QUANTUM LAMPORT ONE-TIME DIGITAL SIGNATURE CRYPTOGRAPHY FOR SECURED DATA COMMUNICATION FOR INDUSTRIAL IOT

Flindon W.G[1], Divya S.V[2*]

[1]Department of Computer Application, Noorul Islam Centre for Higher Education, Thuckalay, Kumaracoil, Tamil Nadu 629180. mrflindon@gmail.com

[2*]Department of Computer Science and Engineering, V.S.B College of Engineering Technical Campus, Coimbatore, Tamil Nadu 642109. divyasadasivam@gmail.com

ABSTRACT

Cloud Computing (CC) as well as Internet of Things is broadly employed in Industrial Internet of Things. Industrial Internet of Things is a promising technology through vast amount of smart connected tools containing sensing, storage, as well as computing capacities. Digital signature lately played an increasingly significant role in security. The security is employed in IIoT to protect stored data from unauthorized user access. In today's growing concern for security, we have developed a novel secured data communication method called Quantum Lamport One-Time Digital Signature Cryptography. It is combined with three major processes: key generation, signing, and verification during secured data communication to enhance the security level of industrial information through improved confidentiality rate, greater integrity, and less time. In a key generation, industrial data as input is considered. The keys are generated by the Cloud Server in the CC for the registered cloud users by Lamport One-Time Key Generation by using linear congruential generator. It employed to sign solitary message and be distinct from another user, therefore ensuring data confidentiality. Next, the Modular Arithmetic-based Digital Signature model is utilized to perform the signing process thereby ensuring authentication accuracy. Finally, verification is carried out for secured data communication for industrial IoT via CC. The proposed Quantum Lamport One-Time Digital Signature Cryptography has estimated by dissimilar metrics where outcomes attained confirm its efficiency in comparison to conventional solutions. It aids to enhance 18% data confidentiality, 9% data integrity, 26% authentication accuracy and reduce 18%

space complexity, 35% message delivery time as compared to existing methods. The development of novel cryptographic methods, like Quantum Lamport One-Time Digital Signature Cryptography, addresses these gaps by enhancing data confidentiality, integrity, and authentication accuracy while reducing space complexity and message delivery time. This research ensures robust protection against unauthorized access, safeguarding industrial operations and fostering trust in IIoT systems, which is vital for technological progress and industrial innovation.

KEYWORDS: Cloud Computing, Internet of Things, Lamport One-Time Key Generation, Digital Signature, Modular Arithmetic

INTRODUCTION

In recent years, the IoT and CC environments have become more prevalent in the circumstances of the industry, owing to the fact that digitization has become a business priority for several organizations. Also, the IoT impacts contemporary society by enhancing the prospect of relocation without leaving the daily life requirements. IoT institutes prevalent digital existence through associating organizations as well as society globally and bestowing succession of relationships between humans and things. The IIoT uses the notion of IoT and is utilized in several real-time industrial applications like logistics, manufacturing, and so on. However, such an encouraging service-provisioning method is surfacing novel security issues in dispersed IIoT framework. For preserving IIoT data security, incremental aggregator subvector commitment (IASVC) scheme was developed by (Jin *et a*l.,2022).In order to save information, traditional blockchain system utilizes Merkle trees. A variety of encryption algorithms were developed to protect the IIoT data privacy. Additionally, the data qualifications upload on nodes by means of IASVC that lessen the nodes storage pressure. This approach was significantly decreases the proof size as well as augments communication efficiency. But, multilinear mapping was not employed to build designed method.

A zerotrust security architecture was developed by (Shan *et al.,*2022) for Future Industry Internet of Things (FIoT). It was attaining zero-trust devices authentication in 5GIoT that offer solutions. But, it failed to consider the data delivery time. For IIoT environment, lattice-basis multi-party collaborative double authentication averting signature system was designed by (Jinhui Liu *et al.,* 2023). It was satisfying post-quantum safety as well as enhance the IIoT network fairness. Also, it offers security requirements of IIOT. For secure communication in IIoT, blockchain-based cross-domain authentication protocol was designed by (Khalid *et al.,* 2023). The blockchain keeps domain's dynamic accumulator that accrue vital substances derived from tools with less overhead. Also, it was successfully validate the cross-domain IIoT devices unlinkable characteristics. But, the protocol's effectiveness was not optimized (Shahid *et al.,*2020).

Blockchain and DL integrated framework was developed by (Prabhat Kumar *et a*l. 2023) that offers data privacy as well as safe data communication. But, federated learning integration inside designed networks was not developed. An elliptic curve depend attack-resistant lightweight digital signature model was designed by (Dr. Dhanashree *et al.*, 2023) for enhancing security in resource constrained applications. It was effectively carried out for signature generation, verification to attack. But, the authentication accuracy was not addressed.

A more efficient quantum digital signature (QDS) protocol was designed by (Hua-Lei Yin *et al*., 2023) using symmetric quantum keys acquired by means of secret sharing. For solving issues of IoT-Fog-Cloud channel privacy as well as storage scalability, Distributed security services structural design based on blockchain and Fog computing was performed by (Tharaka Hewa *et al*., 2021). It was offers transferred data confidentiality, integrity, authentication and unlinkability over the blockchain records. A new signature scheme was introduced by (Muthukumaran *et al.,*2023) for executing communication among devices inside IIoT environment. Privacy Dimensions on IIoT was discussed by (Vasiliki Demertz *et al.,* 2023) for protection of natural persons by means of prevention, investigation, detection of illegal offences. Also, it investigates the privacy requirements and suggestions for secure IIoT environment.

For IIoT deployment, Identity-Based Signcryption (IBSC) method was introduced in (Arijit Karat *et al.,* 2023). Moreover, the IBSC method for IIoT was found to be provably secure according to intractability of decisional-MBDHI as well as MBSDH assumptions under formal

safety method devoid of taking into consideration the random oracle. However, computational cost was not minimized, and therefore it was proven to fail in supporting the revocation facility. For scenarios involving IIoT, block chain-based fair non-repudiation service provisioning method was proposed (Yang Xu *et al* ., 2019). Here, the block chain was utilized as service publisher as well as proof recorder. Also, homomorphic-hash-based service verification method was introduced to function with on-chain proof (Ciulei *et al.,* 2021). But it failed to incorporate additional facets as deposit as well as reputation method to establish sophisticated and effective solution.

Safe Fabric blockchain-based data broadcast technique was proposed in (Liang *et al.*, 2019) for IIoT. The data broadcast method utilized a blockchain-based dynamic secret-sharing device. Also, a power information consensus device and dynamically associated storage were introduced to recognize safe matching of power data broadcast. However, growth of power blockchain was not introduced in large-scale relevance (Sharma *et al.*, 2023). Safe data broadcast method was not applied to industrial IoT applications like power and energy.

For creating reliable as well as secure environment, block chain-enabled efficient data gathering and safe sharing method was introduced in (Chi Harold *et al*., 2019). Here, DRL was utilized for attaining the highest amount of gathered information, and blockchain technology was utilized for guarantying reliability of data sharing. But it failed to promise security involving data sharing (Chawla *et al.,* 2022) in efficient manner. However, deep models failed to execute multiple tasks simultaneousl.

MOTIVATION

Most of conventional safety as well as privacy solutions in IIoT focus on data security or deployment and communication issues of tools. But, most of conventional cryptography methods which employed in Industrial IoT domain give safety depend on asymmetric cryptography resulting in enhanced computational cost. Therefore, IoT devices not capable to support them properly and thus, various security problems occur in IIoT. But, management as well as authentication for IIoT schemes received minimum concentration. Though hash function agrees to it, a random number would not permit computation. This motivates us to implement a secured data communication method with minimum computation cost for ensuring security.

CONTRIBUTIONS

The purpose of the secured data communication can be explained precisely by the design of IIoT. It can be done by imparting the state at three different steps thus a secure way for ensuring data confidentiality and integrity. The method is designing key generation, signing, and verification for secure data. This process is to efficiently ensure secure communication between cloud servers and clients throughout IIoT.

The main contributions are given below:

- For enhancing the security of data transmission, the proposed Cloud Computing-based secured data communication method called QLOT-DSC for IIoT scenarios is designed to generate keys, sign, and validate.

- To generate keys only for the registered cloud users for single data or messages based on mere quantum bits, the key generation model is designed based on Quantum Lamport One-Time Key Generation through using linear congruential generator with a short time rather than for the overall transaction processes. Therefore, it is said to be distinct for different industrial data to be communicated between devices.
- For ensuring authentication accuracy, QLOT-DSC uses the Modular Arithmetic-based Digital Signature model based on digital signatures separately for signing and validation to fairly and efficiently ensure secure communication between cloud servers and IIoT clients.
- Lastly, widespread experiments are performed to estimate performance of QLOT-DSC and conventional works. Experimental outcome shows that QLOT-DSC better than other techniques.

MANUSCRIPT ORGANIZATION

Rest of manuscript is structured as follows: Section 2 discusses some related works in field of IIoT and their security mechanisms. Section 3 presents our main Lamport One-Time Digital Signature Cryptography (LOT-DSC) construction in elaboration. Section 4 shows simulation setup of LOT-DSC method in detail. Lastly, conclusion is summarized in Section 5.

