Post-Quantum Cryptography Enhanced with Machine Learning for Intelligent Cyber Threat Detection

Prof. Gulhane V.M[1], M r . Abhale B. A[2], Miss.Kolhe Rutuja S[3],
Miss.Sonas Gauri U[4], Miss.Thorat Bhakti D[5], Miss.Hon Sanika S[6]
[1,2,3,4,5,6]*S.N. D College of engineering and research center yeola Savitribai Phule Pune University*

***Abstract*—With the rapid advancement of quantum computing, traditional cryptographic algorithms such as RSA and ECC are becoming vulnerable to quantum attacks. Post-Quantum Cryptography (PQC) has emerged as a promising solution to ensure data security in the quantum era. However, while PQC strengthens encryption mechanisms, modern cyber threats are increasingly intelligent, adaptive, and capable of exploiting system vulnerabilities beyond encryption layers. To address this dual challenge, this study proposes an integrated framework combining PQC and Machine Learning (ML) for intelligent cyber threat detection. The PQC component ensures resilience against quantum-based attacks, while ML algorithms enhance system intelligence by identifying anomalous behaviors, zero-day threats, and advanced persistent attacks in real time.**

***Index Terms*—Artificial Intelligence (AI); Anomaly Detection; Cybersecurity; Cyber Threat Detection; Data Protection; Deep Learning; Machine Learning (ML); Network Security; Post-Quantum Cryptography (PQC); Quantum Computing; Quantum-Resilient Encryption; Supervised Learning; Unsupervised Learning; Zero-Day Attack Detection; Intelligent Cyber Defence; Quantum-Safe Cryptographic Algorithms.**

I. INTRODUCTION

Quantum Machine Learning (QML) is an emerging field that leverages principles of quantum mechanics to improve the training, performance, and scalability of machine learning (ML) models. To effectively utilize quantum capabilities, different approaches have been developed in QML as shown in Fig. 1, each focused on different aspects of how quantum principles can be used to advance machine learning. While Quantum-Enhanced machine learning focuses on directly using quantum algorithms for classical methods, the wide range of research on QML also explores how quantum principles have inspired classical methods, leading to the development of Quantum-Inspired Machine Learning. Classical models are enhanced with techniques inspired by quantum processing, such as algorithms based on quantum annealing applied to classical optimization problems. For example, the work in used quantum annealing to solve a problem in polynomial time compared to exponential time in classical methods.

Taking inspiration further, researchers have combined quantum and classical techniques introducing hybrid models for various learning tasks as in Quantum Generalized Machine Learning. Hybrid models integrate quantum and classical techniques to effectively address diverse learning tasks. Beyond developing and combining methodologies, the application of different quantum techniques in real world contexts has marked the significance of Quantum-Applied Machine Learning. This involves practical applications of QML in various domains such as finance, healthcare, and cybersecurity. In this work, we systematically survey the applications of QML across major fields, including cybersecurity, finance, healthcare, and drug discovery. We identify important trends, such as the strong potential of hybrid quantum classical models for near-term practical deployment and the significant challenges due to quantum noise, limited qubit implementations. Scalability, and costly RAM

The high processing requirements of numerous PQC schemes create limitations that reduce their efficiency when used by constrained devices. PQC algorithms need large key dimensions that produce elevated storage requirements besides increasing transmission bandwidth costs in comparison to traditional cryptosystems. New vulnerabilities in actual cryptographic system deployments emerge because

implementation of secure protocols faces risks from side-channel attacks along with optimization inefficiencies.

II. LITERATURE SURVEY

[1] Ravi Kumar Inakoti et al. (2025) proposed a hybrid approach combining Quantum Cryptography with Machine and Deep Learning for enhanced post-quantum security. The model improves key generation, intrusion detection, and scalability, offering an adaptive and intelligent quantum security framework.

[2] Gopalakrishna Karamchand (2025) presented a study on Quantum Machine Learning (QML) for threat detection in high-security networks. The model leverages quantum computing and ML algorithms to quickly identify anomalies and potential cyber threats, enhancing accuracy and response speed in secure environments.

[3] Pradeep Lamichhane and Danda B. Rawat (2025) reviewed recent advances in Quantum Machine Learning (QML), highlighting its applications, challenges, and future prospects. The paper discusses hybrid quantum- classical models, scalability issues, and potential solutions for improving efficiency and security in quantum computing systems.

[4] Lauren Eze, Umair B. Chaudhry, and Hamid Jahankhani (2025) explored Quantum-Enhanced Machine Learning (QEML) for cybersecurity applications, focusing on malicious URL detection. Their approach integrates quantum computing with ML classifiers to achieve faster detection rates and improved accuracy in identifying cyber threats.

