2026 Volume: 02 Issue: 05 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-10

POST-QUANTUM CRYPTOGRAPHY ENHANCED WITH MACHINE LEARNING FOR INTELLIGENT CYBER THREAT DETECTION

***Gulhane V.M., Abhale B.A., Hon Sanika S., Kolhe Rutuja S., Sonas Gauri U., Thorat Bhakti D.**

S.N.D College of engineering and Research Center Savitribai Phule Pune University.

Article Received: 16 April 2026
Article Revised: 06 May 2026
Published on: 26 May 2026

***Corresponding Author: Gulhane V.M.**
S.N.D College of engineering and Research Center Savitribai Phule Pune University.

DOI: https://doi-doi.org/101555/ijrpa.8143

ABSTRACT

Cyber-attacks are becoming more sophisticated with the rise of advanced technologies, posing serious threats to data security and privacy. Traditional cryptographic methods and security systems are increasingly vulnerable, especially with the advent of quantum computing. This project proposes an intelligent cyber threat detection system that combines Post Quantum Cryptography (PQC) with Machine Learning (ML) techniques to ensure both proactive detection and quantum resistant data protection. Machine learning algorithms such as SVM, Random Forest, and Decision Tree are used to identify multiple types of attacks including DDoS, Botnet, Data Theft, and Backdoor. PQC algorithms like lattice-based and hash-based cryptography secure communication against quantum-level threats. The integration of ML and PQC provides a robust, adaptive, and future-ready cyber security framework capable of detecting, classifying, and preventing complex cyber threats in real time.

KEYWORDS: Post-Quantum Cryptography, Machine Learning, Cyber Security, SVM, DDOS, Threat Detection.

I.INTRODUCTION

In today's digital age, the growing dependency on networked systems and online data exchange has made cybersecurity a critical concern. With the increasing complexity of cyber attacks such as DDoS, data theft, botnet infections, and backdoor intrusions, traditional security systems often fail to provide adequate protection. At the same time, the emergence of quantum computing poses a major threat to conventional cryptographic algorithms, as

quantum processors can potentially break existing encryption methods with ease. To address these challenges, this project introduces a hybrid framework that integrates Post Quantum Cryptography (PQC) with Machine Learning (ML) for intelligent cyber threat detection. Machine learning algorithms analyze network traffic patterns to detect anomalies and classify attacks in real time, while PQC ensures data confidentiality and integrity even in the presence of quantum-capable adversaries. The proposed system provides a secure, adaptive, and future-proof solution for modern cyber security needs.

II LITERATURE SURVEY

[1] S. Roselin Mary, M. Maheshwari, and M. Thamaraiselvan (2013) proposed an Attacked Packet Detection Algorithm (APDA) for early detection of Denial of Service (DoS) attacks in Vehicular Ad Hoc Networks (VANETs). Their approach detects attacks before the verification stage, thereby reducing delay overhead and enhancing overall network security in safety-critical vehicular environments.

[2] Faisal Hussain, Syed Ghazanfar Abbas, Muhammad Husnain, Ubaid U. Fayyaz, Farrukh Shahzad, and Ghalib A. Shah (2021) proposed a deep learning-based approach using ResNet for detecting DoS and Distributed DoS (DDoS) attacks in Internet of Things (IoT) networks. The method converts network traffic into image form and applies Convolutional Neural Networks (CNN), achieving 99.99% accuracy in binary classification and high precision in multi-class attack detection.

[3] Faisal Mochamad Teguh Kurniawan, Setiadi Yazid, Abdelrhman Mohammed, and Iman Abuel Maaly Abdelrahman (2020) introduced a detection and mitigation strategy for DoS attacks in Wireless Sensor Networks (WSNs). The approach combines a signature-based Intrusion Detection System (IDS) with a blocking mechanism that isolates attacker nodes, effectively reducing the impact of attacks in resource-constrained environments.

[4] Xiang-Gui Guo, Xiao Fan, Jian-Liang Wang, and Ju H. Park (2020) developed a memory adaptive event-triggered fault detection and isolation (FDI) scheme for nonlinear fuzzy control systems under DoS attacks. Using Takagi–Sugeno fuzzy models, switching controllers, and Lyapunov-based stability analysis, the method ensures system stability while reducing communication overhead.