RELATED WORKS

IoT is defined as environment designed in an inter-device manner and constructed using devices that concentrate on three primary chores: data transmission, data reception, and data processing. Initially, physical devices constructed locally were connected to the internet in real-time via the IoT network. With changes evolving, the scalability of IoT has also increased, both locally and globally, extending to Industrial IoT. Hence, research on IoT portrays the augmentation of IoT in several domains, like healthcare, industrial setup, business analytics, education, and so on.

The proliferation of IoT systems has evolved into competitive framework with inception of novel and innovative products for smart city applications. Routinely deployed framework took advantage of a new challenge with regard to privacy and security. Additionally, certain products not persuade privacy as well as security that remain crucial responsibilities of IoT and smart cities. Most of research work has concentrated on probable applications as well as concerns with smart cities (Rohit Sharma *et al.*, 2021). The security was enhanced but, the message delivery time was not measured. A holistic review of the prevailing IoT framework and communication patterns employed in the healthcare sector was investigated in (Navneet Verma *et al*., 2021). The designed method accurately predicts the disease however, the large dataset was not considered. To overcome problems, Quantum Lamport One-Time Key Generation uses huge data set for evaluating message delivery time performance.

A survey of security concerns with respect to the IoT was proposed in (Rachit, *et al.,* 2020). Over the past few years, automation control systems are nowadays constrained to in-shop prefabrication as far as the construction industry is concerned. By instituting network technologies on the construction site, automated machinery can be modeled on site for cooperative tasks dynamically. However, IoT data broadcast poses a broad diversity of scenarios as well as complicated environments. Hence, prediction and evaluation of secure data transmission are said to be laborious and cumbersome.

Block chain-enabled cyber-security approach as well as algorithm were designed in (Ali *et al.,* 2020) with higher encrypted data processing and transmission. However, the performance of data integrity through the transmission was not minimized. In (Fagen Yin *et al.,* 2021), an Elman-based secured data transmission method was proposed to achieve high-quality precision. The time complexity was lower, however, data confidentiality was not improved. To address problem, a Modular Arithmetic-based Digital Signature is utilized. For IIoT ,A novel Transfer learning-based Secure Data Fusion (TSDF) method was proposed in (Hui *et al.,* 2021). It employed GDDPG algorithm for classifying the task, and security was ensured using multi-blockchain mechanisms, therefore achieving enhanced system throughput and minimum latency under numerous IIoT application scenarios. Through fast evolution of IIoT, enormous amounts of data are continuously created by various sources. Stockpiling all the raw data on the IIoT devices in a localized manner is inadvisable. Moreover, due to their unreliable nature, devices are said to be highly susceptible to several threats.

In (Jun-Song Fu *et al.,* 2021), the upcoming issue in area of data processing, storage in a secured manner, data retrieval, and data gathering in a dynamic manner in IIoT was proposed. However, efficiency was not enhanced. Yet another secure blockchain-based model for data transmission was proposed in (Liang *et al.,* 2018). However, the data security was not enhanced. A survey on contemporary advancements in IIoT application using machine learning techniques was investigated in (Liang *et al*.,2020). In several cases, sensors in the IIoT framework are associated with or correlated by using wireless channels. These types of channels are specifically found to be unreliable and contribute to users' privacy-sensitive data being revealed to malicious users. A review of IIoT as well as its relationships to cyber-physical schemes and Industry 4.0 was investigated in (Hugh Boyes *et al.*, 2024). The security threats are analyzed. But, it failed to enhance data integrity. To conquer the problem, the Lamport function is utilized to ensuring both data integrity and scalability. A review of network optimization for IIoT was designed in (Praveen Kumar *et al*., 2020).

Securing data broadcast between IoT devices is hence identified as an evaluative potentiality of IoT environments .But the cryptographic communication method is said to pose a great issue due to the constrained resource, and hence the utilization of battery-powered sensors would cause a hectic minimize in battery existence. In Srinidhi *et al.,* 2018), with the objective of

reducing resource consumption, a communication protocol consisting of a symmetric key-based method to ensure data broadcast was proposed.

Internet of Things (IoT) has received escalating luminousness between transpiring techniques and beyond doubt transposing our day-to-day chores. Its application is reinforced through broadening of associated tools or things as provided in present-day statistics. But, with increase in associated things, concerns with respect to security aspects also necessitate growth. A literature appraisal concentrated on authentication, access control, data protection, as well as trust (Xi Luo *et al.,* 2020). However, measures were not taken to handle big data. To address the big data aspect of the Industrial Internet of Learning, pervasive knowledge was applied (Evandro *et al*., 2020), which in turn minimized the computational complexity to a greater extent. Centralized cloud-based cross-domain data-sharing scheme was discussed in (Parminder Singh *et al.,* 2021). However, the designed approach failed to employ large-scale data. Hermitian-based cryptosystems (HBC) were introduced in (Parminder Singh *et al.,* 2021). with higher security. But the message delivery time was not reduced. For providing secure transmission of medical data, new privacy-preserving encryption with DL-based medical data transmission and classification (PPEDL-MDTC) model was examined in (Jafar *et al*.,2019). The Hashed Needham Schroeder (HNS) Cost Optimized Deep Machine Learning (HNS-CODML) method was developed in (Mohammed *et al.,*2020) for efficient, secured transmission. New wrapper Feature Selection model was investigated in (Mohammed *etal.*,2023). for obtaining security. For image encryption, a new chaotic map algorithm was designed (Parminder Singh *et al*., 2021). Nevertheless, time was not focused.

To summarize, various researchers presented several works in the IIoT network based on optimization and different other techniques. Still, there remains room for improvement in several security factors. Quantum Lamport One-Time Digital Signature Cryptography (QLOT-DSC) was proposed to ensure data confidentiality, integrity, and message delivery time in a cloud-based IoT environment, specifically for industry management related to secure data communication.

METHODOLOGY

With the strengthened employment of the internet and considerable numbers of cloud users involved in the data communication industrial domain, security has experienced reasonable

consciousness. Also due to better scalability and lower maintenance costs, several cloud users are performing data communication for industrial data based on the data acquired from the sensors, called IoT. In recent years, there has outflow of attempts to apply signcryption methods to ensure secured data communication between cloud users in a cloud computing environment. A secured data communication method called Quantum Lamport One-Time Digital Signature Cryptography (QLOT-DSC) for industrial IoT via Cloud computing is proposed. Lamport One-Time Signature is technique [36] to construct digital signature and characteristically involves employ of cryptographic hash function. As it one-time signature system, it only used to safely sign single message. Lamport's one-time digital signature includes key generation, signature, as well as verification. In the proposed QLOT-DSC, the advantages of cloud infrastructure is to enhance security of data, limited flexibility, less infrastructure price, easy management, data backup and recovery and save of space. Cloud infrastructure includes all hardware and software components to support the delivery of cloud services to the user. The components of cloud infrastructure such as networking equipment, servers and data storage are utilized in this work. The proposed Quantum Lamport One-Time Digital Signature Cryptography (QLOT-DSC) is modified based on reference (Jafar *et al.,* 2019).

The innovation of proposed QLOT-DSC as follows:

- The designed QLOT-DSC uses the innovation of Lamport One-Time Key Generation for creating keys for a single transaction. We introduce the Quantum Random Number Generator as a service publication to generate random double-bit sequences. In this way, higher data confidentiality and shorter message delivery time and space complexity.
- The designed QLOT-DSC employs a novel Arithmetic-based Digital Signature model for performing the signing in process and validation process via by means of modular functions. In addition, we implement an addition and doubling operation separately to ensure an accurate authentication mechanism to help cloud servers as well as IIoT clients determine service disputes fairly and effectively.

