Pioneering Blockchain Assisted Authentication Frameworks for the Industrial Internet of Things

[1*]Derrick Jia Yung Koay, [2]Jin Ming Neoh, [3]Jia Hou Tan, [4]Zhi Hong Teh, [5]Yu Heng Liew and [6]Hashin Elshafie

[1,2,3,4,5]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia
[6]Department of Engineering, College of Computer Science, King Khalid University, Main Campus Al Farah Abha 61421, Kingdom of Saudi Arabia KSA.

email: [1*]74596@siswa.unimas.my, [2]76012@siswa.unimas.my, [3]76946@siswa.unimas.my, [4]76975@siswa.unimas.my, [5]77313@siswa.unimas.my, [6]helshafie@kku.edu.sa

**Corresponding author*

Received: 17 July 2024 | Accepted: 02 October 2024 | Early access: 30 October 2024

Abstract - *In the rapidly evolving landscape of technology, integrating blockchain with Industrial Internet of Things (IIoT) presents a groundbreaking synergy with transformative potential. This paper addresses key security challenges in IIoT environments by proposing a novel authentication mechanism for Industrial Internet of Things (IIoT) systems that enhances security by integrating Quantum-Elliptic Curve Cryptography (QECC) and a blockchain-regulated, automatic key refreshment mechanism. Building on the ECC-based Diffie-Hellman protocol, our approach addresses vulnerabilities such as Man-in-the-Middle (MITM) attacks by combining quantum cryptography with ECC to detect eavesdroppers and secure communications between Base Stations (BS), Relay Stations (RS), and Subscriber Stations (SS). The blockchain-regulated mechanism ensures periodic and verifiable key updates, enhancing key management against MAC layer and spoofing attacks. This integrated framework significantly improves the security of IIoT systems by ensuring confidentiality, integrity, availability, authenticity, and non-repudiation, offering a robust solution for secure data transmission in IIoT environments.*

Keywords: Blockchain, IIoT, Key Refreshment, QECC, spoofing.

1 Introduction

In the rapidly evolving landscape of technology, the marriage of blockchain technology and Industrial Internet of Things (IIoT) has emerged as a groundbreaking synergy with transformative potential.

Blockchain is a system that utilizes a decentralized and dispersed network to transcribe transaction (Liu et al, 2024). It is made up of several interconnected inscribed transactions to assemble a chain of blocks. Decentralization of records discourages the need for mediator entities, such as banks or third-party institutions, ensuring transparency, immutability, and security of data.

On the other hand, IoT encompasses a vast ecosystem of interconnected devices, ranging from smartphones and wearable gadgets to industrial sensors and smart appliances (Wang et al., 2021). These devices collect and exchange data autonomously, enabling seamless communication and automation in various domains, including healthcare, transportation, agriculture, and manufacturing (Mishra et al., 2023).

When combined, blockchain and IoT create a powerful symbiosis that addresses several critical challenges in the IoT applications. Traditional IoT networks often grapple with issues such as data security, privacy concerns, data integrity, and interoperability (F. Wang et al., 2024). Blockchain technology provides new and innovative solutions to these endeavors by providing a tamper-resistant and transparent framework for managing IoT data.

Figure 1 shows a model of a generic blockchain-assisted authentication for IoT. The model consists of two type of nodes which are validation and orderer nodes respectively. The ledger, blockchain and smart contracts are installed in each node. The nodes are responsible to validate new blocks validity before it is added into the blockchain. The nodes receive IoT's transaction proposals, executing smart contracts, endorsing results and return as proposal responses to the respective IoTs. Orderer nodes then package them in new blocks following a certain order.

Based on the related works outlined in section III, the problem statements identified are that IIoT systems are increasingly becoming targets for cyber-attacks, highlighting a significant challenge in enhancing their security measures. In addition, current authentication protocols in IIoT systems face reliability and privacy issues, which compromise their effectiveness and adaptability to future threats. Moreover, the trustworthiness of these authentication systems is under constant scrutiny due to vulnerabilities that can be exploited, undermining user confidence and the overall integrity of IIoT networks.

To address the first problem statement pertaining to the security of IIoT systems, a reliable mechanism which helps in regularly refreshing keys must be implemented by leveraging blockchain technology to provide accountability and mitigate possible security breaches (Mishra et al., 2023).

Moving on, it is imperative for IIoT environments to have strong reliability and privacy of authentication. As such, a decentralized authentication scheme is needed to mitigate single points of failure and susceptibility to various attacks, whilst also reducing maintenance overheads and system complexities as a decentralized scheme introduces more redundant points to confuse potential attackers (Liu et al, 2024). To further enhance this, the current over-reliance on the 40-year-old RSA encryption system leaves current systems with vulnerabilities. A new encryption framework needs to be proposed to provide the necessary privacy and protection from future threats.

Furthermore, with the majority of the web utilizing some form of single-factor authentication (SFA) or multi-factor authentication (MFA), authentication services are in peril of tamper attacks from external or internal forces. To resolve this, blockchain-based authentication can be introduced to enable tamper-proof audit trails with immutable records to increase trustworthiness of security assets and logs.

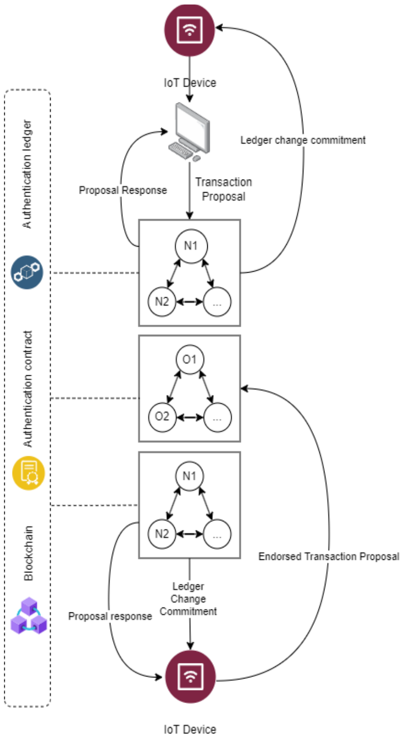

Figure 1: Generic model of blockchain-assisted authentication mechanism for IoT

2 Related Works

This section summarizes 10 articles which are relevant to authentication mechanisms using blockchain technology on Industrial Internet of Things (IIoT). Each article begins with a brief background followed by a problem statement. Additionally, a proposed solution is highlighted to address the problem statement, alongside its strengths and weaknesses. To conclude each summary, we touch upon the respective authors' evaluation metrics used in their assessment.