[5] Mohiuddin Ahmed (2017) proposed a framework for detecting DoS attacks based on collective anomaly detection and clustering techniques. Unlike traditional methods that detect individual anomalies, this approach focuses on identifying group-based abnormal patterns, making it more suitable for large- scale and complex DoS attacks, especially in IoT

environments.

[6] Saifudin Usman and Idris Winarno (2020) implemented a Software-Defined Networking (SDN)- based Intrusion Detection System (IDS) to protect virtualization servers against HTTP DoS attacks. The centralized SDN controller enables real-time monitoring, dynamic policy enforcement, and efficient detection of malicious traffic in cloud computing environments.

[7] Xiaoxue Wu, Dan Tang, Liu Tang, Jianping Man, Sijia Zhan, and Qin Liu (2018) proposed a correlation- based detection method using the Hilbert Spectrum for identifying low-rate DoS (LDoS) attacks. By applying the Hilbert-Huang Transform to network traffic, the method extracts detailed time-frequency features, improving detection accuracy for stealthy low-rate attacks.

[8] Isabel Albandari Alsumayt, John Haggerty, and Ahmad Lotfi (2018) evaluated the Monitoring, Detection, and Rehabilitation (MrDR) method for detecting DoS attacks in Mobile Ad Hoc Networks (MANETs). The trust-based approach was compared with the Trust Enhanced Anonymous On-demand Routing Protocol (TEAP), showing improved packet delivery ratio and reduced network overhead.

[9] Wei Wei, Feng Chen, Yingjie Xia, and Guang Jin (2013) introduced a Rank Correlation-based Detection (RCD) algorithm to detect Distributed Reflection DoS (DRDoS) attacks. The method analyzes correlations among multiple traffic flows, enabling protocol-independent detection and effective differentiation between malicious and legitimate traffic

[10] Wang Zhe, Cheng Wei, and Li Chunlin (2020) proposed a machine learning-based DoS attack detection model for smart grids. The approach uses Principal Component Analysis (PCA) for feature reduction and Support Vector Machine (SVM) for classification, achieving high accuracy and improving real-time detection of cyber threats in smart grid systems.

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.

OBJECTIVE

- To develop a system that can detect and classify different types of cyber attacks using Machine Learning techniques.
- To apply Post Quantum Cryptography (PQC) to secure data and communication against future quantum-based attacks.
- To combine Machine Learning (ML) and PQC for creating a smart and secure cyber de fense framework.
- Toimprove the accuracy and speed of detecting threats like DDoS, Botnet, Data Theft, and Backdoor attacks.
- To ensure data confidentiality, integrity, and authenticity even in post-quantum environ ments. • To design a system that can adapt to new or unknown types of attacks automatically.
- To build a future-proof cybersecurity model that provides reliable protection for organiza tions and network infrastructures.

PROBLEM DEFINATIONS

With the rapid growth of digital technology, cyber- attacks are becoming more frequent, complex, and harder to detect. Traditional security systems, such as firewalls and signature based intrusion detection, are limited because they can only identify known threats and often fail to detect new or evolving attacks. Moreover, the arrival of quantum computing poses a

major challenge, as it can break most existing cryptographic methods, making sensitive data vulnerable to future attacks. Therefore, there is a strong need for a smart and secure cybersecurity system that can not only detect multiple types of attacks using Machine Learning (ML) but also protect data from quantum-level threats using Post Quantum Cryptography (PQC). The goal is to build an intelligent and future-proof system that ensures real- time threat detection, data integrity, and long-term security in modern network environments.

IV SYSTEM ARCHITECTURE

The diagram represents the overall working flow of the system, showing how user input is processed and how cyber attacks (DoS) are detected using Machine Learning along with security enhancement using Post-Quantum Cryptography (PQC).