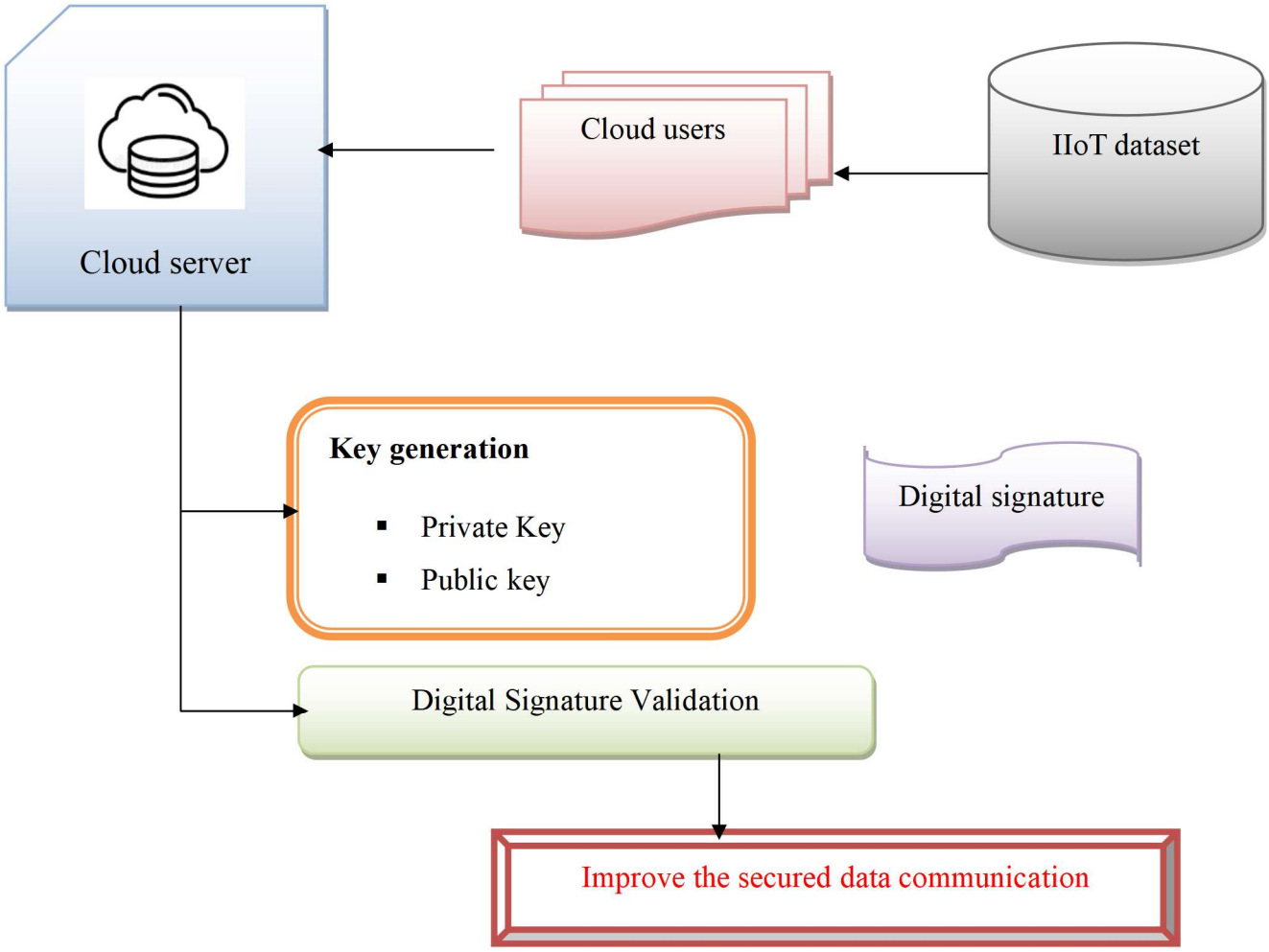

Figure 1. Block diagram of Quantum Lamport One-Time Digital Signature Cryptography (QLOT-DSC)

As depicted in figure 1, QLOT-DSC technique contains three processes. They are key generation, signing, and verification. Key generation is performed using the Quantum Lamport One-Time Key Generation model. Followed by which signing and verification are performed by applying Modular Arithmetic-based Digital signatures.

QUANTUM LAMPORT ONE-TIME KEY GENERATION

During cryptography process, Lamport one-time Key Generation method builds a digital signature. Lamport Key Generation is constructs from cryptographically protected one-way

function. It generally employs a cryptographic hash function. Each Lamport key only sign single data, if numerous information are signed several keys have published. Also, Lamport Key Generation is fused with a list of hashes creates single top hash in place of the entire the hashes in the public key.

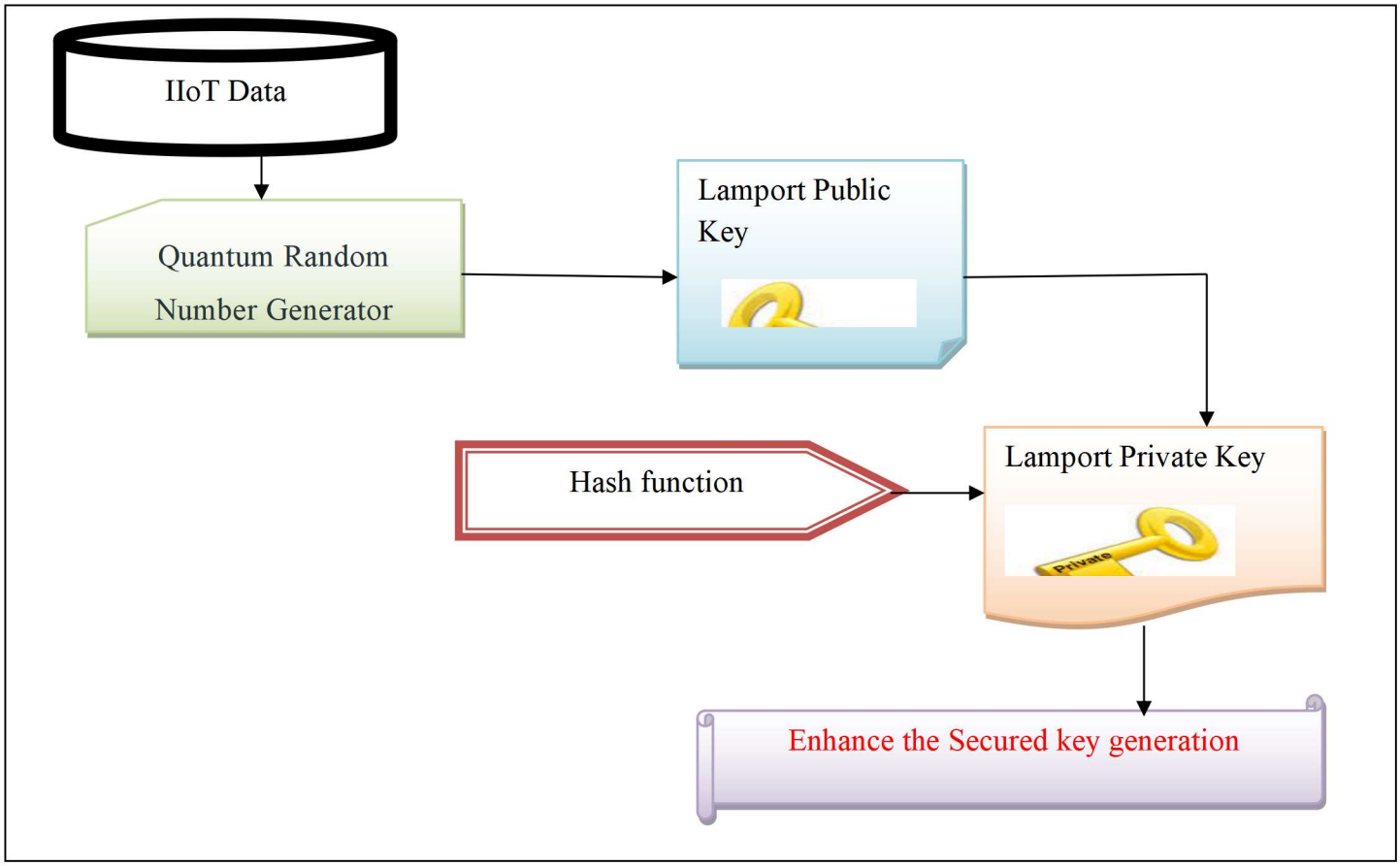

Figure 2. Structure of Quantum Lamport One-Time Key Generation

The first step involved in the secured data communication is the key generation performed in the CC environment. The industrial data '$D = (D_1, D_2, ..., D_n)$' possessed by the user initially registers their information to cloud server 'CS' with use of storing and accessing the information in future. Followed by, the 'CS' acquires key pair employing Lamport One-Time Key Generation and with the obtained result sends the key pair to registered cloud user sharing their industrial data As shown in the figure 2, to start with the sender cloud user node requires create Lamport key pair, private key, as well as a equivalent public key. To produce private key, a secure Quantum multiplicative congruential Generator is utilized to create double bit

sequences, ‘00’, ‘01’, ‘10’ and ‘11’ pairs of random numbers. The sender cloud user node stores this private key in a secure manner. Next to create the public key the sender cloud user node hashes each of the double bit sequences of its private key. This will produce another set of double bit sequences, 16 bits, every containing 8 bits. This is public key which is shared by the other cloud user.

Let ‘n’ be positive number, $A = \{0,1\}^n$ represent set of data ‘D’ to signed, and fun: X $\rightarrow$ Y’ denotes single-way hash function. Then, the sender cloud user generates Quantum Random Number Generator on the basis of the random chosen of quantum entanglement with numerous kinds of quadrature.

Quantum multiplicative congruential Generator is formulated as given below.

$$M_{k+1} = i.M_k \, mod \, r \quad (1)$$

Where the modulus r is prime number of prime number, the multiplier ‘i’ is a constituent of enhanced multiplicative order modulo *r* as well as seed M_k is coprime to r.

