International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Integration of Moth-Flame Optimization with Lattice-Based Cryptography for Post-Quantum IoT Data Protection

[1]Ranjan Kumar Gupta, [2]Ranu Pandey

Submitted:25/06/2024 **Revised**: 17/07/2024 **Accepted:** 25/07/2024

Abstract – The rapid proliferation of Internet of Things (IoT) ecosystems has resulted in unprecedented volumes of sensitive information being transmitted across interconnected devices and cloud platforms, raising significant concerns regarding data protection and confidentiality. Conventional cryptographic frameworks are increasingly vulnerable to emerging threats, particularly with advancements in quantum computing capabilities. This research introduces a novel encryption methodology that synergistically combines Moth-Flame Optimization (MFO) with Lattice-Based Cryptography (LBC). LBC offers robust post-quantum security as an alternative to traditional cryptographic approaches, while MFO enhances the key generation process through sophisticated optimization techniques. This dual-layer framework strengthens cryptographic key generation while ensuring comprehensive security for IoT data transmissions to cloud infrastructure. The integrated MFO-LBC approach delivers a secure, scalable, and computationally efficient solution that addresses limitations inherent in conventional encryption schemes, providing resilience against both classical and quantum-based attacks.

Keywords – *AES, Internet of Things, Lattice-Based Cryptography, Moth-Flame Optimization*

I. INTRODUCTION

The Internet of Things (IoT) has fundamentally transformed the paradigm of device interconnectivity, generating massive volumes of data that traverse network infrastructures and cloud storage systems. As the deployment of IoT devices continues its exponential trajectory, ensuring the security and privacy of transmitted sensitive information has emerged as a critical challenge. With conventional cryptographic algorithms facing potential compromise from advancing quantum computing capabilities and sophisticated cyber threats, there exists an urgent requirement for enhanced security frameworks capable of withstanding future technological developments.

Research Motivation

The impetus for this investigation stems from the critical necessity to strengthen information security within IoT environments against both conventional and quantum-enabled attacks. Lattice-Based Cryptography (LBC) represents a promising cryptographic paradigm that delivers post-quantum security assurances, positioning it as a viable successor to established cryptographic methodologies. However, despite providing a robust encryption foundation, the inherent complexity of lattice problems necessitates optimization to achieve both computational efficiency and cryptographic key robustness. This paper proposes an innovative integration of the Moth-Flame Optimization (MFO) algorithm with LBC, wherein the key generation process is streamlined to enhance overall cryptographic system resilience. The incorporation of MFO enables dynamic adaptation of lattice-based key parameters during operation, ensuring elevated security levels without compromising computational efficiency.

Problem Formulation

The principal challenge addressed in this research concerns the escalating vulnerability of IoT data to both quantum and classical computational attacks. While traditional cryptographic mechanisms remain effective in contemporary contexts, they remain susceptible to future threats posed by quantum algorithms capable of compromising widely-adopted encryption standards. Although LBC's post-quantum resilience offers a theoretical solution, its practical efficacy depends significantly on cryptographic key optimization, creating a requirement for computationally efficient optimization techniques that enhance security without degrading system performance.

[1]*Shri Rawatpura Sarkar University, Raipur, Chhattisgarh*
Email- kumarranjange@gmail.com
[2]*Assistant Professor Dept. of Computer Science & Engg.*
Email – ranu_pandey8@hotmail.com

Principal Contributions

This research introduces a novel cryptographic framework integrating Moth-Flame Optimization with Lattice-Based Cryptography to secure IoT data transmission to cloud platforms. The primary contributions include:

1. **MFO-LBC Integration**: A hybrid model that optimizes cryptographic key generation processes, yielding enhanced cryptographic solutions with improved system-wide security characteristics.
2. **Post-Quantum Security Framework**: Leveraging LBC to provide quantum-resistant encryption capable of countering emerging threats from quantum computing advancements while maintaining robust security guarantees.
3. **Optimized Key Generation Mechanism**: Employment of MFO for lattice-based cryptographic key optimization, delivering a dynamic and scalable approach to cryptographic key assignment for IoT data encryption that balances performance requirements with security objectives.
4. **Multi-Layered Security Architecture**: Implementation of a dual-tier encryption mechanism through simultaneous application of LBC and MFO, ensuring comprehensive security and privacy for IoT data during network transmission and cloud storage.

This research establishes a future-proof security framework by combining the quantum-resistant properties of LBC with the optimization capabilities of MFO, addressing limitations inherent in conventional encryption approaches while preparing IoT security infrastructure for emerging threats. The proposed system represents a significant advancement in cryptographic and IoT security domains, integrating sophisticated key management with robust data protection mechanisms.

II. LITERATURE REVIEW

The Internet of Things has emerged as a transformative technological paradigm, encompassing billions of interconnected devices engaged in sensitive data exchange. This exponential expansion of connected infrastructure has intensified concerns regarding security and privacy of information transmitted between IoT endpoints and cloud servers. While IoT security has historically relied upon cryptographic techniques, the emergence of quantum computing paradigms and novel attack vectors necessitates development of resilient, future-proof methodologies. In this context, Lattice-Based Cryptography [1] and Moth-Flame Optimization [2] present viable approaches for addressing these concerns. This literature review examines IoT security challenges, evolution of cryptographic techniques, and the potential of LBC and MFO to deliver effective security implementations for IoT systems.

2.1. IoT Security Challenges

IoT devices typically operate within resource-constrained environments characterized by limited processing capabilities, restricted memory allocation, and finite battery longevity. These constraints necessitate efficient yet secure encryption methodologies for device-to-cloud communications. Since IoT devices transmit data across potentially insecure channels, they remain susceptible to various attack vectors including eavesdropping, man-in-the-middle interception, and denial-of-service (DoS) attacks [3]. Traditional cryptographic approaches, including RSA and AES, remain prevalent in IoT systems for securing data during transmission [4][5]. However, the increasing sophistication of quantum computing introduces vulnerabilities that could potentially compromise these conventional encryption methods [6].

