authentication protocol, maintaining high security standards without compromising device performance. This efficiency is crucial for IIoT environments, where maintaining operational effectiveness while ensuring security is paramount.

   The proposed authentication mechanism also offers substantial protection against common cyber threats, including replay attacks, relay attacks, and various forms of cyberattacks such as man-in-the-middle, DoS, and impersonation attacks. By generating unique identifiers for each authentication attempt, PUFs ensure that intercepted data cannot be reused by attackers. This capability secures communication channels and enhances overall system integrity, addressing one of the major shortcomings of existing authentication mechanisms. Thus, the proposed solution not only improves security but also ensures the reliability and efficiency necessary for modern IIoT applications.

4.2 Mathematical Analysis

The proposed authentication mechanism's mathematical foundation ensures both security and efficiency. The PUF-based key generation process can be expressed as $K_i = PUF(d_i)$, where d_i represents the unique physical characteristics of device i_i, and K_i is the unique key generated for the device. This method eliminates the need to store K_i in memory, thereby enhancing security against physical attacks. The HMAC-SHA-256 authentication process is defined by the equation:

$$HMAC(K_i M) = H((K_i \oplus opad) \,||\, H((K_i \oplus ipad)||M))$$

where M is the message to be authenticated, H is the SHA-256 hash function, $||$ denotes concatenation, and $opad$ and $ipad$ are the outer and inner padding constants, respectively. This ensures the integrity and authenticity of messages exchanged between devices and servers. In the challenge-response mechanism, the server sends a challenge C to the device, which then computes the response R as follows:

$$R = HMAC(K_i C)$$

The server verifies R by comparing it with the expected response calculated using the same K_i. This mechanism adds an additional layer of security, making it challenging for attackers to predict or reuse authentication data.

The PUF mechanism is further enhanced by adding a registration phase and authentication phase. Table 1 shows the definition of each symbol used.

Table 1: Symbols and cryptographic function

Symbol	Definition
D	Resource-constrained devices in IIoT
GSU	Gateway-Server Unit
TID_j^i	Temporary identity of the device j for i-th round
C_j^i	Challenge of the device j for i-th round
R_j^i	Response of the device j for i-th round
N_d/N_s	Random number generated by device/server
$PUF(\cdot)$	Secure physically unclonable function
$h(\cdot)$	One way Hash Function
$\oplus$	Exclusive-OR operation
$\|\|$	Concatenation operation

i. Registration Phase

During the registration phase, each resource-constrained device (D) must register with the backend server via a secure channel. Initially, the server generates a random challenge C_j^1 and a temporary identity TID_j^1, which are then sent to the device. Upon receiving these, the device stores TID_j^1 and C_j^1, and produces a corresponding response R_j^1 using its PUFs. The device then sends R_j^1 back to the server. Finally, the server securely stores the entry comprising $\{C_j^1, R_j^1, TID_j^1\}$. This process establishes a unique identifier and challenge-response pair for each device, ensuring secure authentication in future interactions (Luo et al., 2022).

ii. Authentication Phase

The resource-constrained D generates a random number N_d and computes its temporary identity TID_j^1. It then sends these values to the GSU. Upon receiving the temporary identity, the GSU uses it as an index to search the corresponding entry in the database. If a matched entry is found, the GSU generates a random number N_s and computes a response message M_2 containing the verification parameter V_1 and Ns. This message is then sent to the D. D verifies the received message M_2 and responds with a message M_3 containing the verification parameter V_2. This message is sent to the GSU. The GSU verifies the parameter V_2 to ensure the legality of D. If the verification is successful, the mutual authentication between the resource-constrained device and the GSU is achieved. Throughout this process, the protocol ensures forward secrecy, resilience against DoS attacks, and mutual authentication between the resource-constrained device and the GSU. These steps collectively contribute to the security and efficiency of the authentication phase in the proposed lightweight protocol (Luo et al., 2022).

The protocol ensures forward secrecy, resilience against DoS attacks, and mutual authentication between the resource-constrained device and the GSU. This is achieved using temporary identities, random challenges, and verification parameters, which collectively contribute to the security and efficiency of the authentication phase.

