Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.029260
Article

Tech Science Press

Novel Homomorphic Encryption for Mitigating Impersonation Attack in Fog Computing

V. Balaji and P. Selvaraj*

Department of Computing Technologies, College of Engineering and Technology, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, 603203, Tamilnadu, India
*Corresponding Author: P. Selvaraj. Email: selvarap@srmist.edu.in
Received: 28 February 2022; Accepted: 11 April 2022

Abstract: Fog computing is a rapidly growing technology that aids in pipelining the possibility of mitigating breaches between the cloud and edge servers. It facilitates the benefits of the network edge with the maximized probability of offering interaction with the cloud. However, the fog computing characteristics are susceptible to counteract the challenges of security. The issues present with the Physical Layer Security (PLS) aspect in fog computing which included authentication, integrity, and confidentiality has been considered as a reason for the potential issues leading to the security breaches. In this work, the Octonion Algebra-inspired Non- Commutative Ring-based Fully Homomorphic Encryption Scheme (NCR-FHE) was proposed as a secrecy improvement technique to overcome the impersonation attack in cloud computing. The proposed approach was derived through the benefits of Octonion algebra to facilitate the maximum security for big data-based applications. The major issues in the physical layer security which may potentially lead to the possible security issues were identified. The potential issues causing the impersonation attack in the Fog computing environment were identified. The proposed approach was compared with the existing encryption approaches and claimed as a robust approach to identify the impersonation attack for the fog and edge network. The computation cost of the proposed NCR-FHE is identified to be significantly reduced by 7.18%, 8.64%, 9.42%, and 10.36% in terms of communication overhead for varying packet sizes, when compared to the benchmarked ECDH-DH, LHPPS, BF-PHE and SHE-PABF schemes.

Keywords: Fog computing; physical layer security; non- commutative ring-based fully homomorphic encryption; impersonation attack

1 Introduction

The existence of pervasively connected smart devices constitutes the modern computing paradigm. The continuous and rapid advent of large-scale wireless sensor networks (WSNs), connected vehicles, smart metering, wearable computing, smart city, and smart home has made the communication process much smarter and highly connected through the Internet of Things. It is observed that the widespread of Fog computing has increased rapidly in the modern IT industry to the maximum level of 22% from the year,

2018 and exponentially increasing as per the reports of International Data Corporation (IDC) [1]. The smart devices involved in the process of communication generally face challenges that are deep-rooted in the perspectives of bandwidth, storage, battery, and computational power, which in turn prevent the user experience and quality of service (QoS). In this context, Cloud Computing is determined as the most predominant computing paradigm to prevent the overhead of restricted resources offered by smart devices [2]. Cloud Computing is capable of delivering significant services in terms of software, platform, infrastructure and enable application with on-demand resources at the very least expense [3]. However, Cloud Computing may not provide a comprehensive solution for different types of modern IT applications. The applications of Fog generally require mobility support, geographical distribution, location awareness, and low latency. Most of the problems present with the enablers of the Fog computing environment remain unsolved. Further, Cloud Computing has attracted major attention and gained more probability among organizations and individuals, as it improves the quality of the service demands cost-effective way [4]. The aforementioned advantages of Cloud Computing resulted in a very large and cost-effective global scaling as it has the potential to facilitate the necessitated extent of resources to the appropriate geographical area [5]. The cloud-based services would also improve organizational productivity by minimizing the number of chores necessitated to be achieved by the team concerned with information technology [6]. The minimization of chores may result in the increased availability, security, and performance of the cloud-based application environment [7]. This fog layer is the most significant layer suitable for satisfying the objective of computing. The fog devices constitute the intermediate tier/level between the cloud layer and the user. It is generally comprised of fog nodes [8] that are constructed in the form of base stations, proxy servers, set-top boxes, routers, etc. The fog nodes play an anchor role in data reception from the centralized cloud data centers if the conditions of the user requirements are not satisfied [9]. Once the data reception is achieved by the fog devices, it then transmits the received data to the end-users and made the data to be available in a centralized and decentralized manner. In addition, the user can comfortably access the data from the fog nodes through secured channel communication. The Impersonation Attack is a type of attack in which an attacker may be able to determine the identity of the legitimate entities participating in a system or a protocol used for communication. In specific, Fog Computing is generally vulnerable to impersonation attacks, as they are much exposed to the wireless channel characteristics existing between the end-users and the fog nodes. This impersonation attack controls the end user nodes and fog nodes and subsequently emerges as a substitute user or node by inheriting a most adaptable forged behavior. This attack also derives the benefits of illegitimate nodes for launching Denial-of-Service (DoS) attacks and man-in-the-middle attacks. The different types of attacks [10] that could be launched in the fog-assisted cloud computing environment are analyzed in the following section.

1.1 Impersonation Attack

It is an attack in which an attacker tries to determine the identity of the legitimate entity participating in a system or a protocol used for communication. In specific, fog computing is generally vulnerable to impersonation attacks, as they are much exposed to the wireless characteristics existing between the end-users and the fog nodes. This impersonation attack comprises the nodes (end-users and fog nodes) to emerge as a substitute user or node by inheriting a most adaptable forged behavior. This attack also derives the benefits of illegitimate nodes for launching Denial-of-Service (DoS) attacks and man-in-the-middle attacks.

1.2 Denial-of-Service (DoS) Attacks

It is a significant attack that mainly targets the system services availability. In the fog computing scenario, DDoS attacks completely concentrate on the services facilitated by the cloud by minimizing their capability in ensuring optimal utilization of network resources.

