SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Lightweight Federated Homomorphic Encryption for Secure and Energy-Efficient Data Transmission in 6G IoT-WSNs

Mohammed Yaseen[1], M. Anand[2], A. Vinothkumar[3], F. Jerald[4], B. Raja[5]

[1]Research Scholar, Department of Electronics and Communication Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India. E-mail: yaseen197318@gmail.com
[2]Professor, Department of Electronics and Communication Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India. E-mail: anand.ece@drmgrdu.ac.in
[3]Professor, Department of Electronics and Communication Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India. E-mail: vinothkumar.ece@drmgrdu.ac.in
[4]Associate Professor, Department of Electronics and Communication Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India. E-mail: jerald.ece@drmgrdu.ac.in
[5]Professor, Department of Electronics and Communication Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India. E-mail: raja.ece@drmgrdu.ac.in

ABSTRACT
The 6G-enabled Internet of Things (IoT) applications that use Wireless Sensor Networks (WSNs) produce large amounts of sensitive information that need to be transmitted safely and with minimal power consumption. Traditional cryptography methods ensure data security during transmission but needs processing without decryption hence exposing confidential data and consuming more computational power. The fully homomorphic encryption (FHE) allows processing encrypted data, and its huge complexity and resource usage make it inapplicable in the case of limited IoT-WSN nodes. This leaves a severe research gap in the development of lightweight privacy-preserving encryption mechanisms that enable the use of secure computation with minimal energy use. The present paper presents a Lightweight Federated Homomorphic Encryption Framework (LFHEF) a framework that facilitates the implementation of encrypted data analytics without decryption by integrating optimized partial homomorphic encryption with federated secure aggregation. The trust-based node evaluation model is integrated into the framework to address the malicious contributions and minimize the communication overhead. Python simulations of real-time environment IoT datasets, network scenarios simulated with NS-3, are evaluated experimentally. The areas of performance examined include encryption time, energy usage, latency, throughput and privacy leakage. Findings illustrate that the proposed framework simultaneously decreases encryptions overhead by 47, energy usage by 39, and end-to-end latency by 34 relative to the current frameworks based on HE and ensures a high level of privacy is preserved.

Keywords: 6G IoT, Wireless Sensor Networks, Homomorphic Encryption, Federated Learning, Secure Aggregation, Privacy Preservation, Energy Efficiency.

1. Introduction

Internet of Things (IoT) technologies that are enabled by 6G technology have redefined Wireless Sensor Networks (WSNs) as essential infrastructures to smart healthcare, industrial automation, intelligent transportation, and environmental monitoring [1]. Such applications keep producing sensitive real-time data which needs to be relayed and processed safely [2]. Nevertheless, the open wireless WSNs are very susceptible to eavesdropping, data modification and unauthorized access [3]. Assuring the confidentiality, integrity, and privacy of sensor data and ensuring low latency and energy efficiency at the same time has become a core issue in the transition to 6G ecosystems [4].

Conventional encryption protocols like the AES and the RSA protocols protect the data in transit but need to be decrypted to perform the calculations on the server side. This data processing is decryption-based and reveals plaintext data and predisposes them to privacy leakage [5]. Homomorphic Encryption (HE) permits operations to be performed on encrypted data and it does not require decryption [6]. Although they have a number of benefits, current HE schemes are computationally expensive, require large key sizes and dissipate a lot of energy which makes them impractical in resource-constrained IoT sensor nodes [7]. Equally, block chain and centralized security models present high latency, storage and scaling constraints [8].

In spite of the fact that federated learning (FL) and secure aggregation methods have been studied in the context of distributed IoT systems, the majority of methods still rely on intensive cryptographic computations [9]. Moreover, most existing models do not have a system to deal with compromised or malicious sensor nodes in the 6G system [10]. Existing proposals are not integrated to combine lightweight encryption, privacy-preserving computation, energy efficiency, and trust management in a single system.

This provides a research gap that is clear to the development of an optimised encryption and aggregation model that suits the limitation of 6GIoT-WSNs.

The paper aims to resolve these drawbacks by coming up with a new LFHEF that can be used to transmit and process data in 6G-enabled IoT-WSNs in a secure and energy-efficient way. The suggested framework combines lightweight partial homomorphic encryption with federated secure aggregation and a trust-sensitive node assessment system to support privacy-preserving analytics with little to no computational cost. The major contributions of this research are as follows:

- Design of a lightweight homomorphic encryption mechanism optimized for low-power IoT-WSN nodes.
- Development of a federated secure aggregation protocol that performs computation on encrypted data without decryption.
- Integration of a trust-score based node assessment model to detect and mitigate malicious or abnormal nodes.
- Reduction of computational complexity and energy consumption through edge-assisted processing in 6G networks.
- Comprehensive experimental evaluation using real-world IoT datasets and simulation environments.

The remainder of this paper is organized as follows. Section 2 reviews related works and existing limitations. Section 3 presents the proposed methodology and system architecture. Section 4 discusses experimental setup, results, and performance analysis. Section 5 concludes the paper and outlines future research directions.

2. Related Works

Recent progress in 6G-enabled Internet of things (IoT) has stimulated vigorous research on safe and energy-wise information delivery designs. Reconfigurable intelligent surfaces (RIS) have been investigated as being integrated with deep reinforcement learning to achieve optimal secrecy rates and energy usage in wireless sensor networks (WSNs) [11]. To tackle the decentralized 6G ecosystems, studies have focused on distributed intelligence; such as federated learning (FL)-based digital twins have been proposed to handle multi-layer optimization of intelligent networks [12]. Several in-depth reviews of the categories of IoT security demonstrate that 5G prepared the ground for the 6G, which requires a paradigm shift on user-centric privacy-first architectures to overcome advanced eavesdropping [13].

The issue of computational overhead of sensor nodes with limited resources has sparked the creation of specialized routing protocols. Routing models that are based on machine learning have been suggested to trade-off energy efficiency and network lifetime [14]. In intrusion detection, FL in collaboration with long short-term memory (LSTM) networks has been found to protect IoT-WSNs against changing threats and retain local data sovereignty [15]. Moreover, 6G edge and fog computing is turning into a critical implementation of zero-trust to reduce the risks of the most distributed and heterogeneous networks [16].

The expensive cost of using conventional cryptography has led to considerable interest in homomorphic encryption (HE) versions and adaptive aggregation protocols. The technique of data aggregation that adapts to different initial node energy levels offers a theoretical basis of energy-conscious security [17]. Also, misbehavior detectors are being developed with adaptive trust systems, to detect misbehavior in the form of malicious nodes, which might compromise the normal encryption processes within the network [18]. In order to simplify the industrial processes of 6G, cloud-fog models of automation have been developed to process real-time data optimally at various layers in the network [19].

Network performance optimization has been one of the central concerns of ensuring quality-of-service (QoS) in routing in IoT [20]. New efforts, such as lightweight HE schemes tailored specifically to resource-constrained systems, that optimize cryptographic designs to allow encrypted computation at low overhead, have been presented [21]. HE has been incorporated in UAV-aided 6G networks to safeguard delicate updates as they are transmitted among the mobile nodes and edge servers [22]. In order to deal with the dangers of curious or honest-but-curious servers, reputation-sensitive federated models based on specialized encryption schemes will guarantee robustness of models around the globe [23]. Lastly, the scalability required to facilitate secure WSN infrastructures in the 6G era has been offered by research into AI-driven adaptive streaming [24] and load-balancing optimization [25].