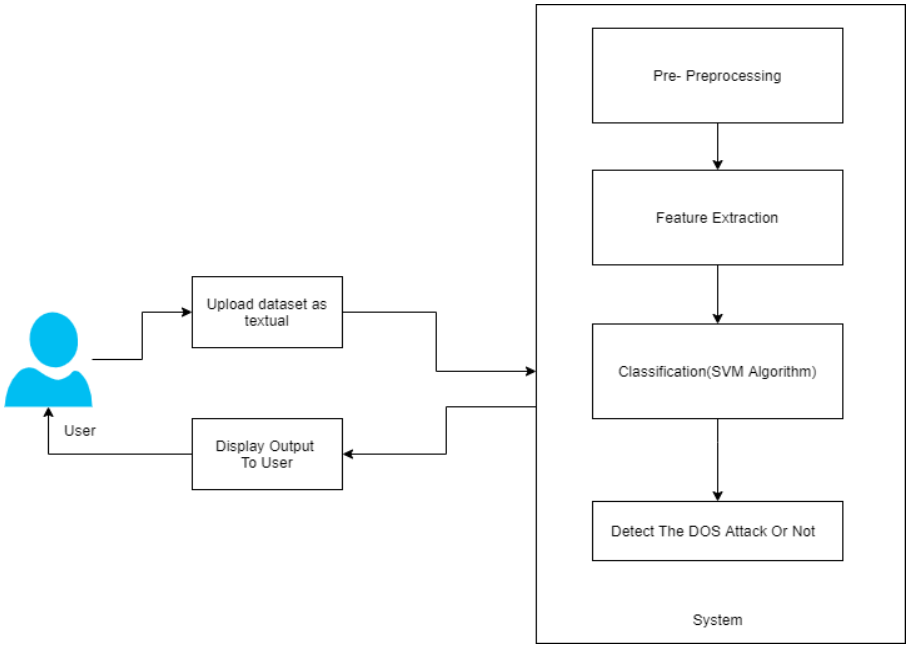

Fig 1. System Architecture.

1. User Input

The process starts with the user.The user uploads a dataset (text/CSV format) containing network traffic data.This dataset includes both normal and malicious (attack) data.

2. Upload Dataset

The uploaded dataset is sent to the system for processing.This acts as the input layer for the detection model.

3. Pre-Processing

The system performs data cleaning: Removes missing values. Eliminates duplicate data.

Normalizes the dataset.This step ensures the data is accurate and suitable for machine learning.

4. Feature Extraction

Important features are extracted such as:

Packet size

Protocol type

Time duration

Traffic behavior

These features help in identifying patterns of cyber attacks.

5. Classification (SVM Algorithm)

- The processed data is passed to the Support Vector Machine (SVM) model.
- The SVM classifier:

-Learns from training data

-Classifies input as Normal Traffic or Attack

6. DoS Attack Detection

- Based on classification:

The system determines whether the traffic is:

- Normal
- DoS Attack

This is the core detection module of your project.

7. Output to User

- The result is displayed to the user:
  - "Attack Detected" OR
  - "Normal Traffic"

ALGORITHM

Support Vector Machine

Support Vector Machine (SVM) is a supervised machine learning algorithm widely used for classification and regression tasks. It is particularly effective for high dimensional data and is commonly applied in mental health prediction systems due to its strong generalization capability and robustness.

Supervised Learning:

Support Vector Machine is a supervised learning technique, which means it learns from labeled training data. The algorithm uses input features along with known output labels to build a predictive model capable of classifying new, unseen data.

Hyperplane Concept:

SVM works by finding an optimal hyperplane that separates data points of different classes in a feature space. The goal is to maximize the margin between the classes, where the margin is the distance between the hyperplane and the nearest data points from each class.

Support Vectors:

Support vectors are the data points that lie closest to the decision boundary (hyperplane). These points play a crucial role in defining the position and orientation of the hyperplane. Removing other points does not affect the decision boundary as long as the support vectors remain unchanged.

Kernel Function: SVM uses kernel functions to handle non-linear data by transforming it into a higher- dimensional space. Common kernel functions include linear, polynomial, and radial basis function (RBF). Kernel functions enable SVM to effectively classify complex and non-linearly separable data.

