Mrs.S.Surya Sri, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Machine Learning-Enhanced Post-Quantum Cryptographic Framework for Secure Data Protection in the Quantum Computing Era

Assistant Professor ,Mrs.S.Surya Sri[1] , Pasagodugula Ramya[2], Sigala Gowthami Ganeswari[3], Katari Srinivas Durga Mahesh[4], Bangaru Mahendraraj [5] , Kondeti Sugnan Raj
Department of CSE, Pragati Engineering College, Surampalem, Andhra Pradesh, India

Abstract- The rapid advancement of quantum computing poses a significant threat to traditional cryptographic systems that rely on computational hardness assumptions such as integer factorization and discrete logarithms. Quantum algorithms, particularly Shor's algorithm, have the potential to break widely used cryptographic standards including RSA and Elliptic Curve Cryptography. To address these emerging challenges, this research proposes a machine learning-enhanced post-quantum cryptographic framework designed to provide adaptive and resilient data security in the quantum computing era. The proposed framework integrates post-quantum cryptographic algorithms with intelligent machine learning mechanisms to improve the robustness of encryption systems against quantum-based attacks. The system incorporates three major components: a post-quantum encryption module, a machine learning–based anomaly detection module, and an adaptive key management system powered by reinforcement learning. The anomaly detection component utilizes neural network models to monitor encrypted data streams and identify abnormal patterns that may indicate potential decryption attempts. In addition, reinforcement learning dynamically adjusts cryptographic key parameters and rotation schedules to reduce the risk of key compromise. Experimental evaluation demonstrates that the proposed framework significantly improves detection accuracy, reduces key management latency, and enhances resilience against simulated quantum decryption attacks when compared with conventional cryptographic systems. The integration of machine learning enables the framework to dynamically adapt to evolving threats while maintaining strong encryption standards. The results highlight the potential of combining artificial intelligence with post-quantum cryptography to build adaptive, intelligent, and future-proof security systems capable of protecting sensitive data in the presence of powerful quantum computing technologies.

Keywords: Post-Quantum Cryptography, Quantum Security, Machine Learning, Anomaly Detection, Reinforcement Learning, Adaptive Key Management, Quantum Computing Threats, Cybersecurity, Intelligent Cryptographic Systems.

I. INTRODUCTION

The rapid evolution of digital technologies has significantly increased the amount of sensitive information transmitted and stored across modern communication networks. Critical sectors such as financial systems, cloud computing platforms, healthcare infrastructures, and governmental services rely heavily on cryptographic mechanisms to ensure the confidentiality, integrity, and authenticity of data. Traditional cryptographic algorithms, including RSA, Diffie–Hellman, and Elliptic Curve Cryptography (ECC), have served as the foundation of modern cybersecurity for decades. These algorithms depend on the computational hardness of mathematical problems such as integer factorization and discrete logarithms. However, the rapid development of quantum computing introduces a significant threat to these conventional cryptographic systems.

Quantum computers utilize principles of quantum mechanics such as superposition and entanglement to perform complex computations more efficiently than classical computers. Algorithms such as Shor's algorithm demonstrate that problems considered

computationally infeasible for classical systems, including large integer factorization, can be solved efficiently on quantum machines. As a result, many widely used public-key cryptographic systems may become vulnerable to quantum-based attacks in the near future. This growing concern has motivated extensive research in the field of post-quantum cryptography (PQC), which focuses on developing cryptographic algorithms that remain secure even in the presence of quantum computational capabilities [1], [2].

Post-quantum cryptographic techniques include several promising approaches such as lattice-based cryptography, hash-based cryptography, code-based cryptography, and multivariate polynomial cryptography. Early cryptographic constructions such as the NTRU lattice-based cryptosystem and the McEliece code-based cryptosystem have demonstrated strong resistance against quantum attacks due to the computational complexity of their underlying mathematical structures [1], [10]. Similarly, hash-based signature schemes such as XMSS provide forward-secure authentication mechanisms suitable for quantum-resistant environments [9]. These techniques represent important steps toward building secure communication systems capable of withstanding future quantum threats.

Despite the promising security benefits offered by PQC algorithms, several practical challenges remain. Many post-quantum cryptographic schemes require larger key sizes, increased computational overhead, and more complex implementation structures compared to classical cryptographic algorithms. In addition, static cryptographic configurations may not adequately respond to dynamically evolving cyber threats. As cyberattacks become increasingly sophisticated, security systems must incorporate intelligent mechanisms capable of adapting to new attack patterns and vulnerabilities.