4.3 Protocol Analysis

To ensure the effectiveness of PUFs and hash algorithms in enhancing the security for IIoT devices, the proposed mutual authentication mechanisms are evaluated against several types of cyberattacks. These assessments are essential to validate the solution's capability to withstand sophisticated threats prevalent in the industrial environment. The cyberattacks are:

i. Replay Attack

Replay attacks involve capturing valid data transmissions and retransmitting them to trick the system into granting unauthorized access. Our proposed mechanism uses timestamps in each communication between the IoT device and the server. Each message includes a timestamp indicating when it was sent. The server and IoT device validate these timestamps against a predefined validity period. If a timestamp is outdated or falls outside the acceptable range, the message is rejected. This ensures that even if an attack captures and retransmits a message, the outdated timestamp will pre-vent it from being accepted. Additionally, the unique CRPs used in each session add another layer of protection, as they cannot be reused.

ii. Machine Learning Attack

Figure 8 illustrates machine learning attacks aimed at predicting the responses of a PUFs (Ganji et al., 2022).In the traditional approach, multiple CRPs from the PUF are obtained, and an empirical learning algorithm is used to model the PUF's behaviour, allowing an attacker to predict future responses given new challenges.

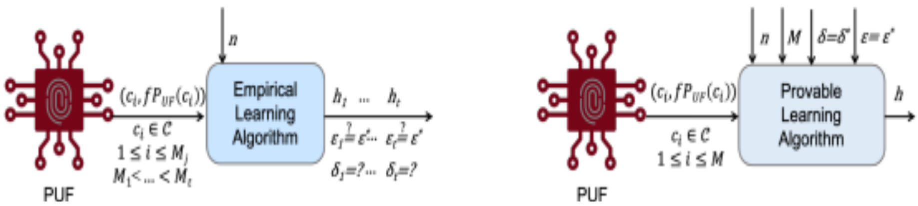

Figure 8: Schematic illustrating the differences between a provable and an empirical ML algorithm applied in the context of PUFs

However, in the proposed protocol, only a single CRP is used per IoT device, and these CRPs are changed regularly. This dynamic approach prevents attackers from gathering sufficient data to effectively train a machine learning model to predict the PUF's responses accurately. Furthermore, the PUF's response is not transmitted in plaintext, making it more difficult for an attacker to obtain the necessary data for modelling. By limiting the exposure of CRPs and never directly transmitting the PUF's response, machine learning attacks become impractical in this proposed protocol

iii. Man-in-the-Middle Attack

In a man-in-the-middle attack, an attacker intercepts and possibly alters communication between two parties. Our proposed mechanism ensures that sensitive data such as SRAM keys, PUF responses, and session keys are never exchanged in plaintext. The only data transmitted in plaintext are the IDd, timestamps (TS1, TS2, TS3), the PUF challenge (C), and hashed messages. Any alteration by a man-in-the-middle attacker will be detected through mismatched hashed messages, causing the connection to be dropped and maintaining data confidentiality.

iv. Invasive Attack

Invasive attacks involve physically tampering with the device to extract its cryptographic keys. The unique characteristics of silicon PUFs make duplication unworkable. Since the initial secret key is not stored on the IoT device chip, there is no useful information that invasive attacks can extract to compromise the device’s security.

v. Firmware Attack

Firmware attacks aim to compromise the software running on the device to extract cryptographic keys stored in non-volatile memory. The proposed authentication scheme uses SRAM PUFs, which do not require storing the secret key in memory. This means that firmware attacks will not reveal any useful information, thus maintaining the security of the IIoT devices.

vi. Impersonating/Spoofing Attacks

Impersonation or spoofing attacks occur when an attacker tries to masquerade as a legitimate de-vice or server. Even if an attack somehow obtains the SRAMS key (SRAMk) of the IoT device, they will also need to know the Arbiter PUF responses to launch a successful spoofing attack. Since the PUF response is not exchanged in plaintext and the Arbiter PUF cannot be duplicated, spoofing attacks against our mutual authentication mechanism are inapplicable.

vii. Eavesdropping Attack

Eavesdropping attacks involve an attacker passively listening to communication between the IoT device and the server to extract sensitive information. Our mutual authentication mechanism does not exchange sensitive data such as SRAM keys, PUF responses, or session keys in plain text. Even if an attacker captures the communication link, they will not obtain any useful information to compromise the device's security.