High-speed railroads (HSR) are rapidly integrating smart technology based on the continued development of railways (LTE-R) mobile communication to connect with control centers (Liu et al, 2024). However, LTE-R adheres to the Evolved Packet System-Authentication and Key Agreement (EPS-AKA), a protocol that has shown multiple security vulnerabilities in recent years. These vulnerabilities include key leakage, susceptibility to privileged user attacks, and significant authentication delays. To mitigate the aforementioned problems, researchers propose a novel approach; a reliable and secure access authentication method for LTE-R that leverages blockchain technology and integrates the secgear framework for privacy protection. This proposal capitalizes on blockchain's decentralized nature, effectively removing the vulnerability of a single point of failure. The secgear framework further enhances privacy by providing robust protection measures. The proposed scheme also introduces a phase for handover authentication and another for password changes, augmenting LTE-R access authentication with additional security attributes. Analysis of security and simulation experiments show that the approach ensures privacy protection with acceptable efficiency. However, it is essential to note that the proposed technique may not be future-proof against unknown attacks. The evaluation metrics used include formal security analysis using tools like ROR and AVISPA, as well as informal security analysis.

The Industrial Internet of Things (IIoT) has witnessed exponential growth, resulting in a massive network of interconnected physical and virtual objects. These objects, ranging from sensors to digital tickets, exchange data collected from their surrounding environment. With the proliferation of IIoT devices, a substantial amount of data is transmitted between heterogeneous sensors and devices at an unprecedented rate. However, this surge in data exchange also increases the risk of security threats, such as eavesdropping and hijacking attacks during communication channels. To address these concerns, certificateless signature (CLS) protocols have gained popularity. These protocols leverage the Schnorr signature mechanism and are designed for resource-constrained IIoT environments (Wang et al., 2021). Unlike traditional public key infrastructure (PKI) schemes, CLS avoids the need for a central Key Generation Center (KGC) responsible for certificate management. However, existing CLS schemes still face security vulnerabilities, such as those posed by KGC compromised, man-in-the-middle (MITM), and distributed denial of service (DDoS) attacks. To enhance security and reduce costs, this paper proposes a novel approach: a pairing-free CLS scheme that leverages blockchain technology and smart contracts. By transforming the KGC logic into smart contract code, the proposed solution achieves decentralization and mitigates DDoS attacks. Formal and informal security analyses, along with performance evaluations, demonstrate that this design offers more reliable security assurance with reduced computation and communication costs compared to other CLS schemes. The evaluation metrics used are computation cost and communication cost

To fortify the integrity of an IoT system, the periodic renewal of cryptographic keys is essential. This process, a cornerstone of robust key management, involves the systematic update of cryptographic keys to maintain stringent security measures. However, this vital practice is often disregarded, with many network operators bypassing the crucial step of refreshing session keys due to a lack of regular maintenance or a robust auditing mechanism (Mishra et al., 2023). Addressing this gap, the proposed blockchain-regulated key refreshment scheme leverages a distributed ledger technology to enhance security. Its primary advantage lies in its ability to prevent adversaries from deducing previous session keys, even if they manage to access a current key, thereby bolstering the system's defense against security breaches. Nevertheless, the scheme is not without its challenges; scalability issues arise as the volume of data processed and stored on the blockchain grows, potentially leading to slower transaction rates2. To validate the efficacy of this solution, the authors have conducted a comprehensive evaluation across three distinct experimental setups: an Ethereum-based setup, a Hyperledger Fabric-based setup, and a non-blockchain MongoDB setup. The performance of these systems was meticulously assessed through various metrics, including cost computation and scalability, to determine their effectiveness in real-world applications.

In the realm of industrial production, the integration of smart devices (SDs) and the adoption of new technologies have become a common practice. This integration is primarily aimed at enhancing production efficiency and reducing the overall cost of production. As part of the production process, data generated by these SDs are shared across various platforms. This sharing of data is instrumental in optimizing decision-making processes. However, it also presents challenges regarding security and efficiency because of the inherent nature of data sharing. The sharing process exposes large volumes of data to an open network. This exposure can potentially harm industrial departments that are particularly concerned about privacy issues. To address these challenges, a method has been suggested. This method is a low-complexity, high-security data-sharing strategy that is based on the concept of proxy re-encryption (F. Wang et al., 2024). The strength of this method lies in its ability to efficiently oversee shared data while also maintaining a low computational cost. The suggested method offers a robust solution to secure data exchange amongst SDs. It does so by significantly reducing the computational and storage overhead typically associated with blockchain technology. This reduction in overhead is a key feature of the suggested method, making it a viable solution for data security in industrial production. To gain access to this suggested security solution, an adversarial-challenger game, known as the "ciphertext indistinguishability game", was established. This game serves as a mechanism to test the robustness of the security solution. Furthermore, a performance assessment was conducted to evaluate the effectiveness of the proposed approach. During this evaluation, the time required for the SD to encrypt data and sign ciphertext was calculated. These calculations were then compared with other similar schemes to determine the effectiveness and efficiency of the suggested method.

IIoT is an open and scalable platform for exchanging data amongst industrial devices in both local and global operations, providing significant opportunities and contributing to Industry 4.0 innovation. However, the security and privacy of data within industrial IoT applications depend heavily on the users' reliability, established through user authentication - a generally employed method for ensuring security (X. Wang et al., 2021). Therefore, the current user authentication systems within industrial IoT face challenges such as single-factor authentication and limited adaptability to accommodate the increasing number and diverse categories of users. Addressing these issues, this article introduces another form of validation solution called ATLB (Authentication Mechanism based on Transfer Learning empowered Blockchain), utilizing blockchain technology and transfer learning. Specifically, ATLB begins by training the user authentication model for the specific region using a guided deep deterministic policy gradient technique. Then, this model is applied locally for authenticating foreign users or transmitted across regions to authenticate users in other areas, thereby significantly reducing the model training time. The strength of ATLB is that it can ensure precise authorizations whilst also attaining superior throughput and minimal latency. Contrarily, the implementation of ATLB may introduce complexity in system design and maintenance. The authors evaluate the solution regarding system throughput, transaction latency, and authentication accuracy.