1.3 Man-in-the-Middle Attacks

This attack possesses the possibility of modifying and secretly relaying the communication established among the interacting parties, which may think that they are interacting directly with one another. For instance, Man-in-the-Middle Attack is an active eavesdropping process in which the attacker performs independent connections to the target and forwards different messages among the communicating parties in order to make them believe that each party is cooperating with one another by transmitting messages between them, while the complete interaction is attacker compromised. In this attack, the attacker attempts to intercept the complete set of relevant messages that are exchanged between the newly injected ones and the two victims.

1.4 Replay Attack

It is an attack in which an attacker eavesdrops on the secure communication channel by intercepting them in order to introduce intentional, fraudulent delays and retransmits or misdirects the recipient as per its requirements. In fog computing, an attacker does not require any advanced knowledge for message decryption once it is being captured from the network. The attempt launches this kind of attack by retransmission of the complete data that are exchanged during the session.

1.5 Key Disclose Attack

In this attack, the attacker intercepts the communication channel established between cooperating parties in order to gain the benefits of keys that are exchanged. The attacker does not utilize the capture session keys rather than they forward to other unsecured communication party for deriving possible degree of benefits from the communication.

1.6 Perfect Forward Secrecy Attacks

This attack eavesdrops on the data being encrypted based on the utilization of distinct and random session keys exchanged between the trusted communication parties. This attack is generally launched during the process of decoding the captured data, even when the secret long-term key is not compromised by the attacker.

1.7 Data Modification Attack

This attack is launched by tampering with the data which is transmitted between the parties of communication in the fog computing scenario. It belongs to the category of integrity attack that interrupts the availability of the resource. This attack targets the illegitimate modification of data, especially adding, deleting, and renaming of data that are shared in the context of fog computing.

The proposed research workflow is given in Fig. 1. In this work, Octonion Algebra-inspired Non-Commutative Ring-based Fully Homomorphic Encryption Scheme (NCR-FHE) was proposed as a secrecy improved technique. The proposed encryption scheme was derived by exploiting the Octonion algebra to facilitate the maximum levels of security for the cloud-based big data applications. The issues of physical layer security were exploited to identify the vulnerable features of the channel that could be established between the fog node and the end-user. The possibilities of impersonation attacks in the fog computing environment were analyzed. This NCR-FHE was designed with the capability of guaranteeing security even at the bit-level data transmission. The proposed mechanism had adopted the merits of circuit switching and modulus switching operation to handle the exploitation happening during the data transmission.

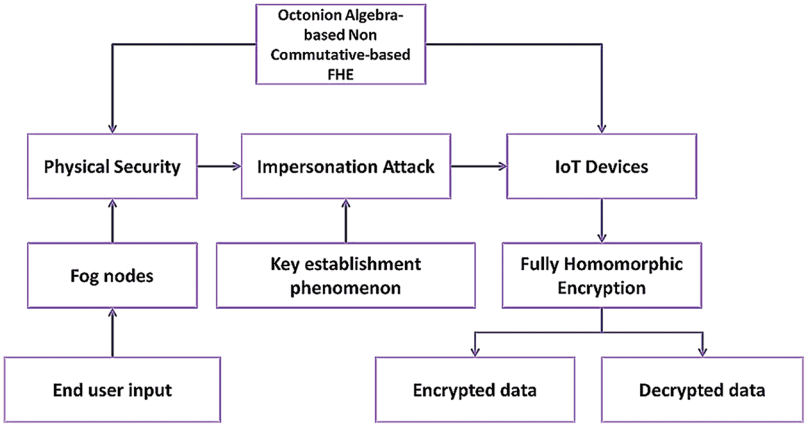

Figure 1: General workflow of proposed technique

The rest of the paper is organized as follows. Section 2 presents a comprehensive review of the existing fully homomorphic encryption scheme-based impersonation attack mitigation schemes contributed to the literature. Section 3 presents the detailed view of the proposed Octonion Algebra-inspired Fully Homomorphic Encryption Scheme proposed for handling the influence of impersonation attacks at the physical layer of the fog environment, Section 4 presents the simulation results and discussion of the proposed NCR-FHE with justifications. Section 5 concludes the paper with the major contributions of the proposed scheme and the future scope of enhancement.

2 Related Works

2.1 ElGamalEncryption-Based Lightweight Data Aggregation Approach

A privacy-preserving data aggregation scheme using Binary protocol was proposed for utilizing the minimal number of local communications among the nodes in the network [11]. This Binary protocol-based security scheme was capable to operate even when a significant number of Fog devices fails to operate. But it guarantees provable privacy to the users utilizing the Fog network. This privacy-preserving data aggregation scheme significantly necessitates less computation without maximal exploitation of heavy cryptography. It was also determined to predominantly reduce the error compared to the traditional privacy-preserving schemes the contributed to securing fog nodes under false injection attacks. An ElGamal encryption-based lightweight data aggregation approach was proposed for handling the impact of false data injection in cloud-assisted Fog devices [12]. This ElGamal encryption approach was contributed to resisting the feasibility of injecting any type of false data by including a reliable and fault-tolerant strategy to prevent data leakages. The security analysis of this technique was realized to be potential in computation time and communication overhead independent of the number of Fog devices deployed in the sensing area. A Secure Homomorphic Encryption scheme using Paillier Algorithm-Based Blinding Factor (SHE-PABF) was proposed for data aggregation with privacy preservation properties [13]. The blinding factor used in this Paillier encryption algorithm for verifying whether the data collected from Fog devices are legitimate or malicious in nature. The computation and communication overhead of the Paillier encryption algorithm was determined to be superior to the baseline schemes under the impact of various Fog sensing nodes in the fog computing context. The security and simulation investigation of the Paillier algorithm was identified to be more effective and efficient independent to the number of fog nodes existing in the context of the application. Elliptic Curve Diffie–Hellman (ECDH) or Diffie–Hellman (DH) integrated with the symmetric homomorphic encryption was proposed for preserving the privacy of user information from being leaked and modified in the network [14]. This