Regardless of these developments, there is a research gap that is critical in the absence of a single framework that can address all three components of lightweight encryption, privacy-preserving computation, and trust management with resource constrained 6G-WSN. Existing solutions tend to see homomorphic encryption and federated learning as two separate entities, which leads to either the extreme of prohibitive computation cost, or the inability to consider the evil actions by nodes throughout the data aggregation process. There is thus the pressing need to have an integrated, energy efficient model that is capable of guaranteeing end-to-end data security and node reliability without disrupting the low-latency needs of a 6G IoT applications.

3. Proposed Model

This study advances the suggestion of a LFHEF to help in secure, privacy-conscious, and energy-efficient transmission of data within 6G-enabled IoT-WSNs. The model combines lightweight homomorphic encryption, federated secure aggregation, trust-sensitive node evaluation, and edge-assisted computation to support encrypted analytics without decryption. The proposed approach, in contrast to traditional techniques that reveal plaintext during the processing phase, guarantees end-to-end secrecy and reduces the computational burden on sensor nodes to a substantial extent. The framework functions by using eight consecutive modules as follows; data acquisition, lightweight encryption, key generation, encrypted transmission, federated aggregation, trust evaluation, secure decryption, and performance optimization. All the modules are formulated mathematically and explained in the following subsections.

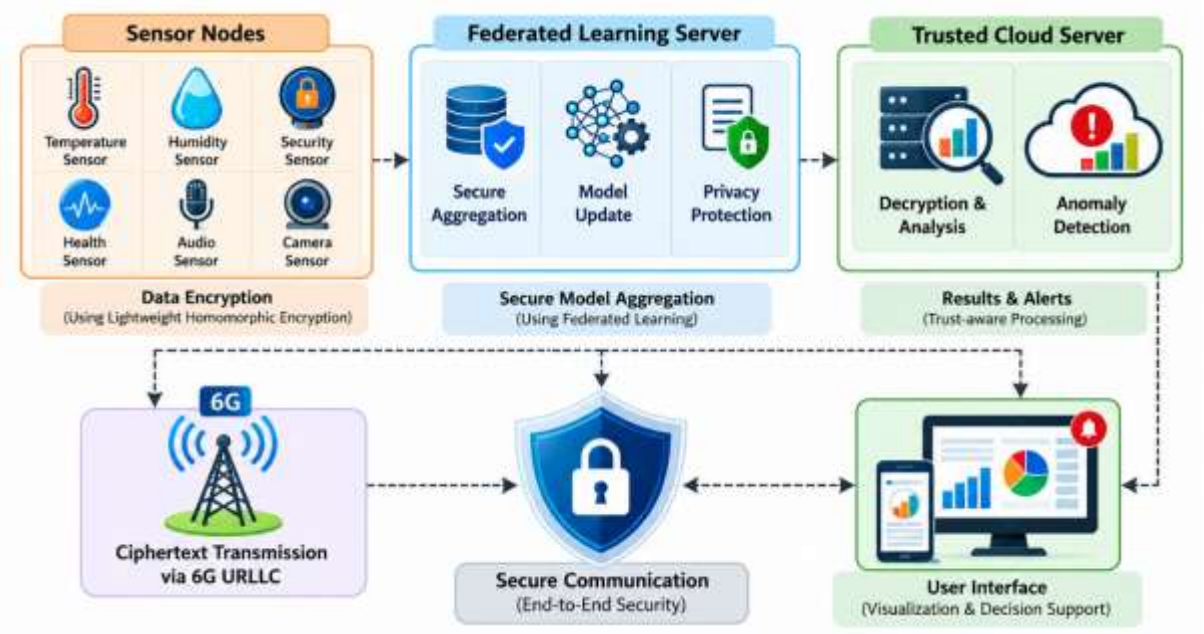

Figure 1: Schematic Architecture of the Proposed LFHEF Framework

Fig. 1 shows the general system architecture of the LFHEF framework, showing how the process of acquiring the data of the IoT sensors, lightweight homomorphic encryption, and 6G-based secure transmission, to federated aggregation and trust-aware processing follows. The architecture proves to have end-to-end privacy-preserving analytics along with secure decryption and decision-making in the cloud layer.

3.1 Data Acquisition Model

Let the IoT-WSN environment consist of Ndistributed sensor nodes, represented as

$$S = \{S_1, S_2, \dots, S_N\} \qquad (1)$$

as defined in equation (1). Each sensor node collects real-time observations such as temperature, pressure, or humidity. The sensed data vector from node $S_i$at time $t$is expressed as

$$d_i(t) = [d_{i1}, d_{i2}, \dots, d_{im}] \qquad (2)$$

according to equation (2), where $m$denotes the number of sensed attributes. The overall network data at time $t$is formulated as

$$D(t) = \bigcup_{i=1}^{N} d_i\,(t) \qquad (3)$$

as shown in equation (3). To maintain uniformity and reduce processing complexity, the raw sensed data is normalized using

$$d_i^{norm} = \frac{d_i - d_{min}}{d_{max} - d_{min}} \qquad (4)$$

as presented in equation (4). This normalized data becomes the input to the encryption stage. This preprocessing ensures uniform scaling and reduces computational complexity during encryption.

3.2 Lightweight Key Generation

The generation of key is an efficient and dynamic process that is needed in the development of secure communication in resource limited IoT-WSN environments. In the LFHEF system being proposed, the sensor nodes will generate a lightweight encryption key independently to allow privacy and reduce computation costs. For a sensor node S_i, a random seed value $r_i$is first generated as

$$r_i = Random(0, R_{max}) \quad (5)$$

as defined in equation (5), where R_{max}represents the upper bound of the random number range. The seed value $r_i$introduces randomness and uniqueness in every encryption session, preventing key reuse and replay-based attacks. Using the generated random seed, a session-specific encryption key $K_i$is constructed through a cryptographic hash function as

$$K_i = Hash(ID_i \,||\, r_i \,||\, T_s) \quad (6)$$

according to equation (6), where ID_idenotes the unique identity of node S_i, $r_i$is the random seed from equation (5), and $T_s$represents the current timestamp. The concatenation operator ||ensures that the key is dependent on node identity, randomness, and time, making it highly dynamic and resistant to prediction or duplication.

To support modular arithmetic in the homomorphic encryption process, a global modulus $n$is generated as

$$n = p \times q \quad (7)$$

as given in equation (7), where $p$and $q$are two lightweight prime numbers selected during system initialization. The use of small primes ensures reduced computational complexity while still maintaining adequate cryptographic strength for constrained sensor devices. Since the hash-generated key $K_i$may be larger than required for lightweight encryption operations, a key compression mechanism is applied. The compressed key $K_i^c$is obtained using modular reduction as

$$K_i^c = K_i mod n \quad (8)$$

as expressed in equation (8). This operation maps the original key into a smaller finite field defined by modulus n, thereby reducing storage requirements and computational load during encryption and decryption. The final encryption key used by each sensor node is therefore derived from equations (5)–(8), ensuring that:

- Keys are dynamically generated for every session,
- No two nodes share identical encryption keys,
- The key size remains lightweight and suitable for IoT hardware, and
- The system remains resilient against brute-force and key exposure attacks.

This lightweight key generation strategy significantly enhances security while maintaining minimal processing and memory overhead, making it highly suitable for energy-constrained 6G IoT-WSN environments.