Industry 4.0 utilizes computing technologies including mobile, IoT, edge computing, embedded software, and virtualization to automate industrial processes. IoT devices are interconnected through a cyber-physical system, which includes both physical and digital entities. It has the potential to revolutionize computing by enabling predictive maintenance for data-intensive applications. Every program includes unique smart intelligence characteristics, including practical and analytical tools for identifying data-driven policies. Despite the chain of interconnected IoT devices, they rely on a centralized hub for authentication and are thus vulnerable to single points of failure (SPOF) (Deebak et al., 2023). This centralization creates a significant risk, as the failure of the central hub can compromise the entire network, leading to potential downtime, security breaches, and loss of critical data. The problem statement now becomes the implementation of a decentralized authentication scheme that is scalable for IOT Applications. Hence, the paper proposes a trust-aware blockchain-based seamless authentication mechanism that preserves privacy (TAB-SAPP) for IoT applications. By splitting the authentication process among numerous nodes, the system may keep operating even when one or more of them fail, thereby significantly reducing the possibility of a complete network shutdown. The positives of utilizing TAB-SAPP are better data traffic analysis and organization, lightweight computational overhead, and reliability in high packet delivery ratio. Additionally, using lightweight crypto operations like one-way hashing and bitwise XOR can reduce costs for computation and communication. However, the TAB-SAPP scheme is not without its drawbacks. It entails a complex system model with several stakeholders and transactions for authentication and maintenance issues due to the complexity of the structure. This complexity can result in increased difficulties in managing and troubleshooting the network, potentially leading to higher maintenance costs and longer downtimes. The evaluation metrics used are computation, the speed of mobility, communication, and packet delivery ratio.

Whilst 5G is still being implemented these days, experts have focused on the transition from 5G to 6G. The high network traffic in this period necessitates the adoption of 6G technology, which will prioritize consumers, mobile devices, service suppliers, and operators of networks, as essential enablers in the environment. The Cell-Free massive Multiple Input Multiple Output (mMIMO) technology has been integrated into future 6G networks is inevitable, acknowledging that the era of 6G technology is just around the corner. This technology ensures seamless connectivity and low-latency services. However, its dynamic nature in highly distributed, high-mobility, and frequent data interchange systems offers issues for authentication protocols and secure communication, including high overhead and costs. To address these challenges, a lightweight multifactor authentication protocol with the ECC-based Deffie Hellman (ECDH) is proposed (Khan et al., 2023). It incorporates timestamping, hash functions, a Blind-Fold Challenge scheme, and technology of blockchain with the proof of stake (POS) consensus for integrity, non-repudiation, and traceability. This solution enables an authorized user to connect to smart industrial equipment to retrieve real-time data using a verified session key. Content servers facilitate mutual authentication and key agreements between users and smart industrial devices. Therefore, it helps to mitigate a myriad of security attacks, which includes replay, spoofing, man-in-the-middle (MITM) attacks, and denial of service (DoS), alongside eavesdropping and user location privacy issues, while also reducing authentication, communication, and computational overhead significantly compared to baseline protocols. The metrics used to evaluate the proposed protocol include communication cost, computational cost, and authentication overhead.

The rapid growth of IoT applications enabled by 5G networks leads to increasingly complex multidomain environments. Within these environments, the need for greater consideration for interdomain authorization and authentication (A&A), combined with the deployment of disparate intradomain A&A mechanisms, leads to significant domain compatibility as well as challenges (Tong et al., 2023). Therefore, a blockchain-assisted intra/inter-domain A&A method for IoT is proposed. This protocol first combined a mutual access control based on a contract to establish secure access between domains, followed by a safe and privacy-preserving authentication protocol using adapted one-out-of-many-proof approaches which allows for efficient and secure verification processes. and a mechanism based on voting to employ a threshold-based cryptosystem. The proposed scheme effectively achieves domain interoperability by providing a secure method for various authentication and authorization methods to grant access between domains. Additionally, it ensure the protection of devices and domains while allowing legitimate audits of threatening devices operating outside the domain. This method is well-suited for IoT devices with limited resources due to its low on-device authentication cost, which remains unaffected by the complexities of the authentication procedures. With a flexible and generic solution, it is readily implemented in IoT applications with different domains which can improve security and compatibility. It ensures security features like domain interoperability (DI), protection of privacy, and accountability. The metrics used to evaluate the proposed protocol include computation cost, communication, storage, and system deployment overheads. These metrics provide a thorough assessment of the protocol's performance and its suitability for complex IoT environments.

Industrial Big Data is essential to the Industrial Internet of Things (IIoT), powering several intelligent applications through exchange of data and computing. By incorporating 5G communication and mobile edge computing, industrial applications may reduce their computational and communication costs. Nowadays, organizations are increasingly hesitant to share sensitive data due to privacy concerns, which hinders collaborative computation efforts essential for optimizing industrial processes (Yang et al., 2022). To address this, there is a pressing need for secure and privacy-preserving methods of data sharing and joint computation. Hence, the proposed scheme integrates blockchain technology to enable privacy preservation and public audibility in multiparty computation, whilst utilizing noninteractive zero-knowledge proofs. It provides privacy protection and public access by segregating data ownership, use, and verification, ensuring data confidentiality while allowing for transparent verification. The use of blockchain technology improves the traceability of illegal data and computation behavior, whereas noninteractive zero-knowledge proof strengthens security by allowing the public validation of consistent data and computational validity. However, this solution requires multiple rounds of connection, and data supplied by participants who lack mutual trust cannot undergo public verification and objectively. Individual participants are typically hesitant to deliver sensitive information, whether in plaintext or ciphertext, preventing leakage of information during the computation procedure. This issue must also be solved through the suggested strategy. The metrics used to evaluate the proposed protocol include the communication overhead and computation latency in the oblivious transfer process.