Random selection through measurement projection is done among quadrate states a given below.

$$|\varphi >= \frac{1}{\sqrt{2}}(|00> + |11>) \quad (2)$$

In a similar manner, random selection by measurement projection is carried out among the anti-quadrate states is formulated as below

$$|\varphi >= \frac{1}{\sqrt{2}}(|01> + |10>) \quad (3)$$

Finally, with the above quadrate and anti-quadrate states, the entangled state of qubits is mathematically formulated as given below.

$$X_{ij} = |Q_i Q_j > \frac{1}{\sqrt{2}}(|00> + |11>) + \frac{1}{\sqrt{2}}(|01> + |10>) \quad (4)$$

From equation (4), entangled state of qubits between the sender cloud user node ‘Q_1’ and the receiver cloud user node ‘Q_2’ is formulated based on the random sequence. To the entangled state of qubits one way hash function is applied and stated as below.

$$Y_{ij} = Hash\,(X_{ij}) \quad (5)$$

From (5), 'Y_{ij}' represents private key whereas 'X_{ij}' refers to public key for sender cloud user node.

MODULAR ARITHMETIC-BASED DIGITAL SIGNATURE

Upon receipt of the Quantum Lamport Key Pair, the sign encryption process is carried out by CU, applying both digital signature and data encryption. It is carried out by modular arithmetic-based Digital Signature. The Modular arithmetic process is nearly similar as the normal whole numbers arithmetic. The major dissimilarity is that functions involve remains after division through specified numbers instead of the integers included. Within public key cryptosystems, modular arithmetic is a key element. It offers finite structures that contain the entire the common integer's arithmetic operations. Modular Arithmetic-based Digital Signature technique is an authentication tool. This designed digital Signature technique employs a pseudo-random number producer that produces random number individually for each IoT device communication with minimal computation overhead. Although, it employs long hash values for covering security, IoT devices are added to use only limited resources thus decrease computational time. The structure of digital signature is shown in Figure 3.

Structure of digital signatures is depended on two keys such as Public Key and Private Key. Whenever the sender needs to broadcast the data, the sender performs encryption and decryption with the help of the private key public key. Encryption is carried out by using hash algorithm sent into the receiver. Digitally signed message is decrypted by signer's public key. On the receiver side, the signature is again generated as well as verified. If the two signatures get matched, then the receiver decrypts the data. Otherwise, the signature is not valid, the decryption is not performed. In our work, the Modular Arithmetic-based Digital Signature is employed as shown in figure 4.

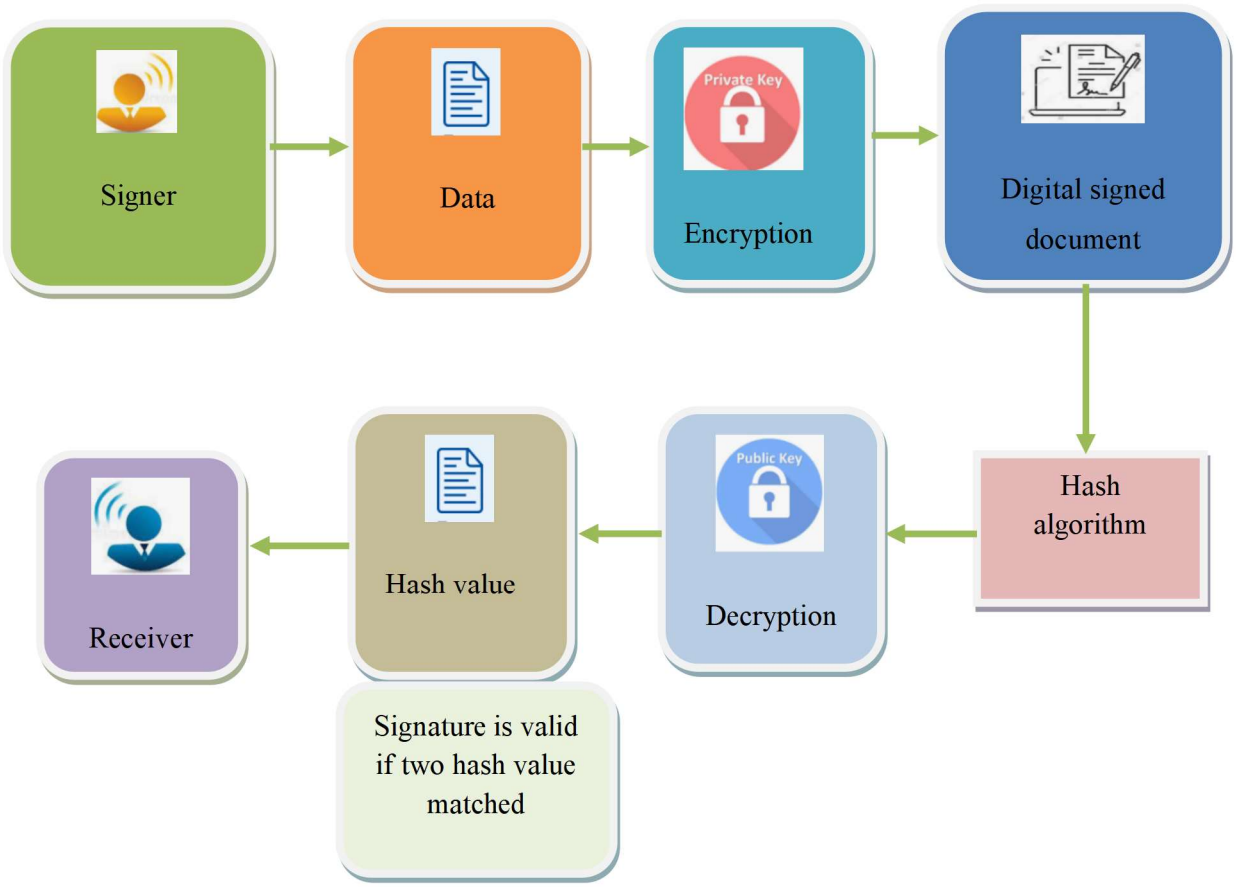

Figure 3. Structure of digital signature

As shown in the figure 4, a Modular Arithmetic-based Digital Signature for signing is utilized. The industrial information is taken as input. The hash function is used to create the hash value. The signing function is performed to generate a digital signature with each message or industrial data. With the aid of the signing process, encrypted data are stored via Lamport private key in 'CS' based on digital signature.

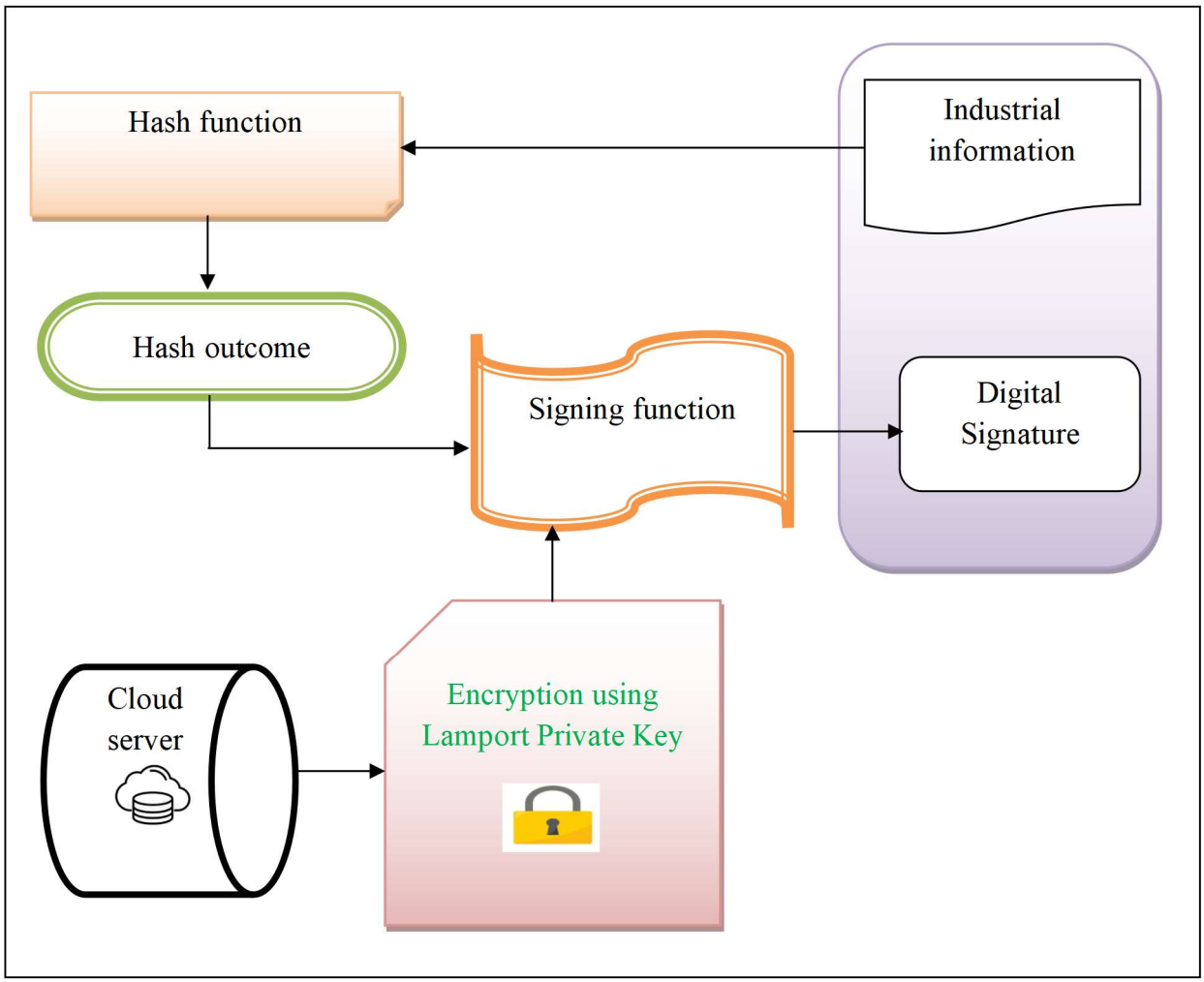

Figure 4. Block diagram of Modular Arithmetic-based Digital Signature for signing