ECDH and DH-based privacy-preserving scheme was proposed for preventing the issue of the existing privacy schemes that suffer from high communication and computation costs. It is identified to be superior to the baseline schemes in incurring low message overhead, high resilience against session key attacks, and reduced transmission. It is also capable of sustaining the degree of data integrity against the problem of data forgery and unauthorized modification with guaranteed authenticity of user utilization data. A deep learning strategy-based false data injection attack mitigation method was proposed for demonstrating its impact on the Fog nodes [15]. It specifically used three algorithms that are related to Convolutional Neural Network, Gated Resources Unit (GRU), and Long Short-Term Memory (LSTM) for forecasting the residual life of hybrid Fog devices The simulation results of this approach exhibited a considerable improvement in residual life on par with other approaches considered for comparison. Lattice-based Homomorphic Privacy Preservation Scheme (LHPPS) was improving confidentiality and integrity for ensuring consumer secrecy under false data injection attacks with respect to smart grid connections [16]. This LHPPS completely depends on simple arithmetic operation inherent with the Lattice-based Homomorphic encryption approach. This utilization of Lattice properties in LHPPS is potent in reducing the number of computations involved in the process of privacy preservation. The security analysis and simulation investigation of this LHPPS scheme confirmed maximum consumer privacy, less computation complexity, lightweight communication, integrity, and message authentication. The simulation results also proved the significance of the LHPPS scheme in reducing the computational load and communication overhead incurred in fog environments.

Furthermore, Fine-grained data analysis-based privacy-preserving data aggregation scheme was proposed for securing the user data from being leaked and fabricated [17]. This privacy-preserving approach was significant enough handling the impacts introduced by the failure of one or more fog nodes in the Fog Computing environment. The communication and computation overhead of this privacy preserving scheme was identified to be improved compared to the binary protocol and ECDH-based privacy preservation techniques. A sparse strategy for mitigating false data injection attacks was proposed to Fog Computing with the optimality of restricted resources [18]. This sparse strategy is propounded for handling the practical situation even when the network possesses incomplete information about energy and limited access to measuring the resources. It especially utilized the merits of the power flow equation for accurately identifying the network energy information. It is also determined to highly fault-tolerant to a range of attacks named bad data detection through the inclusion of the L2-norm test. It also incorporated the algorithm of locally regularized fast recursive for potentially enhancing the attack vectors of sparsity. A fog-assisted privacy-preserving scheme for data aggregation was proposed using a modified version of the Paillier cryptosystem for making it resistant to false data injection attacks [19]. This Paillier cryptosystem approach is resilient against false data injection attacks by eliminating the inserted value from the view of external attackers. It was determined to be fault-tolerant since the malfunctioning of fog nodes does not influence the process of data aggregation. The communication costs, decryption costs, and cost of aggregation associated with this Paillier cryptosystem-based privacy-preserving scheme were identified to be minimal compared to the existing baseline approaches. In specific, this Paillier cryptosystem-based privacy-preserving scheme was confirmed to minimize communication costs by 50%, compared to the LHPPS and ECDH-DH approaches.

Furthermore, Data Aggregation Scheme Using Fully Homomorphic Encryption (DAS-FHE) scheme with privacy awareness was proposed for resolving the issues of false injection attacks under fog computing [20]. This DAS-FHE considered the fog nodes to be curious, but honest with maximized fault-tolerance properties. The number of mathematical operations used by this FHE is highly simplified in a way to handle the impact of the false injection attack. The simulation results of this DAS-FHE scheme were confirmed to decrease the computation costs and communication by 5.72% and 8.43%, compared to LHPPS and ECDH-DH approaches. Then, a secure data aggregation scheme was proposed using some

specific auxiliary ciphertext subtly was proposed for attaining data integrity and privacy preservation with fault tolerance and differential privacy [21]. It was proposed for achieving a better trade-off between security and accuracy during the provision of differential privacy. It inherently used a potential authentication method for significantly generating and sharing session keys in a non-cooperative manner. It also leveraged the benefits Advanced Encryption Scheme (AES) for ensuring data integrity and source authentication over the propagated data.

2.2 Drawbacks of the Existing Methodologies

This efficiency and security degree of this privacy preservation approach is also achieved based on computational overhead decentralization and hub authority entities by preventing false injection attacks. The simulation results of this privacy-preserving scheme are identified to minimize robustness of fault tolerance, communication cost, and computational complexity compared to the baseline approaches used for exploration. A Blinding factors-based Paillier Homomorphic Encryption (BF-PHE) scheme was proposed for ensuring privacy preservation in fog computing during the process of data aggregation [22–23].