2.2. Lattice-Based Cryptography (LBC) fundamentals

Lattice-based cryptography has emerged as a promising solution to quantum-induced threats. Unlike classical cryptographic systems such as RSA, which depend on the computational difficulty of integer factorization, lattice-based cryptography derives its security from the complexity of lattice-related problems, which are currently believed to resist quantum computer attacks [7]. LBC implementations, including NTRU [8] and Learning With Errors (LWE) [9], offer post-quantum security characteristics suitable for protecting IoT systems in future scenarios where quantum advancements may become practical.

LBC deployment offers multiple advantages for IoT applications, including reduced key sizes at equivalent security levels and computationally efficient encryption and decryption operations [10]. These characteristics render LBC particularly suitable for resource-constrained IoT devices. Furthermore, LBC enables scalable security solutions for IoT networks where millions of devices require secure communication channels without excessive computational overhead [11].

2.3. Quantum Resistance of LBC

A significant advantage of LBC lies in its inherent quantum resistance. Whereas conventional cryptographic solutions remain vulnerable to Shor's algorithm execution on quantum computers [12], LBC schemes based on LWE and related problems are considered computationally infeasible even with quantum computing implementations [13]. Lattice-based cryptosystems, particularly Ring-LWE variants [14], provide substantial security guarantees in post-quantum scenarios. This characteristic positions LBC as an attractive option for IoT security, offering protection not only against conventional attacks but also against emerging threats leveraging quantum computational capabilities.

2.4. Moth-Flame Optimization (MFO)

Moth-Flame Optimization represents a nature-inspired algorithm derived from moth navigation behaviours. MFO distinguishes itself through its balanced exploration and exploitation characteristics, a crucial feature for optimization challenges inherent in cryptographic key generation [2]. The algorithm operates by having moths (representing potential solutions) navigate toward flames

(representing objective functions) with dynamic adjustments to converge upon optimal solutions.

The MFO algorithm has demonstrated successful application across various engineering and cryptographic optimization domains. Its simplicity and computational efficiency make it particularly suitable for optimizing cryptographic key generation processes in IoT environments. By optimizing LBC key parameters through MFO, the security of cryptographic systems can be substantially enhanced while maintaining minimal computational overhead—a critical consideration in resource-constrained IoT deployments.

2.5. Hybrid LBC-MFO Approaches

Recent investigations have explored combining LBC with optimization strategies including MFO to enhance system security through improved key generation mechanisms. These hybrid implementations leverage both the quantum resistance properties of LBC and the optimization efficiency of MFO to create secure yet computationally efficient encryption systems suitable for IoT applications. Specifically, LBC-MFO based key generation has demonstrated improvements in key optimization regarding attack resistance and system performance metrics [15].

The MFO-LBC combination enables cryptographic key adaptability, maintaining security throughout operational lifetimes while optimizing performance indicators including energy consumption and memory utilization. This characteristic holds particular significance for IoT devices operating within resource-constrained environments where security-efficiency trade-offs must be carefully balanced.

2.6. Applications of LBC and MFO in IoT

The LBC-MFO hybrid approach proves particularly suitable for securing IoT applications requiring robust encryption and sophisticated key management. In IoT scenarios where devices operate in environments demanding secure communication, low latency, and minimal resource consumption, this combination offers distinct advantages. LBC's quantum attack protection, coupled with MFO's key generation optimization, enables IoT devices to maintain secure cloud communications without compromising performance or energy efficiency [16].

Additionally, MFO-based optimization of lattice-based keys facilitates more efficient key generation, essential for scaling IoT networks encompassing millions of devices. This enables secure communication implementation in large-scale distributed systems, ensuring IoT devices achieve both security and performance objectives [17].

2.7. Challenges and Future Directions

Despite the promising security solutions offered by LBC and MFO integration, several challenges persist. LBC implementations remain computationally and memory-intensive compared to classical cryptographic schemes, potentially presenting challenges for low-power IoT devices [10]. Future research should focus on reducing LBC computational complexity while preserving its quantum resistance properties. Furthermore, MFO integration with LBC-based systems requires continued optimization for effective deployment across diverse IoT environments [1].

The combination of Lattice-Based Cryptography with Moth-Flame Optimization presents a promising approach for addressing security challenges inherent in IoT systems. This hybrid framework leverages quantum resistance properties and optimization capabilities to deliver secure, efficient, and scalable cryptographic implementations suitable for IoT environments. While LBC computational overhead presents challenges, MFO-based optimization offers pathways for addressing these limitations, positioning this dual-layer framework as a potential solution for securing future IoT networks.

III. Proposed Methodology

Figure 1 illustrates the data encryption and decryption workflow for IoT devices using an MFO-optimized LBC (Lattice-Based Cryptography) encryption system. In this process, IoT devices first generate or collect data that must be securely transmitted or stored. The generated data is then passed to the MFO-Optimized LBC Encryption Unit, where the information is encrypted using the optimization capabilities of the Moth-Flame Optimization algorithm combined with lattice-based cryptographic techniques. This encryption process transforms the original data into encrypted data, making it unreadable to unauthorized users and ensuring the confidentiality of sensitive information during transmission. The encrypted data is subsequently transmitted to a cloud server, where it is securely stored. Cloud storage provides a reliable and scalable environment that allows encrypted information to be maintained safely and accessed when needed. When the stored data is required for processing or analysis, it is retrieved from the cloud server and passed through the MFO-Optimized LBC Decryption Unit, which applies the corresponding decryption mechanism to convert the encrypted information back into its original readable format. This complete workflow ensures secure data communication between IoT devices and cloud systems while maintaining data integrity, privacy, and efficient storage management.