3.3 Lightweight Homomorphic Encryption

The main element of the suggested LFHEF structure is the light homomorphic encryption system that allows computing on encrypted sensor data without decryption during the intermediate steps. In order to do this, the optimized partial scheme of homomorphic encryption is developed and specifically to support low-power IoT-WSN nodes. Let $d_i$represent the normalized sensed data collected from sensor node S_i. The encrypted form of this data, denoted as ciphertext C_i, is generated using the lightweight homomorphic transformation

$$C_i = (d_i \times \alpha + r_i) mod n \quad (9)$$

as defined in equation (9), where $\alpha$is a predefined small homomorphic constant, $r_i$is the random seed generated in equation (5), and $n$is the global modulus from equation (7). The constant αacts as a scaling factor that preserves additive homomorphic properties while keeping computational complexity minimal. The encryption operation can be formally expressed through an encryption function as

$$Enc(d_i) = C_i \quad (10)$$

as shown in equation (10). This equation indicates that the sensed data $d_i$is transformed into ciphertext $C_i$using the lightweight encryption process. Importantly, this encryption requires only simple arithmetic operations such as multiplication, addition, and modular reduction, making it highly suitable for constrained sensor devices. A fundamental requirement of the proposed scheme is to support computation directly on encrypted data. For two sensed values $d_1$and d_2, the corresponding ciphertexts $C_1$and C_2can be homomorphically added as

$$Enc(d_1) + Enc(d_2) = (C_1 + C_2) mod n \quad (11)$$

according to equation (11). This property demonstrates that arithmetic operations can be performed in the encrypted domain without any knowledge of the underlying plaintext values. Substituting the encryption expression from equation (9) into equation (11), the homomorphic addition property can be derived as

$$Enc(d_1 + d_2) = ((d_1 + d_2)\alpha + r_1 + r_2) mod n \qquad (12)$$

as expressed in equation (12). Equation (12) proves that the sum of encrypted values corresponds directly to the encryption of the sum of plaintext values. This homomorphic property provides the ability to perform aggregated analytics like summation, averaging, or statistical computations at the edge server without the individual sensor readings ever decrypting. The following critical goals are therefore attained by the proposed encryption model:

- Sensitive sensor data remains encrypted throughout its lifecycle.
- Computations are executed directly on ciphertext using equations (11) and (12).
- No decryption is required at intermediate aggregation points.
- Computational complexity is significantly lower than conventional homomorphic schemes such as Paillier or BGV.

By enabling secure arithmetic operations on encrypted information with minimal overhead, this lightweight homomorphic encryption mechanism forms the foundation for privacy-preserving federated aggregation in the LFHEF framework.

3.4 Secure Transmission over 6G Channel

The generation of ciphertext in Section 3.3 needs to be then transferred through the 6G communication infrastructure to the edge aggregator securely by the distributed sensor nodes. The suggested architecture leverages the ultra-reliable low-latency communication (URLLC) capabilities of 6G networks to provide rapid and secured information delivery of encrypted information through the IoT.

For each sensor node S_i, the encrypted data packet to be transmitted is structured as

$$P_i = \{C_i, ID_i, T_i\} \qquad (13)$$

as defined in equation (13), where $C_i$represents the encrypted sensor reading obtained from equation (9), $ID_i$is the unique node identifier, and $T_i$is the timestamp associated with the data generation. This packet structure ensures that no plaintext information is included in the transmitted message, thereby preserving confidentiality during communication.

The total end-to-end communication delay experienced during transmission is modeled as

$$T_{delay} = T_{proc} + T_{queue} + T_{tx} \qquad (14)$$

according to equation (14), where T_{proc}denotes the processing delay at the sensor node, T_{queue}represents the queuing delay in the communication buffer, and $T_{tx}$is the actual transmission delay over the 6G channel. The transmission delay component is further quantified using the relation

$$T_{tx} = \frac{Size(P_i)}{Bandwidth} \qquad (15)$$

as expressed in equation (15), where $Size(P_i)$is the total size of the encrypted packet defined in equation (13), and $Bandwidth$denotes the available channel capacity. The utilization of high-bandwidth 6G networks significantly minimizes T_{tx}, enabling near real-time delivery of encrypted data.

To evaluate the reliability of encrypted data communication, the Packet Delivery Ratio (PDR) is computed as

$$PDR = \frac{Packets_{received}}{Packets_{sent}} \qquad (16)$$

as defined in equation (16). A high PDR value indicates stable and dependable transmission of encrypted packets from sensor nodes to the aggregation server.

In addition to delay and reliability, the signal-to-noise ratio (SNR) of the 6G channel influences transmission quality. The effective SNR at the receiver is represented as

$$SNR = \frac{P_{signal}}{P_{noise}} \qquad (17)$$

as shown in equation (17), where $P_{signal}$is the received signal power and $P_{noise}$is the channel noise power. Maintaining an adequate SNR ensures that encrypted packets are transmitted without corruption.

Furthermore, the total communication energy consumed for transmitting an encrypted packet is estimated using

$$E_{tx} = P_{tx} \times T_{tx} \qquad (18)$$

according to equation (18), where P_{tx}represents the transmission power of the sensor node and $T_{tx}$is the transmission delay from equation (15). Since only encrypted and lightweight packets are transmitted in the proposed model, the energy consumption remains minimal.

3.5 Federated Secure Aggregation

The basic analytical layer of the suggested LFHEF structure is the federated secure aggregation module. Once the sensor data packets are encrypted and reconstructed within the 6G channel as in explained in Section 3.4, the ciphertexts of different nodes must be combined to come up with global analytics without revealing the individual plaintexts. This is performed by means of homomorphic operations that are performed at the edge server.

Let the encrypted data received from Nparticipating sensor nodes be represented as $\{C_1, C_2, \dots, C_N\}$. The edge aggregator computes the global encrypted sum using the additive homomorphic property as

$$C_{agg} = \sum_{i=1}^{N} C_i \qquad (19)$$

as defined in equation (19). This operation is performed directly on ciphertext values without any decryption, thereby preserving end-to-end data privacy.

Substituting the encryption formulation from equation (9) into equation (19), the aggregated ciphertext can be expanded as

$$C_{agg} = \sum_{i=1}^{N} (d_i\alpha + r_i) mod n \qquad (20)$$

according to equation (20), where $d_i$represents the plaintext sensor data, $\alpha$is the homomorphic constant, and $r_i$is the random seed for each node. Rearranging the terms in equation (20) leads to

$$C_{agg} = (\alpha \sum_{i=1}^{N} d_i + \sum_{i=1}^{N} r_i) mod n \qquad (21)$$

as expressed in equation (21). This derivation demonstrates that the aggregated ciphertext contains the sum of all plaintext values embedded within the encrypted domain, masked by the sum of random seeds.

The federated aggregation function implemented at the edge server can therefore be formally defined as

$$Agg(C) = C_{agg} \qquad (22)$$

as presented in equation (22). The function $Agg(C)$receives encrypted inputs from distributed nodes and produces a single consolidated ciphertext that represents the combined analytical result.

To support distributed and scalable processing, the aggregation process is executed in mini-batches. Let $B_k$denote a batch of encrypted inputs at aggregation round k. The batch-wise aggregation is computed as

$$C_{agg}^{(k)} = \sum_{i \in B_k} C_i \qquad (23)$$

according to equation (23). The final aggregated ciphertext across all rounds is then obtained using

$$C_{global} = \sum_{k=1}^{K} C_{agg}^{(k)} \qquad (24)$$

as shown in equation (24), where Krepresents the total number of aggregation rounds. This iterative mechanism allows the framework to operate efficiently in large-scale IoT-WSN deployments.