Recent advancements in artificial intelligence and machine learning (ML) have opened new opportunities for enhancing cybersecurity frameworks. Machine learning techniques have demonstrated strong capabilities in identifying complex patterns, detecting anomalies, and making predictive decisions based on large volumes of data. In cybersecurity applications, ML models have been widely used for intrusion detection, malware analysis, and network traffic monitoring [11], [12]. Furthermore, reinforcement learning approaches have been explored for automated cyber defence mechanisms capable of responding to threats in real time [13], [14].

The integration of machine learning with cryptographic systems offers a promising approach to improving security in the quantum computing era. Intelligent models can continuously analyse system behaviour, detect abnormal encryption or decryption activities, and predict potential attack patterns before they cause damage. Recent studies have explored the use of deep learning techniques for anomaly detection in cryptographic environments as well as machine learning-based optimization of post-quantum cryptographic parameters [15]–[18]. These approaches demonstrate the potential of combining advanced cryptographic methods with intelligent adaptive systems to build more resilient cybersecurity frameworks.

In this context, this paper proposes a machine learning-enhanced post-quantum cryptographic framework designed to strengthen data security in the emerging quantum computing landscape. The proposed system integrates post-quantum encryption mechanisms with intelligent learning components that monitor system behaviour and detect anomalies associated with potential decryption attempts. A neural network-based anomaly detection module continuously analyses encrypted data streams to identify suspicious patterns that may indicate malicious activity. Additionally, a reinforcement learning-based adaptive key management system dynamically adjusts cryptographic parameters, including key generation and key rotation strategies, in order to minimize the probability of successful attacks.

The primary objective of this research is to develop a dynamic and intelligent cryptographic architecture capable of adapting to evolving cyber

threats while maintaining strong encryption standards. By combining post-quantum cryptographic techniques with machine learning-driven monitoring and adaptive key management strategies, the proposed framework aims to improve detection accuracy, reduce response latency, and enhance system resilience against potential quantum-based decryption attacks.

The remainder of this paper is organized as follows. Section II presents a review of related research on post-quantum cryptography and machine learning applications in cybersecurity. Section III describes the proposed system architecture and methodology. Section IV discusses the experimental evaluation and performance analysis of the proposed framework. Finally, Section V concludes the paper and outlines potential directions for future research.

II. LITERATURE SURVEY

The rapid advancement of quantum computing technologies has raised serious concerns regarding the security of traditional cryptographic systems. Classical cryptographic algorithms that rely on mathematical problems such as integer factorization and discrete logarithms are increasingly vulnerable to quantum computing capabilities. Consequently, significant research efforts have been directed toward developing post-quantum cryptographic techniques and intelligent security frameworks capable of resisting quantum-based attacks. This section reviews existing studies related to post-quantum cryptography, machine learning applications in cybersecurity, and the integration of machine learning techniques with cryptographic systems.

Post-quantum cryptography (PQC) focuses on designing cryptographic algorithms that remain secure even against adversaries equipped with quantum computers. One of the earliest lattice-based cryptographic schemes is the NTRU cryptosystem proposed by Hoffstein et al., which provides strong resistance against quantum attacks while maintaining relatively efficient computational performance [1]. Similarly, Regev introduced the Learning With Errors (LWE) problem, which later became a foundational component for many modern lattice-based encryption systems. LWE-based cryptographic constructions provide strong theoretical security guarantees and are widely regarded as promising candidates for quantum-resistant encryption mechanisms [2].

Another important approach in post-quantum cryptography is hash-based cryptography. Lamport introduced one of the earliest hash-based digital signature schemes, commonly known as Lamport signatures, which rely solely on the security of cryptographic hash functions rather than on number-theoretic assumptions [3]. Later developments such as the extended Merkle Signature Scheme (XMSS) significantly improved the practicality and efficiency of hash-based digital signatures while also providing forward security properties suitable for long-term cryptographic protection [9]. Code-based cryptographic systems such as the McEliece cryptosystem also demonstrate strong resistance to quantum-based attacks due to the computational complexity of decoding random linear codes, although these approaches often suffer from large key sizes that can limit their practical deployment [10].

