Toward Quantum-Resistant Fog-IoT Security: A Dual-Phase Framework with Chaotic Elliptic-Curve Diffie-Hellman and Post-Quantum Encryption

Ali-Alridha Khalil
Department of Information Networks, College of Information Technology, University of Babylon, Babil, Iraq
alialridhakhalili.net@student.uobabylon.edu.iq (corresponding author)

Mehdi Ebady Manaa
Intelligent Medical Systems Department, College of Sciences, Al-Mustaqbal University, Iraq | Department of Information Networks, College of Information Technology, University of Babylon, Iraq
mahdi.ebadi@uomus.edu.iq

Received: 19 April 2025 | Revised: 26 May 2025 and 8 June 2025 | Accepted: 9 June 2025

 DOI: https://doi.org/10.48084/etasr.11600

ABSTRACT

The spread of Internet of Things (IoT) devices along with the distributed nature of fog computing has amplified the necessity for secure, efficient, and quantum-resistant communication protocols, especially in light of emerging quantum threats. This paper presents a two-phase security framework tailored for fog-IoT systems to enhance both data encryption and authentication. In the first phase, a novel lightweight authentication protocol is introduced by integrating the Elliptic-Curve Diffie-Hellman (ECDH) with the Lorenz chaotic system, resulting in highly unpredictable keys and increased resistance to cryptanalytic attacks. In the second phase, quantum-resilient data confidentiality is ensured using the CRYSTALS-Kyber algorithm. Extensive simulations were carried out to evaluate the effectiveness of the framework. Key randomness was statistically validated using the NIST SP 800-22 suite, yielding high *p*-values (0.9414, 0.7659, and 0.9024), confirming strong entropy and cryptographic suitability. The CRYSTALS-Kyber component demonstrated practical performance with a key generation time of 35.64 ms, encryption time of 52.67 ms, and decryption time of 17.62 ms, surpassing comparable schemes in speed. Furthermore, the system maintained a low memory footprint of 71.13 KB and minimal CPU utilization at 7.5%, underscoring its lightweight design. These results confirm the feasibility, scalability, and efficiency of the proposed framework, making it a strong candidate for real-time and secure fog-IoT deployments under classical and quantum threat models.

Keywords-fog computing; IoT; chaotic ECDH; CRYSTALS-Kyber; post-quantum cryptography; secure communication

I. INTRODUCTION

The advent of the Internet of Things (IoT) expanded computing in a way that facilitates high-speed connectivity and real-time data sharing in a wide variety of applications. However, centralized cloud computing poses challenges of latency, bandwidth, and security when it comes to serving huge IoT deployments. To overcome these, there is a new paradigm called fog computing that seeks to bring computational resources near the edge device [1]. However, fog computing is not immune to a variety of security threats, with some of the most significant being authentication and data encryption [2]. Secure communication is essential in the context of IoT nodes and fog nodes and must be associated with confidentiality, integrity, and the ability to work in resource-limited systems [3]. Conventional techniques, such as the use of Elliptic-Curve Diffie-Hellman (ECDH), support secure key exchange but are becoming more vulnerable to new-generation cryptanalysis with the advent of quantum computing [4]. As ECDH deterministically generated keys can be targeted, there is a need to strengthen the randomness and unpredictability of authentication protocols [5].

In parallel to this, data confidentiality is also paramount. Traditional encryption algorithms (i.e., RSA, ECC) are also expected to become outdated in the presence of quantum attackers [6]. This necessitates the use of Post-Quantum Cryptographic (PQC) methods that are both resilient in a

quantum attack context and also provide efficient operation in Fog-IoT networks [7]. Lattice-based cryptographic schemes, such as the recently NIST-standardized CRYSTALS-Kyber, provide potential resilience to quantum attacks, along with efficient practical performance [8].

To address these challenges, this study proposes a two-phase security scheme. In the first phase, a new authentication scheme couples the Lorenz chaotic map to ECDH, using chaotic behavior to enhance the randomness of the generated keys. Chaotic systems, such as Lorenz and other nonlinear dynamical mappings, have been shown to exhibit high sensitivity to initial conditions and are therefore highly viable options for generating keys [9]. This provides improved resilience to replay and brute-force attacks and is lightweight and appropriate for resource-constrained IoT devices [10]. In the second phase, data transmission is encrypted securely in a quantum-resistant fashion using standalone CRYSTALS-Kyber [11]. This study makes two contributions. It first develops a chaotic ECDH-based authentication system that provides security through unpredictability without compromising system performance and uses the CRYSTALS-Kyber encryption method to quantum-secure Fog-IoT communication. This approach makes the proposed system scalable and efficient in computation and practical for deployment in Fog-IoT applications [12].

A. Related Works

The growing convergence of IoT and fog computing has raised serious concerns about secure communication, especially in the context of nascent quantum threats. Recent works have dealt with these challenges using Post-Quantum Cryptography (PQC) protocols and resource-constrained IoT-adapted lightweight authentication protocols.