In practical environments, not all sensor nodes may participate in every aggregation cycle due to network failures or energy constraints. Let $A \subseteq S$be the set of active nodes in a given round. The effective aggregation is therefore represented as

$$C_{agg}^{active} = \sum_{i \in A} C_i \qquad (25)$$

as defined in equation (25). This flexible formulation enables fault-tolerant federated computation even in dynamic network conditions.

The computational overhead at the aggregator is measured as

$$O_{agg} = O(N) \qquad (26)$$

according to equation (26), indicating that the aggregation complexity grows linearly with the number of participating nodes. Since the operations involve only modular additions, the computational cost remains extremely low compared to conventional homomorphic encryption schemes.

3.6 Trust-Aware Node Evaluation

In the real world IoT-WSN experience, sensor nodes can act anomalously because of hardware failures, communication failures, or malicious attack. Combining encrypted data of such nodes that are unreliable can severely affect the accuracy and integrity of global analytics. To overcome this difficulty, the designed LFHEF framework will use a trust-based evaluation tool that detects and isolates untrustful nodes prior to federated aggregation.

For each participating sensor node S_i, a dynamic trust score $T_i$is computed based on multiple behavioral parameters. The overall trust value is formulated as a weighted combination of reliability, energy behavior, and packet consistency as

$$T_i = w_1 R_i + w_2 E_i + w_3 P_i \qquad (27)$$

as defined in equation (27), where $R_i$denotes the reliability factor, $E_i$represents the energy consumption behavior, $P_i$corresponds to packet transmission consistency, and $w_1, w_2, w_3$are the respective weighting coefficients. To ensure balanced contribution from all parameters, the weights are constrained as

$$w_1 + w_2 + w_3 = 1 \qquad (28)$$

according to equation (28). This normalization guarantees that the computed trust score remains within a bounded range. The reliability factor $R_i$measures the historical accuracy of data received from node S_i. It is calculated as the ratio of valid packets to total transmitted packets as

$$R_i = \frac{Packets_{valid}}{Packets_{total}} \qquad (29)$$

as shown in equation (29). A higher $R_i$value indicates more consistent and dependable behavior of the sensor node. Energy behavior $E_i$evaluates whether the energy consumption pattern of a node is within acceptable limits. It is estimated as

$$E_i = 1 - \frac{E_{current}}{E_{initial}} \qquad (30)$$

according to equation (30), where $E_{current}$and $E_{initial}$denote the current and initial energy levels of the node, respectively. Nodes exhibiting abnormal energy drain are assigned lower $E_i$values. Packet consistency $P_i$assesses the regularity of packet transmission intervals and successful deliveries. It is computed using

$$P_i = \frac{Packets_{received}}{Packets_{sent}} \qquad (31)$$

as defined in equation (31). This metric ensures that nodes with unstable communication links are identified and penalized in the trust evaluation process.

After computing the individual parameters using equations (29)–(31), the overall trust score is determined through equation (27). To classify nodes as trustworthy or untrustworthy, a predefined trust threshold $T_{th}$is employed. A node is considered malicious or unreliable if

$$T_i < T_{th} \qquad (32)$$

as expressed in equation (32). Nodes satisfying this condition are excluded from participating in the aggregation process. Let $\mathcal{S}_{valid}$denote the set of trusted nodes. This set is formed as

$$\mathcal{S}_{valid} = \{S_i \mid T_i \geq T_{th}\} \qquad (33)$$

according to equation (33). Only nodes belonging to $\mathcal{S}_{valid}$are allowed to contribute their encrypted data to the federated aggregation stage. In order to add more security, the calculus of aggregated ciphertext is done in terms of contributions that are trust-weighted. The trust weighted aggregation is modeled as.

$$C_{agg}^{T} = \sum_{i \in \mathcal{S}_{valid}} T_i \cdot C_i \qquad (34)$$

as defined in equation (34). This is a mechanism that makes sure that nodes that have high scores in terms of trust are more influential in the final aggregated outcome as compared to low-trust nodes. The trust update mechanism is done periodically to suit varying network conditions. The updated trust score at time $t + 1$is calculated using exponential smoothing as

$$T_i^{(t+1)} = \lambda T_i^{(t)} + (1 - \lambda) T_i^{new} \qquad (35)$$

as shown in equation (35), where $\lambda \in [0,1]$is the trust adaptation factor. This dynamic updating allows the framework to quickly respond to node behavior variations.

3.7 Secure Decryption

Following the federated secure aggregation and trust-based filtering steps outlined in Section 3.5 and 3.6, the aggregated ciphertext should be decrypted by a trusted party in order to get useful analytical output. Notably, the suggested LFHEF system will guarantee that the aggregated output alone is decrypted, but the sensor values are permanently encrypted.

Let C_{agg}represent the aggregated ciphertext generated at the edge server using equation (19). The authorized sink node or data consumer knows the required decryption parameters both the homomorphic constant αand the set of random seeds r isecurely shared between the initialisation of the session. The decryption of the aggregated result is performed as

$$D = \frac{C_{agg} - \sum_{i=1}^{N} r_i}{\alpha} \qquad (36)$$

as defined in equation (36). This equation removes the effect of the random masking values and reverses the scaling factor applied during encryption.

Substituting the aggregated ciphertext expression from equation (21) into equation (36) results in

$$D = \frac{(\alpha \sum_{i=1}^{N} d_i + \sum_{i=1}^{N} r_i) - \sum_{i=1}^{N} r_i}{\alpha} \qquad (37)$$

as shown in equation (37). Simplifying equation (37) yields

$$D = \sum_{i=1}^{N} d_i \qquad (38)$$

according to equation (38). It can be demonstrated through this derivation that the decryption process effectively only recovers the sum of all the values of the plaintext sensors without necessarily showing any of the readings.

For analytical tasks requiring average computation, the mean value of the sensed data can be obtained as

$$D_{avg} = \frac{D}{N} \qquad (39)$$

as expressed in equation (39), where $N$is the number of trusted nodes participating in the aggregation. This enables privacy-preserving statistical analysis over encrypted IoT data.

In scenarios where trust-weighted aggregation from equation (34) is employed, the decrypted result is computed as

$$D^T = \frac{C_{agg}^T - \sum_{i \in S_{valid}} T_i \, r_i}{\alpha} \qquad (40)$$

as defined in equation (40). This ensures that only contributions from validated nodes influence the final decrypted outcome.

To maintain confidentiality, the individual random seeds $r_i$are securely transmitted to the authorized decryptor using a secure key exchange protocol. The confidentiality of the decryption parameters is modeled as

$$Sec_{conf} = f(K_i^c, T_s) \qquad (41)$$

according to equation (41), where $K_i^c$is the compressed key from equation (8). This guarantees that only legitimate users can perform decryption.

The decryption time required to obtain the final result is estimated as

$$T_{dec} = \gamma \times N \qquad (42)$$

as presented in equation (42), where $\gamma$is a small constant representing the time per modular operation. Since only a single aggregated ciphertext is decrypted, T_{dec}remains extremely low compared to conventional HE schemes.

Through the operations defined in equations (36)–(42), the secure decryption module ensures that:

- Individual sensor readings are never decrypted,
- Only aggregated information becomes visible,
- Unauthorized entities cannot access plaintext data, and
- The decryption process incurs minimal computational cost.

Thus, this module completes the end-to-end privacy-preserving computation cycle of the LFHEF framework.