Industrial 4.0 incorporates the Internet, cloud computing, big data, IIoT, and other advanced technologies. Industry 4.0 relies on information physical network, connecting the physical devices to internet. When hundreds of IoT devices connect, IIoT systems are needed to safeguard important applications and prevent unwanted access to data and functionalities. Therefore, this paper highlights the importance of devices connecting to the internet to enhance productivity (Zhang et al., 2024). However, IoT systems that rely on many devices connecting suffer from security and performance challenges in distributed scenarios. The question evolves to how we implement a certification system that has low costs for large-scaling IOT systems. Enter the proposed solution of a Three-Layer System that is based on Blockchain with Fast Consensus Verification Based on VRF (Verifiable Random Function). The benefit of VRF is it improves scalability by randomly selecting block generators to form a consensus of new devices joining the network among smaller committee of devices which reduces computational burden nodes. Nevertheless, the weaknesses of the solution are that it relies on the trustworthiness of the voting committee and randomness of VRF that can be manipulated alongside its complex implementation of the mechanism that may increase maintenance overhead. The evaluation metrics used are Blockchain TPS

(Transactions Packed in the Block Per Second) and communication cost, fault tolerance, and security performance.

Several other researchers have also contributed in end-to-end security mechanism even with the assistance of the counter partners i.e. universities or industries for broaden implications. This research article can act as the guidelines for future young researchers in end-to-end security measures in 6th generation networks. This improved work, elaborated in Proposed Solution, for the given problem statement is adopted from (Mishra et al., 2023; Khan et al., 2023; Khan et al., 2017), which act as a benchmark for this research article.

3 Proposed Solution

Our proposed solution addresses the problem statements outlined in section II and enhances the authentication mechanism discussed in Khan et al. (2023) by implementing Quantum-Elliptic Curve Cryptography (QECC) in conjunction with a blockchain-regulated, verifiable, and automatic key refreshment mechanism. While Khan et al. (2023) proposed an ECC-based Diffie-Hellman (ECDH) solution, our approach builds upon this by incorporating quantum cryptography, thereby adding an additional layer of security. Recognizing the critical role of key refreshment in key management, we introduce a secure, blockchain-regulated method for automatic key refreshment, ensuring robust and reliable key management in IoT systems. This combination of QECC and blockchain technology provides a comprehensive and resilient framework for enhancing the security of IIoT communications.

Transmission of messages across IIoT networks are highly susceptible to security breaches, especially in the context of insecure multi-hop relay communications. The ECDH-based authentication protocol addresses these breaches, but sole reliance on ECC cryptography leaves it vulnerable to Man-in-the-Middle (MITM) attacks. To address these vulnerabilities, our solution integrates Quantum Cryptography (QC) with ECC, leveraging the strengths of both. QC can mitigate MITM attacks by detecting eavesdroppers due to quantum mechanics of the quantum channels. While ECC encrypts the plaintext message to be transmitted with encryption algorithm (Khan et al., 2017).

In QECC, QC is employed between Base Stations (BS) and Relay Stations (RS), while ECC is used between BS and Subscriber Stations (SS) or RS and SS. QC generates a shared secret key between BS and RS. To ensure data integrity, ECC uses this shared key in conjunction with a private key to perform several functions: Key Agreement (KA), Key Derivation Function (KDF), Encryption (ENC), Message Authentication Code (MAC), and Hash (HASH). KA generates a shared secret using the private key derived from QC and the SS's public key. KDF processes this shared secret to produce encryption and MAC keys, while the MAC function generates a tag to ensure message authenticity. The cryptogram includes the public key, encrypted message, and tag. The SS calculates the shared secret from its private key and the received public key from the cryptogram, deriving the encryption and MAC keys, and verifies the tag against a newly computed one. If the tags match, the encryption key decrypts the ciphertext to recover the original plaintext message (Khan et al., 2017).

By employing QECC, data and messages transmitted through IIoT relay communications are securely encrypted. Given the crucial role keys play in securing these transmissions, an additional mechanism must be implemented to manage them effectively. Although the current Privacy Key Management (PKM) protocol is proposed to uphold security in MMR networks, it remains vulnerable to several Medium Access Control (MAC) layer attacks, as well as spoofing attacks where eavesdropper disguises themselves within the network. Therefore, to further bolster this security, we propose the integration of a blockchain-regulated, verifiable, and automatic key refreshment mechanism adopted from (Mishra et al., 2023). This protocol manages cryptographic keys with enhanced robustness, addressing vulnerabilities in the current PKM protocols.

The key refreshment mechanism involves a blockchain-regulated process to ensure security keys used in IoT devices are regularly updated, maintaining the integrity and trustworthiness of the IoT system. This mechanism leverages blockchain technology and smart contracts to enforce and verify key updates automatically and transparently. The process begins with the initialization and registration of devices on the blockchain, followed by the network server communicating with devices to perform key updates, logged, and verified on the blockchain. This ensures all parties can trust the system as key refreshment rules are immutably recorded and updates are verifiable by users. Designed to be lightweight for IoT devices, the mechanism has been analyzed for cost, scalability, and security, demonstrating its economic viability and robust security. It offers advantages such as protection against potential security leaks and public verifiability, contributing to a more secure and trustworthy IoT environment.

Our proposed solution's system architecture shown in Figure 2. describes a blockchain network integrated with a network of IoT communicative devices and automatic key refreshment mechanism. The blockchain-regulated IoT devices and key refreshment mechanism work in tandem together with QECC to mitigate any potential security breaches. By comprehensively addressing both authentication and key management, the proposed solution provides a robust framework for secure and efficient data transmission in IIoT environments. Further detailed results and analysis on authentication and key management mechanisms will be provided in Implementation and Discussion, demonstrating the efficacy and resilience of the enhanced protocol (Mishra et al., 2023).