1) Post-Quantum Cryptography for IoT-Fog Security

Hybrid encryption systems using PQC have become more popular for secure IoT communication. In [13], a hybrid scheme, called QRHE-IoT, combined symmetric encryption and post-quantum key exchange to secure smart grid data transmission and meet real-time requirements while being immune to quantum-level attacks. In [14], PQC was incorporated into MQTT to facilitate safe broadcast communication not dependent on the classical TLS hello handshake. Frequent and low-latency messaging was supported by a quantum-resistant MQTT architecture, which fits IoT scenarios. In [15], CRYSTALS-Kyber, a lattice-based KEM, was modified for data encryption directly in IoT systems. In experiments at the hardware level, Kyber was proven computationally viable in IoT-constrained devices, although key size and power consumption are still crucial considerations.

2) Lightweight Authentication Protocols for Fog-IoT

Various schemes have been proposed to satisfy mutual authentication of IoT devices and fog nodes. In [2], a lightweight anonymous mutual authentication scheme was proposed, which was secure against impersonation and preserved anonymity. This scheme was verified by both security and informal analysis, showing low overhead as appropriate in the context of fog-supporting architectures. In [5], an ECDSA and secure ECC curve lightweight authentication scheme was proposed, which outperformed existing solutions by minimizing computation time by up to 87% and energy consumption by up to 82% compared to RSA and Lindell's protocol. The two-stage architecture, cloud-layer key distribution followed by fog-layer authentication, maintained private key security with minimal loading of end devices. In [16], another authenticated key exchange scheme was proposed using ECC, showing strong security guarantees under the random oracle model and good computational and communication performance. In [17], LAMAS was proposed, which is an ECC-based mutual authentication protocol that runs on device, fog, and cloud layers. This model provides mutual authentication for all parties while keeping them anonymous and resisting replay and MITM threats. The scheme had lower computational and storage overhead compared to similar multilayer schemes.

3) Performance-Optimized and Sustainable Schemes

Modern works focus not only on security but also on energy efficiency and sustainability in authentication protocols. In [18], an authentication method used ECDSA with optimized elliptic curves (such as Curve25519), offering up to 87% improvement in computational time and considerable energy efficiency compared to RSA and conventional ECDSA. For IoT-based healthcare deployments, a hybrid ECC and proxy re-encryption scheme was proposed in [19] to secure Electronic Health Record (EHR) transfer. Using an improved salp swarm algorithm, the proposed scheme showed improved speed and low memory consumption, corroborating its feasibility in time-critical applications. In [20], a green mutual authentication scheme was proposed for Fog-IoT-Cloud networks. The ECC-based scheme, which was formally proved using ProVerif, supported robust security and low computational cost while having low effects on energy consumption, and thus being a feasible solution for green Fog-IoT infrastructures.

II. METHODOLOGY

The adoption of PQC algorithms for strengthening security systems must go beyond standard computer systems to resource-limited IoT settings. In this context, this study proposes a dual-phase security framework tailored for Fog-IoT architectures. This framework separates authentication and encryption functions, each handled by a distinct scheme optimized for its role:

- Chaotic-Enhanced ECDH: A lightweight authentication protocol to enhance the randomness and unpredictability of key generation by integrating the Lorenz chaotic system with the classical ECDH protocol.
- CRYSTALS-Kyber: A post-quantum encryption scheme that ensures long-term data confidentiality and security against quantum adversaries.

These two components operate independently, yet together provide a comprehensive security architecture for Fog-IoT environments.

A. Phase 1: Authentication Using Chaotic ECDH and Lorenz System

This phase is dedicated solely to authentication. The traditional ECDH key exchange is enhanced using the Lorenz chaotic system to introduce greater randomness and unpredictability in the shared key, making it more resistant to cryptographic attacks. The complete process of this chaotic authentication scheme, including key generation, Lorenz-based transformation, and final key derivation, is summarized in Algorithm 1.

1) ECDH Key Exchange

The authentication process commences with the independent generation of ECDH key pairs by the client (c) and server (s) as described in (1):

- Each entity selects a private key:

$$d_{c\in}\mathbb{Z}_n,\ d_s \in \mathbb{Z}_n \quad (1)$$

where n represents the order of the elliptic curve group as shown in (2).

- Public keys are subsequently derived as:

$$P_c = d_c \cdot G,\ P_s = d_s \cdot G \quad (2)$$

where G is the generator point on the elliptic curve.

- Upon the exchange of public keys, both entities compute an identical shared secret independently as given in (3):

$$S = d_c \cdot P_s = d_c \cdot (d_s \cdot G) =$$
$$d_s \cdot (d_c \cdot G) = d_s \cdot P_c \quad (3)$$

This symmetric shared secret ensures mutual authentication while remaining computationally infeasible for adversaries to reconstruct without knowledge of the private keys.