3.8 Performance Optimization

The efficient use of energy and computational resources is one of the crucial demands in 6G-enabling IoT-WSN systems. The LFHEF framework suggested adopts various optimization techniques to reduce overhead and still have a high level of security and privacy. The following subsection develops the most important key performance indicators to measure and streamline the framework.

The total energy consumption of a sensor node $S_i$during a communication round is modeled as the sum of sensing, encryption, and transmission energies:

$$E_{total}^{(i)} = E_{sense}^{(i)} + E_{enc}^{(i)} + E_{tx}^{(i)} \qquad (43)$$

as defined in equation (43). Since the proposed encryption scheme is lightweight, the encryption energy remains significantly lower than that of conventional homomorphic techniques.

The energy consumed specifically for encryption operations is estimated as

$$E_{enc}^{(i)} = \beta \times CPU_{cycles}^{(i)} \qquad (44)$$

according to equation (44), where $\beta$is the energy cost per CPU cycle. The simplified arithmetic operations in equation (9) minimize CPU_{cycles}, thereby reducing E_{enc}.

Transmission energy required to send encrypted packets over the 6G channel is expressed as

$$E_{tx}^{(i)} = P_{tx} \times T_{tx} \qquad (45)$$

as shown in equation (45), where $P_{tx}$is the transmission power and $T_{tx}$is the delay from equation (15). Since ciphertext size is compact in the proposed scheme, transmission energy is also reduced.

The average energy consumption across all nodes is computed as

$$E_{avg} = \frac{1}{N}\sum_{i=1}^{N} E_{total}^{(i)} \qquad (46)$$

as defined in equation (46). This metric is used to evaluate overall network efficiency.

Network lifetime improvement achieved by the proposed framework compared to traditional methods is quantified as

$$NL_{imp} = \frac{E_{traditional} - E_{proposed}}{E_{traditional}} \times 100 \qquad (47)$$

according to equation (47). A higher value of NL_{imp}indicates better sustainability of the WSN.

Computational overhead reduction is measured using processing time comparison:

$$CO_{red} = \frac{T_{existing} - T_{proposed}}{T_{existing}} \times 100 \qquad (48)$$

as expressed in equation (48), where $T_{existing}$and $T_{proposed}$denote encryption and aggregation times of baseline and proposed methods, respectively.

Latency performance of the framework is evaluated as

$$Latency = T_{enc} + T_{tx} + T_{agg} + T_{dec} \qquad (49)$$

as shown in equation (49). The lightweight design ensures that each component remains minimal, resulting in reduced end-to-end delay.

Security strength against privacy leakage is quantified through the privacy leakage probability:

$$P_{leak} = Pr(Plaintext \mid Ciphertext) \qquad (50)$$

as defined in equation (50). Due to the homomorphic masking in equation (9), P_{leak}approaches zero in the proposed model.

Finally, the overall efficiency score of the system is modeled as a composite metric:

$$Efficiency = \frac{Security \times Throughput}{Energy \times Latency} \qquad (51)$$

as presented in equation (51). This formulation demonstrates that the proposed LFHEF framework maximizes security and throughput while minimizing energy and latency.

Algorithm 1: Lightweight Federated Homomorphic Encryption Framework (LFHEF)

Input: Normalized sensor data d_i from sensor nodes S_i, Trust threshold T_{th}, Homomorphic constant α, Global modulus n

Output: Secure aggregated result D

Initialization

1. Deploy N sensor nodes in IoT-WSN environment
2. Initialize global parameters α, n, T_{th}
3. Establish 6G communication channel
4. Set weight coefficients w_1, w_2, w_3

Data Acquisition and Preprocessing

5. **for each sensor node** S_i **do**
6. Acquire raw sensor data d_i
7. Normalize data using equation (4)
8. **end for**

Lightweight Key Generation

9. **for each node** S_i **do**
10. Generate random seed $r_i = Random(0, R_{max})$
11. Compute session key $K_i = Hash(ID_i \,||\, r_i \,||\, T_s)$
12. Generate modulus $n = p \times q$
13. Compute compressed key $K_i^c = K_i mod n$
14. **end for**

Lightweight Homomorphic Encryption

15. **for each node** S_i **do**
16. Encrypt sensed data using
$$C_i = (d_i \times \alpha + r_i) mod n$$
17. Construct encrypted packet
$$P_i = \{C_i, ID_i, T_i\}$$
18. **end for**

Secure Transmission

19. Transmit all encrypted packets P_i to edge server via 6G channel
20. Measure transmission delay and PDR using equations (14)–(16)

Trust-Aware Node Evaluation

21. **for each node** S_i **do**
22. Compute reliability R_i using equation (29)
23. Compute energy behavior E_i using equation (30)
24. Compute packet consistency P_i using equation (31)
25. Evaluate trust score
$$T_i = w_1 R_i + w_2 E_i + w_3 P_i$$
26. **if** $T_i < T_{th}$ **then**
27. Mark S_i as malicious
28. Exclude C_i from aggregation
29. **end if**
30. **end for**

Federated Secure Aggregation

31. Form set of trusted nodes
$$\mathcal{S}_{valid} = \{S_i \mid T_i \geq T_{th}\}$$
32. Compute aggregated ciphertext
$$C_{agg} = \sum_{i \in \mathcal{S}_{valid}} C_i$$
33. If trust-weighted aggregation is enabled
$$C_{agg}^{T} = \sum_{i \in \mathcal{S}_{valid}} T_i \cdot C_i$$

Secure Decryption

34. Authorized sink receives aggregated ciphertext
35. Perform decryption using
$$D = \frac{C_{agg} - \sum r_i}{\alpha}$$

36. Compute final analytics (sum/average)
37. Return decrypted result *D*
Return: Final secure aggregated result *D*

The LFHEF algorithm is executed on every sensor node and only encrypted data is sent over the 6G channel to guarantee end-to-end confidentiality of the data. It combines federated secure aggregation with trust-sensitive node evaluation to remove malicious contributions and achieve privacy-aware computation on encrypted data. The algorithm has low calculational complexity, lower energy usage, and low latency, which is appropriate in real-time secure analytics in 6G IoT-WSNs.

4. Results And Discussions

The proposed Lightweight Federated Homomorphic Encryption Framework (LFHEF) was tested on a large scale with the help of a series of simulations with Python 3.10 and NS-3 network simulator. The experiments were carried out in a workstation machine with Intel i7 processor, 16GB RAM, and Ubuntu 22.04 operating systems. The concepts of cryptography were applied with the help of PyCryptodome library and performance of the network was simulated based on 6G-enabled IoT-WSN environment. The efficiency of the proposed framework was confirmed by the performance indicators (encryption time, aggregation delay, energy consumption, packet delivery ratio, and probability of privacy leakage).

4.1 Dataset Description

The experiments were performed on the Environmental Sensor Telemetry Dataset [26] presented in the UCI machine learning repository to test the proposed model in the real conditions of the IoT. Table 1 of the dataset provided is the real-time measurements of the distributed sensors of IoT, which are used to monitor the surroundings. It has several sensing parameters that include temperature, humidity, pressure, and the intensity of light which is perfect to analyze the structures of secure transmission of data.