For every bit, based on whether bit value is either '0' or '1', the sender cloud user node will select the equivalent number from pair of numbers of Quantum Lamport Private Key. Let 'D $= D_1, D_2, \ldots\ldots, D_n, \in \{0,1\}^n$' be the industrial data suitable for industrial application sender cloud user node wants to sign. Then, the elliptic curve 'E' over the field for 'n' numbers of data to perform secure communication is first formulated as given below.

$$Q^2R + PQR = P^3 + lP^2R + mR^2 \quad (6)$$

Generating the signature is based on the formulas for doubling and addition. Let 'B = (P_1, Q_1, R_1)' and 'C= (P_2, Q_2, R_2)', the addition point in the respective elliptic curve 'E' is 'B+C = (P_3 , Q_3, R_3) '. Then, the addition operation for all the industrial data is mathematically stated as given below.

$$AR_3 = (P_1R_2, R_1P_2)^2 + (P_1R_2)(R_1P_2) \quad (7)$$

Followed by the addition operation as given in above (7), the doubling operation is mathematically formulated as given below.

$$DR_3 = (P_1^2) + (R_1^2) \quad (8)$$

With the above addition 'AR_3' and doubling 'DR_3' operation results as given in (9), the signature is generated as given below.

$$Sig(D_1, D_2, ..., D_n) = \{AR_3(D_1): DR_3(D_1); AR_3(D_2): DR_3(D_2), \ldots . AR_3(D_n): DR_3(D_n)\} \quad (9)$$

$$S = \{S_1, S_2, \ldots, S_n \quad (10)$$

The above digital signature 'DS' (10) is then sent to the receiver cloud user node along with the industrial data. When a cloud user needs to access data, a request message is sent to data owner. Data owner on other hand performs an ID authentication for cloud users from 'CS' by means of validation or verification as shown in the figure 5 given below.

The verification or validation process is executed in the above figure. Industrial Data with digital signatures are considered as input by using the hash function to create hash value outcomes. When the cloud user is an authenticated user, the response is given by 'CS'. After receiving the response, acknowledgment is sent to the data owner for performing the verification function. When the verification is valid, the cloud user decrypts the data. If the verification is not valid, the cloud user not decrypt the data. The data owner finally, requests the cloud server 'CS' to transmit information or data to the cloud user. In this way, a secure data communication process is performed with a higher data confidentiality rate. The pseudo-code representation of Modular Arithmetic-based Digital Signature for industrial IoT via CC is given below

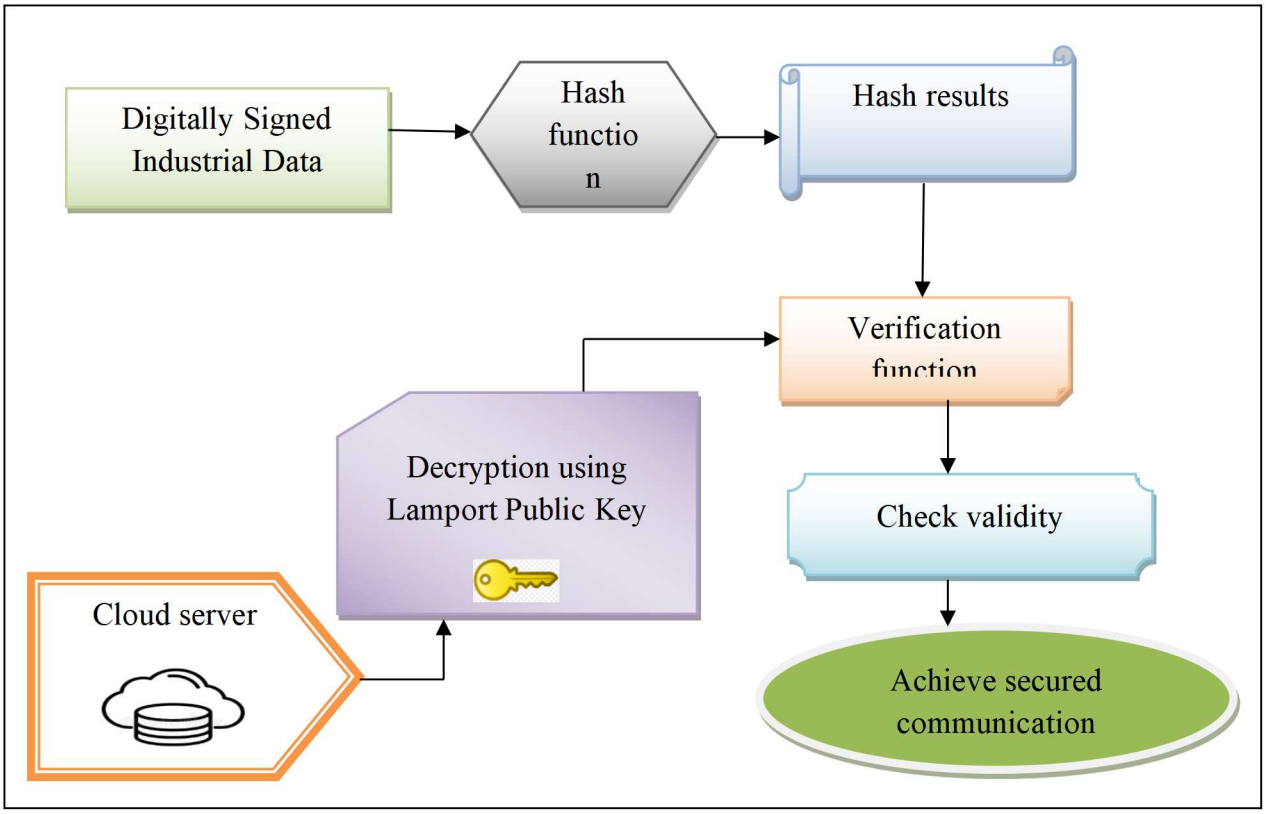

Figure 5. Block diagram of Modular Arithmetic-based Digital Signature for verification or validation

Algorithm Modular Arithmetic-based Digital Signature
Input: Dataset 'DS', Industrial Data 'D =D_1,D_2, ...,D_n', Cloud User 'CU =CU_1,CU_2, ...,CU_n'
Output: Cloud and IoT-based secured industrial data communication
Step 1: **Begin** Step 2: **For** each Dataset 'DS' with Industrial Data 'D =D_1,D_2, ...,D_n' and Cloud User 'CU' **//Key generation** Step 3: **Perform** Quantum multiplicative congruential Generator is formulated as in equation (1) Step 4: **Random selection** by measurement projection between quadrate states as in equation (2) Step 5: **Perform** random selection by measurement projection between anti-quadrate states as in equation (3)

Step 6: **Measure** entangled state of qubits as in equation to be public key as in equation (4)

Step 7: **Obtain** public key as in equation (5)

Step 8: **Return** private key 'Y_{ij}' and public key 'X_{ij}'

Step 9: **End for**

//Signature generation

Step 10: **For** each Industrial Data 'D =$D_1, D_2, \ldots\ldots, D_n$' with private key and public key and Cloud User 'CU'

Step 11: **Formulate** elliptic curve 'E' over the field for 'n' numbers of data as in equation (6)

Step 12: **Perform** addition operation as in equation (7)

Step 13: **Perform** doubling operation as in equation (8)

Step 14: **Obtain** digital signature as in equation (9) and equation (10)

Step 15: **Return** digital signature 'DS'

Step 16: **End for**

//Signature validation or verification

Step 17: **For** each Industrial Data 'D =$D_1, D_2, \ldots\ldots, D_n$' with digital signature 'DS' and Cloud User 'CU'

Step 18: **If** 'f$(S_i) = R_{1,Di}$' (i.e., verification is valid)

Step 19: Cloud user decrypts industrial data

Step 20: Secured data communication

Step 21: **Else**

Step 22: Cloud user cannot decrypt industrial data

Step 23: No data communication

Step 24: **End if**

Step 25: **End for**

Step 26: **End**

ALGORITHM 1. MODULAR ARITHMETIC-BASED DIGITAL SIGNATURE

Algorithm 1 describes the step-by-step process of three processes namely key generation, signing, and verification for secured communication between users for handling industrial IoT data in a cloud computing environment. To start with the industrial data provided as input for carrying out industrial-related applications, key pairs using Quantum Lamport One-Time Key

Generation are acquired by the cloud server. The random selection is carried out between quadrate states and anti-quadrate states separately. The entangled state of qubits is estimated to achieve a public key via a one-time key with higher data confidentiality. After key generation, the signing process is performed by the cloud server by means of Modular Arithmetic-based Digital Signature. With Modular Arithmetic-based Digital signatures, an elliptic curve over the field is employed based on the doubling and addition functions. The digital signature is created and transmitted to the receiver cloud user node. Finally, validation or verification is performed. While the verification is valid, the cloud user decrypts the data. Otherwise, the cloud user does not decrypt the data, therefore ensuring secured communication between devices for industrial data.