2.3 Contribution of the Proposed Work

This BF-PHE scheme confirmed the process of data injection only from legitimate Fog devices with any leakage and modification even when the cloud control center and fog nodes are honest and curious. This BF-PHE scheme was also identified to be fault-tolerant, since the failure of any fog nodes has not influenced the aggregation of data attained from other cooperating devices of the fog-cloud environment. The simulation results of this BF-PHE scheme were confirmed to decrease the computation costs and communication by 10.21% and 13.84%, compared to LHPPS and ECDH-DH approaches. The proposed Octonion Algebra-inspired Fully Homomorphic Encryption Scheme is a novel trustworthy method against impersonation attacks. This encryption scheme is composed of a complex number system which is highly rigid against impersonation attacks.

3 Proposed Octonion Algebra Inspired Fully Homomorphic Encryption Scheme (NCR-FHE)

The components in the fog computing environment are trustworthy but inquisitive in nature. In particular, the components are capable of reasonably accomplishing the tasks allocated to them. However, they are anxious about the confidentiality of the IoT devices. Cloud Control Centre (CCC) can interrupt the data forwarded from each individual IoT device with the significance of gaining secret information related to the device owner. It also provides the related information that assists the fog computing environment in terms of finance. The communicating entities cannot collude even when they desire to be curious. Nevertheless, each individual IoT device demands knowledge of the data received from the cooperating IoT devices for verifying whether the collaboration is beneficial. The IoT devices may possibly enter into a failed state and does not report appropriate information within a specific period of time. Each IoT device forwards packets to the entities in the fog computing environment within the area of coverage. If an attacker exists between the Internet of Things (IoT) device and the Cloud Credential Council (CCC), the possibility of intercepting secret keys becomes more probable. Furthermore, the attackers gaining control over the IoT devices and external attackers may attempt to realize the users' sensitive information that is shared in the fog computing environment.

The Octonion has been considered as the normed division algebra that comprises four norms that include complex numbers, real numbers, Octonion, and Quaternion. The Octonion algebra was invented by Cayley and Greaves in an independent manner. The Octonion algebra is an alternative division algebra that possesses the dimension of 1, 2, 4, and 8 respectively. The proposed Octonion Algebra-inspired Fully Homomorphic Encryption Scheme (NCR-FHE) is striving to improve secrecy by exploiting the benefits of Octonion

algebra. The proposed encryption scheme could enhance the level of security demanded by big data applications. The derived workflow is depicted in Fig. 2. This proposed Octonion algebra-based encryption possesses the probability of interpreting complex numbers $c + id$ with $[c, d]$ as the pair of real numbers by utilizing the formula of Cayley and Dickson under $[c, d] \in H$ (Quaternions). This Octonion algebra holds the properties of addition and multiplication as defined in Eqs. (1) and (2) respectively.

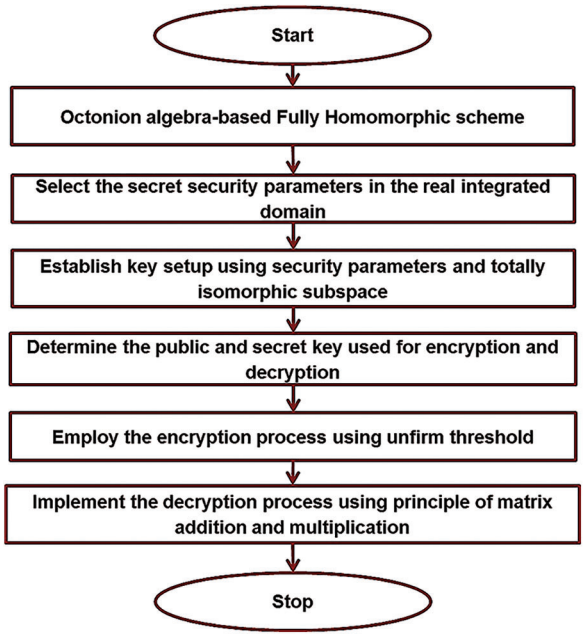

Figure 2: Proposed workflow

$$[\boldsymbol{e},\boldsymbol{f}] + [\boldsymbol{g},\boldsymbol{h}] = [\boldsymbol{e} + \boldsymbol{g},\boldsymbol{f} + \boldsymbol{h}] \tag{1}$$

$$[\boldsymbol{e},\boldsymbol{f}] * [\boldsymbol{g},\boldsymbol{h}] = [\boldsymbol{eg} - \boldsymbol{hf}^*, \boldsymbol{e}^*\boldsymbol{h} + \boldsymbol{fg}] \tag{2}$$

where, $[c, d]$ are $[e, f]$ considered as the elements of quaternions with its conjugate c, d, e and f respectively. The conjugate of the quaternion number $[c, d] \in H$ is defined as $[c, d]^* = [c,^* - d]$.

In Octonion algebra, each of the Octonion number $[C_0, \ldots\ldots, C_7] \in R^8$ is represented through the norm of defined through Eq. (3).

$$\|C\| = \sqrt{\left(C_0^2 + \ldots\ldots + C_7^2\right)} \tag{3}$$

However, the Octonion algebra used in the proposed NCR-FHE scheme is defined over any of the field F_r with $r = s^n$ or on the ring Z_r defined with $r = s_1^{q1} \ldots\ldots\ldots s_{rn}^{qn}$. But the division operation is not utilized in the formulation of the proposed NCR-FHE scheme.