2) Chaotic Transformation of the Shared Secret Using the Lorenz System

To improve unpredictability and protect against pattern-based or brute-force attacks, the shared secret S is used to initialize the Lorenz chaotic system, defined by a set of nonlinear differential equations:

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dx}{dt} = x(\rho - z) - y \\ \frac{dz}{dt} = xy - \beta z \end{cases} \quad (4)$$

where $\sigma = 10.0$ (Prandtl number), $\rho = 28.0$ (Rayleigh number), and $\beta = 8/3$ (geometric factor). These classical values are used to ensure chaotic behavior in the system [21].

The shared secret S is mapped into the Lorenz system's initial conditions as:

$$\begin{cases} x_0 = \frac{S \bmod 256}{256} \\ y_0 = \frac{(S//256) \bmod 256}{256} \\ z_0 = \frac{(S//256^2) \bmod 256}{256} \end{cases} \quad (5)$$

The Lorenz system is then simulated for 100 iterations using a time step $dt = 0.01$. The final chaotic key is derived from the chaotic output using:

$$\begin{cases} K_{part_x} = \lfloor x_N \times 10^{12} \rfloor \bmod 2^{64} \\ K_{part_y} = \lfloor y_N \times 10^{12} \rfloor \bmod 2^{64} \\ K_{final} = (K_{part_x} \ll 64) | K_{part_y} \end{cases} \quad (6)$$

This process ensures high randomness and unpredictability, generating a robust 128-bit authentication key. This chaotic enhancement introduces non-deterministic behavior into the authentication process, increasing the difficulty of key prediction and attack feasibility.

3) Authentication Verification

The verification phase involves comparing the generated keys:

$$K_{client} == K_{server}$$

A successful comparison authenticates the communication channel; otherwise, the connection is immediately terminated to thwart unauthorized access.

Algorithm 1: Chaotic ECDH Authentication (Client–Fog Layer)
Input: Security parameter λ, elliptic curve $secp256r1$
Output: 128-bit shared key K_{shared}
1. Key Exchange:
   Client generates ECDH key pair: $(sk_{client}, pk_{client}) \leftarrow EC.Gen(secp256r1)$
   Fog node generates ECDH key pair: $(sk_{fog}, pk_{fog}) \leftarrow EC.Gen(secp256r1)$
   Exchange public keys: $Client \rightarrow Fog: pk_{client};\ Fog \rightarrow Client: pk_{fog}$
2. Shared Secret: $ss \leftarrow ECDH(sk_{client}, pk_{fog})$
3. Chaotic Key Derivation:
   Convert ss to integer: $ss\_int \leftarrow int.from\_bytes(ss)$
   Iterate Lorenz system ($\sigma = 10.0,\ \rho = 28.0,\ \beta = 8/3,\ \Delta t = 0.01$):
   For $t = 1$ to 100:
   $x_t = x_{t-1} + \sigma(y_{t-1} - x_{t-1})\Delta t$
   $y_t = y_{t-1} + (x_{t-1}(\rho - z_{t-1}) - y_{t-1})\Delta t$
   $z_t = z_{t-1} + (x_{t-1}y_{t-1} - \beta z_{t-1})\Delta t$
   Compute final key: $K_{shared} \leftarrow to\_bin(x_{100}, y_{100})$

4) Performance and Security Evaluation

The authentication method is evaluated based on computational complexity, scalability, security robustness, and randomness assessment.

- Computational Complexity:
  1. ECDH key exchange: $O(\log n)$, ensuring efficiency.

2. Lorenz system transformation: $O(N)$, where N denotes the number of iterations.

- Scalability: Capable of managing multiple simultaneous authentication sessions efficiently.
- Security robustness: Evaluated using the NIST SP 800-22 test suite, the keys demonstrate high unpredictability and pass statistical randomness tests.
- Randomness assessment: Randomness validated using the NIST SP 800-22 test suite.

B. Phase 2: Data Encryption and Decryption Using Modified CRYSTALS-Kyber Algorithm

In this phase, the encryption and decryption processes follow the framework of the Kyber.CPAPKE algorithm, with a modification that aligns with the architecture of this study. Unlike traditional node-based operations, where encryption and decryption are handled by the node itself, here encryption occurs within the fog layer, and decryption is executed on the server. This strategic placement leverages the proximity of the fog layer to IoT devices and the server's computational capabilities, enhancing both security and efficiency within the Fog-IoT environment. Algorithm 2 presents the entire encryption and decryption workflow, adapted for the Fog-IoT environment.