SIMULATION SETUP

The Quantum Lamport One-Time Digital Signature Cryptography (QLOT-DSC) technique in the CC environment for safe IIoT data broadcast employs Cloudsim simulator. Number of CU requests chosen for experimental purposes is 250 for QLOT-DSC technique. To calculate QLOT-DSC technique, it is executed using Java in the Cloudsim simulator by collecting data from varied industrial devices and obtaining industrial data accordingly. Execution is estimated by hardware specifications of the Windows 10 Operating system: a Core i3-4130 3.40 GHz processor, 8 GB of RAM, a 1TB (1000 GB) Hard disc, an ASUSTek P5G41C-M Motherboard, as well as Internet Protocol. To conduct experimentation, WUSTL-IIOT-2021 Dataset for IIoT Cyber security Research is taken from https://www.cse.wustl.edu/~jain/iiot2/index.html for safe data storage on CS by avoiding unauthorized access. Industrial Internet of Things data for IoT analytics [30] is used to conduct the experiments. This dataset comprises industrial demand as well as response IoT data for IoT. In QLOT-DSC method, the number of cloud users requests is selected in range of 25–250, and amount of data points is considered in range of 1000–10000. The industrial data as input is considered to perform industrial connected applications. At first, Lamport One-Time Key Generation is employed to make key pairs to improve data confidentiality. Next, digital signature and data encryption are carried out by means of Modular Arithmetic-based Digital Signature model with maximum data integrity rate as well as authentication accuracy. In verification, secure data communication is executed with a higher data confidentiality rate. An experiment is

conducted on data confidentiality, data integrity, message delivery time, and authentication accuracy number of CU requests. QLOT-DSC technique is compared against conventional methods namely incremental aggregator subvector commitment (IASVC) scheme [1] and zero-trust security model [2], respectively. Table 1 shows Simulation setup

Table 1. Simulation setup

Simulation Parameters	Value
Simulator	Cloudsim
Language	Java
Operating system	Windows 10
Processor	Core i3-4130 3.40 GHz
RAM	8 GB
Hard disc	1000 GB
Motherboard	ASUSTek P5G41C-M
Protocol	Internet
Number of cloud users requests	25, 50, 75, 100, 125,150, 175, 200, 225, 250
Simulation time	250 sec
Number of data	1000,2000,3000,4000,5000,6000,7000,8000 ,9000,10000
Data packets	15,30,45,60,75,90,105,120,135,150
No. of trial runs	10

Table 1 depicted Simulated on CloudSim on window 10 using Java. Hardware: Core i3, 8GB RAM, 1TB HDD. Parameters 250s, 10 trials, 5 randomly chosen cloud requests, one set of reference data for each of five chosen requests, and two packet sizes.

RESULTS ANALYSIS AND DISCUSSION

The experimentation results are investigated for existing as well as proposed QLOT-DSC methods. The performance assessment of the research is achieved with corresponding research methods by conventional techniques dependent upon certain parameters (Mansoor, *et al*., 2025; Tandel, *et al*., 2024). The efficiency of the QLOT-DSC technique is estimated based on data confidentiality, data integrity, message delivery time, and authentication accuracy. The QLOT-DSC method is compared by two other safe communication techniques for IIoT in a CC environment, that is, IASVC [1] and zero-trust security model [2] on CloudSim simulator. In the next section, an elaborate comparison of the QLOT-DSC technique, IASVC [1] and zero-trust security model [2] has been done. From the experimental outcome, it concluded which efficiency of QLOT-DSC method is higher than the conventional system. Security analysis is refers to analyze the value of securities such as shares and other instruments to assess the business's entire value. This security analysis is employed for quantitative analysis. The security parameter such as data confidentiality, integrity, accuracy utilized to conduct the experiments. The effectiveness of the QLOT-DSC method is analyzed along with the following parameters with the aid of tables and graphs:

SCENARIO 1: DATA CONFIDENTIALITY

The underlying criterion of importance for cloud-based secured communication relating to IIoT applications is the data confidentiality rate. To be more particular, data confidentiality points out the confidentiality rate with which the industrial data are sent by the cloud user via the cloud server to the intended cloud user nodes at the receiving end. In other words, it evaluated as percentage ratio of number of data sent by cloud user sender nodes being protected from unauthorized cloud users to total number of industrial data. It is stated as below.

$$DC = \frac{D_{prot}}{D} * 100 \quad (11)$$

From equation (11), data confidentiality 'DC' is estimated depend on industrial data being protected from the unintended recipient 'D_{prot}' and the overall data 'D' involved during the data communication process relating to IIoT applications. It is measured in percentage (%). Table 2 gives bestows data confidentiality outcomes attained from (5.1) for proposed method

QLOT-DSC, existing methods IASVC [1] and zero-trust security model [2]. It is evident from table that QLOT-DSC method gives unique solution by employing digital signature via CC environment relating to IIoT applications for secure data communication.

Table 2. Tabulation for data confidentiality

Number of data	Data confidentiality (%)		
	QLOT-DSC	IASVC	Zero-trust security
1000	96	92	89
2000	95	91	85.5
3000	93.5	87.65	78
4000	91	85.35	75.45
5000	89.65	80	70
6000	89.25	78.75	67.35
7000	85.65	75.35	64
8000	85	75	62.35
9000	80.5	72.65	60.5
10000	80	72	60

Table 2. depicts the data confidentiality with numbers of data. Table 2 portrays the data confidentiality for traditional IASVC [1] and zero-trust security model [2]. As considering 1000 data for performing simulation work, the industrial data is protected from the unintended recipient using QLOT-DSC was found to be 960, 920, and 890 using [1] and [2]. Thus, data confidentiality using the QLOT-DSC method is improved in comparison with [1] and [2]. But, by improving the number of industrial data to sent, number of intended cloud users to receive industrial data increases, and therefore data confidentiality also enhances. However comparatively, data confidentiality of the QLOT-DSC technique is minimum. This is owing to the modular arithmetic-based Digital signature is applied separately for signing and validation. By incorporating Modular Arithmetic-based Digital signatures in the QLOT-DSC method, efficient authentication employing hashes is made possible. It only carries out secured data communication between cloud users for IIoT applications. This assists the QLOT-DSC technique in carry out secured data broadcast by training industrial data via deep-secured mechanisms. This

aids in improving data confidentiality of the QLOT-DSC method by 10% compared to [1] and 26% upon comparison with [2], respectively.

SCENARIO 2: DATA INTEGRITY

The second criterion of significance for secured communication between cloud users in the CC environment for IIoT applications is the data integrity rate. In other words, data integrity refers to number of industrial data which are not changed through unauthorized cloud users during data communication initiated by the cloud user node to total number of industrial data. It is expressed as below.

$$DI = \frac{D_{NA}}{D} * 100 \quad (12)$$

From equation (12), the data integrity 'DI', is measured depend on industrial data not changed during communication as initiated by the cloud user 'D_{NA}' to the industrial data 'D'. It is measured in percentage (%). Table 3 shows comparison between data integrity rates using three different methods, QLOT-DSC, IASVC [1] and zero-trust security model [2] respectively.

Table 3 Tabulation for data integrity

Number of cloud users	Data integrity (%)		
	QLOT-DSC	IASVC	Zero-trust security
25	96	93	91.5
50	94.25	91.15	89
75	92	89.35	86.15
100	91.45	87.25	84
125	90.55	86	82.65
150	91	85.35	80.55
175	90.65	85	78.25
200	89.25	84.25	76
225	88.35	84	73.55
250	87.5	82	73

Table 3 portrays data integrity of three methods. While the number of cloud users is improve, there are more CUs waiting in queue to send their industrial data to planned receiver through secured channel, which decreases data integrity. IASVC [1] and zero-trust security model [2] result in lesser data integrity when the number of cloud users increases compared to QLOT-DSC. Let us assume 250 cloud users are taken as input. The data integrity rate of QLOT-DSC was found to be 96% and the data integrity rate using [1] and [2] was found to be 93% and 91.5%, respectively. Likewise, various performance outcomes were observed with each method. Observed outcomes of QLOT-DSC compared to conventional methods The proposed QLOT-DSC method has maintained constant message delivery time throughout the simulated scenarios because the elliptic curve over the field for numbers of data to perform secure communication based on the additive and doubling of the Lamport function. With this function, changes in industrial data that must be communicated between cloud users in a CC environment decrease. The QLOT-DSC methods decrease data integrity by 5% compared to [1] and 12% compared to [2]. This outcome depicts that QLOT-DSC technique has the capability to sustain application performance even for huge numbers of cloud users, ensuring both data integrity and scalability.

