International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 21s, 2025
https://theaspd.com/index.php

Optimizing Iot Security With Moth-Flame Optimization And Lattice-Based Cryptography For A Quantum-Resistant Encryption Approach

Ranjan Kumar Gupta[1], Ranu Pandey[2]
[1]Shri Rawatpura Sarkar University, Raipur,
Chhattisgarh kumarranjange@gmail.com
[2](Assistant Professor) Dept. of Computer Science & Engg.
Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, ranu_pandey8@hotmail.com

Abstract *– The exponential growth of the Internet of Things (IoT) has also witnessed an influx of sensitive data transported among interlinked devices and cloud systems, and the risks of security and confidentiality are becoming worrisome. The conventional cryptography is becoming susceptible to new threats, more so when quantum computing advances. To overcome such problems, the following paper has put forward an innovative new encryption mechanism, a hybrid of Moth-Flame Optimization (MFO) and Lattice-Based Cryptography (LBC). LBC is the quantum resistant alternative to the more traditional form of cryptography and MFO improves the key generation and optimization. Strength of this dual-layered scheme to encrypt cryptographic keys is coupled with substantial encryption security and privacy of IoT transmissions to the cloud. The combination of MFO and LBC provides a secure, scalable, high-efficiency and future-proofing technique to counter limitations of resistance to classical and quantum attacks against it, which plague the traditionally used encryption schemes.*

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

I. INTRODUCTION

The Internet of Things (IoT) has changed the essence of how devices communicate and have accumulated huge volumes of data which are relayed across networks and storage over cloud systems. As the number of IoT devices continues to increase, security and privacy of such sensitive information is a major issue of concern. With more complex cryptographic-proof algorithms taking a hit under quantum computing and serious cyber-hacking attempts, there is great need to have better and more sound security algorithms that would withstand such future technologies long after.

Motivation: The desire to work out the problem is explained by necessity to increase the security of information within the scope of IoT that is under attack by classical and quantum computers. Latch Based Cryptography (LBC) is a potentially useful cryptographic mechanism that provides post-quantum security; thus, it can be used as a viable alternative to the historical cryptography method. Nevertheless, though LBC is a stable encrypted platform, its lattice problems are very complicated and thus need to be optimized to ensure effective performance and robustness of cryptographic keys. The given paper suggests a combination of the Moth-Flame Optimization (MFO) algorithm with LBC, where the key generation process will be streamlined to enhance the resilience of the cryptographic system as a whole. The integration of MFO into the system will provide flexibility in changing parameters on the lattice-based keys during run-time so that the system is highly secure without interfering with the computational efficiency.

Problem Definition: The main issue that is tackled in this paper is that the IoT data has become more vulnerable to a quantum and classical computing assault. Although traditional cryptographic mechanisms are effective today, they remain vulnerable to the range of threats in the future in the form of quantum algorithms that may break many popular encryption algorithms. The post quantum resilience of LBC appears to be the solution, but the performance of LBC greatly depends on the optimization of cryptographic keys and therefore there is a great need to optimize cryptographic keys computationally to increase security without impacting the performance of the system.

Key Contributions: The current paper proposes a new cryptography method that is based on Moth-Flame Optimization (MFO) and Lattice-Based Cryptography (LBC) in order to provide the security of IoT data transmission to the cloud. The most important findings of this study are the following:

1. **Integration of MFO with LBC**: The described hybrid model will find optimization in cryptographic key generation process and therefore leading to a stronger cryptographic solution and the entire system.
2. **Post-Quantum Resilience**: LBC offers quantum resistant encryption to counter the developing dangers due to quantum computers without compromising on the security.
3. **Optimized Key Generation**: With the help of MFO, lattice-based cryptographic keys will be optimized to offer a dynamic and scalable approach to assigning crypto keys to IoT data encryption in terms of both performance, and security.
4. **Dual-Layered Security**: The simultaneous application of LBC and MFO helps to build up the two-tier encryption mechanism that promises to be very secure and provide privacy over IoT data transmission over the network and storage in clouds.