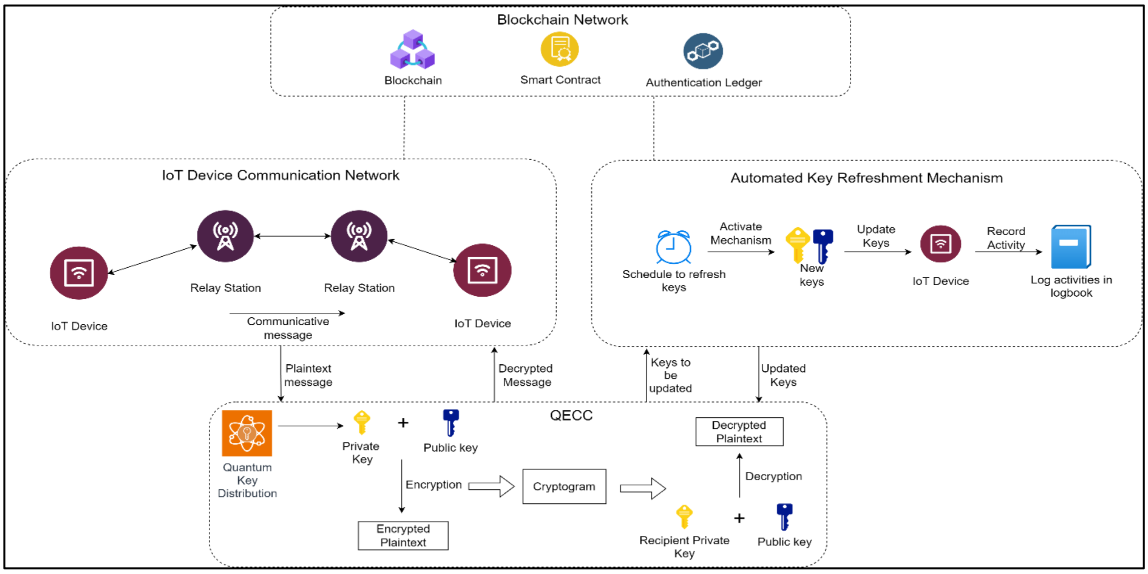

Figure 2: Framework of proposed solution by integrating Quantum Cryptography (QC) and Automated Key Refreshment leveraging blockchain

4 Implementation and Discussion

As mentioned previously in the proposed solution section, the implementation of the blockchain-based lightweight multifactor authentication framework adapted from Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Networks) in conjunction with a blockchain-regulated, verifiable, and automatic key refreshment mechanism that incorporates QECC seeks to improve the security of the overall framework. As such, it aligns in solving the problem statements of enhancing IIOT systems and addressing the challenges of single-factor authentication and limited adaptability in IoT applications.

To further prove the effectiveness and efficacy of the proposed solution framework, the current section will delve deeper into the details of QECC and the blockchain-based lightweight multifactor authentication framework adapted from Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Networks and their comparisons to other systems that share similar components.

4.1 Quantum Cryptography

The "Q" in QECC is the Quantum part of the cryptography system. The proposal of QECC effectively allows for a SS or in this case, a customer device to detect the presence of an eavesdropper with a relatively shorter key and retaining the same level of security in Rivest-Shamir-Adleman (RSA) Cryptography. The magic behind it is the Quantum Key Distribution (QKD) with BB84 protocol of deriving a complex key instead of a complex process of encryption and decryption. QKD employs two types of channels (Khan et al., 2017):

- Public channel
    - Communication of handshaking protocols between stations.
    - Transmission of encrypted messages
- Quantum channel
    - Specializes in the transmission of shared key in polarized bits (Qubits).

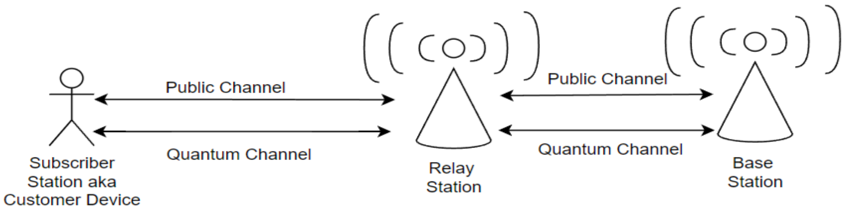

Figure 3: Implementation scenario of Quantum Channel and Public Channel between SS to RS to BS courtesy of [17]

The QKD transmitter is basically implied to be a modified version of a fiber optic cable that is capable of polarizing and preserving the quantum states of its photons. Therefore, enabling the following steps to be done to secure the transmitting Quantum Channel, summarized into 4 clusters of actions:

- Performing QKD from BS to RS
- Measuring Photons from BS
- Relaying the upcoming message
- Measuring the Photons from RS.

Steps for Performing QKD from BS to RS:

i. Bit Generation: BS generates a random string of bits, α = [0 1 1 0 1 0 0 1].

ii. Bit Polarization: The QKD transmitter at BS polarizes these bits into qubits using either Rectilinear or Diagonal Basis, resulting in β = [+ + × + × × × +].

iii. Polarized Qubits: This produces polarized qubits, p = [| - \ | \ / / -].

iv. Transmission: The qubits p is transmitted through the quantum channel to RS1.

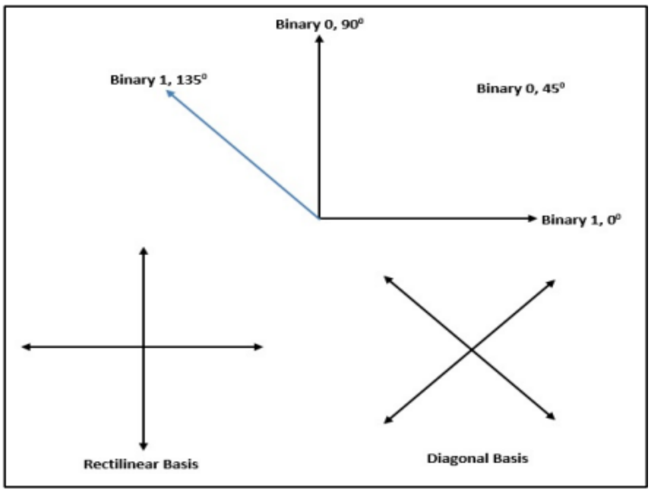

Figure 4: Polarizing Filters courtesy of Khan et al. (2017)

Steps for RS to Measure Photons from BS:

v. Random Basis Generation: RS1 generates a random basis, β’ = [+ × × × + × + +], to measure incoming photons.

vi. Photon Measurement: The qubits p pass through β’, resulting in new polarized qubits, p’ = [| / \ / - / - -], and corresponding bits α’ = [0 0 1 0 1 0 1 1].

vii. Basis Comparison: RS1 sends β’ to BS via a public channel. BS compares β with β’ and obtains the matching result r = [√ × √ × × √ × √].

viii. Sifted Key Generation: BS sends r back to RS1, which uses r to distill α’ by retaining only matching bits, producing the sifted key s = [0 _ 1 _ _ 0 _ 1].

ix. Shared Secret Key: BS and RS1 agree on the shared secret key s = [0 1 0 1] for encryption and decryption.

x. Encryption and Decryption: BS uses s to encrypt the plaintext into ciphertext and sends it to RS1, which then decrypts it back into plaintext.