The list of activities involved in the proposed NCR-FHE scheme to enhance the security is as follows: (i) Key set up phase, (ii) Encryption phase and (iii) Decryption phase.

3.1 Key Setup Phase

In this proposed NCR-FHE, initially $r = s_1 s_2 s_3 s_4$ is selected based on a security parameter γ. Let $r_0 = s_1 s_2$ with a chosen totally isomorphic subspace $W \subset Z_r^8$, which is considered to be closed under

Octonion addition and multiplication. Then, $\varphi = H_2(r)$ is selected randomly with 8×8 matrix with random invertible characteristics designated as. In this context, the private key and the system public parameter are considered as (r_0, M, φ, W) and Z_r respectively.

3.2 Encryption Phase

In this encryption phase, select $q \in Z_r$ and $z \in W$ with the property satisfying the condition for any considered message $n \in Z_{r0}$. At this juncture, $n^1 = (\varphi(n + qr_0)1 + z)$ and B_n^1 is the associated matrix considered for the Octonion number n. As the probability for converges to a uniform threshold, similar characteristics of q and z must be selected in constant rounds. Thus, the ciphertext derived based on Octonion Algebra is represented in Eq. (4)

$$C_n = Octon..Encryption(key, n) = M^{-1}B_n^L M \in Z_r^{8x8} \tag{4}$$

3.3 Decryption Phase

In this decryption process, the plaintext can be decrypted for the received ciphertext derived based on Eq. (5)

$$n = Octon..Dec(key, C_n) = \varphi^{-1}(1\left(MC_nM^{-1}\right) mod\ W\ mod\ r_0 \tag{5}$$

Apparently the condition $1(MC_nM^{-1}) = 1B_n^1 = n$ is satisfied during the phase of decryption.

In the proposed NCR-FHE scheme, the addition of any ciphertexts C_{n0} and C_{n1} is defined based on the principle of matrix addition, derived over regular component represented through Eq. (6)

$$C_{n0+n1} = C_{n0} + C_{n1} \tag{6}$$

Similarly, the addition of any ciphertexts C_{n0} and C_{n1} is defined based on the principle of matrix multiplication, derived over regular component represented through Eq. (7)

$$C_{n0n1} = C_{n0} * C_{n1} = M^{-1}B_{n0}^1 M * M^{-1}B_{n1}^1 M = M^{-1}B_{n0}^1 B_{n1}^1 M \tag{7}$$

The proposed NCR-FHE scheme is considered to verify the addition Homomorphic property of the aforementioned encryption scheme based on Eqs. (8)–(14)

$$Octon..Dec(key, C_n) = \varphi^{-1}(1\left(MC_nM^{-1}\right) mod\ W\ mod\ r_0 \tag{8}$$

$$= \boldsymbol{\varphi^{-1}(n_0(n_1 1))\ mod\ W\ mod\ r_0} \tag{9}$$

$$= \boldsymbol{\varphi^{-1}(n_0 n_1 1))\ mod\ W\ mod\ r_0} \tag{10}$$

$$= \boldsymbol{\varphi^{-1}(\varphi(n_0 1 + q_0 r_0 1 + z_0)(n_1 1 + q_1 r_1 1 + z_1)1\ mod\ W\ mod\ r_0} \tag{11}$$

$$= \boldsymbol{(n_0 + q_0 r_0 = z_0)(n_1 + q_1 r_1 + z_1)1\ mod\ W\ mod\ r_0} \tag{12}$$

$$= \boldsymbol{(n_0 + q_0 r_0)(n_1 + q_1 r_1)\ 1\ mod\ r_0} \tag{13}$$

$$= \boldsymbol{n_0 n_1 1} \tag{14}$$

In the aforementioned decryption process, if the private secret key of the encryption process is (r_0, M, φ, W) with $\delta = [1, a_1, \ldots\ldots, a_7] \in Z_r^8$ as the orthogonal vector to $\varphi(W)$ then $n + qr_0 = \varphi((n + qr_o)1 + z)\alpha^T$ is equal to the original data n. Hence, the ciphertext C_n is imposed to the vectorization process for concerting into $Vector(C_n) = [f_{0,0}, \ldots f_{7,0}, f_{1,0}, \ldots . f_{7,7}]^T$ such that the attacker needs to determine the value of r_0 for recovering the plaintext data. The decryption process of the proposed NCR-FHE scheme is reformulated and presented in Eq. (15)

$$n + qr_0 = \varphi((n + qr_o)1 + z)\alpha^T = \left(1\boldsymbol{M}\boldsymbol{C_n}\boldsymbol{M}^{-1}\right)\alpha^{\boldsymbol{T}} = \left[\sum_{i,j=0}^{7}\boldsymbol{f}_{o,i,j}^{1}\boldsymbol{C}_{i,j,}\ldots\ldots\sum_{i,j=0}^{7}\boldsymbol{f}_{7,i,j}^{7}\boldsymbol{C}_{i,j}\right]\alpha^{\boldsymbol{T}}$$

$$= \sum_{i,j=0}^{7}(\boldsymbol{k}_{i,j}*\boldsymbol{C}_{i,j}) = \gamma\boldsymbol{Vector}(\boldsymbol{C_n}) \quad (15)$$

Thus, the determination of r_0 for recovering the plaintext data is difficult in making the entire decryption process difficult in manner.