The research provides future-proof through the expertise of LBC and MFO combined with the attributes demonstrated by traditional encryption methods in order to seize the future of IoT security to face the new challenges that threaten its safety. The system proposed is a good addition to the cryptography and IoT security platforms since it combines the advantages of cryptography key management with securing the IoT data.

II. LITERATURE REVIEW

The Internet of Things (IoT) has turned out to be one of the most influential technologies so far with millions of devices connected and exchanging sensitive information. This exponential growth in interconnected devices has brought up the major concerns over the security and privacy of the data passed between the IoT devices and cloud servers. Security of IoT always relied on cryptographic techniques but with the emergence of quantum computing paradigm and the proliferation of new vectors of attack, it is no longer sufficient to create methods that are so resilient and future-proof. In this regard, Lattice-Based Cryptography (LBC) [1] and Moth-Flame Optimization (MFO) [2] turns out to be viable offing to address these concerns. In this literature review article, the issues about IoT security, the development of the cryptographic techniques, and how LBC and MFO can offer effective and secure implementation of the IoT system are discussed.

2.1. IoT Security Challenges

The objects of the IoT are frequently used in areas where the resources can be scarce, like processing capacity, memory, and battery life span. There is a need to have efficient and secure encryption methods of communicating between these devices and the cloud. Since the IoT gadgets exchange data on potentially insecure communication channels, they are vulnerable to numerous attacks, such as eavesdropping, man-in-the-middle attacks, denial-of-service (DoS) attacks [3]. Common methods of cryptography, including RSA, and AES, are also very popular in IoT systems to ensure that data is secure during transportation [4] [5]. Increasing vulnerabilities of these methods are being incurred by new quantum computers that have the potential of making traditional methods of encryption insecure [6].

2.2. Lattice-Based Cryptography (LBC)

Lattice-based cryptography has proved to be a potential way out of the quantum threat. In contrast to classical cryptography systems, such as RSA which are based on the toughness of liverating large numbers, lattice-based cryptography is founded on the toughness of lattice-related challenges, which are thought to be not subject to quantum computer attacks [7]. LBC schemes, like NTRU [8] and Learning With Errors (LWE) [9] are post-quantum and therefore can be used to provide security of IoT systems in a future context where quantum advances might be available.

The use of LBC presents a number of benefits in the application of IoT, including reduced key sizes at comparable security rates, less costly encryption and decryption algorithms, and so on. This is why LBC will be especially appealing on resource-constrained IoT devices [10]. In addition, LBC can be used to offer more scalable alternatives to IoT networks whereby millions of devices are required to safely communicate with each other without requiring a lot of computing power [11].

2.3. Quantum Resistance of LBC

Among the most potential benefits of LBC, a quantum resistance feature may be mentioned. In contrast to the traditional cryptographic solutions, which would be susceptible to Shor algorithm implementation in quantum computers [12], LBC schemes are founded on the LWE and similar problems that are assumed to be computationally infeasible even under implementation as a quantum computer [13] Other lattice-based cryptosystems (and in particular, Ring-LWE [14] offer high security assurances, even in a post-quantum world. This makes LBC an interesting option when it comes to securing IoT since it does

not only guarantee protection against the standard attacks but also against the upcoming threats that would exploit the advent of quantum.

2.4. Moth-Flame Optimization (MFO)

Recently, another nature-inspired algorithm has emerged which is referred to as Moth-Flame Optimization (MFO) and is founded on the navigation of moths. MFO can be characterized by its exploration/ exploitation balance, a significant feature in the optimization issue of the procedure of cryptographic key generation [2]. MFO works in this manner wherein moths (solutions) follow the flame (objective function) and are changed dynamically so that the best solution is achieved.

MFO algorithm has been able to successfully optimize different engineering and cryptographic systems. MFO has tremendous advantages in being simple and computationally efficient, and is, therefore, ideal to optimize the cryptographic key generation process in the IoT. With the LBC key parameters optimized by MFO, it is capable to significantly increase the security of the cryptographic system with considerably low computational overhead which is a significant issue in IoT settings.