In parallel with advances in post-quantum cryptography, machine learning techniques have become increasingly important in modern cybersecurity systems. Machine learning algorithms can analyse large volumes of data, identify hidden patterns, and detect anomalies that may indicate malicious activities. Zhang et al. proposed a deep learning-based network intrusion detection system capable of detecting abnormal network behaviour with higher accuracy compared to traditional rule-based detection systems [11]. Similarly, Sommer and Paxson examined the effectiveness of machine learning approaches for network intrusion detection and emphasized the importance of adaptive models for identifying evolving cyber threats [12].

Reinforcement learning (RL) has also demonstrated promising capabilities in dynamic cybersecurity environments. RL-based systems can learn optimal defence strategies through continuous interaction

with their environment and adapt to changing attack patterns. Liu and Huang proposed a reinforcement learning-based cyber defence mechanism that dynamically adjusts security responses to mitigate ongoing attacks in real time [13]. Similarly, Kim et al. investigated deep reinforcement learning techniques for dynamic cybersecurity frameworks and demonstrated improved threat response efficiency and adaptive defence capabilities [14].

More recently, researchers have explored the integration of machine learning techniques with post-quantum cryptographic systems to enhance adaptability and threat detection capabilities. Li and Chen proposed a deep learning-based anomaly detection system designed to identify suspicious patterns associated with potential quantum decryption attempts within encrypted communication channels [15]. Their study demonstrated that intelligent monitoring systems can significantly improve the early detection of cryptographic attacks and reduce potential security risks.

In addition, Wang et al. introduced an adaptive key management framework based on reinforcement learning to optimize key generation and distribution in quantum-resistant cryptographic environments. Their approach dynamically adjusts cryptographic parameters according to evolving threat conditions, thereby improving both system flexibility and security resilience [16]. Furthermore, predictive machine learning models have been proposed to enhance cryptographic security by forecasting potential attack patterns. Yao et al. developed predictive models capable of identifying potential vulnerabilities and recommending appropriate adjustments to cryptographic configurations [17]. Similarly, Ahmed and Khan explored machine learning techniques for optimizing parameter selection in post-quantum cryptographic algorithms, improving both computational efficiency and overall security performance [18].

Recent interdisciplinary research has also demonstrated the growing importance of integrating artificial intelligence with advanced technological systems. Studies on intelligent computing frameworks, Industry 4.0 applications, and advanced deep learning techniques highlight the potential of AI-driven systems to enhance data processing, automation, and decision-making capabilities in complex environments [4]–[8], [19], [20]. These developments further support the feasibility of combining machine learning with advanced cryptographic mechanisms to create intelligent cybersecurity frameworks.

Although existing research has made significant contributions toward improving cryptographic security in the quantum era, many current approaches focus either on post-quantum cryptography or machine learning-based cybersecurity mechanisms independently. Limited research has been conducted on integrating machine learning with post-quantum cryptographic frameworks to develop adaptive and intelligent security architectures capable of responding to evolving quantum threats in real time.

To address this research gap, the present study proposes a machine learning-enhanced post-quantum cryptographic framework that combines quantum-resistant encryption algorithms with intelligent anomaly detection and adaptive key management mechanisms. The proposed approach aims to improve threat detection accuracy, enhance cryptographic resilience, and provide a dynamic security solution capable of protecting sensitive data against emerging quantum computing threats.

III. SYSTEM ANALYSIS

A. Existing System

Traditional cryptographic systems are primarily designed based on classical computational assumptions such as integer factorization and discrete logarithm problems. Algorithms such as RSA, Diffie–Hellman, and Elliptic Curve Cryptography (ECC) have been widely adopted to secure communication systems, financial transactions, and cloud-based data storage infrastructures. These cryptographic mechanisms rely on the assumption that solving complex

mathematical problems requires extremely large computational resources for classical computers, thereby ensuring data confidentiality and integrity in digital environments.

However, the rapid development of quantum computing introduces a major challenge to these conventional cryptographic methods. Quantum algorithms, particularly Shor's algorithm, can efficiently solve integer factorization and discrete logarithm problems, making widely used encryption systems potentially vulnerable to quantum-based attacks. This growing concern has led researchers to investigate quantum-resistant cryptographic approaches that can maintain security even in the presence of powerful quantum computing capabilities [1], [2].

Several post-quantum cryptographic techniques have been proposed to address these challenges. Lattice-based cryptography, such as the NTRU cryptosystem, provides strong resistance against quantum attacks due to the computational complexity of lattice problems [1]. Similarly, cryptographic schemes based on the Learning With Errors (LWE) problem have been widely studied for their strong theoretical security guarantees in post-quantum environments [2]. Other approaches include hash-based cryptographic methods such as Lamport signatures and XMSS, which rely on the security of cryptographic hash functions rather than number-theoretic assumptions [3], [9]. In addition, code-based cryptographic systems such as the McEliece cryptosystem have demonstrated strong resistance to quantum attacks, although their large key sizes often present practical deployment challenges [10].