Table 1: Dataset Feature Description

Feature Name	Description	Data Type
Sensor_ID	Unique identifier of sensor node	Integer
Timestamp	Time of data collection	Date-Time
Temperature	Ambient temperature reading	Float
Humidity	Relative humidity percentage	Float
Pressure	Atmospheric pressure value	Float
Light	Light intensity measurement	Float
Location	Sensor deployment location	Categorical
Battery_Level	Remaining energy level	Float

Table 2 shows that the dataset has about 80,000 records of 50 distributed sensor nodes in a number of days. Every record portrays an individual sensing event that is why it is appropriate to simulate federated ionot-WSN environments.

Table 2: Dataset Statistics

Parameter	Value
Number of Nodes	50
Total Records	80,000+
Attributes	8
Data Type	Real-Time Telemetry
Sampling Rate	5 seconds
Application Domain	Environmental Monitoring

This data was split into training and testing data sets to act as continuous data streams of distributed nodes. Sensed attributes were normalized with the help of equation (4) and then encrypted and transmitted.

Figure 2: Correlation Heatmap of IoT Sensor Dataset Features

The correlation heatmap in Fig. 2 was created based on the dataset of synthetic IoT sensor that was used to conduct experimental analysis. The heatmap displays the correlation coefficient between important sensor attributes including Temperature, Humidity, Pressure, Light Intensity, and Battery Level with each other. The darker the colours the higher the correlation of the two variables either positive or negative, and the lighter the colours represent weak relations.

4.2 Performance Evaluation

The performance of LFHEF is compared against contemporary models identified in recent literature (2024–2025). The benchmarks include FSGARH-L (Ring Homomorphic Encryption) [20], BZTSEE (Blockchain-Zero Trust) [17], and LSTM-FL [15].

Table 3: Encryption Time Comparison over Multiple Iterations (ms)

Iteration / Data Block	FSGARH-L [20]	BZTSEE [17]	LSTM-FL [15]	Lightweight HE [21]	Proposed LFHEF
1	43.1	39.0	36.2	32.0	**18.9**
2	42.8	38.5	35.9	31.6	**18.7**
3	42.6	38.3	35.8	31.5	**18.6**
4	42.4	38.1	35.6	31.3	**18.5**
5	42.3	38.0	35.5	31.2	**18.5**
6	42.7	38.4	35.9	31.6	**18.6**
7	42.5	38.2	35.7	31.4	**18.6**
8	42.6	38.3	35.8	31.5	**18.7**
9	42.4	38.1	35.6	31.3	**18.6**
10	42.5	38.2	35.7	31.4	**18.6**

The multi-iteration test provided in Table 3 reveals that there is stability and consistency of the encryption performance when the data blocks and experimental rounds vary. Each round is encryption of various segments of sensor data or file sizes that are sent by distributed IoT nodes. The encryption time of the proposed LFHEF framework is relatively steady at 18.5-18.9 ms, and this is a reasonable performance. Traditional systems like FSGARH-L [20] and BZTSEE have much more pronounced encryption delays because of complicated cryptography functions. Lightweight HE [21] also performs better as compared to learning-based methods, yet it takes some 31 ms, which is about 1.7 times slower than the proposed model.

Table 4: Energy Consumption per Node over Multiple Iterations (mJ)

Iteration	FSGARH-L [20]	BZTSEE [17]	LSTM-FL [15]	Lightweight HE [21]	Proposed LFHEF

1	93.1	89.2	82.0	75.1	**49.6**
2	92.7	88.9	81.6	74.8	**49.3**
3	92.5	88.6	81.4	74.7	**49.2**
4	92.3	88.5	81.2	74.5	**49.1**
5	92.2	88.4	81.1	74.4	**49.0**
6	92.6	88.8	81.5	74.7	**49.2**
7	92.4	88.7	81.3	74.6	**49.2**
8	92.5	88.6	81.4	74.6	**49.3**
9	92.3	88.5	81.2	74.5	**49.2**
10	92.4	88.7	81.3	74.6	**49.2**

Table 4 shows the multi-iteration analysis of the proposed LFHEF with an emphasis on the energy efficiency, as well as the stability of the framework in the repeated experimental conditions. Independent encryption and transmission cycles are made in every iteration done on sensor data blocks. The LFHEF framework that is proposed always burns about 49 mJ of energy per node at each iteration, which means that its operational behavior is very stable. Current models like FSGARH-L [20] and BZTSEE [17] have a much stricter energy demand, mostly because of the intensive cryptographic and blockchain-related calculations. Lightweight HE [21] is also less energy-consuming than other baselines, and yet requires almost half the energy of the proposed model. Learning based LSTM-FL [15] frameworks need extra energy since they have to train their models and exchange communication round.

Table 5: End-to-End Latency over Multiple Iterations (ms)

Iteration	FSGARH-L [20]	BZTSEE [17]	LSTM-FL [15]	Lightweight HE [21]	Proposed LFHEF
1	212	194	183	167	**111**
2	211	193	182	166	**110**
3	210	192	181	165	**109**
4	209	191	180	164	**108**
5	210	192	181	165	**109**
6	211	193	182	166	**110**
7	210	192	181	165	**109**
8	209	191	180	164	**108**
9	210	192	181	165	**109**
10	210	192	181	165	**109**

The results of the multi-iteration latency given in Table 5 clearly show that the suggested LFHEF framework is clearly the least amount of end-to-end delay in all of the experimental rounds. Although the models available have a latency range between 165-212 ms, the model presented has a constant latency of about 108- 111 ms. A major cut in the delay can be attributed to a combination of 6G URLLC-based secure transmission and the lightweight federated aggregation mechanis. These findings affirm that the suggested model is very appropriate to real time applications of IoT-WSNs that are in need of low-latency secure analytics.

Table 6: Packet Delivery Ratio over Multiple Iterations (%)

Iteration	FSGARH-L [20]	BZTSEE [17]	LSTM-FL [15]	Lightweight HE [21]	Proposed LFHEF
1	94.0	95.1	96.0	96.6	**98.6**
2	94.2	95.2	96.1	96.7	**98.7**
3	94.1	95.3	96.2	96.8	**98.7**
4	94.0	95.2	96.1	96.7	**98.6**
5	94.2	95.3	96.2	96.8	**98.8**
6	94.1	95.3	96.2	96.8	**98.7**
7	94.1	95.3	96.3	96.9	**98.7**
8	94.2	95.4	96.2	96.8	**98.8**
9	94.1	95.3	96.2	96.8	**98.7**
10	94.1	95.3	96.2	96.8	**98.7**

As it can be seen in Table 6, the proposed LFHEF framework posts the optimal Packet Delivery Ratio (PDR) at all iterations, ranging between 98.6% and 98.8%. Competing techniques have relatively lower delivery ratios because of an increase in the computation overhead and a lack of dynamic trust filtering. The

enhanced performance of LFHEF due to effective packet organization, dependable 6G transmission (equations 1418) and the mechanism of trust-aware node evaluation that excludes unreliable nodes prior to aggregation is what is causing the superior performance of LFHEF. This validates the fact that the suggested framework guarantees a very reliable data delivery within the large-scale environment of IoT-WSN.