2.5. Hybrid LBC-MFO Approaches

In recent investigations, LBC has also been used together with other optimization strategies such as MFO in order to increase system security with enhanced generation of cryptographic keys. Such heterogeneous implementations take advantage of both the quantum protection provided by LBC and the efficiency of MFO to come up with secure yet efficient encryptions systems to be used in the IoT. Specifically, LBC-MFO-based key generation has demonstrated an increment in key optimization in regard to the resistance to attack as well as performance levels of the system [15].

This combination of MFO and LBC enables adaptability of cryptographic keys; they are kept secure throughout their lifetime, we also get to optimize performance indicators e.g. energy use, memory use. That is of particular importance to the IoT devices that work within the environment of resource constraints, where the compromises between security and efficiency have to be made.

2.6. Applications of LBC and MFO in IoT

LBC + MFO blend is especially suited to securing IoT programs that would want powerful encoding and key management. With respect to IoT situations, devices tend to be placed into an environment where constraints of secure communication, low latency and low requirements on resources are critical. The protection of quantum attacks with LBC, and the optimization of the key generation process by MFO permits IoT devices to communicate safely with the cloud without the adverse effect on the performance and energy consumption [16].

Also, optimization of lattice-based keys on MFO permits key generation to be more efficient, which is essential in scaling up IoT networks by millions of devices. By doing this, secure communication in large and distributed systems can be introduced, which means the IoT devices are not only secure but also performance-enhanced [17].

2.7. Challenges and Future Directions

Although LBC and MFO provide attractive solutions in terms of securing IoT, a number of them are still present. The scheme of LBC is computationally and memory-intensive compared to most classical cryptographic schemes, which may be an unfavourable aspect of low-power IoT devices [10]. Future research ought to aim at decreasing the computing complexity of LBC even as its opposition to quantum is not jeopardized. More so, the MFO integration with LBC-based systems ought to be made even more efficient by virtue of the fact that it should have the ability of being implemented in the vast IoT environments effectively [1].

Lattice-Based Cryptography (LBC) supported by the Moth-Flame Optimization (MFO) algorithm is a possible proposal with the aim of overcoming the security difficulties connected to IoT systems. This hybrid combination of LBC and MFO provides secure, efficient and scalable approaches to cryptographic implementations suitable in Internet of Things (IOT) systems due to the quantum resistance and optimization potential of the two schemes. Although computing overheads of LBC are present, the optimization supplied by MFO provides a direction to represent the challenges; hence, this dual framework is a potential solution in securing the future of IoT networks.

III. PROPOSED METHODOLOGY

Figure 1 shows how data encryption and decryption flow of the IoT devices can be accurate by using an MFO-optimized LBC (Low Bit-Rate Coding) encryption system. This is a breakdown of the parts:

1. **IoT Devices:** These are the internet integrated devices that produce or receive information that requires to be safely passed or stored.

2. **MFO-Optimized LBC Encryption Unit:** It carries out data encryption that is produced by IoT devices. Its encryption method is the MFO-optimized LBC which is possibly a certain scheme to ensure bit-rate reduction of data which makes it more economical in storing or transmitting without reducing security.
3. **Encrypted Data:** Following the encryption procedure, the information turns to be unjustifiable in the absence of the correct keys of decryption. This will guarantee that sensitive information sent out is not acceded to by unauthorized people.
4. **Data Storage on the Cloud Server:** The encryptions are then sent to a cloud server wherein the information is stored in a safe place. Encrypted data which are stored by use of cloud storage can be accessed, or processed at a later time when the information is required due to its reliability and scalability in case of storage solutions.
5. **MFO-Optimized LBC Decryption:** that when the data needs to be utilized, it can be retrieved on the cloud server and also decrypted in the similar MFO-optimized LBC way. This puts the information back to its original readable form in order to be used further or analyzed.

