International Journal of Computer Technology and Science
Volume. 1 No. 3 July 2024
e-ISSN :3048-1961, And p-ISSN :3048-1899, Page. 71-86
DOI: https://doi.org/10.62951/ijcts.v1i3.26
Available online at: https://international.arteii.or.id/index.php/IJCTS

Advancements in Multi-Factor Authentication: A Quantum-Resilient and Federated Approach for Enhanced Security

Nur Syahrina Binti Juni[1], Grasila Huney Wan[1], Siti Aisyah Nabilah Binti Banchi[1], Estella Blessings Anak Bajau[1], Venetha A/P Loganathan[1], & Muhammad Faisal[2]
[1] *Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak,*
[2] *Director HRIMS, Ministry of Human Rights*

Kota Samarahan 94300, Malaysia;
76309@siswa.unimas.my 74928@siswa.unimas.my ; 76795@siswa.unimas.my 74741@siswa.unimas.my
77080@siswa.unimas.my dr.faisalshabbir88@gmail.com

Abstract: *The Internet of Things (IoT) phenomenon is centered around linking various devices and objects to the Internet, enabling them to communicate, collect, and exchange data [1]. The IoT needs strong, lightweight, and secure authorization schemes to regulate many devices with varying levels of ability. Quantum-resilient federated Multi-Factor Authentication (QRF-MFA) is a solution presented in this paper to address the above-discussed issues. Featuring quantum-resistant cryptographic protocols, high-speed and low-energy Physically Unclonable Functions (PUFs), decentralized identity management, and optimized communication protocols, QRF-MFA provides a complete solution for secure cross-domain device identification and authentication. This is done by leveraging blockchain technology for immutable and transparent management of identities yet limiting on-chain storage overhead. It also provides secure, lightweight communication well-suited for resource constrained IIoT devices, and it is designed for fog and edge computing environments as well. QRF-MFA eliminates the challenges of current methods by combining security, efficiency, and scalability and delivering a resilient and future-ready solution to secure IIoT authentication.*

Keywords—*Quantum-Resilient Federated Multi-Factor Authentication, Industrial Internet of Things (IIoT)*

1 INTRODUCTION

When it comes to the Industrial Internet of Things (IIoT), secure and efficient device identification spanning cross-domains is crucial for ensuring robust and seamless operations. IIoT involves the interconnection of numerous industrial devices and systems, such as sensors, machinery, and control units, across various sectors like manufacturing, energy, and logistics. Secure device identification ensures that only authorized devices can access and communicate within the network, thereby preventing unauthorized access and potential cyber threats. It maintains data integrity by validating the authenticity of each device, ensuring that the data transmitted is reliable and trustworthy. Efficient device identification also facilitates interoperability between devices across different domains, enabling smooth integration and communication, which is essential for optimizing industrial processes and enhancing operational efficiency. Moreover, in the context of scalability, efficient identification systems allow for the seamless addition of new devices without compromising security or performance. As industries increasingly rely on interconnected systems for real-time monitoring, predictive maintenance, and automation, the need for secure and efficient device identification becomes paramount to safeguard sensitive data, ensure uninterrupted operations, and achieve higher levels of productivity and innovation.

Received: May 10, 2024; Revised: June 15, 2024; Accepted: July 15, 2024; Published: July 18, 2024;
* Nur Syahrina Binti Juni , 76309@siswa.unimas.my

2 PROBLEM STATEMENT

Existing approaches to authentication in the Industrial Internet of Things (IIoT) often face challenges related to lower efficiency, inadequate privacy protection, and high on-chain storage overhead. This paper presents a novel multifactor authentication technique specifically designed to address these issues within IIoT environments. The proposed method aims to enhance efficiency by optimizing the authentication process, ensuring that devices can be verified swiftly and accurately, even in large-scale industrial networks. It prioritizes privacy protection by employing advanced cryptographic techniques that safeguard sensitive data against unauthorized access and potential breaches. Additionally, the technique is designed to minimize on-chain storage overhead, reducing the burden on blockchain systems used for secure data storage and management. By tackling these critical challenges, the proposed multifactor authentication technique promises to significantly improve the security and functionality of IIoT systems.