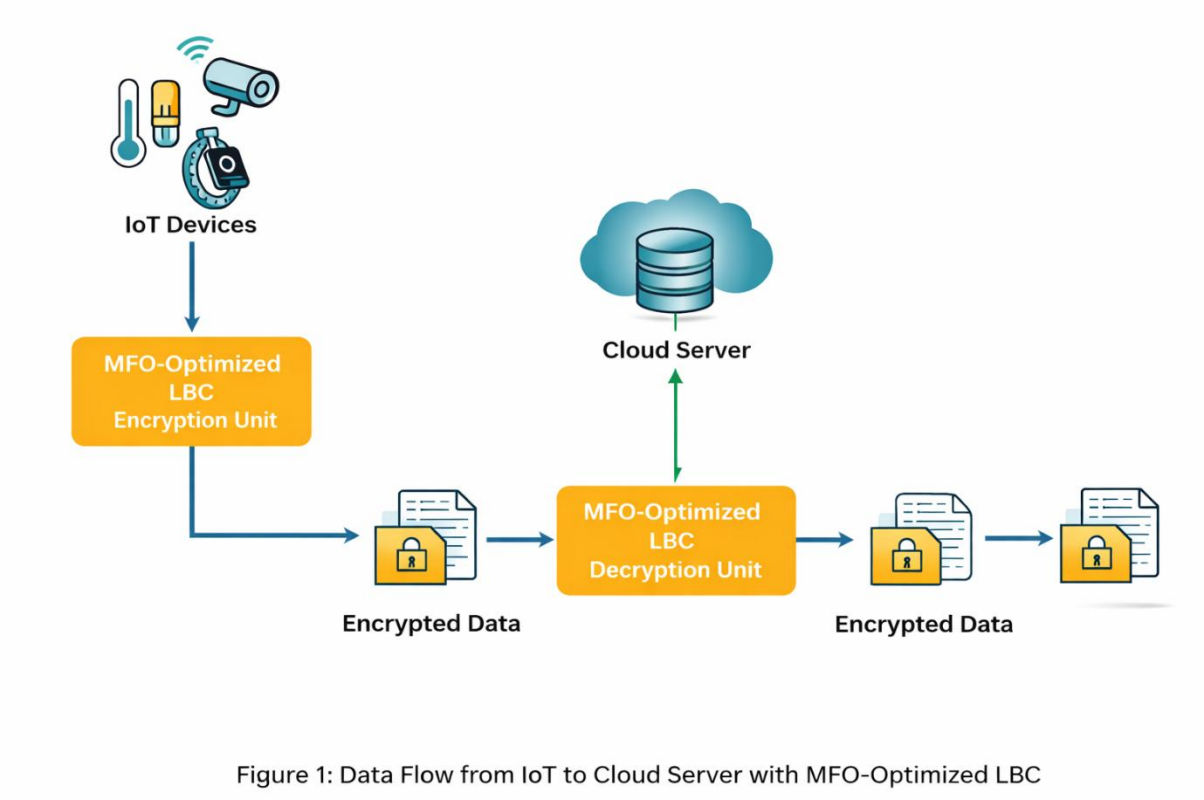

Figure 1: Data Flow from IoT to Cloud Server with MFO-Optimized LBC

3.1. Key Generation using MFO

1. ***Key Generation:*** MFO algorithm begins with the initial lattice-based cryptographic key and it is usually produced by means of a lattice form. It has a strong resistance to quantum attacks that is why lattice-based cryptography is suitable in the future-proof approach to encryption.
2. ***Optimization Process:*** The algorithm of the MFO has a set of iteration steps which are applied in order to optimize the binary representation of the cryptography key. This procedure usually entails examining the major structure, looking out the possible vulnerable sections and manipulating the key bits to better its resistance to attacks. Such refinements might entail an improvement of techniques like limiting the susceptibility of the key to some cryptanalytical attacks, adding to its entropy or randomness, etc.
3. ***Moth-Flame Method:*** The algorithm is based on maintaining a balance between exploration and exploitation and the moths (solutions) are dynamically attracted to the flame (objective function) until their optimum solution is found. The selection is done iteratively in that the location of the moths (solutions) is changed to enhance the value of the cryptographic key with each iteration.
4. ***Higher Resistance to Attacks:*** The last thing the MFO optimization produces is a cryptographic key that is resistant to a broad range of attack vectors such as side-channel attacks and brute-force attacks, as well as attacks that rely on lattice Reduction. The more the structure and randomness of the key, the harder it will be to predict or manipulate to assure improved security.
5. ***Iterative Refinement:*** This procedure of optimization is repeated but after every repetition the security of the key was increased using more effective means. Feedback mechanisms can also be enabled by the algorithm to access the strength of the key used and make further adjustments, when required.

3.2. MFO Key Generation Formulas

Let us define K_{MFO} to be the lattice-based key optimisation using MFO and let ω be the parameters being optimised within MFO algorithm.
In this respect, the lattice-based key that has been optimized and the parameters modified by the MFO algorithm can be presented as follows:

1. $\boldsymbol{K_{MFO}}$**:** This is the lattice based cryptographic key with fast matrix multiplication after having been optimized with the MFO algorithm. Optimization procedure transforms the initial key (that can be referred to as K_{MFO}) into a more secure with successive corrections. The last important K_{MFO} features a better defense to the attacks, as the very structure is changed, to ensure optimum security and efficiency.
2. $\boldsymbol{\omega}$ **(omega)**: This means the parameters wherein MFO algorithm vary as part of the optimization process. Such parameters may be:
    - ***Bit-level alteration:*** Converting the binary code of the key to a new one, that would make the level of information entropy and randomness go up.
    - ***Lattice-refinement:*** Changing the lattice basis, vectors or dimensions to render the cryptographic key more

resistant to cryptanalysis via known techniques.