1) Key Generation Process

After successful authentication, all data exchanged between IoT nodes and fog servers is encrypted using the CRYSTALS-Kyber algorithm. This post-quantum encryption mechanism operates independently from the authentication phase. The encryption mechanism initiates with the generation of a public-private key pair:

- Public matrix A is generated using a rejection sampler.
- Noise vectors e and s are sampled from a Centered Binomial Distribution (CBD). The key computation is described as:

$$pk = A \cdot s + e \tag{7}$$

2) Encryption in the Fog Layer

The encryption process is delegated to the fog layer, leveraging its computational resources. Given an input message m, random coins r, and the public key pk, the ciphertext components u and v are calculated by:

$$u = A \cdot r + e_1 \tag{8}$$

$$v = pk \cdot r + e_2 + m \tag{9}$$

The ciphertext (u, v) is then transmitted securely.

3) Decryption on the Server

The decryption phase employs lattice-based cryptographic principles to recover the original plaintext from the received ciphertext while mitigating the impact of intentionally introduced noise. Upon receiving the ciphertext pair (u, v), the server leverages its private key $s \in R_q^k$ (a component of the Kyber secret key) to invert the encryption mechanism. The process unfolds as follows:

a) Message Recovery

The server computes the inner product $s^T u$ over the polynomial $R_q = \mathbb{Z}_q[x]/(f(x))$, where $f(x)$ defines the irreducible polynomial modulus. Subtracting this product from the second ciphertext component v yields:

$$m = v - s^T u \tag{10}$$

This operation eliminates the public matrix A contribution, isolating the encoded message combined with residual error terms.

b) Noise Suppression via Thresholding

The recovered polynomial m contains coefficients perturbed by the error terms $e_2 - s^T e_1$. To decode the binary message, a thresholding mechanism is applied to each coefficient $c_i \in m$ as outlined in:

$$m_i' = \begin{cases} 0, & if \ |c_i| < \frac{q}{4} \\ 1, & otherwise \end{cases} \tag{11}$$

This step exploits the structured error distribution (x) to distinguish between encoded 0 and 1 bits, as the original message is scaled by $\lfloor q/2 \rfloor$ during encryption.

c) Message Reconstruction:

The binary sequence$\{m_i'\}$ is aggregated into 8-bit blocks and converted to ASCII characters through a deterministic mapping function. The final plaintext m' is thus reconstructed, ensuring fidelity to the original message m transmitted by the IoT device.

```
Algorithm 2: Kyber-Enhanced Data Transmission (Fog-Server)
Input: Plaintext m, public key pk = (A, t)
Output: Decrypted plaintext m'
1. Encryption (Fog Node):
   Encode message: m_enc ← ⌊q/2⌋ · Binary(m)
   Sample random vectors r, e1, e2 ← χ
   Compute ciphertext:
   u = A^T · r + e1
   v = t^T · r + e2 + m_enc
   Send (u, v) to the Server
2. Decryption (Server):
   Recover message: m̃ ← v − s^T · u mod q
   Decode m̃:
   For each coefficient c_i ∈ m̃:
       If |c_i| < q/4 → m'_i = 0
       Else → m'_i = 1
   Reconstruct m' ← BinaryToASCII(m'_i)
```

This phase significantly enhances computational efficiency while maintaining robust security within the distributed Fog-IoT. The proposed method integrates advanced cryptographic techniques with chaotic systems and post-quantum algorithms to establish a secure, efficient, and scalable framework for Fog-IoT environments, ensuring robust protection against a wide spectrum of cyber threats while optimizing resource utilization and maintaining low computational overheads.