[5] Nazeer Shaikh, Dr. B. Harichandana, and Dr. P. Chitralingappa (2024) discussed the integration of Quantum Computing and Machine Learning to transform network security. Their study emphasizes how quantum algorithms enhance encryption strength, intrusion detection, and overall data protection efficiency in modern networks.

[6] Forhad Hossain, Kamrul Hasan, Al Amin, and Shakik Mahmud (2024) proposed a hypothetical framework using Quantum Machine Learning (QML) to enhance cybersecurity. The study outlines a next-generation model aimed at real-time threat prediction, adaptive encryption, and intelligent defense mechanisms against evolving cyberattacks.

[7] P. Ramya, R. Anitha, J. Rajalakshmi, and R. Dineshkumar (2024) explored the integration of Quantum Computing and Natural Language Processing (NLP) for advanced cyber threat detection. Their model enhances threat analysis, pattern recognition, and response accuracy in detecting complex cyberattacks.

[8] Muhammed Azeez, Christopher Tetteh Nenebi, Victor Hammed, Lawrence Kofi Asiam, Edward James Isoghie, Oluwaseun R. Adesanya, and Tomisin Abimbola (2024) focused on developing intelligent cyber threat detection systems using quantum computing. Their work demonstrates how quantum algorithms can improve threat prediction, detection speed, and system resilience against advanced cyberattacks.

[9] Dankan Gowda V, Swathi Pai M, Dileep Kumar Pandiya, Arun Kumar Katkoori, and Anil Kumar Jakkani (2024) examined the use of Quantum Cryptography and Machine Learning to enhance security in AI systems. Their study integrates quantum encryption with ML models to strengthen data privacy, authentication, and resistance to quantum attacks.

III. METHODOLOGY

- Data Collection: Data Collection Collect dataset (e.g., CICIDS2017 or UNSW- NB15). These datasets contain information similar as IP addresses, anchorages, protocols, timestamps, and colorful inflow statistics.
- Preprocessing: Preprocessing Remove missing data, homogenize features, and elect the stylish attributes. Raw data frequently contains noise, missing values, or inapplicable information. Preprocessing ensures that the data is clean and harmonious before it's used for training.
- Model Training: Model Training Train SVM, Random Forest, and Decision Tree models. Once the data is preprocessed and features are uprooted, different machine literacy models are trained. The training process involves feeding the model with labeled data so it can learn patterns that distinguish normal from attack business.

- Testing and Evaluation: Testing and Evaluation Test the models and compare their performance. After training, each model is tested using unseen data to measure its performance. The thing is to determine how directly the model can descry attacks.
- Deployment: Deployment The best- performing model will be used for real- time detection. The model that achieves the loftiest delicacy and stylish overall performance is named for deployment. It's integrated into a real- time Intrusion Discovery System (IDS) to cover live network business.
- Outcome: Quantum-safe encryption for data integrity and confidentiality. Intelligent, adaptive, and real-time detection of cyber threats. A unified model capable of securing next-generation digital infrastructures against both classical and quantum-era attacks.

IV. OBJECTIVE

The primary goal of this research is to develop a hybrid cybersecurity framework that combines Post-Quantum Cryptography (PQC) and Machine Learning (ML) to provide quantum-resistant data security and intelligent threat detection. The specific objectives are:

1. To ensure quantum-resilient data protection
- Implement and evaluate Post-Quantum Cryptographic algorithms such as lattice-based and hash-based encryption schemes.
- Achieve secure communication channels that remain resistant to both classical and quantum computing attacks.

2. To design an intelligent cyber threat detection system
- Integrate machine learning models (supervised and unsupervised) capable of identifying and classifying various cyber threats, including zero-day attacks and advanced persistent threats (APTs).
- Utilize feature extraction and pattern recognition techniques to detect anomalies in real-time network traffic.

3. To develop a hybrid PQC–ML security framework
- Combine PQC for encryption security with ML for behavioral threat detection.
- Enable dynamic response mechanisms where detected threats trigger automated cryptographic actions (e.g., key rotation or access blocking).

4. To evaluate system performance and efficiency
- Assess the proposed framework using metrics such as accuracy, precision, recall, F1-score, encryption speed, and computational overhead.
- Compare the hybrid PQC–ML model with traditional cryptographic and intrusion detection systems.

5. To contribute toward next-generation cybersecurity solutions
- Provide a scalable, adaptive, and intelligent model that can be integrated into cloud, IoT, and enterprise systems.
- Support the global transition to quantum-secure and AI-driven cybersecurity infrastructures.