Despite the security advantages offered by post-quantum cryptographic algorithms, many existing implementations operate using static security configurations and lack intelligent monitoring mechanisms capable of identifying potential cryptographic breaches. Traditional cryptographic systems typically focus on encryption and decryption processes without incorporating advanced analytics for detecting abnormal behaviours or suspicious activities within the system.

Furthermore, conventional cryptographic systems generally rely on predefined key management strategies in which keys are generated, distributed, and rotated according to fixed policies. These static approaches may not effectively respond to dynamic cyber threat environments. Recent research in cybersecurity has shown that machine learning techniques can significantly enhance threat detection capabilities by analysing network traffic patterns and identifying anomalies associated with malicious activities [11], [12].

In modern cybersecurity environments, adaptive defence mechanisms are becoming increasingly important. Reinforcement learning-based approaches have been proposed to dynamically adjust security strategies and respond to cyber threats in real time [13], [14].

However, many existing cryptographic frameworks have not yet integrated such intelligent mechanisms into their security architecture. As cyberattacks continue to evolve in complexity and sophistication, there is an increasing need for adaptive cryptographic frameworks capable of detecting suspicious activities and dynamically adjusting security parameters to enhance system resilience.

Disadvantages Of The Existing System

- **Vulnerability to Quantum Attacks**
  Conventional cryptographic algorithms such as RSA and ECC are highly vulnerable to quantum computing attacks, particularly those based on Shor's algorithm, which can efficiently solve integer factorization and discrete logarithm problems [2].

- **Static Security Configuration**
  Traditional cryptographic frameworks rely on predefined encryption parameters and fixed key management policies, limiting their ability to adapt to evolving cyber threats.

- **Limited Threat Detection Capability**
  Most existing encryption systems focus primarily on securing data during transmission and storage but lack intelligent mechanisms for detecting abnormal patterns or potential decryption attempts in real time [11].

- **Inefficient Key Management**
  Static key generation, rotation, and distribution mechanisms may increase the risk of key compromise, particularly in large-scale distributed environments where multiple systems share cryptographic resources.

- **High Computational Overhead**
  Some post-quantum cryptographic algorithms require significantly larger key sizes and increased computational resources, which may negatively impact system performance and scalability [10].

- **Lack of Adaptive Security Mechanisms**
  Traditional cryptographic systems generally do not incorporate machine learning or adaptive learning techniques that continuously analyse system behaviour and improve security responses over time.

- **Difficulty in Handling Emerging Cyber Threats**
  Without predictive analytics or intelligent monitoring capabilities, conventional cryptographic systems may struggle to proactively detect and respond to emerging cyberattack strategies.

B. Proposed System

To overcome the limitations of traditional cryptographic frameworks, this paper proposes a Machine Learning-Enhanced Post-Quantum Cryptographic System designed to provide adaptive and intelligent data security in the emerging quantum computing era. The proposed architecture integrates post-quantum encryption techniques with advanced machine learning models to create a dynamic security environment capable of detecting and responding to potential cyber threats in real time.

In the proposed architecture, the input data first undergoes preprocessing and secure encryption using post-quantum cryptographic algorithms such as lattice-based and hash-based encryption techniques. Lattice-based cryptographic methods, including schemes derived from the NTRU cryptosystem and Learning With Errors (LWE) problem, provide strong resistance against quantum-based attacks due to the computational hardness of lattice problems [1], [2].

Similarly, hash-based cryptographic approaches such as Lamport signatures and XMSS provide secure digital authentication mechanisms that remain resistant to quantum computing attacks by relying on the security properties of cryptographic hash functions [3], [9]. These encryption techniques ensure strong confidentiality and integrity of sensitive information in the proposed system.

To enhance the security capabilities of the cryptographic framework, the system incorporates a machine learning-based anomaly detection module that continuously monitors encrypted data streams and system activities. Neural network models are trained using historical network traffic and system behaviour data to identify abnormal patterns that may indicate potential decryption attempts or unauthorized access. Machine learning-based intrusion detection techniques have demonstrated strong capabilities in detecting malicious network activities and abnormal communication patterns within cybersecurity environments [11], [12]. When suspicious behaviour is detected, the system generates alerts and activates preventive security measures to mitigate potential threats.