4 Simulation Results and Discussion

The simulation of the proposed work is analyzed for communication overhead and is compared with existing methodologies. The proposed work is tested using Netskope and is tested against impersonation attacks. The computation cost of the proposed NCR-FHE was compared with the benchmarked approaches with respect to the number of hybrid Fog devices and different data packet sizes. Tab. 1 depicts the computation cost incurred by the proposed Quantum Fully Homomorphic Encryption with Verification (VQFHE) scheme for performing the cryptographic operations at the CCC, Fog nodes, and hybrid edge devices. Figs. 3 and 4 demonstrate the CO in bytes for the different numbers of hybrid IoT devices and sizes of data packets. The CO in bytes of the proposed NCR-FHE is identified to be superior in contrast to the benchmarked schemes, as it integrates the benefits of Quantum Fully Homomorphic Encryption (QFHE). It involves the least number of bytes of communication while interacting between CCC, hybrid IoT devices, and Fog nodes. Thus, the CO of the proposed NCR-FHE scheme is identified to be significantly reduced by 9.21%, 10.64%, 11.84%, and 12.94% in contrast to the benchmarked ECDH-DH, LHPPS, BF-PHE, and SHE-PABF schemes. The percentage decrease in communication overhead with varying sizes of data packets confirm to be significant due to the inclusion of Quaternion algebra that adaptively alternates the number of bytes used for essential communication. The percentage decrease in CO obtained by the proposed NCR-FHE for different data packet sizes is identified to be significantly reduced by 5.74%, 6.94%, 7.14%, and 8.46% in contrast to the baseline ECDH-DH, LHPPS, BF-PHE, and SHE-PABF schemes.

Table 1: Computation cost of the proposed NCR-FHE

Schemes used for comparison	Mean cost incurred in computation (milliseconds)		
	Hybrid Fog devices	Edge devices	Fog nodes
Proposed NCR-FHE	176	264	132
ECDH-DH	203	312	184
LHPPS	216	414	224
BF-PHE	234	452	23
SHE-PABE	252	464	264

Figs. 5 and 6 shows the computation cost in milliseconds incurred by the proposed NCR-FHE for varying numbers of hybrid Fog devices and sizes of data packets. The computation cost of the proposed NCR-FHE is identified to be better when compared to the benchmarked schemes, as it includes the benefits of QFHE. It involves the least number of bytes for interacting with CCC, hybrid Fog devices, and Fog nodes. The computation cost of the proposed NCR-FHE is identified to be significantly reduced by 7.18%, 8.64%, 9.42%, and 10.36% when compared to the benchmarked ECDH-DH, LHPPS, BF-PHE, and SHE-PABF schemes. The percentage decrease in computation cost for varying sizes of data

packets is determined to be potentially reduced. The percentage decrease in computation cost attained by the proposed NCR-FHE with different data packet sizes is identified to be significantly reduced by 6.48%, 7.84%, 8.96%, and 9.42% in contrast to the baseline ECDH-DH, LHPPS, BF-PHE, and SHE-PABF schemes. Figs. 7 and 8 demonstrate the potential of the proposed NCR-FHE scheme and the baseline approaches in terms of privacy preservation degree and attack resistivity degree with different packet sizes involved during transmission. The degree of preservation attained by the proposed NCR-FHE approach is significant on par with the comparable approaches since it adopted different homomorphic operators in confirmed maximized security during sensitive data transmission.

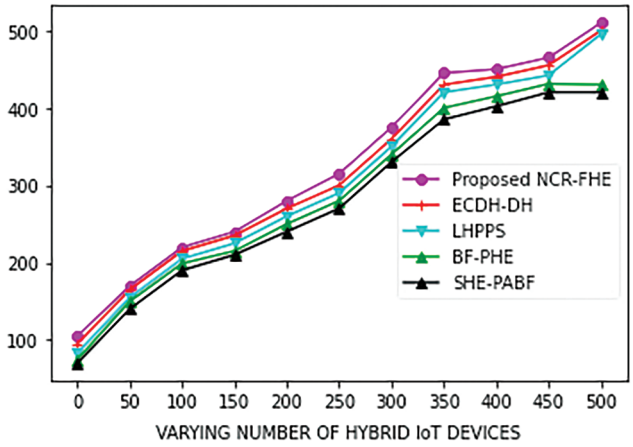

Figure 3: Communication Overhead of the Proposed NCR-FHE based on the Number of Hybrid Fog Devices

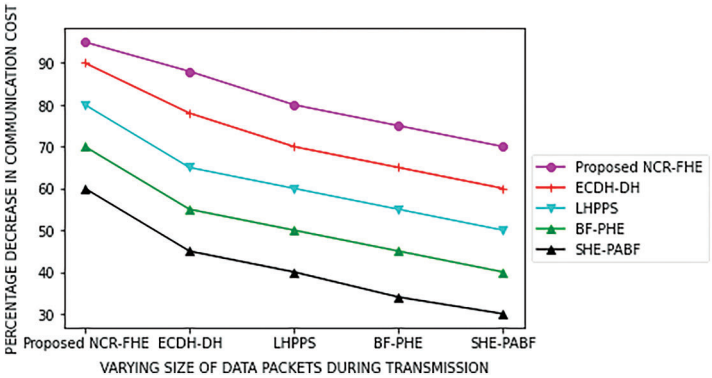

Figure 4: Communication Overhead of the Proposed NCR-FHE based on varying larger size of data packets

On the other hand, the degree of attack resistivity is also improved independent of the size of packets involved in transmission as it adaptively handles the change in bits and reputation level incurred during data dissemination. The privacy preservation degree achieved by the proposed NCR-FHE with different packet sizes involved during transmission is identified to be significantly maximized by 7.21%, 9.86%, 11.65%, and 14.32% in contrast to the baseline ECDH-DH, LHPPS, BF-PHE, and SHE-PABF schemes. The attack resistivity degree achieved by the proposed NCR-FHE with different packet sizes involved during transmission was also maximized by 8.94%, 11.56%, 14.82%, and 16.87% in contrast to the compared schemes used for comparison.