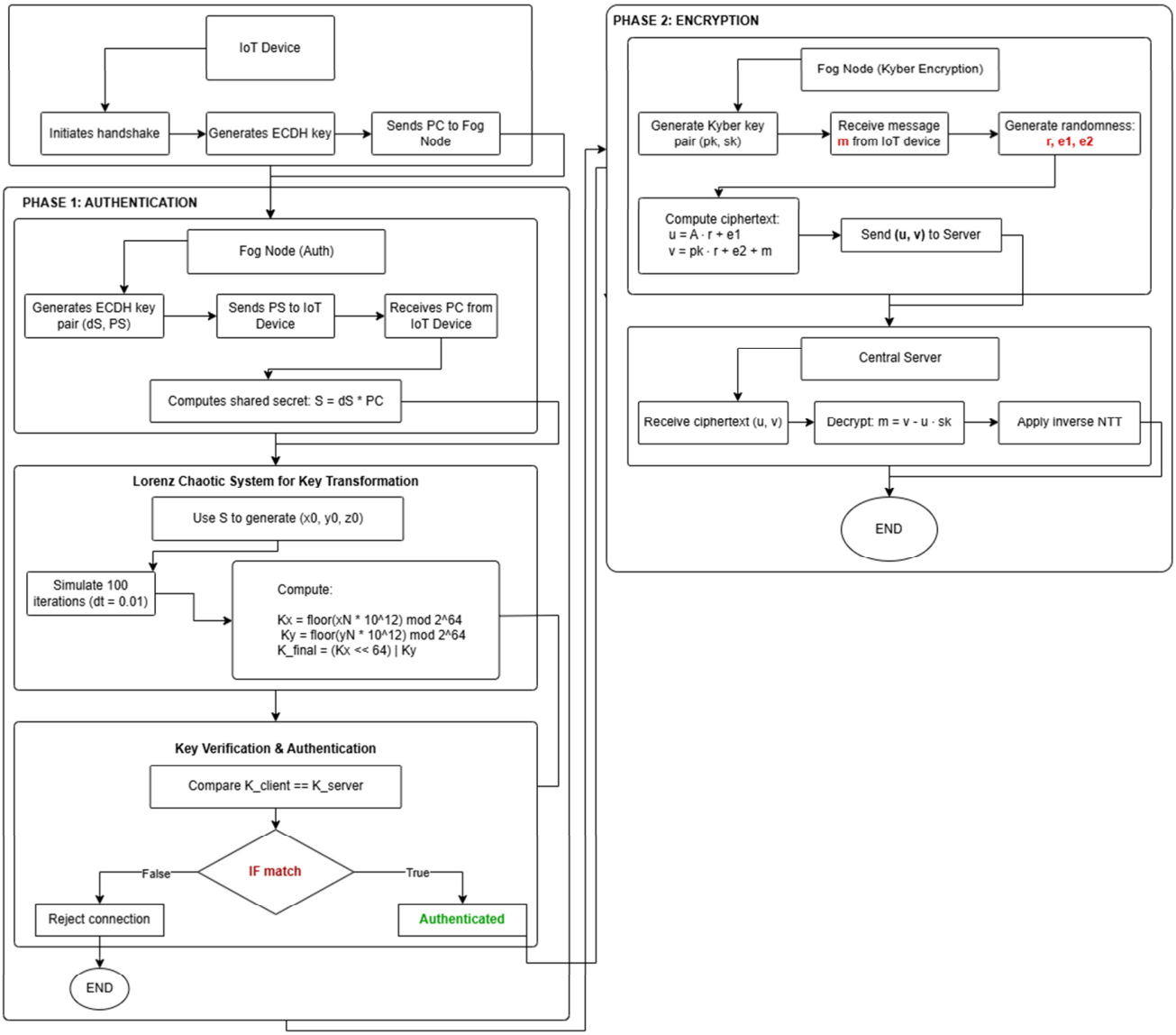

Fig. 1. System design.

III. SIMULATION AND RESULTS

The performance of the proposed security framework was measured by carrying out simulations using Python on a PC with an Intel i7-14700K processor, an NVIDIA 4070Ti Super GPU, 32GB of RAM, utilizing Windows 11. This machine helped with the optimal processing of cryptographic operations as well as network simulations.

A. Chaotic Elliptic Curve Diffie-Hellman Evaluation

In order to evaluate the statistical stability and randomness of the keys generated by the developed framework [22], the NIST SP 800-22 test suite was employed for randomness tests. Three basic randomness tests, the Block Frequency Test, Runs Test, and Approximate Entropy Test, were used for evaluation. These tests ensure the randomness and entropy values of the generated key sequences, making them appropriate for secure cryptographic operations.

1) Block Frequency Test

The Block Frequency Test examines the ratio of ones and zeros within fixed blocks of a binary string. The test calculates the Chi-squared value as a measure of the departure from an optimal uniform distribution. The test was applied with a block size of 128 bits, totaling 859 substrings, and 48 bits of the string were discarded for alignment purposes.

- Chi-square value: 795.0625
- p-value: 0.9414

The high value of p (0.9414) signifies that the ratio of ones and zeros for each block is very well within the expected uniform distribution. This establishes that the generated key is free from any bias in its bit pattern, thus establishing its suitability for cryptographic purposes.

2) Runs Test

The Runs Test examines the overall count of unbroken sequences of identical bits within the key string. This test ensures there is not excessive bunching of ones or zeros, which can be an indicator of non-randomness. The test is carried out by comparing the actual count of runs with the theoretical expected value.

- Total Number of Runs (Vn_{obs}): 20530
- Pi (proportion of ones): 0.4987
- p-value: 0.7659

Since the p-value is 0.7659, the test verifies that the run count is consistent with expected randomness. The balance of the value of Pi (0.4987) indicates that ones and zeros occur with virtually identical probability, minimizing the probability of structural patterns within the key.