Since the existing approaches have many challenges, this paper will explain how we can improve the traditional multifactor authentication mechanism especially for Industrial Internet of Things (IIoT). As we know a traditional multi-factor authentication (MFA) mechanism and a Quantum-Resilient Federated Multi-Factor Authentication (QRF-MFA) mechanism differ primarily in their approach to security, particularly in the context of emerging threats posed by quantum computing, as well as in their integration and management of identity across multiple systems.

As shown in Figure 1, Multi-Factor Authentication (MFA) is a security measure designed to add an extra layer of protection to digital accounts, systems, and data by requiring users to provide multiple forms of verification. Unlike traditional single-factor authentication, which typically relies solely on a password or PIN, MFA combines two or more independent factors that fall into different categories: something the user knows (like a password), something they have (such as a smartphone or hardware token), and something they are (like biometric data). The purpose of MFA is to significantly enhance security by mitigating the risks associated with stolen or weak passwords.

Figure 1. Multi-Factor Authentication (MFA) mechanism

Quantum-Resilient Federated Multi-Factor Authentication (QRF-MFA) is an advanced authentication mechanism designed to address the security challenges posed by quantum computing advancements. Unlike traditional Multi-Factor Authentication (MFA), which primarily focuses on combining multiple factors (such as passwords and biometrics) to secure access, QRF-MFA incorporates quantum-resistant cryptographic algorithms and federated identity management principles.

3 RELATED WORKS

3.1. Article 1

One category of IoT items are smart toys, which are equipped with sensors, motors, and robotics functionality. These smart toys save information about their users' lives and have direct or indirect internet connection through companion programs. If an IoT toy is compromised, a cyber-predator may communicate with kids virtually or obtain private information about them without having to be there [1].

Compared to other IoT devices, smart toys are more vulnerable to dangers because their primary users are kids and teenagers. All internet-connected programs require authentication to confirm the user's identity, depending only on authentication is not seen as secure, particularly for apps intended for younger users [1]. Kids frequently utilize simple passwords in intelligent applications related to the Internet of Things (IoT) for toys.

The report suggested adding two-factor authentication to kid-friendly smart games that are linked to the internet by companion programs. The multi-authentication mechanisms are such as password and another authentication type, either mobile phone SMS, security token, digital certificate, or biometric authentication [1].

There are benefits and drawbacks for each of the four varieties. A one-time password (OTP) SMS is a software-based SMS format used on mobile phones. This authentication mechanism's ease of use is one of its main benefits [1]. However, when the mobile phone is not connected to a line, it is becoming more difficult to obtain the OTP PIN.

Security token comes next. The OTP symbol format is a token-based OTP-based device. Integration of the user ID or user mail and the passwords generated by the token as the user's credentials is required to access the system. Ownership is the basis for validation. When the user hits the token device, a randomly generated password is created; however, it can only be used once in a short amount of time. A digital certificate might be hardware or software-based, such as those included in smartcards. The user needs to have digital certificates and be aware of their PIN [1].

Finally, biometric authentication. The theory behind biometrics is that they are more accurate identity predictors than traditional systems like passwords and PINs since they are observable physiological or behavioural attributes. Biometric implementation has several drawbacks, one of which is that it intrudes upon a user's attributes [1].

Based on this article, a thorough trial examination of eleven intelligent games and the apps that go along with them showed that a lot of modern games still expose kids to a variety of risks. prevent this situation from occurring, the report suggested adding two-factor authentication to kid-friendly smart games [1].

3.2. Article 2

Authentication is the process of verifying the identity of a person or device before allowing access to resources or a system. Strong device authentication is required to ensure that linked IoT devices may be trusted to be who they claim to be.[2]

Device authentication is a widely recognized concern in IoT security. IoT devices usually lack adequate security systems. These gadgets often use hard-coded passwords that hackers can easily guess. To prevent attacks, it's important to authenticate all IoT devices on the network. However, as the number of devices grows, the attack surface area will increase. Standard password-based or secret-key-based authentication systems, which rely solely on a shared secret, cannot address these security concerns [2].

This article outlined a strategy whereby a device will only be allowed to connect to the network after completing multi-factor authentication successfully; if not, the authentication process will fail and must be started over. The method also verifies the server and device using digital signatures through multifactor authentication [2].

One of the advantages of the technique proposed in this article is a mutual authentication ensure that both the server and the device authenticate each other, enhancing trust in the communication process. Maintains the anonymity of IoT devices by using hashed IDs, preventing attackers from discovering device identities [2].