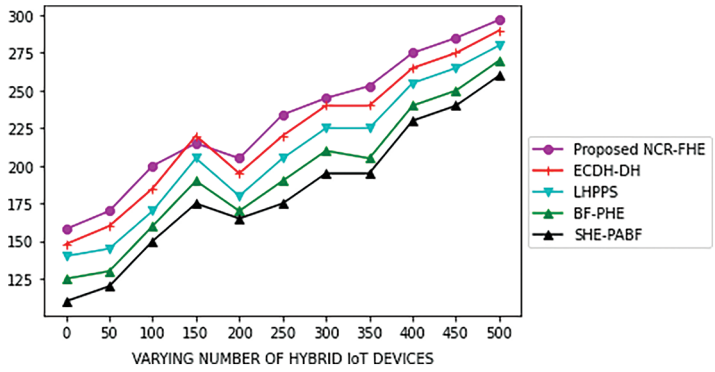

Figure 5: Computation Cost of the Proposed NCR-FHE based on the Number of Hybrid Fog Devices

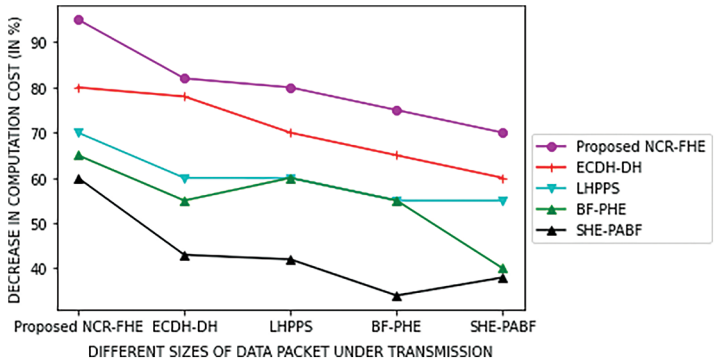

Figure 6: Computation Cost of the Proposed NCR-FHE based on varying size of data packets

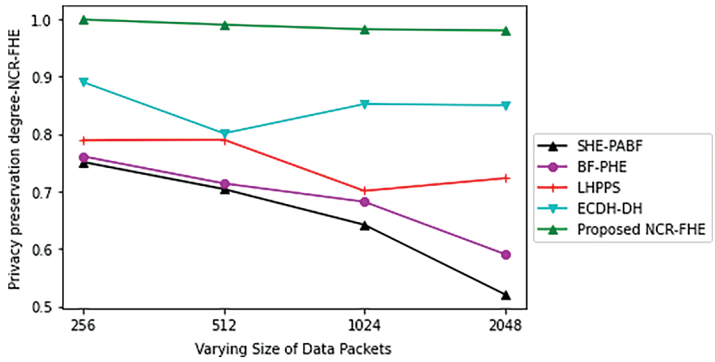

Figure 7: Privacy preservation degree-NCR-FHE based on varying size of data packets

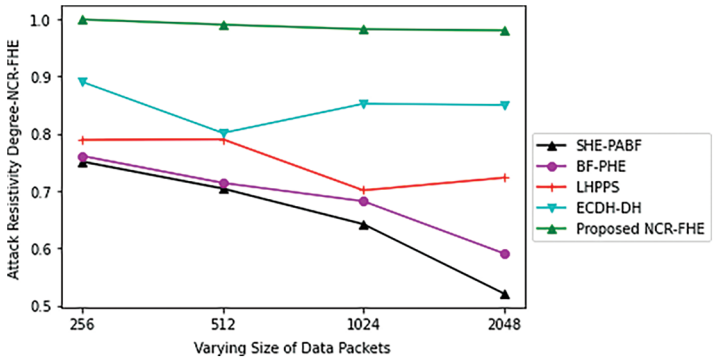

Figure 8: Attack Resistivity Degree-NCR-FHE based on varying size of data packets

5 Conclusion

A novel Non- Commutative Ring-based Fully Homomorphic Encryption (NCR-FHE) scheme was proposed by exploring the physical layer characteristics of the secured channel that could be established between the fog node and the end-user. The proposed scheme was determined to detect the possibilities of impersonation attacks in the fog computing environment. The experimentation of the proposed NCR-FHE scheme confirmed that the communication overhead of the proposed NCR-FHE scheme has been identified to be significantly reduced by 9.21%, 10.64%, 11.84%, and 12.94% in contrast to the benchmarked ECDH-DH, LHPPS, BF-PHE, and SHE-PABF schemes. The results confirmed that the computation cost of the proposed NCR-FHE with different data packet sizes was identified to be significantly reduced by 6.48%, 7.84%, 8.96%, and 9.42% in contrast to the baseline ECDH-DH, LHPPS, BF-PHE, and SHE-PABF schemes respectively. Hence in the proposed encryption approach, the physical layer channel characteristics were exploited in a cost-effective way. The root cause of the impersonation was identified to decide the appropriate encryption scheme, in the way to maximize the overall privacy preservation degree and attack resistivity degree. This proposed work can be extended to be rigid against all sorts of attacks by incorporating modular number systems.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. A. Z. Bhuiyan, J. Wu, G. Wang and J. Cao, "Sensing and decision making in cyber-physical systems: The case of structural event monitoring," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2103–2114, 2016.