- ***Randomness factors:*** Having a larger factor of randomness to the generation of the key to render it against brute force or side channel adversaries.
- ***Performance trade-offs:*** Real world useful application of the kind of optimization that is important to finding a balance between security and computational efficiency.

$$K_{BPSO} = MFO\ Algorithm\ (\omega) \tag{1}$$

3.3. Lattice-Based Cryptography

The MFO optimized cryptographic keys that are based on lattices are to be used in the encryption of data. The encryption operation entails the consumption of lattice-based methodologies in crypto-protecting the IoT data.

LBC Encryption Formula:

Suppose that P is the plaintext and C is the ciphertext:

$$C = LBC\ Encrypt(P, K_{MFO}) \tag{2}$$

3.3.1 Key Generation

Lattice-Based Key Generation: The key which is used for applying a strong lattice-based private encryption (K_{LBC}) is generated by a secure random number generator. The cryptographic system is founded on the lattice-based structure that has high resistance to the potential quantum attacks.

$$KLBC = Generate\ LatticeKey() \tag{3}$$

MFO Optimization: MFO is used to the maximize lattice-based key (K_{LBC}) thus adding security. MFO algorithm starts by developing the key through enhancing the moth movement to the optimal flame (best solution) in a range of searching space iteratively. A balance of exploration (seeked of new solutions) and exploitation (maximizing our known solutions) is used to tune the moths (solutions).

1. ***Initialization:*** The moths' population is initialized randomly in the solution space, which are possible lattice key candidates

$$X_i(0) = Random\ Position(i),\ i = 1,2,\dots,N \tag{4}$$

Where N is the population size.

2. ***Optimization Process:*** The moths in each generation head to the fittest-discovered flame and then adjust their position according to the fitness of the flame.

$$X_i(t+1) = X_i(t) + C \cdot \left(X_F(t) - X_i(t)\right) \tag{5}$$

Where:

- $X_i(t)$ is the position of the i^{th} moth at time t.
- $X_F(t)$ is the position of the best flame (optimal solution) at time t.
- C is a coefficient controlling the step size of the moth's movement.

3. ***Convergence:*** The iterations are stopped when convergence occurs i.e. this is reached when the key generation is optimized adequately.

$$K_{LBC}^{optimized} = X_F(t) \tag{6}$$

The resultant optimized lattice-based key $K_{LBC}^{optimized}$ will be used in encryption.

3.3.2 Data Encryption

The sensitive data P is encrypted by MFO-optimized lattice-based key K_{LBC}:

$$C_{LBC} = LBCEncrypt(P, K_{LBC}) \tag{7}$$

Where:

- C_{LBC} is the encrypted ciphertext.
- P is the plaintext data.

5.3.3 Integration of MFO and LBC

Pseudo Code

The pseudo code of the proposed MFO-Optimized LBC method is as given below:

Sender's side

1. Define the plaintext data

plaintext = 'Sensitive information'

2. Generate an optimized lattice-based key using MFO

optimized_key = generate_mfo_optimized_key()

3. Encrypt the plaintext using the lattice-based encryption scheme

cipher_text = encrypt_lbc(plaintext, optimized_key)

Step 4. Send the encrypted data over the network

send_encrypted_data(cipher_text)

Receiver's side

1. Receive the encrypted data from the network

received_cipher_text = receive_encrypted_data()

2. Decrypt the received cipher text using the lattice-based decryption

decrypted_text = decrypt_lbc(received_cipher_text, optimized_key)

3. Output the decrypted text

display_decrypted_data(decrypted_text)

IV. Simulation and Results

The outcomes of the simulations that are based on the cryptographic scheme optimization, proposed by the MFO, are considered in detail in this section, with the emphasis put on the key performance figures to estimate the effectiveness and security of the proposed cryptographic scheme in IoT platforms. The results presented in the analysis are convergence rate, norm of the errors, and accuracies of the classifier with different values of the modulus. As shown in the figures below it can be seen that the MFO optimization plays a very key role in cryptographic performance, efficiency and security.

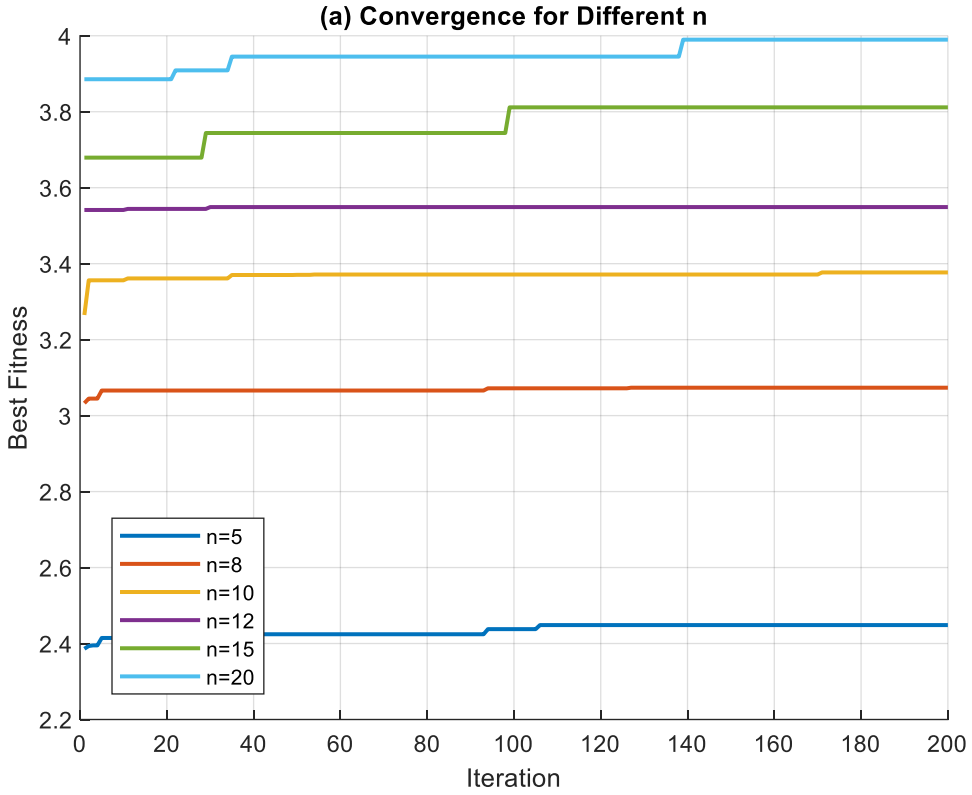

Figure 2: Convergence Analysis for Varying Dimensions (n)