viii. Side Channel Attack

Side Channel attacks exploit physical implementation of cryptosystem, such as power consumption or electromagnetic emissions, to extract cryptographic keys. While it is possible for a side channel to attack to recover the Arbiter PUF response, this response is not used to generate the session key and does not contain any sensitive data. Thus, even if the Arbiter response is com-promised, it will not be useful to the attack. Additionally, research on securing SRAM PUF keys against side channel attacks enhances the reliability of using SRAM PUFs in IIoT authentication scheme. This method reduces the effectiveness of side channel attacks compared to mechanisms deploying only (Bhatia et al., 2023) one PUF.

ix. Denial of Service (DoS)

The protocol is designed to combat DoS attacks, a significant concern in network security. It achieves this through a resynchronization mechanism, ensuring robustness even in the face of potential threats. Key strategies include the use of temporary identities, random challenges, and dynamic verification parameters, updated after each authentication process. This prevents desynchronization issues caused by blocked messages. Additionally, the protocol ensures collaboration between the GSU and resource-constrained devices (D), maintaining the latest authentication entries together. These measures aim to secure communication in resource-constrained systems within the IIoT environment, effectively mitigating the impact of DoS attacks.

Table 2 below is the summary table of the protocol analysis against different types of cyberattacks:

Table 2: Protocol analysis against types of cyberattacks

Attacks	Protected
Replay Attack	Yes
Machine Learning Attack	N/A
Man-in-the-Middle Attack	Yes
Invasive Attack	Yes
Firmware Attack	Yes
Impersonating/Spoofing Attack	Yes
Eavesdropping Attack	Yes
Side Channel Attack	Yes
Denial of Service (DoS) Attack	Yes

4.4 Security Analysis

In this section, security analysis demonstrates that our method can overcome certain security characteristics and harmful behaviors. We determine that our proposed system meets the needed security properties to tolerate various known authentication threats in IIoT by thorough informal security research.

i. User Anonymity

Anonymity encompasses untraceability and unlinkability. Untraceability implies that an opponent cannot determine which identities in the same group belong to whom. In contrast, unlinkability indicates that an adversary is unable to determine if two identities belong to the same user. The devices do not reveal their true identities or secrets during each authentication occurrence in our proposed approach since all sent messages are calculated with a random integer. Moreover, the temporary identities TDI_j^i are calculated by random challenge $C_j^{i+1}$and one-way hash function.

ii. Confidentiality

The confidentiality of our protocol is ensured by using the secret response parameter, R_{ij}, in all transmitted messages (M_1, M_2, and M_3) between the Device and the GSU. Without R_{ij}, an adversary cannot forge valid parameters needed for authentication. Additionally, all verified messages and parameters are protected by a hash function, making it impossible for an adversary to recover other secrets, even if they obtain temporary identities and challenges from the device's memory.

iii. Forward Secrecy

Our protocol ensures resilience against DoS attacks by achieving mutual authentication between Device and the GSU through verified messages M_2, and M_3. D authenticates GSU by verifying $V_1 = h(R_{ij} || N_s || N_d)$ which an attacker cannot generate without knowing R_{ij} . Similarly, GSU authenticates D by verifying $V_2 = h(C_{ij+1} || R_{ij+1}) *)$ ensuring that attackers cannot generate a legitimate V_2 without the correct R_{ij} . This mutual authentication mechanism protects against DoS attacks.

iv. Mutual Authentication

An authentication protocol should ensure forward secrecy to safeguard past sessions from future secret key compromises. In our protocol, following each successful mutual authentication, the challenge parameter C_{ij} and the response number R_{ij} will be updated with the new random number.

v. The Resilience of DoS Attacks

Our proposed scheme ensures resilience against DoS attacks and desynchronization by implementing an innovative resynchronization mechanism. Both communicators update their temporary identity (TID), challenge (C), and response (R) after each authentication. The GSU preserves the current and previous authentication entries, while Device (D) retains the last and current challenge parameters. If synchronization is lost, D can resend the previous TID to GSU to reestablish synchronization, thereby protecting against DoS attacks caused by message blocking.

vi. AI for Robust Authentication

The incorporation of AI techniques into the proposed authentication mechanism enhances its robustness against various security threats and attack vectors. One critical aspect is the use of AI for continuous monitoring and anomaly detection during the authentication process. By training machine learning models on a diverse dataset of legitimate authentication patterns, the AI com-ponents can effectively identify deviations or anomalies that may indicate potential attacks or unauthorized access attempts.