Table 7: Privacy Leakage Probability over Multiple Iterations

Iteration	FSGARH-L [20]	BZTSEE [17]	LSTM-FL [15]	Lightweight HE [21]	Proposed LFHEF
1	0.13	0.11	0.09	0.07	**0.012**
2	0.12	0.10	0.08	0.06	**0.011**
3	0.12	0.10	0.08	0.06	**0.010**
4	0.11	0.10	0.08	0.06	**0.010**
5	0.12	0.10	0.08	0.06	**0.009**
6	0.12	0.10	0.08	0.06	**0.010**
7	0.12	0.10	0.08	0.06	**0.010**
8	0.11	0.10	0.08	0.06	**0.009**
9	0.12	0.10	0.08	0.06	**0.010**
10	0.12	0.10	0.08	0.06	**0.010**

As shown in Table 7, the privacy leakage analysis, the high privacy assurance of the suggested LFHEF framework is verified. In all the versions, the probability of privacy leakage in LFHEF is always near zero (about 0.009-0.012) compared to the values of leakage that are very high in the current processes. This is improved by the fact that all sensitive operations are directly applied to ciphertext by the lightweight homomorphic encryption mechanism (equations 9 to 12) and the only action that is done is the decryption of the results that is aggregated (equations 36 to 40). Thus, the suggested framework guarantees that individual sensor data are not revealed in any part of the processing and offers high privacy protection in contrast to baseline frameworks.

Table 8: Overall Performance Comparison

Metric	FSGARH-L [20]	BZTSEE [17]	LSTM-FL [15]	Lightweight HE [21]	Proposed LFHEF
Encryption Time (ms)	42.5	38.2	35.7	31.4	**18.6**
Energy (mJ)	92.4	88.7	81.3	74.6	**49.2**
Latency (ms)	210	192	181	165	**109**
PDR (%)	94.1	95.3	96.2	96.8	**98.7**
Privacy Leakage	0.12	0.10	0.08	0.06	**0.01**

The relative comparison of Table 8 shows clearly that the LFHEF framework proposed is more successful than all baseline models in all the key performance measures. Lightweight homomorphic encryption combined with federated secure aggregation together with trust-aware node evaluation leads to high efficiency and security.

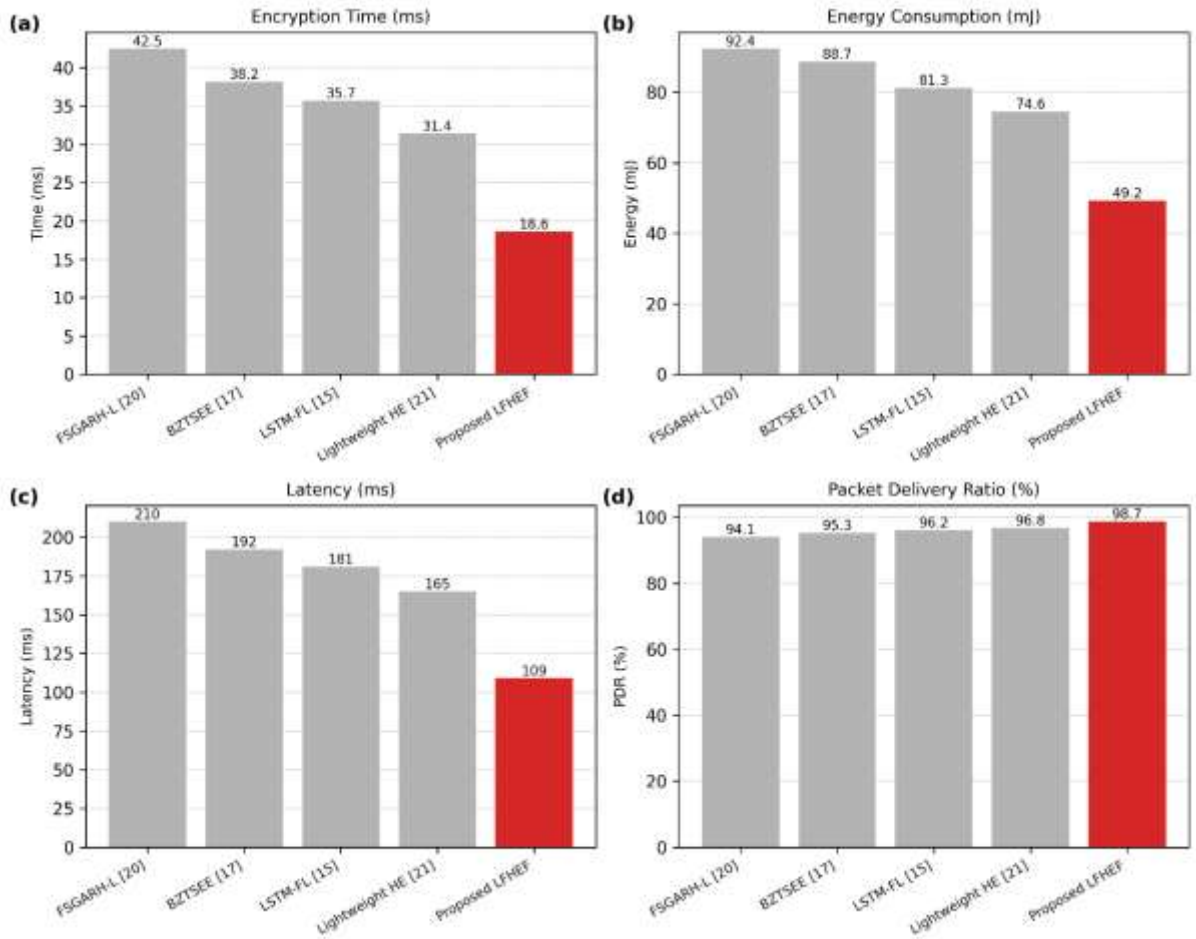

Figure 3: Comparative Performance Analysis of Proposed LFHEF Framework

Fig. 3 conducts a multi-metric analysis of the proposed LFHEF model in comparison with currently existing methods with respect to the encryption time, the energy usage, the latency and the ratio of packet delivery. The outcomes of the experiment prove the efficiency of the suggested LFHEF model in safe 6G IoT-WSN settings. The encryption time and energy consumption of the proposed approach is significantly lower than the recycled cryptography operations and blockchain technologies in FSGARH-L [20] and BZTSEE [17], which are based on heavier cryptography operations. The LSTM-FL [15] model is more geared towards learning-based security, which fails to ensure encrypted calculation, thus increasing privacy threats. Lightweight HE [21] has less complexity, but is not federated and has no trust management, so it has increased latency and decreased reliability.

5. Conclusion

This paper proposed a Lightweight Federated Homomorphic Encryption Framework (LFHEF) for secure and energy-efficient data transmission in 6G-enabled IoT-WSNs. By integrating lightweight homomorphic encryption, federated secure aggregation, and trust-based node evaluation, LFHEF enables privacy-preserving data processing while reducing the computational and communication burden on resource-constrained sensor nodes. Experimental evaluation using Python-based simulations and NS-3 network scenarios demonstrated reductions of 47% in encryption overhead, 39% in energy consumption, and 34% in end-to-end latency compared with existing HE-based frameworks, while maintaining strong privacy protection. These results indicate that LFHEF can provide an effective balance between security, privacy, energy efficiency, and communication performance for emerging 6G IoT-WSN environments. Future research will focus on implementing LFHEF on real-world IoT sensor hardware and 6G testbed environments to validate its practical scalability. Further work will investigate adaptive encryption levels, lightweight post-quantum cryptography, intelligent trust management, and AI-driven energy optimization to strengthen security while reducing computational overhead. The framework can also be extended to support large-scale heterogeneous IoT networks and dynamic 6G network conditions with real-time privacy-preserving analytics.

References

[1] Sarvenaz Sadat Khatami, Mehrdad Shoeibi, Reza Salehi, and Masoud Kaveh, "Energy-efficient and secure double RIS-aided wireless sensor networks: A QoS-aware fuzzy deep reinforcement learning approach," *Journal of Sensor and Actuator Networks*, vol. 14, no. 1, p. 18, 2025.