Steps for Relaying Messages from RS to SS using QKD:

xi. Bit Generation at RS1: RS1 generates a new random string of bits and polarizes them, similar to steps (1) to (3).

xii. Transmission to RS2: The polarized qubits are transmitted through the quantum channel to RS2.

Steps for SS to Measure Photons from RS:

xiii. Measurement at RS2: RS2 follows the same steps as RS1 did in steps (5) to (10) to measure the photons and establish a shared secret key for secure communication.

4.2 QKD and the Five Pillars of Information Assurance

QKD, like any other security framework is also compliant with the five pillars of information assurance such as confidentiality, integrity, availability, authenticity, and non-repudiation. Each pillar plays a crucial role in maintaining a robust and secure communication system.

To ensure confidentiality, QKD employs a technique where each secret key is used only once, following the One Time Pad (OTP) rule, which is theoretically unbreakable when used correctly. Any eavesdropping activity alters the quantum state of the qubits, making it detectable. If an eavesdropper is detected, the key is discarded before any confidential information is transmitted, ensuring that no sensitive data is compromised.

While QKD ensures the secure distribution of the cryptographic key, it does not inherently guarantee data integrity. To ensure data integrity, encryption algorithms such as ECC (Elliptic Curve Cryptography) are used in conjunction with the QKD-generated secret key. This combination helps maintain the integrity of the transmitted data.

Early detection of eavesdroppers allows BS and RS to discard compromised keys before using them, ensuring the information remains secure and available. This preemptive action ensures the data transmission channel is not intercepted by an unauthorized party. If a key is compromised, BS and RS can generate another secret key using QKD, ensuring the continuous availability of secure communication.

To prevent Man-in-the-Middle (MITM) attacks, counter-based authentication methods are employed. This method enhances the security and efficiency of QKD by ensuring that both parties involved are legitimate. Furthermore, Future improvements with quantum repeaters aim to relay quantum keys without measurement, reducing vulnerability and enhancing authenticity in communication.

A public key signature is used to authenticate the QKD session, ensuring that neither party can deny their participation in the communication. Both stations verify each other's digital signatures, providing proof of the origin and integrity of the transmitted messages. This process ensures non-repudiation, whereby both parties are accountable for their actions within the communication session, further solidifying the trustworthiness of the system.

In summary, QKD's alignment with the five pillars of information assurance makes it a robust framework for secure communication. By ensuring confidentiality, data integrity, availability, authenticity, and non-repudiation, QKD addresses the critical aspects of modern cybersecurity needs. Proactive measures and advanced techniques, such as early eavesdropper detection and counter-based authentication, ensure that communication remains secure and trustworthy, paving the way for future advancements in quantum cryptography.

4.3 Comparative Analysis of QKD vs conventional RSA

Table 1: Comparison Analysis between Quantum Cryptography and Rivest-Shamir-Adleman Cryptography

Feature	**Quantum Cryptography (QKD)**	**RSA Cryptography**
Security Basis	Based on the principles of quantum mechanics	Based on the mathematical difficulty of factoring large prime numbers.
Encryption Strength	Theoretically unbreakable due to quantum mechanics, any eavesdropping attempt is detectable.	Strong, but vulnerable to attacks by quantum computers using algorithms like Shor's algorithm (Gilbert & Hamrick, 2000; What Is Quantum Computing? | IBM, n.d.)
Current Vulnerabilities	Requires perfect implementation; practical issues include photon loss and a dedicated quantum channel.	Vulnerable to potential future quantum computers
Key Exchange	Uses QKD to securely exchange keys over a quantum channel; key is discarded if tampered.	Uses public-key infrastructure (PKI) for secure key exchange over classical channels.
Computational Efficiency	Slower due to current technological limitations in photon transmission	Generally faster and more efficient with current technology and infrastructure.
Infrastructure Requirements	Requires specialized hardware	Can be implemented with existing infrastructure.
Future Resilience	Considered future proof against advances in quantum computing.	Likely to be broken by sufficiently powerful quantum computers
Use Cases	Ideal for highly sensitive information requiring long-term security, such as government or military data.	Widely used in secure communications like online banking, emails, and digital signatures.

4.4 Securing Quantum Framework with ECC

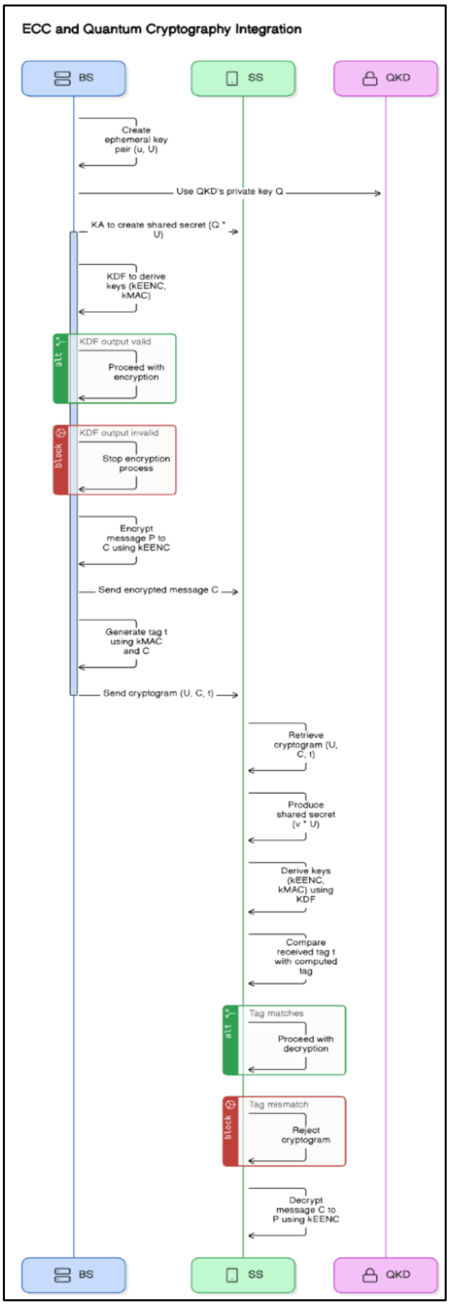
ECC and Quantum Cryptography Integration
BS
SS
QKD
Create ephemeral key pair (u, U)
Use QKD's private key Q
KA to create shared secret (Q * U)
KDF to derive keys (kEENC, kMAC)
alt
KDF output valid
Proceed with encryption
block
KDF output invalid
Stop encryption process
Encrypt message P to C using kEENC
Send encrypted message C
Generate tag t using kMAC and C
Send cryptogram (U, C, t)
Retrieve cryptogram (U, C, t)
Produce shared secret (v * U)
Derive keys (kEENC, kMAC) using KDF
Compare received tag t with computed tag
alt
Tag matches
Proceed with decryption
block
Tag mismatch
Reject cryptogram
Decrypt message C to P using kEENC
BS
SS
QKD