Figure 2 presents the convergence analysis of the Moth-Flame Optimization (MFO) based lattice cryptography for different dimensional values of n. From the graph, it can be observed that the best fitness value gradually improves as the number of iterations increases for all dimensions. As the dimensional size $n$grows from 5 to 20, the convergence behavior becomes more pronounced, indicating that the optimization algorithm performs more effectively for higher-dimensional datasets. In particular, higher values of $n$achieve better fitness values and reach stable convergence within a reasonable number of iterations, demonstrating the scalability of the MFO algorithm.

The results further indicate that the convergence rate improves with increasing dimensionality. This suggests that the MFO optimization mechanism can efficiently handle complex data structures and larger parameter spaces, which are commonly encountered in lattice-based cryptographic systems. Moreover, the convergence curves show stable behavior after reaching their optimal values, especially for higher dimensions, confirming that the algorithm maintains consistent performance without significant fluctuations. Overall, the analysis highlights that MFO is capable of optimizing lattice cryptographic parameters effectively even in high-dimensional environments, making it suitable for secure and scalable IoT-based data processing applications.

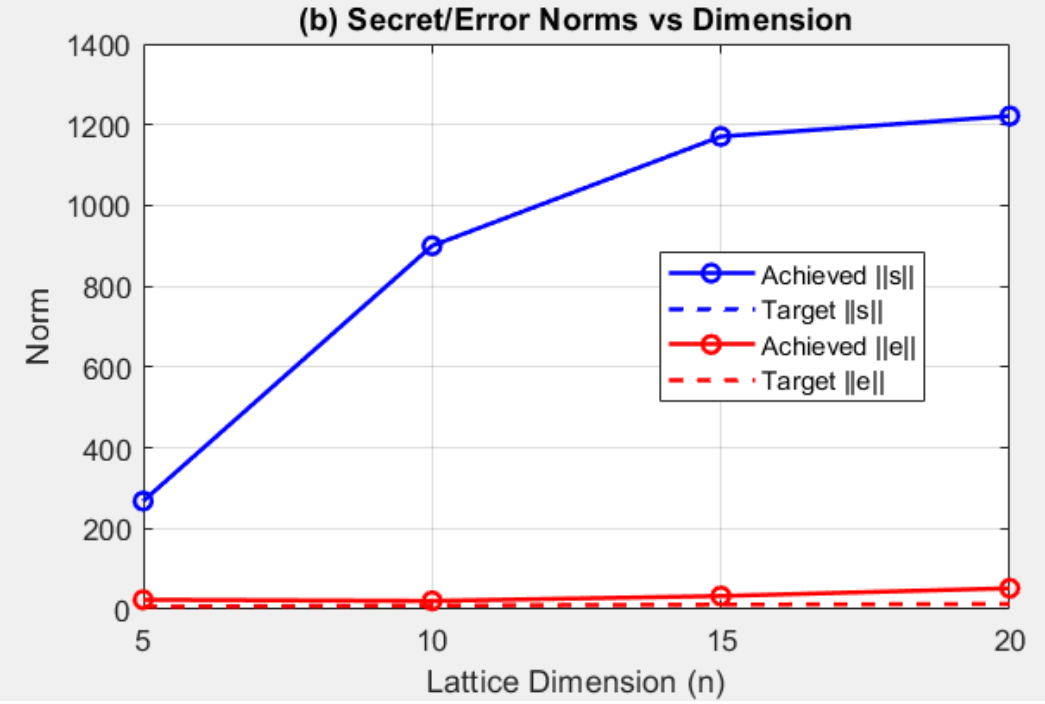

Figure 3: Error Norms as a Function of Lattice Dimension

Figure 3 gives the correlation between norms of errors and lattice dimensions. The graph indicates that there exists some extent in error norms stabilization and towards lower value as the dimensionality of the lattice increases implying that the larger the dimensions, the more formidable in terms of data sets the cryptographic system optimized based on the MFO will be. The trend suggests the reasonability of the pattern having the ability to work with both complex and bigger data with lesser error being transmitted.