Classification Mechanism:

For classification tasks, SVM assigns a class label to a data point based on which side of the hyperplane it lies. The decision is made using a mathematical function derived during the training process.

The working process of the Support Vector Machine can be explained in the following steps and diagram: Step-1: Collect and preprocess the mental health dataset. Step-2: Select relevant features influencing mental health prediction.

Step-3: Choose an appropriate kernel function for the SVM model.

Step-4: Train the SVM model using labeled training data.

Step-5: Construct the optimal hyperplane.

Step-6: Test the trained model using unseen data to evaluate performance.

Step-7: Use the trained SVM model to predict the mental health status of new input data.

Figure 2. User Registration.

Figure 3.Output of proposed System.

Advantages

1. Provides high accuracy in detecting cyber attacks using Machine Learning (SVM)
2. Detects multiple types of attacks like DoS, DDoS, Botnet, etc.
3. Ensures future security using Post-Quantum Cryptography (quantum-resistant)
4. Works in real-time detection of network threats
5. Reduces false positives and false alarms
6. Scalable system – can handle large datasets and networks
7. Combines intelligent detection + strong encryption

APPLICATIONS

1. Network Security Systems (IDS/IPS)
2. Cloud Computing Security
3. Banking and Financial Systems
4. Government and Defense Networks
5. IoT (Internet of Things) Security
6. Smart Grid and Smart City Security
7. E-commerce and Online Platforms

CONCLUSION

The proposed system for Multi-Type Network Attack Detection using Support Vector Ma chine (SVM) with Post-Quantum Cryptography (PQC) integration demonstrates an effective ap proach to securing network infrastructures against a broad spectrum of cyber threats. Through systematic phases ˆa ranging from data collection and preprocessing to feature extraction, classification, and PQC-based encryption framework achieves both intelligent threat detection and resilient data security. The SVM classifier successfully distinguishes between various network traffic types, identifying attacks such as DDoS, Botnet, Data Theft, and Backdoor intrusions with high accuracy. By incorporating post-quantum encryption mechanisms, the system ensures that both communication channels and stored model data remain secure even in the face of emerg ing quantum-computing threats. The structured project plan, as reflected in the timeline, enabled smooth progression through each phase data preparation, model training, system integration, and testing a culminating in a robust and secure network monitoring solution. Overall, this work con tributes to the development of future-proof cybersecurity systems by combining machine learning intelligence with quantum- resistant cryptography, paving the way for scalable and secure real world deployments in smart networks and critical infrastructure environments.

REFERENCES

1. S. RoselinMary, M. Maheshwari, and M. Thamaraiselvan, Early Detection of DOS Attacks in VANETUsing Attacked Packet Detection Algorithm (APDA), 2013.
2. F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, IoT DoS and DDoSAttack Detection using ResNet, 2021.
3. F. M. T. Kurniawan, S. Y. A. Mohammed, and A. M. Abdelrahman, Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking

Approach and Intrusion Detection System, 2020.

4. X.-G. Guo, X. Fan, J.-L. Wang, and J. H. Park, Event-triggered Switching-type Fault Detection and Isolation for Fuzzy Control Systems under DoS Attacks, 2020.
5. M. Ahmed, Thwarting DoS Attacks: A Framework for Detection based on Collective Anomalies and Clustering, 2017.
6. S. Usman and I. Winarno, Implementation of SDN-based IDS to Protect Virtualization Server against HTTP DoS Attacks, 2020.
7. X. Wu, D. Tang, L. Tang, J. Man, S. Zhan, and Q. Liu, A Low-Rate DoS Attack Detection Method Based on Hilbert Spectrum and Correlation, 2018.
8. I. A. Alsumayt, J. Haggerty, and A. Lotf, Evaluation of Detection Method to Mitigate DoS Attacks in MANETs, 2018.
9. W. Wei, F. Chen, Y. Xia, and G. Jin, A Rank Correlation Based Detection against Distributed Reflection DoS Attacks, 2013.
10. Z. Wang, W. Cheng, and C. Li, DoS Attack Detection Model of Smart Grid Based on Machine Learning Method, 2020.