For instance, the AI model can detect suspicious patterns such as rapid authentication attempts from multiple locations, unusual device behaviour, or authentication requests deviating from the user's typical usage patterns. In such cases, the AI system can trigger additional verification steps, request additional authentication factors, or temporarily block access until the anomaly is resolved.

Furthermore, AI can play a crucial role in adaptive authentication, where the authentication requirements are dynamically adjusted based on contextual factors and perceived risk levels. If an authentication request originates from a new or untrusted location, the AI system may prompt additional biometric authentication or employ more stringent challenge-response mechanisms. Conversely, if the request comes from a trusted location and exhibits normal behaviour patterns, the authentication process can be streamlined for a seamless user experience.

vii. AI for Resilience against Attacks

The proposed authentication mechanism leverages AI techniques to enhance its resilience against various types of attacks, including replay attacks, man-in-the-middle (MITM) attacks, impersonation attacks, and machine learning attacks. By incorporating AI, the system ensures robust security for IIoT devices.

Replay attacks are mitigated through AI models trained to detect and prevent such occurrences. These models analyse the contextual information associated with each authentication attempt, such as timestamps, device identifiers, and environmental factors. By scrutinizing this data, the AI system can identify anomalies and flag any attempts to reuse previously captured authentication data, effectively blocking replay attacks.

Man-in-the-Middle attacks are addressed by employing AI to continuously monitor communication channels. The AI system analyses traffic patterns, packet characteristics, and other relevant network-level features to detect potential man-in-the-middle attacks. By identifying suspicious activity or deviations from normal communication patterns in real-time, the AI can promptly mitigate these threats, ensuring secure communication.

Impersonation attacks are inherently resisted by leveraging the unique and unpredictable nature of PUFs. AI further enhances this protection by learning the typical behaviour patterns of legitimate devices and users. By understanding these patterns, the AI system can detect potential impersonation attempts based on deviations, providing an additional layer of security against such attacks.

Machine learning attacks pose a significant threat, but the proposed mechanism employs various countermeasures to mitigate this risk. AI models are trained using robust techniques, such as adversarial training and data augmentation, to improve their resilience against adversarial examples. The dynamic nature of PUF-based authentication, where unique challenge-response pairs are generated for each authentication attempt, makes it difficult for attackers to gather sufficient data to mount effective machine learning attacks. This combination of AI techniques and PUF properties ensures robust defense against adversarial machine learning.

By leveraging the capabilities of AI in conjunction with the inherent security properties of PUFs, the proposed authentication mechanism offers a multi-layered defense against a wide range of security threats. This approach ensures robust and resilient authentication for IIoT devices, safeguarding them against sophisticated attacks and enhancing overall security.

5 Conclusions

In conclusion, the proposed MFA mechanism significantly enhances the security and efficiency of IIoT systems. By integrating PUFs and HMAC-SHA-256, the solution effectively mitigates vulnerabilities inherent in traditional authentication methods, particularly those reliant on stored secret keys susceptible to extraction and cloning. Moreover, the incorporation of AI to optimize challenge-response pairs and detect anomalies can significantly enhance the robustness of the authentication mechanism, providing a dynamic and adaptable security solution capable of evolving in response to emerging threats. This approach not only prevents impersonation attacks but also maintains high security standards without imposing substantial computational and storage overhead, making it suitable for resource-constrained IIoT devices. Furthermore, the protocol offers robust protection against a range of cyber threats. By generating unique identifiers for each authentication attempt, it ensures that intercepted data cannot be reused by attackers, thereby securing communication channels and enhancing overall system integrity. Thus, the proposed solution not only improves security but also ensures the reliability and efficiency necessary for modern IIoT applications.