3.3. Article 3

IoT authentication is a process used to build trust in the identities of IoT technologies and systems. It ensures the security of data and controls access when it is transmitted across an unsecured network [3]. Traditional authentication methods often fall short in IoT environments due to resource constraints and scalability issues, prompting the authors to propose a novel solution leveraging blockchain technology and smart contracts.

The problem statement revolves around the inadequacies of existing authentication methods for IoT devices [3]. These methods often struggle to scale effectively, and their

resource-heavy nature can hinder performance on devices with limited computing power. The authors aim to address these challenges by devising a lightweight and user-centric two-factor authentication mechanism specifically tailored for IoT environments.

The proposed blockchain-based two-factor authentication technique for web-based sensor data access is user-centric and lightweight, using Ethereum blockchain and smart contracts technology [3]. The recommended strategy uses blockchain's inherent security and prioritizes user experience, although it has limitations. Blockchain infrastructure may delay and expense authentication, reducing efficiency.

The authors probably used various measures to assess their method's efficacy. Security, scalability, usability, efficiency, and resilience are possible metrics [3]. These essential considerations can help people comprehend the pros and cons of their proposed authentication solution. This insight may be utilized to improve and adjust the technique to meet IoT security needs.

3.4. Article 4

The Internet of Things (IoT) is rapidly expanding, making gadgets essential to many sectors and daily life. But their rising prominence also poses security risks. One of the most significant security risks confronting the Internet of Things is device forging or impersonation, which may be prevented via schemes based on a single authentication factor [4]. It is difficult to define a lightweight mutual authentication system that protects against current threats [4]. Current authentication approaches are often vulnerable to a range of attacks, including brute-force attacks and replay attacks. This vulnerability highlights the urgent need for an advanced, secure, and efficient authentication mechanism that is tailored to the unique constraints and security requirements of IoT environments.

The authors present a two-factor, lightweight mutual authentication approach for IoT entities, applicable to device, control, aggregation node, gateway, and server levels [4]. The solution uses knowledge-based (passwords or PINs), possession-based (physical tokens or OTP generators), and biometric (facial or fingerprint) authentication elements [4]. The authors also offer a lightweight cryptographic technique to improve authentication security and make it efficient for IoT devices. However, the solution has flaws. Multiple authentication elements and cryptographic techniques complicate implementation, especially on low-resource devices. Multiple factors may increase login times, hurting user experience.

The authors evaluate their strategy by measuring MFA device authentication time using numerous criteria. The lightweight cryptographic algorithm's memory, processing power, and storage are also examined. Brute-force, replay, and man-in-the-middle attacks are used to test

security. Finally, user input is collected to evaluate the solution's usability and applicability in real-world situations.

3.5. Article 5

The integration of IoT into corporate networks requires robust security measures, particularly in establishing trusted authentication mechanisms between devices and servers to ensure secure communication and data sharing, crucial for protecting critical infrastructures [5].

The paper recommends using security keys for encryption and authentication in IoT, emphasizing the drawbacks of password-based methods and advocating for Multi-Factor Authentication (MFA) to enhance security, with a focus on preventing account hacking and establishing a secure authentication framework [5].

The article's problem statement focuses on the vulnerabilities of single-factor authentication, such as passwords, in IoT security, stressing the need for stronger, mutual authentication between devices and servers to prevent unauthorized access and enhance overall security, highlighting the inadequacy of current techniques in ensuring the required levels of trust and protection [5].

The proposed solution, "Three-way Mutual Authentication using Security Keys," involves using a secure vault of keys to encrypt and authenticate IoT devices and servers, ensuring secure communication through a three-way authentication process that creates a shared secret session key for encrypting future communication [5].

The proposed technique's strength lies in its ability to prevent common password-based attacks, enhancing IoT system security, but its potential weakness includes the complexity of managing and securely distributing security keys, particularly in large-scale deployments, which could pose logistical and security challenges [5].

The authors evaluated their proposed solution using metrics such as security, usability, hardware performance, deployment experience, time spent authenticating, authentication failure rate, and hardware cost, providing a comprehensive assessment of its effectiveness, efficiency, and practicality in real-world IoT deployments [5].

3.6. Article 6

The articles discuss the benefits of IIoT in improving communication and efficiency in industries, but also highlight security concerns, proposing a multi-factor authentication scheme that is secured to address them [6].