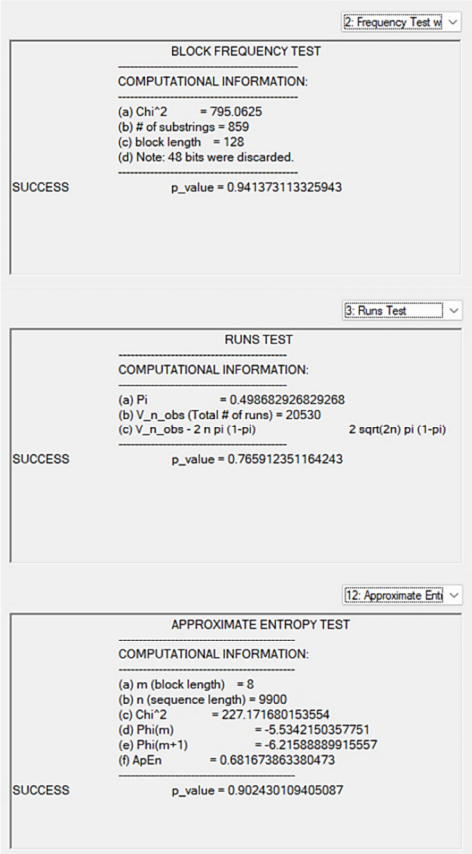

Fig. 2. NIST test results.

3) Approximate Entropy Test

The Approximate Entropy test assesses the randomness of the key sequence by comparing the occurrence of patterns of length m with patterns of length $m + 1$.

- Block Length (m): 8
- Sequence Length (n): 9900
- Chi-square value: 227.17
- p-value: 0.9024

The p-value of 0.9024 indicates that the sequence exhibits a high degree of randomness, with no discernible patterns in bit transitions. Figure 2 presents the results of the framework under several NIST tests for estimating the security of the system.

B. CRYSTALS-Kyber Performance Evaluations

To assess the performance of the CRYSTALS-Kyber post-quantum encryption algorithm used in the proposed fog computing security framework, a set of performance metrics was compared. These performance metrics encompass key generation time, encryption and decryption times, processing capacity, memory usage, and CPU utilization when performing cryptographic operations. The time taken for key generation was captured at 35.64 ms, reflecting a decently fast initialization phase ideal for dynamic Fog-IoT environments. It took an average of 52.67 ms for encryption and 17.62 ms for decryption, reflecting a desirable asymmetry ideal for real-time data access on fog nodes. Figure 3 illustrates the time it took to perform the operation.

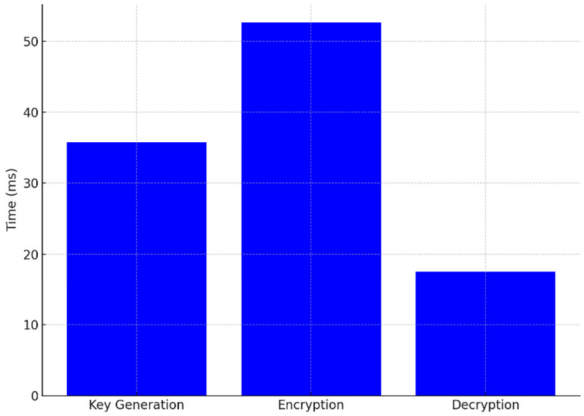

Fig. 3. Times for cryptographic operations.

Additionally, the deployment achieved a low memory footprint of 71.1362 KB and exhibited a low CPU load at 7.5%, verifying the lightness of the Kyber algorithm when used in limited fog environments. The above findings validate the feasibility of CRYSTAL-Kyber in improving fog computing security without contributing a high amount of overhead resources to the host system. These results are shown in Figures 4 and 5.

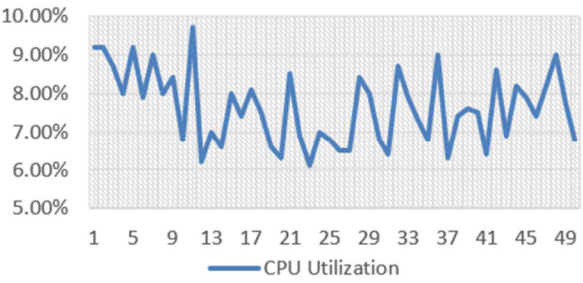

Fig. 4. CPU utilization.

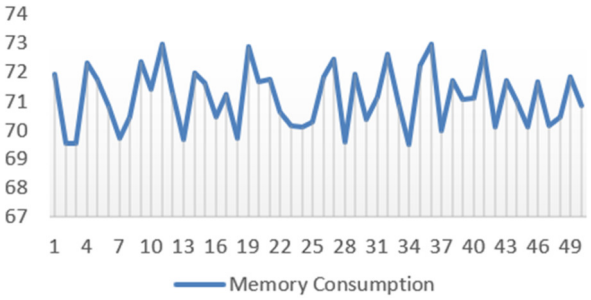

Fig. 5. Memory consumption.

1) Result Comparison

This section offers a comparative evaluation of the proposed system against notable existing implementations of the CRYSTALS-Kyber post-quantum encryption algorithm. The comparison focuses on three primary performance indicators: key generation time, encryption time, and decryption time, as shown in Table I. These metrics are critical in assessing the algorithm's suitability for deployment in time-sensitive and resource-constrained Fog-IoT environments.