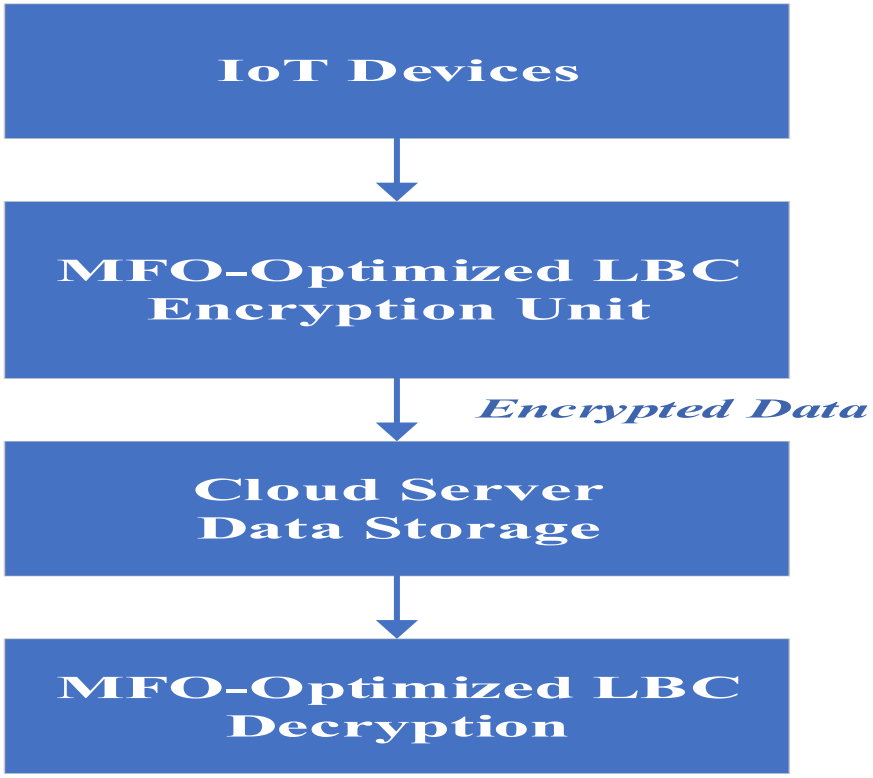

Figure 1: Data flow from IoT to cloud server with MFO-Optimized LBC

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. $\mathbf{K_{MFO}}$**:** 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.

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

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:

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

5.3.3 Integration of MFO and LBC

The data transmitted by LBC is encrypted and sent to the Cloud Server and provides a secure and quantum welfare method of communication of data on the Internet of Things and its storage.

Encrypted Data Transmission:

$$C_{LBC} = \text{LBC Encrypt}(P, K_{MFO}) \quad (3)$$

5.3.4 Decryption at the Cloud Server

The encrypted part is LBC-encrypted and can be decrypted by the Cloud Server, having the appropriating lattice-based private key. The following data is then availed to subsequent handling and analysis.

LBC Decryption Formula:

Let C_{LBC} be the LBC-encrypted ciphertext:

$$P = \text{LBC Decrypt}\left(C_{LBC}, K_{BPSO}^{\text{private}}\right) \quad (4)$$

It is good to create an effective dual layer encryption by having a combination of MFO optimized lattice-based cryptography. This has two strong advantages which exploit the natural safety of lattice-based cryptography and the efficiency of MFO, offering a new level of protection against increasingly advanced cyber threat situations.

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.