The document examines security challenges in fog computing for IIoT, proposing a multifactor authentication scheme using cryptographic algorithms and authentication methods

to enhance security, and it includes a review of related works and a security analysis of the proposed scheme [6].

The problem statement underscores the necessity of a secure, lightweight multi-factor authentication scheme for cross-platform IIoT systems, aiming to enhance security, secure communication, and mutual authentication in resource-constrained IoT devices, while also tackling trust challenges in fog computing environments [6].

The proposed solution is the SELAMAT scheme, a lightweight multi-factor authentication scheme for cross-platform industrial IoT systems. It utilizes the AES-ECC algorithm for key management encryption and adopts the Kerberos workflow for secure communication between edge devices and fog node servers. The scheme reduces communication and computation costs, is verified for security using the AVISPA tool, and is proven for mutual authentication using BAN logic [6].

The SELAMAT technique's strengths lie in its use of the AES-ECC algorithm for secure key management and the Kerberos workflow for secure communication, reducing costs and offering robust security. However, it is weak to server spoofing and denying service attacks, and due to identity-based cryptographic techniques, requires increased computational effort [6].

The authors evaluated their solution using metrics such as communication and computation costs, security properties, and performance compared to existing schemes. They conducted formal and informal security analyses, verified their scheme using BAN logic, and used the AVISPA tool to ensure its security and efficiency [6].

3.7. Article 7

The article discusses a multi-factor homomorphic encryption-based method for authenticated access to IoT devices. It addresses the need for secure authentication in IoT environments, where traditional solutions mainly provide single-level protection [7].

The authors highlight the necessity for interaction-based, multi-factor, and multi-level authentication in IoT environments, addressing concerns like security attacks, authentication overhead, computational powers, and processing time [7].

The proposed solution involves the M2I (Multi-Factor Multi-Level and Interaction Authentication) framework, extended for multi-device authentication scenarios. Homomorphic encryption is employed to reduce verifications with asymmetric-key ciphers [7].

The technique enables interaction-based, multi-factor, and multi-level authentication in IoT environments. However, using homomorphic encryption may introduce computational overheads due to its complexity [7].

The authors used formal security verification tools like AVISPA to assess protocol correctness regarding authentication, confidentiality, and attack resilience. Work factor analysis was employed to evaluate the computational complexity of breaching security via brute force attacks [7].

3.8. Article 8

The article delves into an MFA based on homomorphic encryption for secure access to IoT devices. It highlights the necessity for robust authentication in IoT settings, where conventional methods often fall short in providing comprehensive protection [8].

The authors identify the pressing need for interaction-based, multi-factor, and multi-level authentication in IoT environments. They aim to tackle issues such as security breaches, authentication overhead, computational demands, and processing time [8].

The proposed solution revolves around the M2I (Multi-Factor Multi-Level and Interaction Authentication) framework, tailored to suit multi-device authentication scenarios in IoT. Also, the authors advocate for homomorphic encryption to streamline verifications, particularly with asymmetric-key ciphers [8]

The strength of the proposed technique lies in its capacity to support interaction-based, multifactor, and multi-level authentication in IoT environments. However, the use of homomorphic encryption could potentially introduce computational overheads due to its inherent complexity [8].

The authors employ formal security verification tools such as AVISPA (Automated Validation of Internet Security Protocols and Applications) to evaluate protocol correctness concerning authentication, confidentiality, and resilience to attacks. Furthermore, they conduct work factor analysis to gauge the computational complexity needed to breach security through brute force attacks [8].

3.9. Article 9

MFA is a security measure that includes using multiple factors of authentication to prove a user's identity. In healthcare and the IoT, MFA is important for protecting private details, such as patients' health data, and reducing the greater risk of cyber-attacks [9].

The problem statement in the article is the need to develop and apply effective MFA systems to improve security measures and protect sensitive information, especially in the healthcare and IoT areas. The current solutions of MFA on the Internet of Healthcare Things (IoHT) poorly identify the key security requirements of next-generation authentication apps [9].

The article suggests several solutions for MFA in the IoHT. These options are web authentication systems and biometric systems. These two systems respectively use public/private key cryptography and physical key devices to create and store private keys and biometric identification, such as fingerprint recognition, to improve security [9].

The strength of the suggested methods for MFA in the IoHT is improved security [9]. The suggested method provides stronger security features compared to standard password-based authentication. It combines factors like biometrics, physical keys, and encryption methods to protect against illegal entry.