SCENARIO 3: MESSAGE DELIVERY TIME

Finally, message delivery time is analyzed. This message delivery time refers to the time consumed in delivering messages or industrial data concerning IIoT applications. The message delivery time is formulated as below.

$$MDT = \sum_{i=1}^{n} CU_i \ * \ Time[SDC] \quad (13)$$

From equation (13), the message delivery time 'MDT' is measured depend on cloud user requests placed in the cloud server for validation 'CU_i' and the time involved in the actual data communication or data delivery '$Time\ [SDC]$'. It is measured in milliseconds (ms). Message delivery time outcomes obtained from (12) for the proposed method QLOT-DSC, conventional methods IASVC [1] and zero-trust security model [2] is demonstrated in below Table 4.

Table 4. Tabulation for message delivery time

Number of cloud users	Message delivery time (ms)		
	QLOT-DSC	IASVC	Zero-trust security
25	14	17.5	22.75
50	15.55	19.25	27.45
75	19.45	26.35	34.15
100	23.25	30.45	42.45
125	27.35	37.65	49.15
150	29.5	39.15	55.15
175	32.45	46	60.45
200	36.25	52.15	65.15
225	40.45	59.35	71.25
250	46	66.25	83.55

The message delivery time for IIoT services is measured to recognize its influence on last performance, i.e., secured communication. Table 4 depicts message delivery time for three dissimilar methods. The message delivery time for QLOT-DSC is minimum compared to [1] and [2] for varying numbers of cloud users. The unit of message delivery time is milliseconds (ms). When number of cloud users (CUs) is 25, 50, or 100, the message delivery time of IBSC [1] and blockchain-based fair non-repudiation service provisioning [2] shows steady enhances, however QLOT-DSC shows quick changes. The simulation results in Table 4 illustrate that when the number of cloud users increases, the QLOT-DSC technique achieves improved message delivery times compared to the existing IASVC [1] and zero-trust security model [2]. This is because of the application of the Quantum Lamport One-Time Key Generation model. With this model, only after successful registration among two CUs and between the cloud user and the CS is a session established. Through this established session, a one-time key called public key, and private key are generated. So, upon establishment among the cloud a public key is generated, followed by that communication is take place. Therefore, message delivery time is said minimized as keys are not generated for every user however only for authenticated users and are also distinct for each session. Therefore, the message delivery time is found to be reduced using

QLOT-DSC by 26% when compared to IASVC [1] and 44% when compared to zero-trust security model [2].

SCENARIO 4: AUTHENTICATION ACCURACY

It is referred to as ratio of number of users appropriately authenticated as authorized or unauthorized to total number of users. It is expressed as below,

$$AA = \left(\frac{Number\ of\ users\ correvtly\ authenticated}{n}\right) * 100 \quad (14)$$

From equation (14), authentication accuracy AA is measured depend on number of cloud users 'n'. It is estimated in percentages (%).

Table 5. Tabulation for Authentication Accuracy

Number of cloud users	Authentication accuracy (%)		
	QLOT-DSC	IASVC	Zero-trust security
25	93	87	80
50	92.65	85	79.65
75	92.25	81.5	79
100	92	79	77.35
125	91.55	76.45	74
150	91.43	74	70.65
175	91.25	72.65	67.45
200	91	70	62.35
225	90.65	68.8	60.15
250	90.25	65	60

Performance of authentication accuracy for dissimilar cloud users is represented in Table 5. As exposed in table outcomes, numbers of cloud users are considered in counts from 25 to 250. Different outcomes are examined for different inputs. Examined outcomes denote that QLOT-DSC method enhances authentication accuracy over existing methods. This is proven during

sample calculation performed with 25 users. By using QLOT-DSC method, 22 users are properly authenticated as authorized or unauthorized, and the accuracy is 93%. Furthermore, '21' users and 20 users are correctly authenticated as authorized or unauthorized, and accuracy is 89% and 85% using [1] and [2]. From these outcomes, it is inferred that the authentication accuracy is higher by QLOT-DSC method than [1] and [2]. Ten results are observed for each method. The overall outcomes demonstrate that the authentication accuracy of the IoT QLOT-DSC method enhanced by 22% and 30% than the [1] [2]. This enhancement is attained because of the application of the Modular Arithmetic-based Digital Signature separately for signing and validation. In this way, efficient authentication employing hashes is achieved. As a result, the verification function correctly authenticates authorized or unauthorized users by enhanced accuracy.

SPACE COMPLEXITY

It is measured as memory space needed to store data to server. It is estimated in megabytes (MB) using the following mathematical equation (15),

Space complexity = number of data * space (storing single data) (15)

Table 6. Tabulation for Space Complexity

Number of data	Space complexity (MB)		
	QLOT-DSC	IASVC	Zero-trust security
1000	20	25	27
2000	23	27	31
3000	25	29	35
4000	27	31	36
5000	29	33	39
6000	31	36	40
7000	35	39	43
8000	37	41	45
9000	39	43	47
10000	41	47	50

Table 6 displays space complexity for proposed and existing methods. QLOT-DSC method, IASVC [1] and zero-trust security model [2]. The outcome denotes which complexity is minimum by QLOT-DSC method than two traditional methods. This is owing to application of the Arithmetic-based Digital Signature Cryptography method. Authorized CU transmits their data to CS for storage. CS employs one-way hash function to generate hash for every industrial data previous to storage. Hence, hash value of data utilized less space. Space complexity of QLOT-DSC method is considerably decreased by 13% and 23% than the [1] and [2].

COMPARISON WITH PRECEDING LITERATURE

As of simulation comparisons by preceding literature, QLOT-DSC method offers superior performance through enhanced data confidentiality and integrity. We compare data confidentiality rate, data integrity rate, message delivery time, authentication accuracy, and space complexity of QLOT-DSC method by preceding work.

Table 7. Comparison between QLOT-DSC method and previous literature

Method	**Proposed method**	**Existing method [1]**	**Existing method [2]**
	QLOT-DSC method	IASVC	zero-trust security model
Contribution	To attain security	To protect IIoT data security	To provide huge secure device access
Merits	Enhanced confidentiality rate, integrity, authentication accuracy with less space complexity	Augments communication efficiency as well as decreases the proof size	Achieving zero-trust devices authentication in 5GIoT
Demerits	Only one dataset is considered.	Multilinear mapping was not used	data delivery time was not focused

Data Confidentiality Rate (%)	89 %	81 %	71 %
Data Integrity Rate (%)	91 %	87 %	82 %
Message delivery time (ms)	28 ms	39 ms	51 ms
Authentication accuracy (%)	92 %	76 %	71 %
Space complexity (MB)	31MB	35 MB	o MB

CONCLUSION AND FUTURE WORK

The combination of IIoT as well as cloud is at cusp of altering our everyday lives and society as entire. As well, promising confidentiality as well as authenticity of IIoT data are significant issues for IIoT. To address this problem, novel QLOT-DSC method is introduced in this manuscript. Compared to previous works, QLOT-DSC method achieves the security of data communication in IIoT with a higher data integrity and confidentiality rate. In order to reduce the message delivery time and space complexity, we utilized Quantum Lamport One-Time Key Generation to create a key generation. The security analysis is carefully conducted with the aid of Modular Arithmetic-based Digital signatures for digital signature and data encryption. Based on two distinct keys (i.e., Quantum Lamport Private Key and Public Key), flags are generated via doubling and additive operations. Hence, it improves data confidentiality and integrity in a minimum amount of time. The signing process is executed through Modular Arithmetic-based Digital Signature model by means of digital signature and data encryption. Thus, it enhances authentication accuracy. The proposed QLOT-DSC method is implemented and assessed by a comprehensive performance analysis using WUSTL-IIOT-2021 datasets. Quantitative analysis is performed using the QLOT-DSC method and the other existing methods with different metrics.

Results showed that the pros of the QLOT-DSC method provide superior performance through an enhancement in data confidentiality and integrity as well as minimize message delivery time compared to conventional methods. The cons of proposed research work are that it uses only one dataset for assessment. In future work, proposed technique is extending to consider secured data storage on a cloud server by using novel cryptography methods. Also, more data sets are utilizing to exhibit and evaluate the robustness of proposed technique for safe data broadcast in cloud environment.

LIST OF ABBREVIATIONS

IIoT	Industrial IoT
CC	Cloud Computing
IoT	Internet of Things
QLOT-DSC	Quantum Lamport One-Time Digital Signature Cryptography
CS	Cloud Server
IBSC	Identity-Based Signcryption
MBDHI	Modified bilinear Diffie-Hellman inversion
LOT-DSC	Lamport One-Time Digital Signature Cryptography
TSDF	Transfer learning-based Secure Data Fusion
GDDPG	Guidance-based Deep Deterministic Policy Gradient
HBC	Hermitian-based cryptosystems
PPEDL-MDTC	Privacy-preserving encryption with DL-based medical data transmission and classification
HNS-CODML	Hashed Needham Schroeder Cost Optimized Deep Machine Learning

QLOT-DSC	Quantum Lamport One-Time Digital Signature Cryptography
IBSC	Identity-Based Signcryption
MB	Megabytes

DATA AVAILABILITY STATEMENTS

Dataset name: WUSTL-IIOT-2021 Dataset for IIoT Cybersecurity Research

Download link: https://www.cse.wustl.edu/~jain/iiot2/ftp/wustl_iiot_2021.zip

COMPETING INTERESTS

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this manuscript.