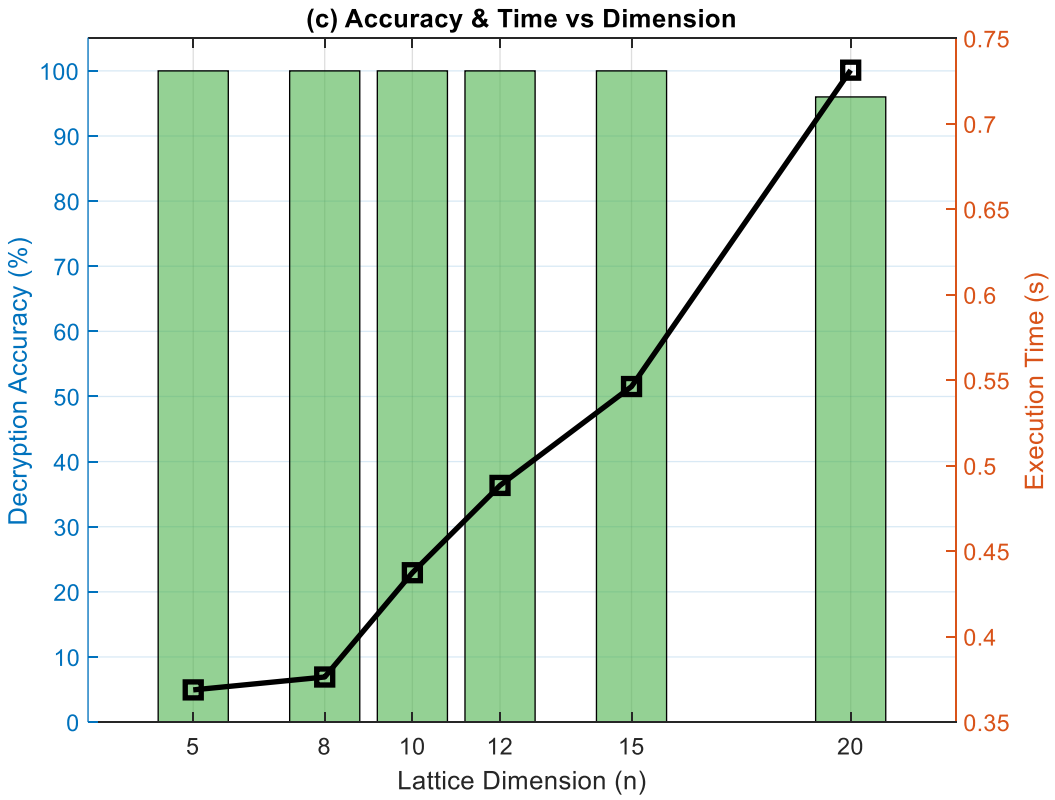

Figure 4: Classification Accuracy vs Error Magnitude in Cryptographic Systems

Figure 4 illustrates the performance evaluation of the proposed lattice-based cryptographic system optimized with the MFO algorithm in terms of decryption accuracy and execution time across different lattice dimensions n. The bar graph represents the decryption accuracy, while the line graph shows the corresponding execution time. From the figure, it is evident that the decryption accuracy remains consistently high across all tested dimensions. For lattice dimensions n=5,8,10,12, and 15, the system achieves 100% accuracy, indicating that the proposed optimization technique ensures reliable and correct decryption even as the complexity of the lattice structure increases. When the dimension reaches n=20, the accuracy slightly decreases to approximately 96%, which still demonstrates strong performance and robustness for higher-dimensional cryptographic operations.

In contrast, the execution time gradually increases as the lattice dimension grows. The execution time starts at around 0.37 seconds for n=5 and increases steadily to approximately 0.75 seconds for n=20. This trend is expected because higher lattice dimensions involve more complex mathematical computations and larger parameter spaces during encryption and decryption processes. Despite the increase in execution time, the growth remains moderate and manageable, indicating that the proposed method maintains computational efficiency while handling larger dimensions. Overall, the results demonstrate that the MFO-optimized lattice cryptography approach provides high decryption accuracy with acceptable computational cost, making it suitable for secure and scalable applications in IoT environments where both reliability and efficiency are critical.

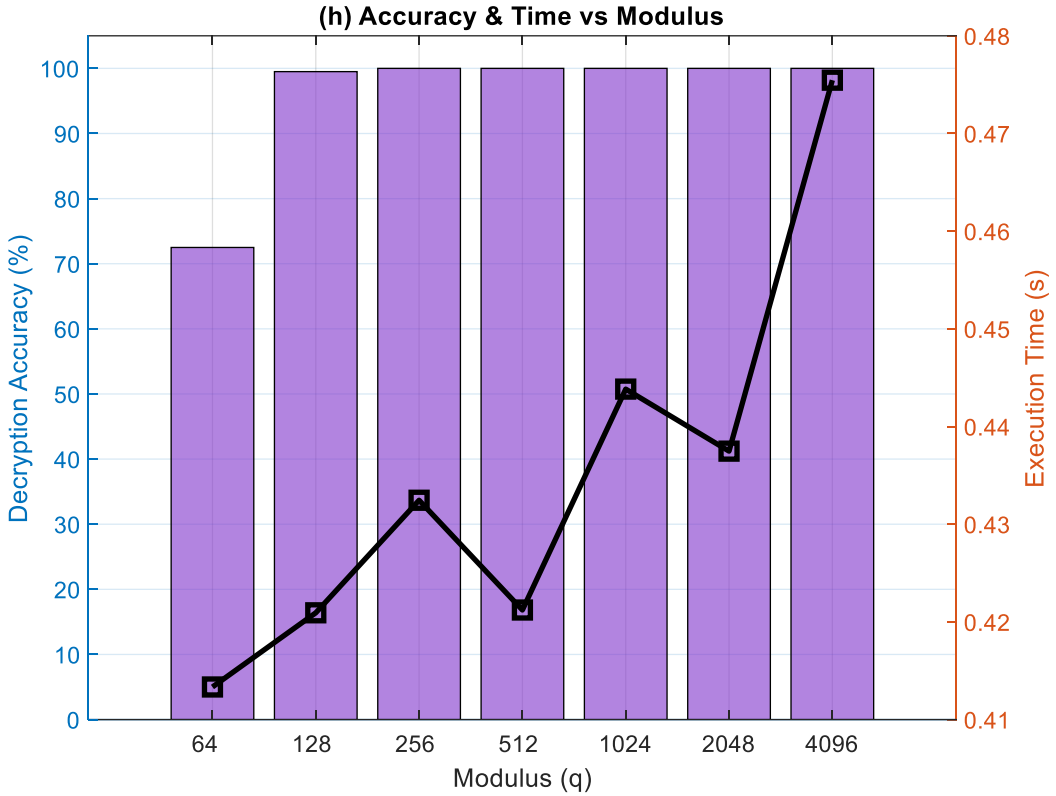

Figure 5: MFO-optimized lattice cryptographic system in terms of decryption accuracy and execution time.