[2] X. Xu, L. Zhang, S. Sotiriadis, E. Asimakopoulou, M. Li *et al.,* "CLOTHO: A large-scale internet of things-based crowd evacuation planning system for disaster management," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3559–3568, 2018.

[3] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of Fog computing," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 27–32, 2014.

[4] I. Stojmenovic, "Fog computing: A cloud to the ground support for smart things and machine-to-machine networks," in *Proc. Australasian Telecommunication Networks and Applications Conf. (ATNAC)*, Southbank, VIC, Australia, pp. 117–122, 2014.

[5] C. Feng, H. Xu and B. Li, "An alternating direction method approach to cloud traffic management," *Transactions on Parallel and Distributed Systems, IEEE*, vol. 28, no. 8, pp. 2145–2158, 2017.

[6] A. Atashpendar, B. Dorronsoro, G. Danoy and P. Bouvry, "A parallel cooperative coevolutionary SMPSO algorithm for multi-objective optimization," in *Proc. Int. Conf. on High Performance Computing & Simulation (HPCS)*, Innsbruck, Austria, pp. 713–720, 2016.

[7] R. Deng, R. Lu, C. Lai, T. H. Luan and H. Liang, "Optimal workload allocation in Fog-cloud computing toward balanced delay and power consumption," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1171–1181, 2016.

[8] A. Khosravi and R. Buyya, Energy and carbon footprint-aware management of geo-distributed cloud data centers: A taxonomy state of the art. In: *Advancing Cloud Database Systems and Capacity Planning with Dynamic Applications*. Hershey, PA, USA: IGI Glob, pp. 13– 27, 2017.

[9] S. Iturriaga, B. Dorronsoro and S. Nesmachnow, "Multiobjective evolutionary algorithms for energy and service level scheduling in a federation of distributed datacenters," *International Transactions in Operational Research*, vol. 24, no. 1–2, pp. 199–228, 2017.

[10] T. A. Ell, N. L. Bihan and S. J. Sangwine, "Quaternion Fourier Transforms for Signal and Image Processing," *Digital Signal and Image Processing Series*, Wiley-ISTE, vol. 2, pp. 1–19, 2014.

[11] K. Grining, M. Klonowski and P. Syga, "On practical privacy-preserving fault-tolerant data aggregation," *International Journal of Information Security*, vol. 18, no. 3, pp. 285–304, 2019.

[12] H. Zhong, D. Du, C. Li and X. Li, "A novel sparse false data injection attack method in smart grids with incomplete power network information," *Complexity*, vol. 2018, no. 1, pp. 1–16, 2018.

[13] M. Wolf and D. Serpanos, *Safe and secure cyber-physical systems and internet-of-things systems*, First. ed., Switzerland: Springer, pp. 73–83, 2020.

[14] M. Badra and S. Zeadally, "Lightweight and efficient privacy-preserving data aggregation approach for the Smart Grid," *Ad Hoc Networks*, vol. 64, no. 3, pp. 32–40, 2017.

[15] D. Zhang, F. Haider, M. St-Hilaire and C. Makaya, "Model and algorithms for the planning of fog computing networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3873–3884, 2019.

[16] A. Abdallah and X. S. Shen, "A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 396–405, 2016.

[17] V. Ford, A. Siraj and M. A. Rahman, "Secure and efficient protection of consumer privacy in Advanced Metering Infrastructure supporting fine-grained data analysis," *Journal of Computer and System Sciences*, vol. 83, no. 1, pp. 84–100, 2017.

[18] J. Jiu, A. Ren, R. Sun, X. Du and M. Guizani, "A novel chaos-based physical layer security transmission scheme for Internet of things," in *Global Communications Conf. (GLOBECOM)*, Hawaii, USA, pp. 23–34, 2019.

[19] Y. Zhang, D. Zheng, Q. Zhao, C. Lai and F. Ren, "PADA: Privacy-aware data aggregation with efficient communication for power injection in 5G smart grid Slice," in *Proc. Int. Conf. on Networking and Network Applications (NaNA)*, Kathmandu, Nepal, pp. 78–85, 2017.

[20] W. Yu, D. Griffith, L. Ge, S. Bhattarai and N. Golmie, "An integrated detection system against false data injection attacks in the Smart Grid," *Security and Communication Networks*, vol. 8, no. 2, pp. 91–109, 2015.

[21] A. Tripathi and S. K. Pasupuleti, "A secure lightweight data aggregation scheme for cloud assisted Fog," in *Proc. Fifth Int. Conf. on Parallel, Distributed and Grid Computing (PDGC)*, Solan, India, pp. 56–64, 2018.

[22] R. Gennaro, "Verifiable outsourced computation," in *Proc. ACM Symposium on Principles of Distributed Computing - PODC '17*, Washington, USA, pp. 21–26, 2017.

[23] D. Prabakaran and S. Ramachandran, "Multi-factor authentication for secured financial transactions in cloud environment," *CMC-Computers, Materials & Continua*, vol. 70, no. 1, pp. 1781–1798, 2022.