Figure 5: State diagram of ECC and Quantum Cryptography Integration

In the context of securing the Quantum Framework, Elliptic Curve Cryptography (ECC) offers robust encryption mechanisms. The encryption process starts with the Base Station (BS) generating an ephemeral key pair (u,U), where U is the public key and u is the private key. The plaintext P is prepared for encryption. Using a Key Agreement (KA) function, the BS creates a shared secret value Q×U, where Q is derived from Quantum Key Distribution (QKD) and Vis the public key of the Subscriber Station (SS). This shared secret value is then input into a Key Derivation Function (KDF) to generate a symmetric encryption key kEand a Message Authentication Code (MAC) key kM. If the KDF output is invalid, the process halts. The symmetric encryption key kE encrypts the plaintext P to produce ciphertext C, and the MAC function generates a tag t using C and kM . The BS then sends a cryptogram (U,C,t) to the SS.

For decryption, the SS retrieves the cryptogram and uses its private key v and the ephemeral public key U to produce the shared secret value v×U. This shared secret, along with the same parameters used by the BS, allows the SS to derive the same encryption and MAC keys using the KDF procedure. The SS then compares the received tag t with the computed tag. If the tags do not match, the cryptogram is rejected. If they match, the SS decrypts C using the symmetric key to obtain the plaintext P.

ECC ensures several security features in 5G networks. Confidentiality is maintained by encrypting messages such that only the intended recipient can decrypt them, effectively tackling spoofing and sniffing attacks. Integrity is protected using HASH functions, which produce unique identifiers for data, allowing the detection of any alterations. Availability is ensured by maintaining resource access for legitimate users and detecting attacks like Denial of Service (DoS). Non-repudiation is achieved using digital signatures and certificate verification, preventing both the sender and receiver from denying the message transmission.

The integration of QKD with ECC enhances security by securely distributing the private key Q, which is used in the ECC process for encryption and decryption.

4.5 Automatic Key Refreshment Mechanism

An automatic key refreshment mechanism is implemented in QECC to further eliminate its vulnerability against MITM attacks. The proposed automatic key refreshment mechanism follows the Key Updating Scheme (KUS) (Mishra et al., 2023) where there are two types of triggers to refresh the keys in the QECC, namely the event-based and time-based triggers.

The event-based trigger initiates the key refresh process every time a suspicious behavior is detected. In this context, QECC already has a built-in event-based key refreshment mechanism where an early detection of eavesdroppers is the event-based trigger that initiates the aforementioned key refreshment mechanism by discarding the compromised key and regenerating a new secret key using QKD, essentially refreshing the key.

However, there is still a chance that the eavesdropper may not be detected in time to trigger event-based key refreshment, thereby compromising the security measures of QECC. This is where the proposed time-based key refreshment mechanism comes into place.

The time-based trigger initiates the key refreshment process after a certain time or when a counter reaches a certain amount or after a random predetermined duration. In this case, an additional time-based key refreshment mechanism is proposed to act as a fail-safe and an extra layer of protection against any impersonation attacks to QECC if the event-based key refreshment fails.

4.6 Key Refreshment Mechanism Process in Blockchain Environment

The time-based key refreshment mechanism in a blockchain environment starts off with the network operator sending a message,

$$\mathrm{M} = \{\mathrm{ID}_i, H_i^n, TS_n, \Delta\mathrm{TS}\} \tag{1}$$

to the blockchain. This message is cryptographically signed by the network operator using a method like the Schnorr Signature Scheme to ensure authenticity and integrity. Here, TS_n represents the registration time of the device, and ΔTS indicates the maximum duration allowed in between two key refreshes. Additionally, a smart contract is created where the network operator is reminded to refresh the key at an interval of $\Delta\mathrm{TS} - \epsilon$, with ϵ representing the duration required for the key refreshment process with the device. Warning messages are sent to subscribed application servers if the network operator fails to submit the preceding hash chain value of the device to the blockchain. The successful update of the device is also recorded in the blockchain.

4.7 Formal Analysis on the Security of Blockchain-Based Key Agreement Update Protocol

The RUBIN logic, which is a non-monotonic logic-based approach for verification, is utilized to formally validate the security aspects of the blockchain-based key refreshment protocol in terms of confidentiality, integrity, and mutual authentication. The analysis is conducted by tracking the evolution of global and local sets, as well as actions involved.

The global setting, which is publicly accessible, comprises four distinct sets containing protocol-related information. Firstly, participants within the protocol are identified by the principal set P = {D, NS, BS}. Secondly, inference rules are encompassed in the rule set to derive new statements. Thirdly, the secret set S denotes an instance of secrets at a specific point in time, initially defined as follows:

$$\mathrm{S} = \{S_s^1 ,S_s^2 ,S_{s+1}^2, (\mathrm{H}_i^0,\ldots, \mathrm{H}_i^{s-1} , \mathrm{H}_i^s)\} \tag{2}$$

Finally, participants who are aware of the secrets within S are included in observer sets. These observer sets are categorized as follows:

- Obs(H_i^0, . . . , H_i^{s-1}) = {D}
- Obs(H_i^s) = {D, NS, BS}
- Obs(S_s^1 ,S_s^2 ,S_(s+1)^2) = {D, NS}

The local sets differ for each participant and include a possession set, belief set, and behaviour list. All known secrets for the participant P are contained within the possession set *Poss(*P). The belief set *Bel*(P) comprises of all beliefs within P regarding aspects such as key freshness and secrets possessed by other participants. Actions performed by the participants is defined in the behaviour list *BL*.