The weakness of the suggested methods is implementation complexity [9]. Implementing the proposed techniques may take major technical knowledge and funding. Integrating new authentication methods into current systems can be difficult and may require changes to hardware and software.

The article does not clearly state the specific evaluation measures used by the writers to rate their suggested solutions for MFA in the IoHT. The authors may test the security efficiency of their suggested solutions by measuring their ability to protect against common cyber threats [9]. Factors like encryption power, resistance to threats, and the general reliability of the verification methods may have been considered by the authors as well.

3.10. Article 10

The article provides a brief background on the challenges of securing cross-domain device collaborations in the Industrial Internet of Things (IIoT) and proposes a protocol that uses MFA with blockchain technology to address these challenges.

The problem statement in the article is the need for a safe and efficient cross-domain device identification method in the Industrial Internet of Things (IIoT) [10]. The goal is to create a multi-factor authentication system that uses blockchain for cross-domain IIoT that achieves both high efficiency and privacy preservation while reducing on-chain storage overhead and solving the possible loss of factor attack.

There are three proposed solutions which are to design a multi-factor key derivation that is assisted by hardware via physically unclonable functions (PUFs), a novel cross-domain trust-building method by leveraging the on-chain dynamic accumulator to accumulate derived keys for IIoT devices with multiple factors and integrating the on-chain accumulator into cross-domain device authentication to efficiently verify the unlinkable identities of devices from different IIoT domains [10].

The strength of the suggested methods is enhanced security. By combining multi-factor authentication and blockchain technology, it provides a higher level of security for crossdomain

device authentication [10]. By using factors protection, hardware-assisted key derivation, and dynamic accumulators, attacks are prevented, and the authentication process's integrity is ensured. [10].

The weakness of the suggested methods is implementation complexity. The proposed technique involves the integration of multiple technologies, including multi-factor authentication, blockchain, and hardware-assisted key derivation [10]. Implementing and deploying such a complex system may require significant expertise and resources.

The authors used efficiency to assess their proposed solution. The efficiency of their protocol is evaluated by measuring the time cost of different authentication requests, including intradomain and cross-domain requests. They recorded the actual time cost of each request and analyzed the average time [10]. The stability of the request execution time was also considered.

Several other researchers have contributed to end-to-end security mechanisms, often collaborating with universities or industries to broaden implications [11-21]. For example, a research article proposes a new security scheme called 6-CMAS to address the security challenges in Cell-Free mMIMO (multiple-input multiple-output), a technology expected to be integrated into future 6G ultra-dense cellular networks [12]. The 6-CMAS scheme aims to provide a lightweight yet secure solution for authentication and communication in Cell-Free networks [12]. It utilizes a combination of cryptographic techniques, including ECC-based Diffie-Hellman (ECDH) for key agreement, timestamping, one-way hash functions, and the Blind-Fold Challenge scheme [12]. Additionally, it integrates blockchain technology with a Proof of Stake (POS) consensus mechanism to ensure data integrity, non-repudiation, and traceability [12]. The proposed scheme is designed to mitigate various security attacks, including spoofing, eavesdropping, user location privacy breaches, replay attacks, denial of service attacks, and man-in-the-middle (MITM) attacks [12]. It also aims to reduce authentication, communication, and computational overheads compared to existing authentication protocols [12]. These research articles can serve as a guideline for future young researchers in end-to-end security measures in sixth-generation (6G) networks. The proposed solution for the given problem statement is adopted from the following articles, which act as benchmarks for this research article: "Efficient and Privacy-Preserving Blockchain-Based Multifactor Device Authentication Protocol for Cross-Domain IIoT"[10] and "SELAMAT: A New Secure and Lightweight Multi-Factor Authentication Scheme for Cross-Platform Industrial IoT Systems (IIoT)" [6]. These foundational works provided critical insights and methodologies that guided the development of the QRF-MFA solution.

4 PROPOSED SOLUTION

The QRF-MFA method, which is a fusion of the solutions in the problem statement, namely the blockchain-based multifactor device authentication protocol and the SELAMAT lightweight multi-factor authentication scheme. With the integration of these parts, QRF-MFA increases safety and performance in IIoT surroundings. First, the lattice-based cryptographic technique is separately combined with state-of-the-art AES-ECC for key generation and encryption. This combination guarantees the system is resistant to current as well as future attacks, especially the ones from quantum computing, as corroborated in [6], [10].