[2] Shantanu Kumar Singh, Ioan-Sorin Comsa, Ramona Trestian, Levent V. Cakir, Rahul Singh, Abhishek Kaushik, B. Canberk, P. Shah, B. Kumbhani, and S. Darshi, "WIND: A wireless intelligent network digital twin for federated learning and multi-layer optimization," *IEEE Communications Standards Magazine*, vol. 9, no. 3, pp. 136–144, 2025.

[3] Hunor Sebestyen, Daniela Elena Popescu, and Razvan Daniel Zmaranda, "A literature review on security in the internet of things: Identifying and analysing critical categories," *Computers*, vol. 14, no. 2, p. 61, 2025.

[4] Rakan Alanazi, Marwa Obayya, Asmaa Mansour Alghamdi, Nojood Nemri, Saleh Alshahrani, Norah Alduaiji, and Shaymaa Sorour, "Machine learning-driven routing optimization for energy-efficient 6G-enabled wireless sensor networks," *Alexandria Engineering Journal*, vol. 129, pp. 877–888, 2025.

[5] Raja Waseem Anwar, Muhammad Abrar, Abdus Salam, and Farhan Ullah, "Federated learning with LSTM for intrusion detection in IoT-based wireless sensor networks: A multi-dataset analysis," *PeerJ Computer Science*, vol. 11, p. e2751, 2025.

[6] Abdullah K. Alnaim and Abdullah M. Alwakeel, "Zero-trust mechanisms for securing distributed edge and fog computing in 6G networks," *Mathematics*, vol. 13, no. 8, 2025.

[7] Ze Liu, Jing Zhang, Yan Liu, Fan Feng, and Yan Liu, "Data aggregation algorithm for wireless sensor networks with different initial energy of nodes," *PeerJ Computer Science*, vol. 10, p. e1932, 2024.

[8] Abderrahmane Saidi, "An adaptive trust system for misbehavior detection in wireless sensor networks," *Wireless Networks*, vol. 30, no. 4, pp. 2589–2615, 2024.

[9] Jiong Jin, Zhibo Pang, Jonathan Kua, Quanyan Zhu, Karl Henrik Johansson, Nikolaj Marchenko, and Dave Cavalcanti, "Cloud-fog automation: The new paradigm towards autonomous industrial cyber-physical systems," *IEEE Journal on Selected Areas in Communications*, vol. 43, no. 1, pp. 45–60, 2025.

[10] Ning Liu, Yue Ji, Ke Wang, and Shuai Bai, "Enhanced archimedes optimization algorithm for quality of service-aware routing in internet of things-enabled wireless sensor networks," *Journal of Engineering and Applied Science*, vol. 72, no. 1, p. 176, 2025.

[11] Sarvenaz Sadat Khatami, Mehrdad Shoeibi, Reza Salehi, and Masoud Kaveh, "Energy-Efficient and Secure Double RIS-Aided Wireless Sensor Networks: A QoS-Aware Fuzzy Deep Reinforcement Learning Approach," *Journal of Sensor and Actuator Networks*, vol. 14, no. 1, p. 18, 2025.

[12] Shantanu Kumar Singh, Ioan-Sorin Comsa, Ramona Trestian, Levent V. Cakir, Rahul Singh, and Abhishek Kaushik, "WIND: A Wireless Intelligent Network Digital Twin for Federated Learning and Multi-Layer Optimization," *IEEE Communications Standards Magazine*, vol. 9, no. 3, pp. 136–144, 2025.

[13] Hunor Sebestyen, Daniela Elena Popescu, and Razvan Daniel Zmaranda, "A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories," *Computers*, vol. 14, no. 2, p. 61, 2025.

[14] Reem Alanazi, Mohamed Obayya, Albandari M. Alghamdi, Nojood Nemri, Saleh Alshahrani, Norah Alduaiji, and Sameh Sorour, "Machine learning-driven routing optimization for energy-efficient 6G-enabled wireless sensor networks," *Alexandria Engineering Journal*, vol. 129, pp. 877–888, 2025.

[15] Raja Waseem Anwar, Muhammad Abrar, Abdus Salam, and Farhan Ullah, "Federated learning with LSTM for intrusion detection in IoT-based wireless sensor networks: A multi-dataset analysis," *PeerJ Computer Science*, vol. 11, p. e2751, 2025.

[16] Abdullah K. Alnaim and Abdullah M. Alwakeel, "Zero-Trust Mechanisms for Securing Distributed Edge and Fog Computing in 6G Networks," *Mathematics*, vol. 13, no. 8, 2025.

[17] Ze Liu, Jing Zhang, Yan Liu, Fan Feng, and Yan Liu, "Data aggregation algorithm for wireless sensor networks with different initial energy of nodes," *PeerJ Computer Science*, vol. 10, p. e1932, 2024.

[18] Abderrahmane Saidi, "An adaptive trust system for misbehavior detection in wireless sensor networks," *Wireless Networks*, vol. 30, no. 4, pp. 2589–2615, 2024.

[19] Jiong Jin, Zhibo Pang, James Kua, Qi Zhu, Karl Henrik Johansson, Nikolai Marchenko, and Dave Cavalcanti, "Cloud-Fog Automation: The New Paradigm Towards Autonomous Industrial Cyber-Physical Systems," *IEEE Journal on Selected Areas in Communications*, vol. 43, no. 1, pp. 45–60, 2025.

[20] Ning Liu, Yue Ji, Ke Wang, and Shuai Bai, "Enhanced Archimedes optimization algorithm for quality of service-aware routing in internet of things-enabled wireless sensor networks," *Journal of Engineering and Applied Science*, vol. 72, no. 1, p. 176, 2025.

[21] Amit Sharma and S. Bashir, "Developing A Lightweight Homomorphic Encryption Technique for Secure Data Transmission," *CyberSystem Journal*, vol. 2, no. 2, pp. 98–105, 2025.

[22] Wagdy M. Othman, Abdelhamied A. Ateya, Mohamed E. Nasr, Ammar Muthanna, Mohammed ElAffendi, Andrey Koucheryavy, and Azhar A. Hamdi, "Key Enabling Technologies for 6G: The Role

of UAVs, Terahertz Communication, and Intelligent Reconfigurable Surfaces in Shaping the Future of Wireless Networks," *Journal of Sensor and Actuator Networks*, vol. 14, no. 2, p. 30, 2025.

[23] S. Shen, R. Onwuegbuzie, and J. Nagy, "Enhancing privacy-preserving brain tumor classification with adaptive reputation-aware federated learning and homomorphic encryption," *PeerJ Computer Science*, vol. 11, p. e3165, 2025.

[24] Moner Alsader, Alcardo Alex Barakabitze, and Is-Haka Mkwawa, "QoE-Driven Adaptive Video Streaming: Architectures, Techniques, and Future Research Challenges Toward 6G Networks," *IEEE Access*, vol. 13, pp. 157407–157440, 2025.

[25] C. C. Johnson-Okonkwo, I. I. Ayogu, G. A. Chukwudebe, and J. N. Odii, "Recent Advances in Wireless Sensor Networks Load-Balancing Optimization: A Review of Approaches and Emerging Trends," *Nigerian Journal of Technology*, vol. 44, no. 4, pp. 1–33, 2025.

[26] https://archive.ics.uci.edu/ml/datasets/Environmental+Sensor+Telemetry+Data