According to the evaluation conducted in Mishra et al. (2023) ,the following conclusions regarding confidentiality, integrity, and mutual authentication can be drawn:

- The data S_(s-1)^1, S_(s-1)^2, S_s^2 utilized for generating new keys for the following session remains fresh and is solely accessible to the authorized entities NS and D.
- The key material utilized in the ongoing session is fresh, resulting in the generation of key material K, exclusively known to the NS and D of the legitimate participants
- The possession of H_i^(s-1) by D and H_i^s by NS and BS ensures the unique authentication of D due to the robustness of the hash function.

5 Conclusions

In conclusion, our proposed authentication mechanism for Industrial Internet of Things (IIoT) systems integrates Quantum-Elliptic Curve Cryptography (QECC) with a blockchain-regulated, automatic key refreshment mechanism to address the pressing security concerns inherent in IIoT communications. Review of existing works are reviewed, in which inspired and informs our approach for the proposed solution. By building upon the ECC-based Diffie-Hellman (ECDH) protocol, our solution mitigates vulnerabilities such as Man-in-the-Middle (MITM) attacks through the innovative combination of quantum cryptography and ECC. Additionally, to bolster security against spoofing attacks, we incorporate a time-driven trigger mechanism for automatic key refreshment within our blockchain network. Through analysis of our proposed mechanism, security requirements such as confidentiality, integrity, availability, and non-repudiation is fulfilled.

References

Deebak, B. D., Memon, F. H., Dev, K., Khowaja, S. A., Wang, W., & Qureshi, N. M. F. (2023). TAB-SAPP: a Trust-Aware Blockchain-Based seamless authentication for massive IoT-Enabled industrial applications. *IEEE Transactions on Industrial Informatics*, *19*(1), 243–250. https://doi.org/10.1109/tii.2022.3159164

Gilbert, G., & Hamrick, M. (2000). Practical Quantum Cryptography: A Comprehensive Analysis (Part One). *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.quant-ph/0009027

How will quantum technologies change cryptography? (n.d.). Caltech Science Exchange. https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography

Khan, A. S., Abdullah, J., Khan, N., Julahi, A., & Tarmizi, S. (2017). Quantum-Elliptic curve Cryptography Multihop Communication in 5G Networks. *International Journal of Computer Science and Network Security(IJCSNS)*, *17*(5), 357–365. https://ir.unimas.my/id/eprint/17233/

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. https://doi.org/10.1166/asl.2017.7350

Khan, A. S., Lenando, H., Abdullah, J., & Fisal, N. (n.d.). Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks. *Jurnal Teknologi/Jurnal Teknologi*, *73*(1).https://doi.org/10.11113/jt.v73.3258

Khan, A. S., Mehdi, M. H., Uddin, R., Abbasi, A. R., BSChowdhry, & Nisar, K. (2023). Ensemble based automotive paint surface defect detection augmented by order statistics filtering using machine learning. *Authorea (Authorea)*. https://doi.org/10.22541/au.169735587.77641533/v1

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. https://doi.org/10.1109/access.2023.3249969

Khan, A., Yasir, J., Johari, A., Nazim, J., & Khan, N. (2017). Security issues in 5G device to device communication. *IJCSNS*, *17*(5). https://ir.unimas.my/17236/

Khan, N., Abdullah, J., & Khan, A. S. (2017). Defending malicious script attacks using machine learning classifiers. *Wireless Communications and Mobile Computing*, *2017*, 1–9. https://doi.org/10.1155/2017/5360472

Liu, X., Wang, J., Wang, M., & Zhang, R. (2024). Improved LTE-R access authentication scheme based on blockchain and SECGear. *IEEE Internet of Things Journal*, *11*(6), 10537–10550. https://doi.org/10.1109/jiot.2023.3325904

Mishra, R. A., Kalla, A., Braeken, A., & Liyanage, M. (2023). Blockchain regulated verifiable and automatic key refreshment mechanism for IoT. *IEEE Access*, *11*, 21758–21770. https://doi.org/10.1109/access.2023.3251651

Tong, F., Chen, X., Huang, C., Zhang, Y., & Shen, X. (2023). Blockchain-Assisted secure Intra/Inter-Domain authorization and authentication for internet of things. *IEEE Internet of Things Journal*, *10*(9), 7761–7773. https://doi.org/10.1109/jiot.2022.3229676

Wang, F., Cui, J., Zhang, Q., He, D., Gu, C., & Zhong, H. (2024). Lightweight and secure data sharing based on proxy Re-Encryption for Blockchain-Enabled industrial internet of Things. *IEEE Internet of Things Journal*, *11*(8), 14115–14126. https://doi.org/10.1109/jiot.2023.3340567

Wang, W., Xu, H., Alazab, M., Gadekallu, T. R., Han, Z., & Su, C. (2022). Blockchain-Based reliable and efficient certificateless signature for IIoT devices. *IEEE Transactions on Industrial Informatics*, *18*(10), 7059–7067. https://doi.org/10.1109/tii.2021.3084753

Wang, X., Garg, S., Lin, H., Piran, M. J., Hu, J., & Hossain, M. S. (2021). Enabling secure authentication in industrial IoT with transfer learning empowered blockchain. *IEEE Transactions on Industrial Informatics*, *17*(11), 7725–7733. https://doi.org/10.1109/tii.2021.3049405

What is Quantum Computing? | IBM. (n.d.). https://www.ibm.com/quantum-computing/what-is-quantumcomputing/

Yang, Y., Wu, J., Long, C., Liang, W., & Lin, Y. (2022). Blockchain-Enabled multiparty computation for privacy preserving and public audit in industrial IoT. *IEEE Transactions on Industrial Informatics*, *18*(12), 9259–9267. https://doi.org/10.1109/tii.2022.3177630

Zhang, P., Yang, P., Kumar, N., Hsu, C., Wu, S., & Zhou, F. (2024). RRV-BC: Random Reputation voting mechanism and blockchain Assisted access authentication for industrial internet of Things. *IEEE Transactions on Industrial Informatics*, *20*(1), 713–722. https://doi.org/10.1109/tii.2023.3271127