FUNDING STATEMENT

No funding received for the research

AUTHOR'S CONTRIBUTIONS

Flindon W.G. contributed to the design, execution of the research, analysis of the results and to writing of the paper. Dr. Divya S.V.contributed to the design of research and review of article. All authors reviewed the manuscript.

ACKNOWLEDGMENTS

The authors are thankful to Department of Computer Science, Noorul Islam Centre for Higher Education for supporting the research.

REFERENCES

Wang, J., Chen, J., Ren, Y., Sharma, P. K., Alfarraj, O., & Tolba, A. (2022). Data security storage mechanism based on blockchain industrial Internet of Things. *Computers & Industrial Engineering*, *164*, 107903.

Li, S., Iqbal, M., & Saxena, N. (2022). Future industry internet of things with zero-trust security. *Information Systems Frontiers*, 1-14.

Liu, J., Wen, J., Zhang, B., Dong, S., Tang, B., & Yu, Y. (2023). A post quantum secure multi-party collaborative signature with deterability in the Industrial Internet of Things. *Future Generation Computer Systems*, *141*, 663-676.

Mahmood, K., Shamshad, S., Saleem, M. A., Kharel, R., Das, A. K., Shetty, S., & Rodrigues, J. J. (2024). Blockchain and PUF-based secure key establishment protocol for cross-domain digital twins in industrial Internet of Things architecture. *Journal of Advanced Research*, *62*, 155-163.

Kumar, P., Kumar, R., Kumar, A., Franklin, A. A., Garg, S., & Singh, S. (2022). Blockchain and deep learning for secure communication in digital twin empowered industrial IoT network. *IEEE Transactions on Network Science and Engineering*, *10*(5), 2802-2813.

Toradmalle, D. K., & Amarendra, K. (2023). An Attack-Resistant Light-Weight Digital Signature Based On An Elliptic Curve For Improved Security In Resource Constrained Applications. 1-14

Yin, H. L., Fu, Y., Li, C. L., Weng, C. X., Li, B. H., Gu, J., ... & Chen, Z. B. (2023). Experimental quantum secure network with digital signatures and encryption. *National Science Review*, *10*(4), nwac228.

Hewa, T., Braeken, A., Liyanage, M., & Ylianttila, M. (2022). Fog computing and blockchain-based security service architecture for 5G industrial IoT-enabled cloud manufacturing. *IEEE transactions on industrial informatics*, *18*(10), 7174-7185.

Muthukumaran, V., & Arun, K. (2023). Efficient Digital Signature Scheme for Industrial Internet of Things using semi-group. *International Journal of Human Computations & Intelligence*, *2*(1), 34-39.

Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An Overview of Privacy Dimensions on the Industrial Internet of Things (IIoT). *Algorithms*, *16*(8), 378.

Karati, A., Islam, S. H., Biswas, G. P., Bhuiyan, M. Z. A., Vijayakumar, P., & Karuppiah, M. (2017). Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of Things environments. *IEEE Internet of Things Journal*, *5*(4), 2904-2914.

Xu, Y., Ren, J., Wang, G., Zhang, C., Yang, J., & Zhang, Y. (2019). A blockchain-based nonrepudiation network computing service scheme for industrial IoT. *IEEE Transactions on Industrial Informatics*, *15*(6), 3632-3641.

Liang, W., Tang, M., Long, J., Peng, X., Xu, J., & Li, K. C. (2019). A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things. *IEEE Transactions on Industrial Informatics*, *15*(6), 3582-3592.

Liu, C. H., Lin, Q., & Wen, S. (2018). Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning. *IEEE Transactions on Industrial Informatics*, *15*(6), 3516-3526.

Sharma, R., & Arya, R. (2022). Secure transmission technique for data in IoT edge computing infrastructure. *Complex & Intelligent Systems*, *8*(5), 3817-3832.

Verma, N., Singh, S., & Prasad, D. (2022). A review on existing IoT architecture and communication protocols used in healthcare monitoring system. *Journal of The Institution of Engineers (India): Series B*, *103*(1), 245-257.

Rachit, Bhatt, S., & Ragiri, P. R. (2021). Security trends in Internet of Things: A survey. *SN Applied Sciences*, *3*, 1-14.

Sodhro, A. H., Pirbhulal, S., Muzammal, M., & Zongwei, L. (2020). Towards blockchain-enabled security technique for industrial internet of things based decentralized applications. *Journal of Grid Computing*, *18*(4), 615-628.

Yin, F. (2021). Elman-Based Secure Data Transmission Quality Prediction for Complex IoT Networks. *Mobile Information Systems*, *2021*(1), 4132622.

Lin, H., Hu, J., Wang, X., Alhamid, M. F., & Piran, M. J. (2020). Toward secure data fusion in industrial IoT using transfer learning. *IEEE Transactions on Industrial Informatics*, *17*(10), 7114-7122.

Fu, J. S., Liu, Y., Chao, H. C., Bhargava, B. K., & Zhang, Z. J. (2018). Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing. *IEEE Transactions on Industrial Informatics*, *14*(10), 4519-4528.

Liang, W., Tang, M., Long, J., Peng, X., Xu, J., & Li, K. C. (2019). A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things. *IEEE Transactions on Industrial Informatics*, *15*(6), 3582-3592.

Donta, P. K., Srirama, S. N., Amgoth, T., & Annavarapu, C. S. R. (2022). Survey on recent advances in IoT application layer protocols and machine learning scope for research directions. *Digital Communications and Networks*, *8*(5), 727-744.

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in industry*, *101*, 1-12.

Srinidhi, N. N., Kumar, S. D., & Venugopal, K. R. (2019). Network optimizations in the Internet of Things: A review. *Engineering Science and Technology, an International Journal*, *22*(1), 1-21.

Luo, X., Yin, L., Li, C., Wang, C., Fang, F., Zhu, C., & Tian, Z. (2020). A lightweight privacy-preserving communication protocol for heterogeneous IoT environment. *IEEE Access*, *8*, 67192-67204.

Macedo, E. L., De Oliveira, E. A., Silva, F. H., Mello, R. R., França, F. M., Delicato, F. C., ... & de Moraes, L. F. (2019). On the security aspects of Internet of Things: A systematic literature review. *Journal of Communications and Networks*, *21*(5), 444-457.

Qin, J., Li, Z., Wang, R., Li, L., Yu, Z., He, X., & Liu, Y. (2021). Industrial Internet of Learning (IIoL): IIoT based pervasive knowledge network for LPWAN—concept, framework and case studies. *CCF Transactions on Pervasive Computing and Interaction*, *3*(1), 25-39.

Singh, P., Masud, M., Hossain, M. S., & Kaur, A. (2021). Cross-domain secure data sharing using blockchain for industrial IoT. *Journal of Parallel and Distributed Computing*, *156*, 176-184.

Wei, M., Hong, S. H., & Alam, M. (2016). An IoT-based energy-management platform for industrial facilities. *Applied energy*, 164, 607-619.

Alzubi, O. A., Alzubi, J. A., Dorgham, O., & Alsayyed, M. (2020). Cryptosystem design based on Hermitian curves for IoT security. *The Journal of Supercomputing*, 76(11), 8566-8589.

Alzubi, J. A., Alzubi, O. A., Beseiso, M., Budati, A. K., & Shankar, K. (2022). Optimal multiple key-based homomorphic encryption with deep neural networks to secure medical data transmission and diagnosis. *Expert Systems*, 39(4), e12879.

Alzubi, J. A., Manikandan, R., Alzubi, O. A., Qiqieh, I., Rahim, R., Gupta, D., & Khanna, A. (2020). Hashed Needham Schroeder industrial IoT based cost optimized deep secured data transmission in cloud. *Measurement*, 150, 107077.

Alweshah, M., Hammouri, A., Alkhalaileh, S., & Alzubi, O. (2023). Intrusion detection for the internet of things (IoT) based on the emperor penguin colony optimization algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 14(5), 6349-6366.

Alzubi, J. A., Alzubi, O. A., Suseendran, G., & Akila, D. (2019). A novel chaotic map encryption methodology for image cryptography and secret communication with steganography. *Int J Recent Technol Eng,* 8(1C2), 1122-1128.

Chang, M. H., & Yeh, Y. S. (2005). Improving Lamport one-time signature scheme. *Applied mathematics and computation*, 167(1), 118-124.

Mansoor, K., Afzal, M., Iqbal, W., & Abbas, Y. (2025). Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices. *Cluster Computing*, *28*(2), 93.

Tandel, P., & Nasriwala, J. (2024). Secure authentication framework for IoT applications using a hash-based post-quantum signature scheme. *Service Oriented Computing and Applications*, 1-12.