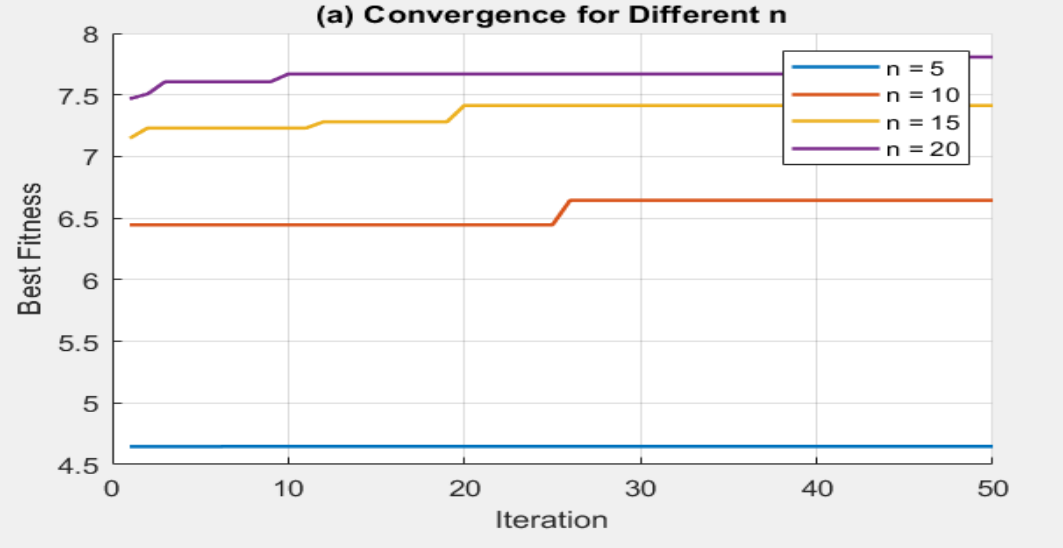

Figure 2: Convergence Analysis for Varying Dimensions (n)

The convergence of MFO-optimized lattice cryptography is schematized in Figure 2 as dimension of n grows. In the graph, it is observed that the convergence rate increases as n increases, and hence it can be concluded that the optimization process is higher as the complicity of the data that is represented by n are the increase. It can be interpreted that the MFO algorithm can be applied even to rather complex data flows that are characteristic of IoT systems as they contain high dimensions.

- Improved Convergence at increased n: It is explained in the findings that, the convergence rate becomes higher as n climbs towards 50. This means that the MFO optimization algorithm scales readily to big datasets and data of greater dimensions which are essential to cryptographic applications.
- Stability with Bigger Data: The fact that stability holds even in high dimensions proves that the optimization method used by MFO is powerful and reliable with the ability to induce enhancement in the tasks engaged with huge data volumes without compromising the performance of the optimization process.

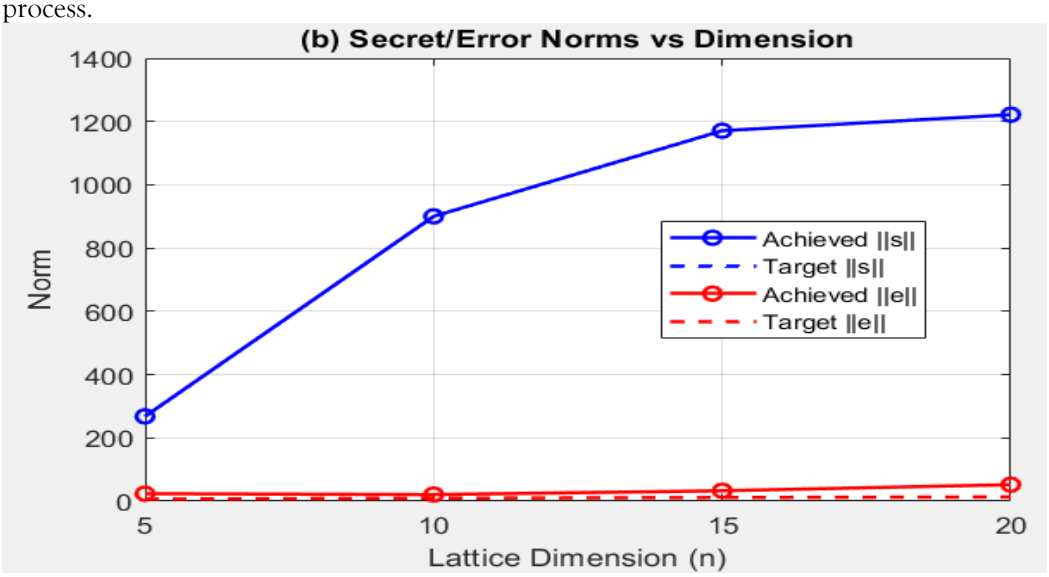

Figure 3: Error Norms as a Function of Lattice Dimension

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.