References

Aminian Modarres, A. M., & Sarbishaei, G. (2022). An Improved Lightweight Two-Factor Authentication Protocol for IoT Applications. IEEE Transactions on Industrial Informatics, 1–11. https://doi.org/10.1109/tii.2022.3201971

Asif, R., Ghanem, K., & Irvine, J. (2020). Proof-of-PUF Enabled Blockchain: Concurrent Data and Device Security for Internet-of-Energy. Sensors, 21(1), 28. https://doi.org/10.3390/s21010028

Bhatia, K., Pandey, S. K., Singh, V. K., & Gupta, D. N. (2023). Hash and Physical Unclonable Function (PUF)-Based Mutual Authentication Mechanism. Sensors, 23(14), 6307. https://doi.org/10.3390/s23146307

Ganji, F., & Shahin Tajik. (2022). Physically Unclonable Functions and AI. Lecture Notes in Computer Science, 85–106. https://doi.org/10.1007/978-3-030-98795-4_5

Han, Y., Guo, H., Liu, J., Ehui, B. B., Wu, Y., & Li, S. (2024). An Enhanced Multi-Factor Authentication and Key Agreement Protocol in Industrial Internet of Things. *IEEE Internet of Things Journal*, 1–1. https://doi.org/10.1109/JIOT.2024.3355228

Khalid, H., Hashim, S. J., Ahmad, S. M. S., Hashim, F., & Chaudhary, M. A. (2021). SELAMAT: A New Secure and Lightweight Multi-Factor Authentication Scheme for Cross-Platform Industrial IoT Systems. Sensors, 21(4), 1428. https://doi.org/10.3390/s21041428

Li, Z., Yang, Z., Szalachowski, P., & Zhou, J. (2020). Building Low-Interactivity Multi-Factor Authenticated Key Exchange for Industrial Internet-of-Things. *IEEE Internet of Things Journal*, 1–1. https://doi.org/10.1109/jiot.2020.3008773

Luo, H., Zou, T., Wu, C., Li, D., Li, S., & Chu, C. (2022). Lightweight Authentication Protocol Based on Physical Unclonable Function. Computers, Materials & Continua, 72(3), 5031–5040. https://doi.org/10.32604/cmc.2022.027118

Ming, Y., Yang, P., Mahdikhani, H., & Lu, R. (2023). A Secure One-to-Many Authentication and Key Agreement Scheme for Industrial IoT. *IEEE Systems Journal*, 17(2), 2225–2236. https://doi.org/10.1109/jsyst.2022.3209868

Mostafa, A., Lee, S. J., & Peker, Y. K. (2020). Physical Unclonable Function and Hashing Are All You Need to Mutually Authenticate IoT Devices. Sensors (Basel, Switzerland), 20(16). https://doi.org/10.3390/s20164361

Xiao, M., Chen, Y., Li, Z., Chen, Q., & Xu, R. (2023). Proving Mutual Authentication Property of Industrial Internet of Things Multi-Factor Authentication Protocol Based on Logic of Events. Electronics, 13(1), 177–177. https://doi.org/10.3390/electronics13010177

Xu, H., Hsu, C., Harn, L., Cui, J., Zhao, Z., & Zhang, Z. (2023). Three-Factor Anonymous Authentication and Key Agreement Based on Fuzzy Biological Extraction for Industrial Internet of Things. *IEEE Transactions on Services Computing*, 16(4), 3000–3013. https://doi.org/10.1109/tsc.2023.3257569

Zhang, Y., Li, B., Wu, J., Liu, B., Chen, R., & Chang, J. (2022). Efficient and Privacy-preserving Blockchain-based Multi-factor Device Authentication Protocol for Cross-domain IIoT. *IEEE Internet of Things Journal*, 1–1. https://doi.org/10.1109/jiot.2022.3176192

Zou, S., Cao, Q., Lu, R., Wang, C., Xu, G., Ma, H., Cheng, Y., & Xi, J. (2023). A Robust and Effective 3-Factor Authentication Protocol for Smart Factory in iot. https://doi.org/10.2139/ssrn.4469456

Zulkifli, M.S., Hassan, N.H., Maarop, N., Rahim, F.A., & Anuar, M.S. (2023). A Proposed Multifactor Authentication Framework for SME in Cloud Computing Environment. *2023 IEEE 13th International Conference on System Engineering and Technology (ICSET)*, 307-312.https://doi.org/10.1109/icset59111.2023.10295159