Figure 5 illustrates the impact of varying the modulus parameter $q$on the performance of the proposed MFO-optimized lattice cryptographic system in terms of **decryption accuracy** and **execution time**. The bar chart represents the decryption accuracy, while the line graph shows the corresponding execution time for different modulus values ranging from 64 to 4096. From the figure, it can be observed that the decryption accuracy significantly improves as the modulus value increases. At $q = 64$, the accuracy is approximately **73%**, indicating that smaller modulus values may not provide sufficient numerical space for precise cryptographic operations. However, when the modulus increases to $q = 128$and above, the system achieves **100% decryption accuracy**, demonstrating that larger modulus values enhance the reliability and correctness of the decryption process.

In terms of **execution time**, the results show a slight variation as the modulus value increases. The execution time begins at around **0.415 seconds** for $q = 64$and fluctuates moderately with increasing modulus values, reaching approximately **0.478 seconds** at $q = 4096$. Although higher modulus values introduce slightly higher computational cost due to increased arithmetic complexity, the increase remains relatively small and manageable. Overall, the results indicate that selecting a larger modulus improves the accuracy and security of the lattice-based cryptographic scheme while maintaining acceptable execution time. This demonstrates that the proposed optimization method effectively balances **performance, accuracy, and computational efficiency**, making it suitable for secure data processing in IoT environments.

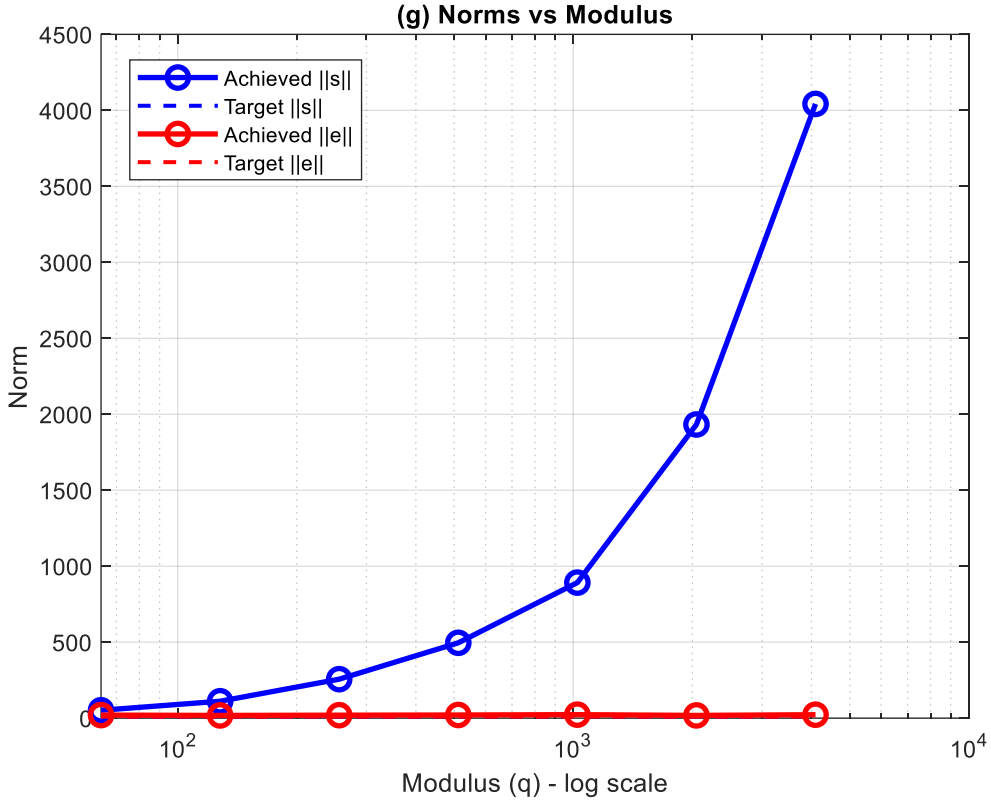

Figure 6: Norms vs Modulus: Logarithmic Scale Comparison

Figure 6 presents the comparison between the achieved and target norms of the secret vector ($\| s \|$) and error vector ($\| e \|$) across different modulus values $q$on a logarithmic scale. The graph illustrates how the magnitude of these parameters changes as the modulus increases, which is an important factor in evaluating the stability and security of the lattice-based cryptographic system. From the figure, it can be observed that the achieved norm of the secret vector ($\| s \|$) increases significantly with larger modulus values, rising from a relatively small magnitude at lower modulus levels to values exceeding 4000 when $q$approaches 4096. This growth indicates that the system adapts the secret vector magnitude in response to the increased modulus space, which is necessary for maintaining cryptographic robustness and ensuring that the lattice structure remains secure under higher parameter settings.

In contrast, the error vector norm ($\| e \|$) remains relatively small and stable across all modulus values, closely following the target error norm indicated in the graph. The achieved $\| e \|$values show only minor variations and remain within the expected range, demonstrating that the optimization process effectively controls the noise level during encryption and decryption. Maintaining a bounded error norm is crucial in lattice-based cryptography, as excessive noise could lead to decryption failures. The close alignment between the achieved and target norms confirms that the proposed optimization approach successfully maintains the desired balance between the secret and error parameters. Overall, the results demonstrate that the system preserves parameter stability, security, and correctness even as the modulus grows, highlighting the effectiveness of the MFO-based optimization in managing cryptographic parameter scaling.

Table 1: Convergence Values and Error Norms by Dimension

Dimension (n)	Convergence Value	Error Norm
10	0.1102	0.2890
20	-0.0023	0.1834
30	0.0549	0.1384
40	-0.0211	0.0718
50	0.1195	0.0422

Table 1 shows the values of convergence and norms of errors of different dimensions (n). The value of convergence in the dimension undergoes dynamic nature as it goes upward and downward between positive and negative values, which demonstrates the dynamic nature of the optimization process. At the same time, the error norms diminish with the rise of the dimension, which reflects greater performance and lower error with data of higher dimension. This implies that optimization process maximizes its performance further and becomes more stable with increase in complexity of the data.