TABLE I. COMPARISON TABLE

	Key generation time (ms)	**Encryption time (ms)**	**Decryption time (ms)**
[23]	38.23	37.35	36.55
[24]	87.8	99.0	113.3
[25]	58.2	67.9	86.2
Proposed system	35.64	52.67	17.62

Table I presents the performance metrics (in ms) of three recent studies along with the results obtained from the proposed system. In particular, the proposed system demonstrates superior performance across all categories, achieving the lowest key generation time (35.64 ms) compared to the system in [23] (38.23 ms), and significantly improving over the system in [24] (87.8 ms). Similarly, the encryption and decryption processes in the proposed system are faster (52.67 and 17.62 ms, respectively), indicating better computational efficiency and reduced latency. These results underscore the system's potential for real-time Fog-IoT deployments, highlighting its optimization for both speed and post-quantum resilience.

IV. CONCLUSION

This study presented a novel two-phase security framework designed specifically for Fog-IoT architectures, addressing the dual challenges of authentication and data confidentiality in the face of both classical and quantum threats. The first major contribution is the integration of the Lorenz chaotic system into the ECDH key exchange protocol, significantly improving key randomness and resistance to statistical, brute-force, and replay attacks. This enhancement introduces nonlinearity and unpredictability into the authentication process, which is particularly beneficial for resource-constrained IoT environments. The second contribution is the deployment of the NIST-approved CRYSTALS-Kyber algorithm as a post-quantum encryption mechanism within the fog layer, offering robust protection against quantum adversaries. Unlike conventional frameworks, the encryption phase is strategically offloaded to the fog node, while decryption is handled at the server, optimizing both latency and resource allocation.

Widespread simulations corroborate cryptographic security, key randomness, and system efficiency. The framework ensures measurable latency reductions and reasonable consumption of resources, while retaining substantial security guarantees. These findings corroborate the feasibility, scalability, and flexibility of the method for real-world application within the newly evolving Fog-IoT systems. Future research will focus on extending this model to support dynamic node mobility, integrating real-time Intrusion Detection Systems (IDS), and optimizing the protocol for hardware-constrained IoT devices. Additionally, formal security proofs and deployment in testbed environments will be pursued to further validate robustness under diverse threat scenarios.

REFERENCES

[1] A. K. Jumani, J. Shi, A. A. Laghari, Z. Hu, A. ul Nabi, and H. Qian, "Fog computing security: A review," *Security and Privacy*, vol. 6, no. 6, 2023, Art. no. e313, https://doi.org/10.1002/spy2.313.

[2] S. Singh and V. K. Chaurasiya, "Mutual authentication scheme of IoT devices in fog computing environment," *Cluster Computing*, vol. 24, no. 3, pp. 1643–1657, Sep. 2021, https://doi.org/10.1007/s10586-020-03211-1.

[3] A. M. Ghalwah and G. A. Al-Sultany, "Leveraging Community-based Approaches for Enhancing Resource Allocation in Fog Computing Environment," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 20372–20378, Feb. 2025, https://doi.org/10.48084/etasr.9206.

[4] V. Tanksale, "Efficient Elliptic Curve Diffie–Hellman Key Exchange for Resource-Constrained IoT Devices," *Electronics*, vol. 13, no. 18, Sep. 2024, Art. no. 3631, https://doi.org/10.3390/electronics13183631.

[5] M. A. Shaaban, A. S. Alsharkawy, M. T. AbouKreisha, and M. A. Razek, "Efficient ECC-based authentication scheme for fog-based IoT environment." arXiv, 2024, https://doi.org/10.48550/ARXIV.2408.02826.

[6] T. Tripathi, A. Awasthi, S. P. Singh, and A. Chaturvedi, "Post Quantum Cryptography and its Comparison with Classical Cryptography." arXiv, 2024, https://doi.org/10.48550/ARXIV.2403.19299.

[7] N. Alnahawi *et al.*, "Post-Quantum Cryptography in eMRTDs: Evaluating PAKE and PKI for Travel Documents." Cryptology ePrint Archive, 2025, [Online]. Available: https://eprint.iacr.org/2025/812.

[8] R. H. Joudah and M. E. Manaa, "A New Approach to Improving the Security of the 5G-AKA Using Crystals-Kyber Post-Quantum Technologies and ASCON Algorithm," *International Journal of Safety and Security Engineering*, vol. 14, no. 6, pp. 1729–1742, Dec. 2024, https://doi.org/10.18280/ijsse.140608.

[9] A. H. Khaleel and I. Q. Abduljaleel, "Chaotic Image Cryptography Systems: A Review," *Samarra Journal of Pure and Applied Science*, vol. 3, no. 2, pp. 129–143, Sep. 2021, https://doi.org/10.54153/sjpas.2021.v3i2.244.