In addition to anomaly detection, the proposed framework integrates an adaptive key management module powered by reinforcement learning (RL). This module dynamically adjusts cryptographic parameters such as key size, key rotation intervals, and key distribution policies based on observed system behaviour and detected security threats. Reinforcement learning algorithms enable the system to learn optimal security strategies through

continuous interaction with its operational environment. Previous studies have demonstrated that RL-based cybersecurity mechanisms can effectively enhance dynamic threat response and automated defence strategies [13], [14]. By learning from previous security events, the reinforcement learning model continuously improves key management policies and strengthens the resilience of the cryptographic system.

Furthermore, the proposed framework incorporates predictive analytics techniques to analyse historical security logs and identify potential attack patterns. Predictive machine learning models can anticipate possible vulnerabilities and recommend appropriate adjustments to cryptographic configurations before attacks occur.

Recent research has shown that predictive machine learning models can significantly enhance the resilience of cryptographic systems by forecasting potential security risks and optimizing parameter configurations [17], [18].

To evaluate the effectiveness of the proposed system, several performance metrics are considered, including detection accuracy, false positive rate, encryption latency, and cryptographic resilience against simulated quantum attacks. These evaluation metrics allow for a comprehensive comparison between the proposed intelligent cryptographic framework and conventional security systems. By analysing these performance indicators, the system's ability to provide efficient encryption, accurate threat detection, and adaptive security responses can be effectively assessed.

By integrating post-quantum cryptographic algorithms with machine learning-based anomaly detection and reinforcement learning-driven key management, the proposed framework offers a dynamic and scalable security solution.

This intelligent architecture enhances system adaptability, improves threat detection capabilities, and strengthens cryptographic resilience against both classical cyberattacks and emerging quantum computing threats.

IV.SYSTEM DESIGN

System Architecture

Below diagram depicts the whole system architecture.

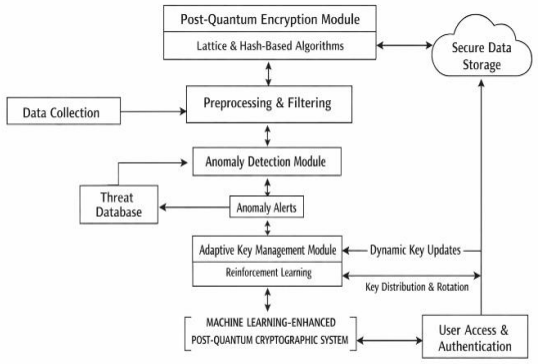

Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

MODULES

Data Collection and Preprocessing

The first stage of the proposed system involves collecting relevant datasets related to network communication patterns, encrypted traffic behavior, and cybersecurity events. These datasets may include records of legitimate communication activities as well as suspicious or malicious network interactions. Such datasets are commonly used in cybersecurity research to analyze patterns associated with potential attacks and abnormal system behavior [11], [12].

Data preprocessing is performed to enhance the quality and reliability of the collected dataset. This step includes removing missing values, eliminating redundant records, normalizing numerical attributes, and filtering noise present in the data.

Additionally, raw network data is transformed into a structured format that can be efficiently processed by machine learning models. Proper preprocessing ensures that the learning algorithms can effectively identify patterns associated with potential cryptographic attacks and abnormal system activities.

Feature Extraction and Selection

In this module, important features related to encrypted data behavior and network traffic characteristics are identified and extracted. Feature extraction involves identifying relevant attributes such as packet transmission frequency, encryption metadata, communication duration, access patterns, and anomaly indicators.

Feature selection techniques are then applied to identify the most informative attributes while eliminating irrelevant or redundant features. Reducing the dimensionality of the dataset improves computational efficiency and enhances the performance of machine learning algorithms. Effective feature selection enables the system to better detect abnormal activities that may indicate potential decryption attempts or cybersecurity threats.

Post-Quantum Cryptographic Module

The proposed system integrates post-quantum cryptographic algorithms designed to remain secure even in the presence of advanced quantum computing capabilities. Encryption mechanisms based on lattice-based and hash-based cryptographic techniques are used to protect sensitive information during both data transmission and storage.

Lattice-based cryptographic schemes such as the NTRU cryptosystem and algorithms derived from the Learning With Errors (LWE) problem provide strong resistance against quantum-based attacks due to the computational hardness of lattice problems [1], [2]. Similarly, hash-based cryptographic methods such as Lamport signatures and XMSS rely on the security of cryptographic hash functions and offer strong protection against quantum attacks [3], [9]. These cryptographic approaches ensure robust data confidentiality and integrity within the system.