It uses Physically Unclonable Functions (PUFs) for secure key derivation and storage. They are referred to as PUFs because they produce keys that stem from the physical characteristics of the device hardware, and this improves security as the keys are dependent on the hardware, not to mention that they are tamper and clone-resistant [10].

It also uses a federated identity management system to deploy a decentralized system for secure and seamless authentication among different IIoT domains. This system enhances scalability and trust, mitigates single points of failure, and facilitates seamless cross-domain authentication [6].

It also includes a blockchain-based dynamic accumulator for the identification and proofing of device identities over domains. This leads to immutable and transparent identity management built on the blockchain, saving vastly on throughput costs and on-chain storage overhead, while now being private [10].

This section presents the implementation of a simplified protocol, suitable for lightweight, resource-constrained IIoT devices aimed at securing communication. It guarantees secure session management, mutual authentication, and encrypted data traffic without much overhead which makes CoAP very well suited for the restricted environments in which IIoT devices operate [6].

Finally, the scheme is designed to be able to be integrated with fog and edge computing environments as well. It can support offloading part of computation and storage to nearby fog nodes, which minimizes latency and improves real-time capacity needed for IIoT applications [6].

In the registration phase, devices create a unique key pair based on strong PUFs with minimal side-channel leakage. This public key is lodged in blockchain, and the private key is within hardware of the due device actively. It also generates a unique identifier for the device that is linked to this key pair. Then, during the authentication phase, the device combines this identifier with a challenge-response generated using the PUF-based private key. The verifier

will then crosscheck this response with the public key, that is stored on the blockchain. With the help of the Federated Identity Management system, we can get cross-domain authentication, where trust is maintained between different domains. The latter is the mechanism for setting up a secure session following a successful authentication in combination of a hybrid cryptographic scheme. The protocol is designed to be lightweight and ensures secure data exchange with low overheads making it ideal for even resource-constrained IIoT devices. This will allow computational tasks and data storage to be offloaded to nearby fog nodes, making it more efficient and real-time.

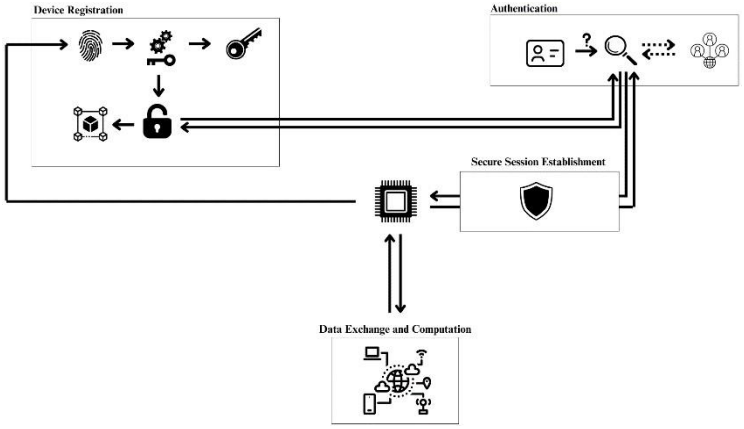

Figure 2. Diagram of QRF-MFA

5 RESULTS AND ANALYSIS

The QRF-MFA scheme offers superior solutions to the problem statements in existing approaches. In conclusion, it provides an effective cross-domain device identity solution to support the described multifactor device authentication for the blockchain-based IoT and integrates the hybrid cryptographic approach and advanced PUFs to secure and fasten the processing in the IoT blockchain network. The blockchain-based dynamic accumulator and federated identity management system support efficient and scalable cross-domain trust establishment and verification while reducing on-chain storage overhead and factor loss prevention [10].

Secure Lightweight Autonomous Multifactor Authentication (SELAMAT) is a secure and efficient multi-factor authentication scheme designed for integration with fog computing environments. The proposed protocol takes that one step further, by significantly minimizing the communication and computation cost constraints of IoT devices, all the while maintaining the secure communication properties and mutual authentication [6].