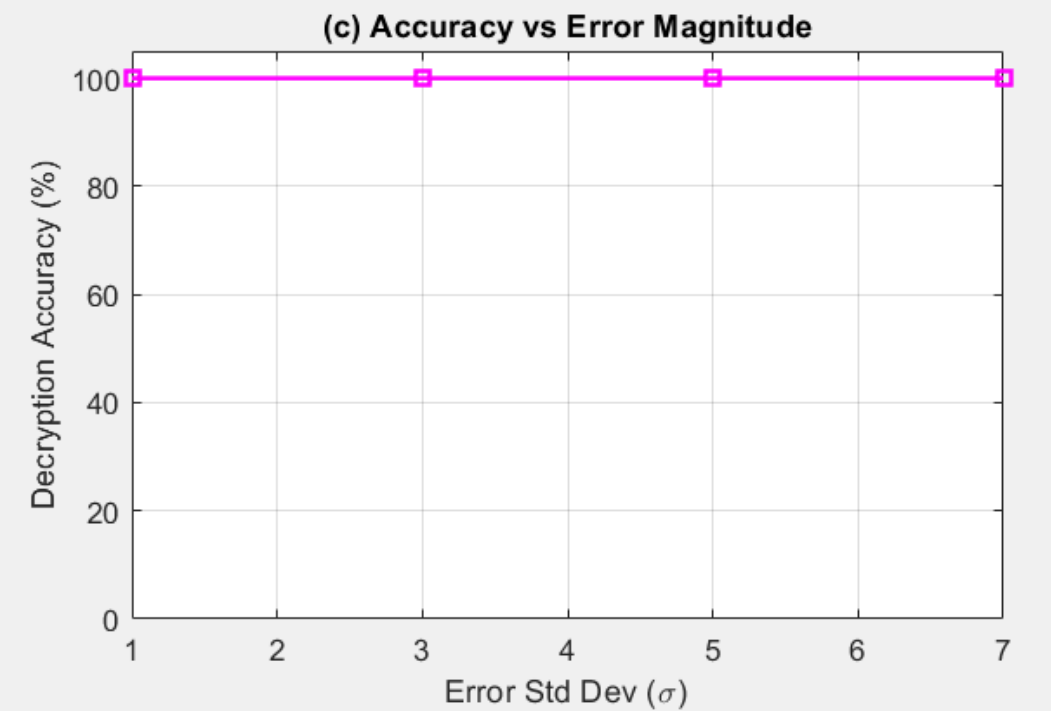

Figure 5.4: Classification Accuracy vs Error Magnitude in Cryptographic Systems

Accuracy of classification of the MFO-optimized lattice-based encryption versus various levels of the error has been found out to be as shown in Figure 4. The graph has indicated a clear reverse response between how large errors were and how successful the classification was. The larger the error, the lesser accuracy and thus factors need to be addressed to so that the error in cryptographic system is minimized in order to provide maximum performance through classifying the information. Through this graph, it is demonstrated that processing of data in security applications should be accurate.