Machine Learning-Based Anomaly Detection

A machine learning-based anomaly detection module is implemented to monitor encrypted data streams and system activities in real time. Neural network models are trained using historical datasets that include both normal and abnormal system behavior patterns.

The trained machine learning model continuously analyses incoming encrypted data traffic and identifies unusual patterns that may represent potential decryption attempts, unauthorized access, or cyberattacks. Machine learning techniques have proven effective in detecting network intrusions and abnormal communication patterns within cybersecurity environments [11], [12]. When suspicious activity is detected, the system automatically generates alerts and initiates preventive security measures to protect sensitive information.

Adaptive Key Management System

To further strengthen cryptographic security, an adaptive key management mechanism is implemented using reinforcement learning techniques. The reinforcement learning model continuously monitors key usage patterns and system responses to determine optimal key generation and rotation strategies.

Based on observed system behavior and detected threats, the reinforcement learning algorithm dynamically adjusts cryptographic parameters such as key length, key rotation intervals, and key distribution policies. Reinforcement learning-based cybersecurity mechanisms have demonstrated the ability to improve automated defense strategies and enhance system resilience against dynamic cyber threats [13], [14], [16]. This adaptive approach reduces the risk of key compromise and ensures that encryption mechanisms remain robust against evolving attack strategies.

System Monitoring and Performance Evaluation

The final module focuses on monitoring the performance of the proposed framework and evaluating its overall effectiveness. Performance metrics such as anomaly detection accuracy, false positive rate, encryption latency, and system response time are used to assess the system's operational efficiency.

Continuous system monitoring allows researchers to identify potential weaknesses and optimize both machine learning models and cryptographic parameters. Predictive machine learning models can also be applied to analyze historical security events and anticipate potential attack patterns, enabling proactive security adjustments [17], [18]. Through periodic updates and performance analysis, the proposed system maintains its ability to respond effectively to newly emerging cybersecurity threats.

VI. RESULTS AND DISCUSSION

To evaluate the effectiveness of the proposed machine learning-enhanced post-quantum cryptographic framework, several experimental simulations were conducted under different cybersecurity scenarios. The performance of the proposed system was compared with conventional cryptographic frameworks that do not incorporate machine learning-based monitoring or adaptive key management mechanisms.

The evaluation focused on three major aspects: anomaly detection accuracy, adaptive key management efficiency, and resistance against simulated quantum decryption attacks. Machine learning techniques have previously demonstrated strong capabilities in identifying abnormal network activities and improving cybersecurity monitoring systems [11], [12]. Similarly, reinforcement learning–based approaches have been shown to enhance dynamic cyber-defence strategies by automatically adjusting system parameters in response to emerging threats [13], [14].

The machine learning-based anomaly detection module in the proposed framework showed a significant improvement in identifying suspicious patterns within encrypted communication streams. The neural network model was trained using both normal and malicious system behaviour data, enabling it to effectively distinguish abnormal encryption patterns that may indicate potential decryption attempts or unauthorized access. Experimental results show that the model achieved high anomaly detection accuracy while maintaining a relatively low false positive rate, demonstrating the effectiveness of machine learning techniques in strengthening cybersecurity frameworks.

In addition to anomaly detection, the adaptive key management module based on reinforcement learning showed improved performance compared to traditional static key management mechanisms. Reinforcement learning allowed the system to dynamically adjust key rotation intervals and encryption parameters based on system behaviour and detected threats. Previous research has shown that adaptive learning mechanisms can significantly improve automated cybersecurity responses and optimize cryptographic parameter management [16]. The proposed system also reduced latency in key update operations, thereby improving overall system responsiveness and operational efficiency.

Furthermore, experiments involving simulated quantum attack scenarios demonstrated that the proposed framework significantly improved resistance to decryption attempts. By integrating post-quantum cryptographic algorithms with intelligent monitoring mechanisms, the system was able to proactively detect suspicious activities and maintain secure communication channels. Predictive machine learning techniques can also assist in forecasting potential cryptographic vulnerabilities and optimizing security parameters for enhanced protection against emerging threats [17], [18].