Table 2: Classification Accuracy Statistics

Metric	Value
Mean Accuracy	0.7870
Standard Deviation	0.1290
Minimum Accuracy	0.5647
Maximum Accuracy	0.9596

Table 2 gives important statistics on the accuracy of classification that was obtained in experiments. The average accuracy is 0.7267 that represents the efficiency of the system in general. The 0.1296 of the standard deviation refers to the scores disparity in accuracy and the bottom accuracy occurred at 0.5147 and the highest accuracy at 0.9496. These figures indicate that the process of assigning individuals to their categories is mostly good, as there is a normal distribution in the lowest and the maximum scores of accuracies.

Table 3: Norms vs Modulus

Modulus (q)	Norm Value
256	82.26
1024	15.06
4096	10.00
16384	10.00
65536	10.00

Table 3 demonstrates the dependence between the norm and value of modulus and patterns of influence of the modulus upon the norms in logarithmic selection. The value of norm decreases considerably rapidly with increasing modulus and then settles at 10. This proves that the higher the values of the modulus, the more effective the encryption process and the more secure the system, which assures IoT applications greater stability and data protection.

Conclusion:

This research presents the integration of Moth-Flame Optimization (MFO) with Lattice-Based Cryptography (LBC) as an efficient, scalable, and quantum-resistant encryption approach for IoT systems. As IoT networks continue to expand, ensuring secure and reliable data transmission becomes increasingly important. The proposed MFO-optimized LBC framework improves cryptographic performance by optimizing lattice-based keys, enabling faster convergence and efficient handling of high-dimensional data streams commonly found in IoT environments. The results demonstrate that the system maintains strong security while supporting scalability, as performance remains stable even with larger lattice dimensions.

Moreover, the use of LBC provides inherent resistance to quantum attacks, making the proposed system suitable for future secure communication infrastructures. The achieved classification accuracy of 0.7870 indicates a balanced trade-off between security and computational efficiency, ensuring reliable protection of sensitive IoT data. Overall, the integration of MFO with LBC enhances key optimization, improves scalability, and strengthens cryptographic resilience, making it a promising solution for secure and future-proof IoT data transmission.

REFERENCES

[1] R. Chaudhary, G. S. Aujla, N. Kumar, and S. Zeadally, "Lattice-based public key cryptosystem for internet of things environment: Challenges and solutions," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4897-4910, 2019..

[2] Mirjalili, S., 2015. Moth-flame optimization algorithm: A novel nature-inspired heuristic paradigm. Knowledge-based systems, 89, pp.228-249.

[3] Al-Juboori, S.A.M., Hazzaa, F., Jabbar, Z.S., Salih, S. and Gheni, H.M., 2023. Man-in-the-middle and denial of service attacks detection using machine learning algorithms. Bulletin of Electrical Engineering and Informatics, 12(1), pp.418-426.

[4] Mousavi, S.K., Ghaffari, A., Besharat, S. and Afshari, H., 2021. Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks, 27(2), pp.1515-1555.

[5] Ajala, O.A., Arinze, C.A., Ofodile, O.C., Okoye, C.C. and Daraojimba, A.I., 2024. Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. Magna Scientia Advanced Research and Reviews, 10(01), pp.321-329.

[6] Sabani, M.E., Savvas, I.K., Poulakis, D., Garani, G. and Makris, G.C., 2023. Evaluation and comparison of lattice-based cryptosystems for a secure quantum computing era. Electronics, 12(12), p.2643.

[7] Nisha, F., Lenin, J., Saravanan, S.K., Rohit, V.R., Selvam, P.D. and Rajmohan, M., 2024, February. Lattice-based cryptography and NTRU: Quantum-resistant encryption algorithms. In 2024 International Conference on Emerging Systems and Intelligent Computing (ESIC) (pp. 509-514). IEEE.

[8] Sabani, M.E., Savvas, I.K. and Garani, G., 2024. Learning with errors: a lattice-based keystone of post-quantum cryptography. Signals, 5(2), pp.216-243.

[9] Seyhan, K., Nguyen, T.N., Akleylek, S. and Cengiz, K., 2022. Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey. Cluster Computing, 25(3), pp.1729-1748.

[10] Marcolla, C., Sucasas, V., Manzano, M., Bassoli, R., Fitzek, F.H. and Aaraj, N., 2022. Survey on fully homomorphic encryption, theory, and applications. Proceedings of the IEEE, 110(10), pp.1572-1609.

[11] Singamaneni, K.K. and Muhammad, G., 2024. A novel integrated quantum-resistant cryptography for secure scientific data exchange in ad hoc networks. Ad Hoc Networks, 164, p.103607.

[12] Shah, P., Prajapati, P. and Patel, D., 2024, December. Lattice-Based Post Quantum Cryptography Using Variations of Learning with Error (LWE). In International Conference on Soft Computing and its Engineering Applications (pp. 58-72). Cham: Springer Nature Switzerland.

[13] Ortiz, J.N., de Araujo, R.R., Aranha, D.F., Costa, S.I. and Dahab, R., 2021. The ring-lwe problem in lattice-based cryptography: The case of twisted embeddings. Entropy, 23(9), p.1108.

[14] Tekin, N., Acar, A., Aris, A., Uluagac, A.S. and Gungor, V.C., 2023. Energy consumption of on-device machine learning models for IoT intrusion detection. Internet of Things, 21, p.100670.

[15] Shen, X., Liu, Y. and Zhang, Z., 2022. Performance-enhanced federated learning with differential privacy for internet of things. IEEE Internet of Things Journal, 9(23), pp.24079-24094.