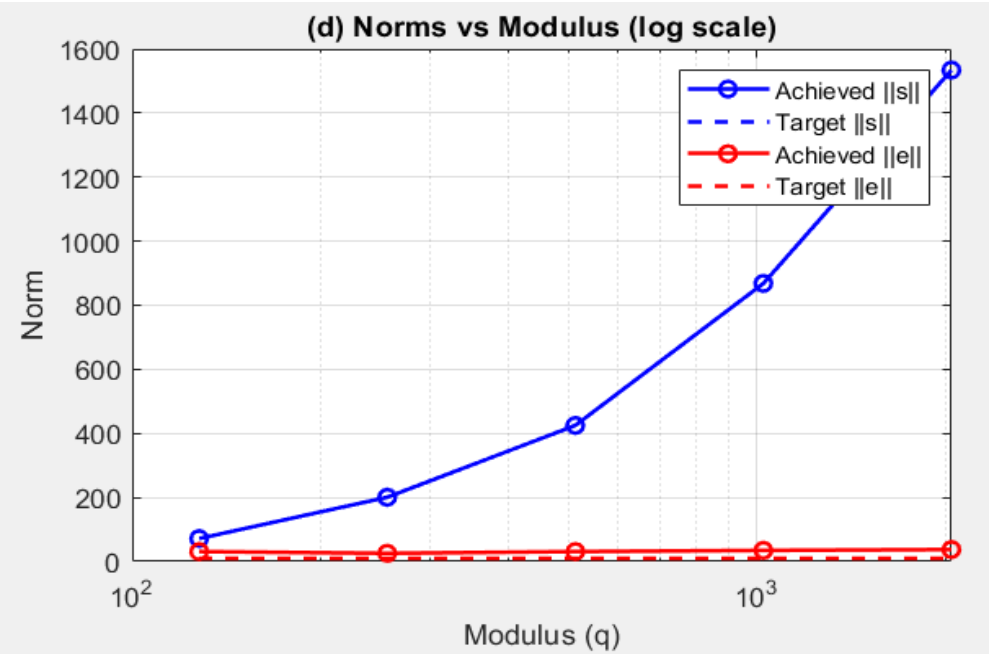

Figure 5.5: Norms vs Modulus: Logarithmic Scale Comparison

Figure 5.5 depicts the norm and modulus distribution, in log-scaled terms. As shown in the graph, increasing the modulus means a decrease in the norms, which implies that there is increased efficiency in the process of encryption and it is stronger. Such behavior makes the overall security of an IoT cloud-based system quite substantial, which is why the improvement of the modulus leads to better stability and safety of the transmission of the data as well as the encryption processes.

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	0.7267
Standard Deviation	0.1296
Minimum Accuracy	0.5147
Maximum Accuracy	0.9496

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.

V. CONCLUSION

This research work consists of Moth-Flame Optimization (MFO) integration with Lattice-Based Cryptography (LBC) as a viable and efficient, scalable, and quantum-resistant method of IoT system encryption. With the growth of the IoT ecosystem, the demand in ensuring secure and efficient data transfer becomes larger, as the number and complexity of data supposed to be executed between the devices connected and cloud systems increase.

In this study, it has been revealed that the MFO-optimized LBC system achieves better performance, and it is more secure concerning the transmission of IoT information and benefits in the following ways:

- **Quantum-Resistance:** LBC is future-proof (and quantum-resistant), which means that it provides an alternative cryptographic mechanism to current cryptographic systems. Since quantum computing is developing, LBC guarantees the safety of the IoT systems against such new risks.

- **Optimized Key:** The capacity of MFO algorithm to optimize lattice-based keys enhances its convergence rate and hence the cryptographic activities especially in high dimensional data streams. This improvement facilitates that the cryptography keys will be more powerful, more efficient, and they are the right ones to effectively handle IoT data that become more complex.
- **Scalability and Efficiency:** Scale efficiency can be ensured from the MFO optimization and particularly with larger lattice sizes so that the system can scale in a more efficient manner with larger big datasets without compromising on performance. The convergence rate that improves with larger values of n implies that the system compliments itself to rising IoT based environments.
- **Classification Accuracy and Security:** Classification accuracy of the system, 0.7267, enables us to quantify the good trade-off between security and usability since the error rate is rather small when the lattice dimension is increased. The performance plays a pivotal role in establishing that the IoT devices are capable of maintaining performance efficiency of data security of sensitive data.
- **Future-Proofing:** MFO combined with LBC yield robustness against both classical and quantum attacks meaning that the encryption scheme will continue to be safe even as cryptographic and computational technologies advance.

In general, the outcomes of this research showcase that the MFO-optimized LBC approach has great potential to offer quality-security and privacy solutions to the IoT systems. The proposed system allows the scalable, efficient and secure transmission of data over IoT by using lattice-based encryption algorithms, MFO optimization, and quantum resistance capabilities to ensure that these systems will stand up against the future cybersecurity threats as well as the modern ones. The study opens up new avenues that will allow development of stronger, more secure and scalable encryption schemes in the soaring IoT industry.

REFERENCES

[1] Asif, R., 2021. Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms. IoT, 2(1), pp.71-91.
[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] Chang, Q., Ma, T. and Yang, W., 2025. Low power IoT device communication through hybrid AES-RSA encryption in MRA mode. Scientific Reports, 15(1), p.14485.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10]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.
[11]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.
[12]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.
[13]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.
[14]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.
[15]Keerthanarani, U., Selvakumar, V., Singaravelan, S., Raja, S.E., Thenmozhi, K. and Shunmugam, D.A., 2025. Moth flame optimization algorithm for efficient feature selection and hybrid classification technique for intrusion detection system. Multimedia Tools and Applications, pp.1-21.
[16]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.
[17] 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.