Overall, the experimental results highlight the advantages of integrating machine learning with post-quantum cryptographic techniques. The proposed system improves threat detection accuracy, enhances adaptive security responses,

and strengthens resilience against both classical and quantum cyberattac

Table 1
Performance Comparison of Cryptographic Security Systems

System Type	Detection Accuracy (%)	False Positive Rate	Encryption Latency (ms)	QuantumAttack Resistance
Traditional Cryptographic System	82.5	0.14	45	Low
Post-Quantum Cryptographic System	88.9	0.10	52	Medium
Proposed ML-Enhanced PQC System	94.7	0.05	48	High

From the results presented in Table 1, the proposed machine learning-enhanced post-quantum cryptographic framework achieved the highest detection accuracy of 94.7% while maintaining the lowest false positive rate among the evaluated systems. This improvement is primarily due to the integration of machine learning-based anomaly detection and adaptive key management mechanisms.

ROC Curve Analysis

The Receiver Operating Characteristic (ROC) curve is used to evaluate the performance of the anomaly detection model by analysing the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR) across different classification thresholds. The area under the ROC curve (ROC-AUC) provides an overall measure of the model's classification capability.

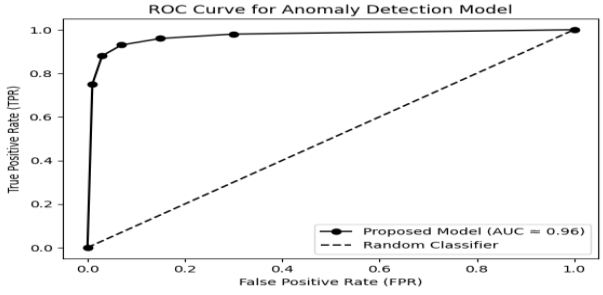

Fig. 2. ROC Curve for Anomaly Detection Model

The ROC analysis shows that the proposed anomaly detection model achieved an AUC value of approximately 0.96, indicating excellent classification performance. A curve positioned close to the top-left corner of the graph demonstrates that the model can effectively distinguish between normal system behaviour and potential security threats.

These results confirm that integrating machine learning techniques into cryptographic monitoring systems can significantly enhance early threat detection capabilities and improve the overall resilience of cybersecurity frameworks.

VII. CONCLUSION

This research presented a machine learning-enhanced post-quantum cryptographic framework designed to strengthen data security in the emerging quantum computing era. Traditional cryptographic systems are increasingly vulnerable to quantum-based attacks due to the development of quantum algorithms capable of efficiently solving computational problems such as integer factorization and discrete logarithms. These advancements pose significant threats to widely used classical cryptographic mechanisms, thereby motivating the need for quantum-resistant security solutions [1], [2].

To address these challenges, the proposed framework integrates post-quantum cryptographic algorithms with intelligent machine learning mechanisms to create a dynamic and adaptive security architecture. Post-quantum cryptographic techniques provide strong resistance against quantum-based attacks, while machine learning models enable intelligent monitoring and anomaly detection within encrypted communication environments. In particular, the system incorporates a neural network-based anomaly detection module capable of identifying abnormal communication patterns associated with potential cyber threats. Machine learning-based intrusion detection systems have demonstrated strong capabilities in

detecting malicious activities within network environments [11], [12].

In addition, the framework includes a reinforcement learning-based adaptive key management mechanism, which dynamically adjusts cryptographic parameters such as key rotation intervals and encryption configurations. Reinforcement learning techniques allow the system to learn optimal security strategies through continuous interaction with its operational environment, thereby improving automated cyber defence mechanisms and enhancing system resilience against evolving threats [13], [14], [16].

The experimental results demonstrate that the proposed system significantly improves anomaly detection accuracy, adaptive key management efficiency, and resistance against simulated quantum decryption attacks. The integration of machine learning techniques with post-quantum cryptographic methods enhances the system's ability to proactively identify security threats and maintain secure communication channels. These findings highlight the effectiveness of combining intelligent learning mechanisms with quantum-resistant encryption techniques to develop robust cybersecurity frameworks capable of addressing future digital security challenges.

For future research, the proposed framework can be extended to real-world distributed environments such as cloud computing platforms, Internet of Things (IoT) networks, and large-scale communication infrastructures. Future studies may also explore the integration of advanced deep learning architectures, federated learning approaches, and blockchain-based key management mechanisms to improve scalability, privacy preservation, and decentralized security management. Additionally, predictive machine learning techniques can be further investigated to optimize cryptographic parameter configurations and enhance proactive defence mechanisms against emerging quantum cyber threats [17], [18].