[10] A. Aljaedi, A. R. Alharbi, A. Aljuhni, M. K. Alghuson, S. Alassmi, and A. Shafique, "A lightweight encryption algorithm for resource-constrained IoT devices using quantum and chaotic techniques with metaheuristic optimization," *Scientific Reports*, vol. 15, no. 1, Apr. 2025, Art. no. 14050, https://doi.org/10.1038/s41598-025-97822-6.

[11] L. H. Mahdi and A. A. Abdullah, "Fortifying Future IoT Security: A Comprehensive Review on Lightweight Post-Quantum Cryptography," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21812–21821, Apr. 2025, https://doi.org/10.48084/etasr.10141.

[12] J. Choi and J. Lee, "Secure and Scalable Internet of Things Model Using Post-Quantum MACsec," *Applied Sciences*, vol. 14, no. 10, May 2024, Art. no. 4215, https://doi.org/10.3390/app14104215.

[13] J. Xiong, L. Shen, Y. Liu, and X. Fang, "Enhancing IoT security in smart grids with quantum-resistant hybrid encryption," *Scientific Reports*, vol. 15, no. 1, Jan. 2025, Art. no. 3, https://doi.org/10.1038/s41598-024-84427-8.

[14] L. Malina, P. Dobias, P. Dzurenda, and G. Srivastava, "Quantum-Resistant and Secure MQTT Communication," in *Proceedings of the 19th International Conference on Availability, Reliability and Security*, Vienna, Austria, Jul. 2024, pp. 1–8, https://doi.org/10.1145/3664476.3670463.

[15] R. Ristov and S. Koceski, "Quantum Resilient Public Key Cryptography in Internet of Things," in *2023 12th Mediterranean Conference on Embedded Computing (MECO)*, Budva, Montenegro, Jun. 2023, pp. 1–4, https://doi.org/10.1109/MECO58584.2023.10154994.

[16] C. M. Chen, Y. Huang, K. H. Wang, S. Kumari, and M. E. Wu, "A secure authenticated and key exchange scheme for fog computing," *Enterprise Information Systems*, vol. 15, no. 9, pp. 1200–1215, Oct. 2021, https://doi.org/10.1080/17517575.2020.1712746.

[17] M. Hamada, S. A. Salem, and F. M. Salem, "LAMAS: Lightweight anonymous mutual authentication scheme for securing fog computing environments," *Ain Shams Engineering Journal*, vol. 13, no. 6, Nov. 2022, Art. no. 101752, https://doi.org/10.1016/j.asej.2022.101752.

[18] M. A. Shaaban, A. S. Alsharkawy, M. T. AbouKreisha, and M. A. Razek, "Efficient ECC-Based Authentication Scheme for Fog-Based IoT Environment," *International journal of Computer Networks & Communications*, vol. 15, no. 04, pp. 55–71, Jul. 2023, https://doi.org/10.5121/ijcnc.2023.15404.

[19] P. B. Corthis, G. P. Ramesh, M. García-Torres, and R. Ruíz, "Effective Identification and Authentication of Healthcare IoT Using Fog Computing with Hybrid Cryptographic Algorithm," *Symmetry*, vol. 16, no. 6, Jun. 2024, Art. no. 726, https://doi.org/10.3390/sym16060726.

[20] S. P. Satpathy, S. Mohanty, and M. Pradhan, "A sustainable mutual authentication protocol for IoT-Fog-Cloud environment," *Peer-to-Peer Networking and Applications*, vol. 18, no. 1, Jan. 2025, Art. no. 35, https://doi.org/10.1007/s12083-024-01843-3.

[21] E. N. Lorenz, "Deterministic Nonperiodic Flow," in *The Theory of Chaotic Attractors*, B. R. Hunt, T. Y. Li, J. A. Kennedy, and H. E. Nusse, Eds. New York, NY: Springer New York, 2004, pp. 25–36.

[22] A. Rukhin et al., A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institure of standards and Technology, 2010.

[23] P. Sanal, E. Karagoz, H. Seo, R. Azarderakhsh, and M. Mozaffari-Kermani, "Kyber on ARM64: Compact Implementations of Kyber on 64-Bit ARM Cortex-A Processors," in *Security and Privacy in Communication Networks*, vol. 399, J. Garcia-Alfaro, S. Li, R. Poovendran, H. Debar, and M. Yung, Eds. Springer International Publishing, 2021, pp. 424–440.

[24] "Kyber." https://pq-crystals.org/kyber/index.shtml.

[25] Y. Xing and S. Li, "A Compact Hardware Implementation of CCA-Secure Key Exchange Mechanism CRYSTALS-KYBER on FPGA," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 328–356, Feb. 2021, https://doi.org/10.46586/tches.v2021.i2.328-356.