The improvements of QRF-MFA are significant. Quantum resistance hardens the system against future quantum threats, thereby securing the system over the long run. Advanced PUFs

can provide hardware-tied, tamper-resistant key derivation and storage, improving both the uniqueness of device keys and overall security. Using a federated identity management system provides decentralized cross-domain identity management allowing greater scalability, more trust, and less single points of failure. This is integrated with a technology that benefits from all the clarity which blockchain provides, along with its inexorable audibility and its finality and efficiency, while removing the on-chain storage overhead. Finally, optimization for fog and edge computing environments, which is important for the IIoT, lowers latency and improves real-time processing capabilities.

Table 1 Results and Analysis: Comparison of IIoT Authentication Approaches Approach

Approach	Strengths	Weaknesses	Key Findings
SELAMAT	Secure key management, secure communication, reduced communication and computation costs	Vulnerable to server spoofing and DoS attacks, increased computational effort due to identity-based cryptography	Suitable for resourceconstrained devices but lacks quantum resistance and robust cross-domain trust mechanisms.
Blockchainbased	Enhanced security, factor loss prevention, reduced on-chain storage overhead, efficient cross-domain trust	Implementation complexity, requires significant expertise and resources	Offers strong security and cross-domain trust but may face challenges in real-world IIoT deployments due to complexity
QRF-MFA	Quantum resistance, hardware-tied key security, decentralized cross-domain identity, fog/edge optimization	Implementation complexity, potential for resource constraints on some devices	Shows the most promise in terms of security, efficiency, and scalability, but requires further research and optimization for real-world use.

The comparison of SELAMAT, the blockchain-based approach, and QRF-MFA reveals the disadvantages and advantages of different strategies for securing IIoT device authentication. While SELAMAT prioritizes lightweight design and cost reduction, it may not be suitable for scenarios requiring robust cross-domain trust or quantum resistance. The blockchain-based approach offers enhanced security and cross-domain trust but faces challenges in implementation complexity. QRF-MFA, by incorporating elements from both approaches, presents a more comprehensive solution that addresses both security and efficiency concerns.

6 CONCLUSION

The proposed solution, Quantum-Resilient Federated Multi-Factor Authentication (QRFMFA) mechanism, provides a robust, future-proof, and efficient approach specifically

designed for Industrial Internet of Things (IIoT) environments. By integrating quantum-resistant cryptography, the solution ensures that the system remains secure against the advanced computational threats posed by emerging quantum technologies. The incorporation of advanced Physically Unclonable Functions (PUFs) adds an extra layer of security by leveraging unique, unclonable physical characteristics of devices, making it nearly impossible to replicate or forge device identities. Furthermore, decentralized identity management distributes the verification process across multiple nodes, eliminating single points of failure and enhancing the resilience of the authentication framework.

Blockchain technology is utilized to provide a tamper-proof ledger for recording authentication events and transactions, ensuring transparency and integrity. Optimized communication protocols are designed to minimize latency and maximize efficiency, crucial for the seamless operation of IIoT systems that require real-time data exchange. This comprehensive solution addresses the unique needs and characteristics of IIoT, proposing an integrated framework that ensures secure device authentication and reliable communication across different fields and domains. By combining these advanced technologies, the QRF-MFA mechanism not only enhances security and privacy but also ensures scalability and efficiency, making it an ideal solution for the dynamic and complex landscape of IIoT environments.

7 ACKNOWLEDGEMENT

This research work is the result of a class project for the Computer Security course at the Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak.

REFERENCES

[1] Abubakar, M., Jaroucheh, Z., Al Dubai, A., & Liu, X. (2022). A Lightweight and User-centric Two-factor Authentication Mechanism for IoT Based on Blockchain and Smart Contract. In *Proceedings - 2022 2nd International Conference of Smart Systems and Emerging Technologies, SMARTTECH 2022* (pp. 91–96). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SMARTTECH54121.2022.00032

[2] Alanazi, M., & Aborokbah, M. (2022). Multifactor Authentication Approach on Internet of Things: Children's Toys. In *Proceedings of 2022 2nd International Conference on Computing and Information Technology, ICCIT 2022* (pp. 6–9). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCIT52419.2022.9711596

[3] Aljanah, S., Zhang, N., & Tay, S. W. (n.d.). A Multi-factor Homomorphic Encryption Based Method for Authenticated Access to IoT Devices.