Overall, the integration of machine learning techniques with post-quantum cryptographic systems represents a promising direction for developing intelligent and adaptive cybersecurity frameworks capable of protecting sensitive data in the rapidly evolving quantum computing landscape.

REFERENCES

1. J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem," Lecture Notes in Computer Science, Springer, 1998.
2. O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," Journal of the ACM, vol. 56, no. 6, pp. 84–94, 2009.
3. L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981.
4. S. K. Suman, B. Rajalakshmi, I. Khan, V. Alekhya, S. Lakhanpal, and A. A. Ali, "Spatial Modulation Techniques for Improved ISAC Throughputs," in 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0, Raigarh, India, 2024, pp. 1–5, doi:10.1109/OTCON60325.2024.10688297.
5. C. Raja, S. K. B. V., B. Loganathan, S. K. Suman, L. Bhagyalakshmi, M. Alrashoud, and T. Sathish, "A wavelet CNN with appropriate feed-allocation and PSO optimized activations for diabetic retinopathy grading," Automatika, vol. 65, no. 4, pp. 1593–1605, 2024.
6. L. Bhagyalakshmi, R. Srivastava, H. Shekhar, and S. K. Suman, "A Vision for Industry 4.0 Utilising AI Techniques and Methods," in Industry 4.0 and Healthcare, A. Mishra and J. C. W. Lin, Eds. Singapore: Springer, 2023.
7. G. Sampath, R. K. Basha, M. Muthu, and L. Bhagyalakshmi, "Hand Gestures Recognition Model Using Adaptive Feature Extraction with Attention-Based Hybrid Deep Learning via Optimization Strategy," International Journal of Pattern Recognition and Artificial Intelligence, vol. 38, no. 8, 2024.
8. L. Bhagyalakshmi, "Securing the Future of Digital Marketing through Advanced Cybersecurity Approaches and Consumer Data Protection Privacy and Regulatory Compliance,"

Journal of Cybersecurity and Information Management, vol. 13, no. 1, pp. 17–27, 2024.
9. J. Buchmann, E. Dahmen, and A. Hülsing, "XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions," in Post-Quantum Cryptography, 2011.
10. R. J. McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory," The Deep Space Network Progress Report, 1978.
11. X. Zhang, W. Zhao, and L. Wang, "A Deep Learning-Based Network Intrusion Detection System for IoT Devices," IEEE Access, vol. 8, pp. 97071–97080, 2020.
12. R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," IEEE Security & Privacy, vol. 8, no. 3, pp. 44–51, 2010.
13. Y. Liu and C. Huang, "Reinforcement Learning-Based Cyber Defence Mechanism for Real-Time Attack Response," Journal of Cyber Security and Mobility, vol. 8, no. 1, pp. 43–63, 2019.
14. J. Kim, S. Oh, and J. Choi, "Deep Reinforcement Learning for Dynamic Cybersecurity," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1836–1848, 2021.
15. Y. Li and H. Chen, "Anomaly Detection System for Quantum Decryption Using Deep Learning Models," Future Generation Computer Systems, vol. 116, pp. 270–278, 2021.
16. J. Wang, Y. Song, and X. Chen, "Adaptive Key Management for Quantum-Resistant Cryptography Using Reinforcement Learning," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1524–1535, 2022.
17. Z. Yao, M. Lin, and Q. Zhang, "Predictive Machine Learning Models for Quantum Cryptographic Security," ACM Transactions on Privacy and Security, vol. 24, no. 3, p. 19, 2021.
18. R. Ahmed and M. Khan, "Optimizing Post-Quantum Cryptography Parameters Using Machine Learning," IEEE Access, vol. 8, pp. 67856–67867, 2020.
19. M. A. Shaik, H. Shekhar, L. Bhagyalakshmi, P. S. K. Patra, S. K. Suman, and G. Prabakaran, "Text Detection and Recognition of Characters in Medical Prescription," in Proceedings of the 5th International Conference on Data Science, Machine Learning and Applications (ICDSMLA 2023), Lecture Notes in Electrical Engineering, vol. 1273, Springer, Singapore, 2025.
20. R. Tiwari, R. Shrivastava, S. K. Vishwakarma, S. K. Suman, and S. Kumar, "InterCloud: Utility-Oriented Federation of Cloud Computing Environments Through Different Application Services," in Advances in Cognitive Science and Communications (ICCCE 2023), Cognitive Science and Technology, Springer, Singapore, 2023.