V. PROBLEM DEFINATIONS

In today's digital ecosystem, data security and privacy are facing unprecedented challenges due to the rapid evolution of computing technologies and cyber threats. Traditional cryptographic algorithms such as RSA, ECC, and AES have long been the backbone of data protection. However, with the advent of quantum computing, these classical algorithms are becoming increasingly vulnerable. Quantum algorithms like Shor's and Grover's are capable of factoring large numbers and breaking symmetric key encryption in polynomial time, rendering current cryptographic systems ineffective. This looming threat of quantum-enabled attacks creates an urgent need for quantum-resistant cryptographic mechanisms that can safeguard sensitive information in the post-quantum era.

At the same time, the cybersecurity landscape is witnessing an exponential rise in the complexity and frequency of cyberattacks, such as ransomware, zero-day exploits, phishing, and advanced persistent threats (APTs). Conventional intrusion detection and prevention systems, which rely on static signatures or rule-based logic, often fail to identify new or evolving attack patterns. Although machine learning (ML) techniques have shown promise in detecting anomalies and predicting malicious activities, most

existing ML-based security solutions operate independently of cryptographic frameworks. This disconnect limits their ability to provide holistic protection that addresses both data confidentiality and dynamic threat detection.

Therefore, the fundamental problem addressed in this research is the lack of an integrated, intelligent cybersecurity framework that combines Post-Quantum Cryptography (PQC) for quantum-resilient encryption with Machine Learning (ML) for adaptive, real-time cyber threat detection. The challenge lies in developing a unified system that ensures secure communication against quantum attacks, continuously learns from evolving threat behaviors, and maintains computational efficiency suitable for deployment in modern network environments. Solving this problem is crucial for achieving sustainable, intelligent, and future-proof cybersecurity solutions.

VI. FLOW CHART

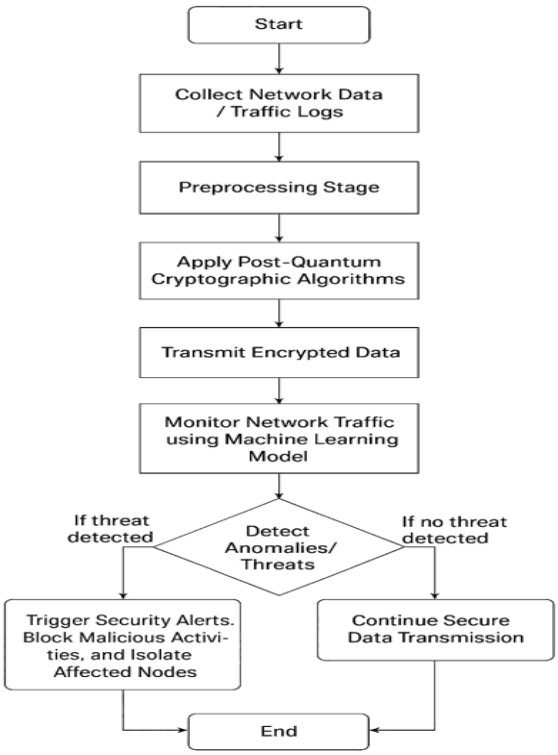

Fig. Flow Chart

Data Flow Diagram:

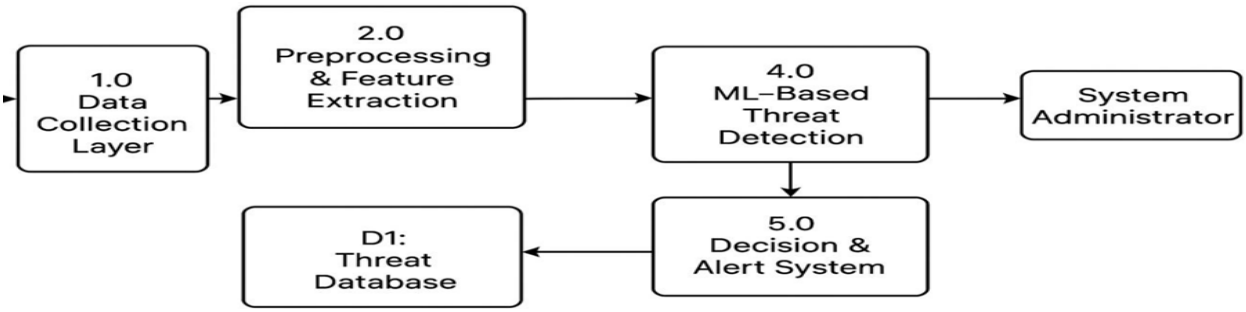

Fig. Data Flow Diagram

Algorithm:

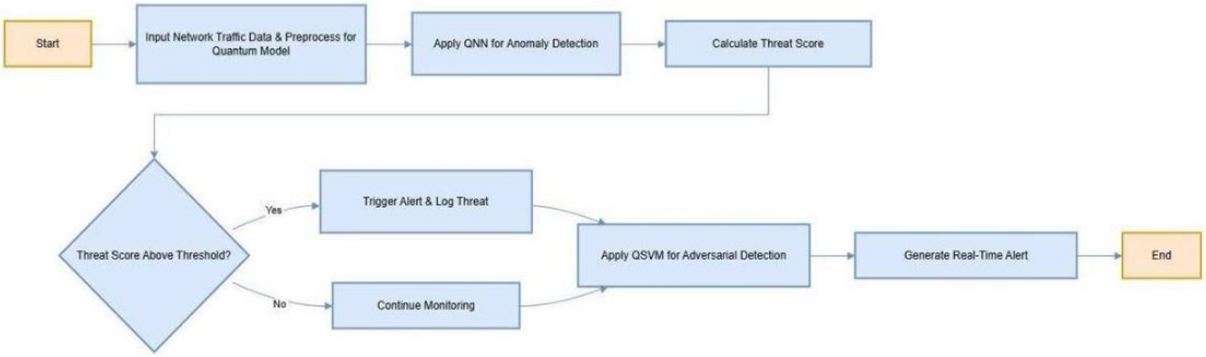

Fig.Algorithm

Architecture:

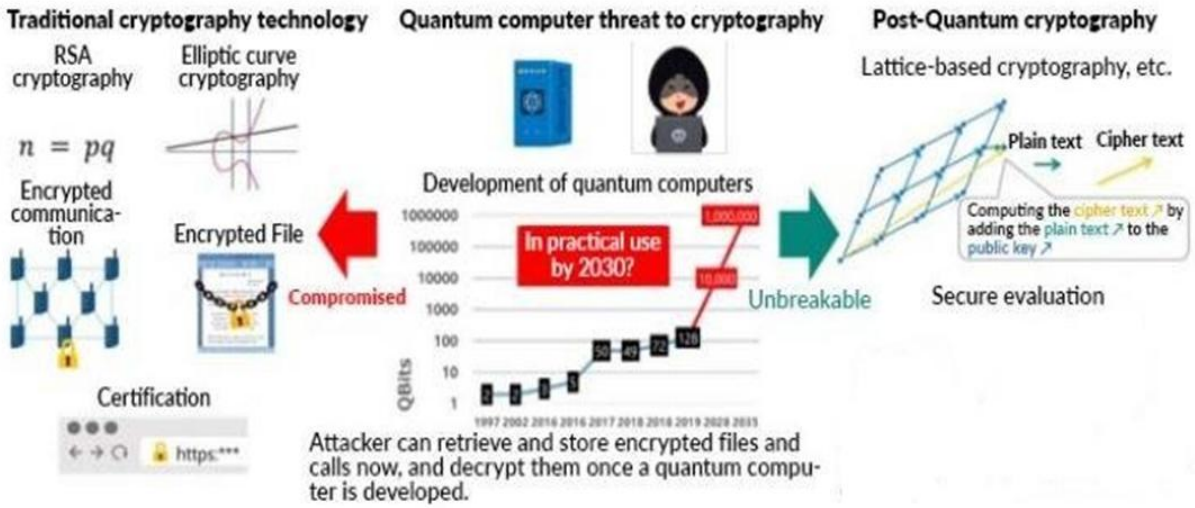

Fig: Architecture

UML Diagram

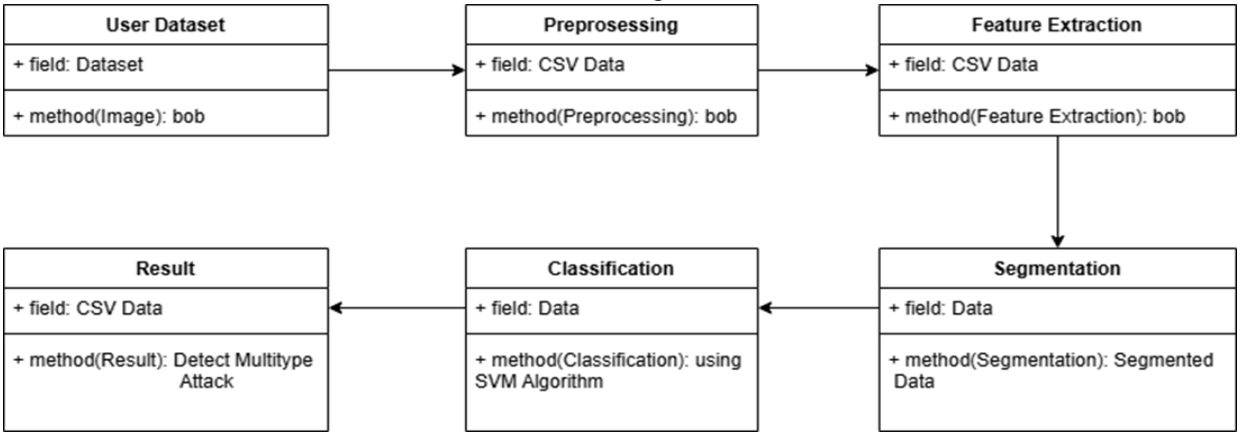

Fig. UML Diagram

VII. ADVANTAGES

- Detects multiple types of cyber-attack (DDoS, botnet, backdoor, data theft) using machine literacy rather than counting on traditional hand-grounded detection.
- Reduces false cons and improves bracket delicacy through comparative model evaluation (SVM, RF, DT)
- Scalable and adaptable to new traffic patterns by retraining with streamlined datasets.
- Enables real- time discovery after optimal model deployment.
- Provides bettered decision- making support for cybersecurity judges and network directors.

VIII. DISADVANTAGES

- Model performance largely depends on the quality and representativeness of the training dataset.
- High computational cost during training of complex models or large

Datasets.

- May bear frequent retraining to remain effective against evolving attack strategies.
- Imbalanced datasets may lead to prejudiced prognostications toward maturity classes.

IX. APPLICATIONS

1. Network security monitoring in enterprise and pall surroundings.
2. Real- time intrusion discovery systems (IDS) for data centers and ISPs.
3. Cyber defense fabrics in government and military networks.
4. Smart home and IoT- grounded networks taking intelligent trouble mitigation

X. CONCLUSION

In conclusion, Prophetic conservation using IoT, Big Data, and Machine literacy provides a smart result to help unanticipated machine failures in diligence. By continuously covering machine conditions and assaying data in real time, it helps prognosticate implicit problems before they do. This approach reduces time-out, saves conservation costs, improves outfit effectiveness
, and ensures smoother product operations. Overall, it enables diligence to make intelligent, data- driven opinions and maintain a more dependable and productive terrain.

REFERENCES

[1] M. Pech, "Predictive Maintenance and Intelligent Sensors in Smart Factories," Sensors, vol. 21, no. 22, pp. 1–20, Nov. 2021.

[2] S. Elkateb, M. Elhoseny, and H. S. Al-Raweshidy, "Machine Learning and IoT–Based Predictive Maintenance for Industrial Applications," Computers, Materials & Continua, vol. 67, no. 3, pp. 2467–2484, 2024.

[3] A. Benhanifia, M. A. Boudia, and M. A. Boudia, "Systematic Review of Predictive Maintenance Practices in Manufacturing," Procedia CIRP, vol. 108, pp. 1–6, 2025.

[4] P. Ngwa, M. S. A. Hossain, and S. S. Gill, "Big Data Analytics for Predictive System Maintenance," Journal of Industrial Information Integration, vol. 28, pp. 100-118, 2023.

[5] G. A. Susto, A. Schirru, S. Pampuri, and A. Beghi, "Machine Learning for Predictive Maintenance: A Multiple Classifier Approach," IEEE Transactions on Industrial Informatics, vol. 11, no. 3, pp. 812–820, Jun. 2015.

[6] . Li, K. Wang, and Y. He, "Industry 4.0 - Potentials for Predictive Maintenance," in Proceedings of the 2016 IEEE International Conference on Industrial Engineering and Engineering Management, 2016, pp. 1051–1055.

[7] Y. He, X. Han, C. Gu, and Z. Chen, "Cost-Oriented Predictive Maintenance Based on

[8] Mission Reliability State for Cyber Manufacturing Systems," Advances in Mechanical Engineering, vol. 10, no. 1, p. 168781401775145, Jan. 2018.

[9] A. Vasilache, S. Nitzsche, D. Floegel, T. Schuermann, S. von Dosky, T. Bierweiler, M. Mußler, F. Kälber, S. Hohmann, and J. Becker, "Low-Power Vibration-Based Predictive Maintenance for Industry 4.0 using Neural Networks: A Survey," arXiv preprint arXiv:2408.00516, Aug. 2024.

[10] H. Zheng, A. R. Paiva, and C. S. Gurciullo, "Advancing from Predictive Maintenance to Intelligent Maintenance with AI and IIoT," arXiv preprint arXiv:200900351, Sep. 2020.