[4] Alnahari, W., & Quasim, M. T. (2021). Authentication of IoT Device and IoT Server Using Security Key. In *2021 International Congress of Advanced Technology and Engineering, ICOTEN 2021*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICOTEN52080.2021.9493492

[5] Alshahrani, M. M. (2021). Secure Multifactor Remote Access User Authentication Framework for IoT Networks. *Computers, Materials and Continua*, *68*(3), 3235–3254. https://doi.org/10.32604/cmc.2021.015310

[6] Fauzi, A. H., & Khan, A. S. (2017). Threats Advancement in Primary User Emulation Attack and Spectrum Sensing Data Falsification (SSDF) Attack in Cognitive Radio Network (CRN) for 5G Wireless Network Environment. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *9*(2-10), 179-183.

[7] Institute of Electrical and Electronics Engineers. (2019). *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall): Proceedings: Honolulu, Hawaii, USA, 22-25 September 2019*.

[8] 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), 1–32. https://doi.org/10.3390/s21041428

[9] Khan, A. S., Abdullah, J., Zen, K., & Tarmizi, S. (2017). Secure and Scalable Group Rekeying for Mobile Multihop Relay Network. *Advanced Science Letters*, *23*(6), 5242-5245.

[10] Khan, A. S., Halikul, I., & Abdullah, N. F. J. (2015). Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks. *Jurnal Teknologi*, *73*(1), 75-81.

[11] Khan, A. S., Javed, Y., Abdullah, J., Nazim, J. M., & Khan, N. (2017). Security Issues in 5G Device to Device Communication. *IJCSNS*, *17*(5), 366.

[12] Khan, A. S., Mehdi, M. H., Uddin, R., Abbasi, A. R., & Nisar, K. (2023). Ensemble Based Automotive Paint Surface Defect Detection Augmented by Order Statistics Filtering Using Machine Learning. *Authorea Preprints*.

[13] Khan, A. S., Yahya, M. I. B., Zen, K. B., Abdullah, J. B., Rashid, R. B. A., Javed, Y., Khan, N. A., & Mostafa, A. M. (2023). Blockchain-Based Lightweight Multifactor Authentication for Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Network. *IEEE Access*, *11*, 20524-20541.

[14] Khan, N., Abdullah, J., & Khan, A. S. (2017). Defending Malicious Script Attacks Using Machine Learning Classifiers. *Wireless Communications and Mobile Computing*, *2017*.

[15] Khan, S., Abdullah, J., Khan, N., Julahi, A. A., & Tarmizi, S. (2017). Quantum-Elliptic Curve Cryptography for Multihop Communication in 5G Networks. *International Journal of Computer Science and Network Security (IJCSNS)*, *17*(5), 357-365.

[16] Odyuo, N., Lodh, S., & Walling, S. (2023). Multifactor Mutual Authentication of IoT Devices and Server. In *Proceedings - 5th International Conference on Smart Systems and Inventive Technology, ICSSIT 2023* (pp. 391–396). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICSSIT55814.2023.10061113

[17] Shoaib, M., Ullah, A., Abbasi, I. A., Algarni, F., & Khan, A. S. (2023). Augmenting the Robustness and Efficiency of Violence Detection Systems for Surveillance and Non-Surveillance Scenarios. *IEEE Access*, *11*, 123295-123313.

[18] Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A Review of Multi-factor Authentication in the Internet of Healthcare Things. *Digital Health*, *9*. SAGE Publications Inc. https://doi.org/10.1177/20552076231177144

[19] Zen, K., Javed, M., Lenando, H. B., Zen, H., & Khan, A. S. (2015). Intelligent Coordinator Selection Mechanism (ICSM) for IEEE 802.15.4 Beacon-Enabled MAC Protocol in Mobile Wireless Sensor Networks. *International Review on Computers and Software*, *10*(2), 164.

[20] Zhang, Y., Li, B., Wu, J., Liu, B., Chen, R., & Chang, J. (2022). Efficient and Privacy-Preserving Blockchain-Based Multifactor Device Authentication Protocol for Cross-

Domain IIoT. *IEEE Internet of Things Journal*, *9*(22), 22501–22515. https://doi.org/10.1109/JIOT.2022.3176192

[21] Zubair, S., Fisal, N., Abazeed, M. B., Salihu, B. A., & Khan, A. S. (2015). Lightweight Distributed Geographical: A Lightweight Distributed Protocol for Virtual Clustering in Geographical Forwarding Cognitive Radio Sensor Networks. *International Journal of Communication Systems*, *28*(1), 1-18.