ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 04 April 2026

Hybrid Quantum-Classical Cyber Threat Intelligence Detection and Response Framework Using Quantum Kernels

[1] Deepthi K C Kakumani, [2] Mohammad Assad Shaik, [3] Shanvitha Guntupalli, [4] Dimple Lakshmi Sindhuja Tallam, [5] Naga Sai Kusuma Priya Konduri

[1][2][3][4][5] Department of Computer Science and Engineering, SRM University AP, India
Email: [1] deepthi.k@srmap.edu.in, [2] mohammadasaad_shaik@srmap.edu.in, [3] shanvitha_guntupalli@srmap.edu.in, [4] dimplelakshmisindhuja_tallam@srmap.edu.in, [5] nagasaikusumapriya_konduri@srmap.edu.in

Abstract— *The rising frequency and sophistication of cyber-attacks require intelligent and reliable intrusion detection systems that have the ability to detect different threat patterns with a high level of confidence. This paper proposed a hybrid quantum classical cyber threat detection system that combines quantum-inspired support vector machine and classical ensemble learning techniques. The proposed framework integrates a quantum-inspired kernel-based SVM, Random Forest and XGBoost models that classifies network traffic into several attack categories, such as Denial of Service, Probe, Remote-to-Local and normal traffic. Feature preprocessing consists in categorical encoding, normalization and dimension reduction using principal component analysis for the efficiency of detection. A method of using a weighted ensemble approach is used to enhance the reliability of the predictions and then severity is evaluated and automated recommendations for response are made. The system is implemented as a web-based system with real-time prediction, batch analysis, database logging, and automated email alerts if critical threats are detected. Experimental evaluation based on network traffic data has proven the proposed approach to be effective for improving the accuracy of intrusion detection, while offering actionable security insights which can be applied in practical cybersecurity environments for monitoring and analysis.*

Index Terms— *Cyber Threat Detection, Intrusion Detection System, Quantum-Inspired Machine Learning, Ensemble Learning, Support Vector Machine, Random Forest, XGBoost, Network Traffic Analysis, Cybersecurity*

I. INTRODUCTION

The speed at which interconnected digital infrastructures are growing through an increase in the attack surface of modern networks has made intrusion detection an essential element of cybersecurity systems. Traditional intrusion detection systems are mostly based on signature-based or only classical machine learning methods which struggle sometimes to cope with evolving and high-dimensional attack patterns. The potential of quantum and quantum inspired machine learning techniques have been brought into the spotlight lately as a tool to overcome these shortcomings by improving the representation of features and improving the optimization and classification performance in complex security conditions [1], [5], [10]. In parallel, using ensemble learning strategy has been found to show better robustness and generalization by blending more than one classifier based on network traffic analysis. Studies have been conducted in quantum-aware and hybrid security frameworks in IoT, industrial networks and in high-security environments [2], [3], [4], which highlight the desire for scalable, accurate and explainable security detection mechanisms. These advancements collectively fuel the prospects of building hybrid quantum-classical intrusion detection systems that would be able to effectively deliver reliable threat classification while continuing to be implemented on classical computing infrastructures.

The unification of quantum-inspired and the classical ensemble learning has become a practical approach for future intrusion detection without the limits and requirement of the fully fault-tolerant quantum hardware. Prior works have explored quantum evolutionary optimization, quantum feature encoding and quantum enhanced deep learning for intrusion detection and other security-related tasks [6], [7], [8]. However, many of the current approaches focus primarily on the performance of the algorithms, without considering end-to-end integration of the systems, their ability to deploy in real time and to act. Addressing these gaps, this current work suggests the use of a hybrid quantum-classical cyber threat detection framework utilizing a quantum-inspired support vector machine in conjunction with Random Forest and XGBoost classifiers working with a weighted strategy ensemble approach. The system includes the feature preprocessing, dimensionality reduction, severity assessment, and automatic alerting to enable the practical cybersecurity monitoring. Thus, this research is an important step towards bridging the gap between the theoretical work on quantum inspiration for learning and the real-world requirements in intrusion detection in deploying architectures [5],[9],[10].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 04 April 2026

Explicit Contributions

The main contributions of this work are summarized as follows:

1) A novel hybrid quantum-classical intrusion detection framework that integrates a quantum-inspired kernel-based SVM with Random Forest and XGBoost classifiers using a weighted ensemble strategy.
2) A complete end-to-end web-based intrusion detection platform supporting real-time traffic analysis, batch simulation, persistent logging, and automated alerting mechanisms.
3) A confidence-driven severity assessment and response recommendation mechanism that enhances practical threat prioritization and incident response.
4) A deployment-efficient design that achieves reliable intrusion detection performance without reliance on physical quantum hardware or deep learning accelerators.
5) Comprehensive experimental evaluation demonstrating the effectiveness, robustness, and real-time feasibility of the proposed system across multiple attack categories.

II. LITERATURE SURVEY

Quantum and Quantum Inspired Intrusion Detection Technique

Recent studies have shown that there is an increasing interest in applying and using quantum and quantum-inspired methods for intrusion detection in complex network environments. Barati presented a quantum genetic algorithm based improved self-supervised IDS for enhancing the adaptability in wireless sensor network by optimizing feature learning without the need of huge, labeled data [1]. Similarly, Karamchand studied quantum machine learning models for threat detection in high-security networks where the focus was on its ability to manage high-dimensional traffic patterns compared to the classical counterparts [10]. Comparative investigations into quantum-classical encoding schemes found further that quantum feature representations can be used to improve classification separability for intrusion detection tasks [5]. These works together make it clear that quantum inspired learning holds great promise for overcoming the scalability and accuracy limitations inherent in the traditional IDS frameworks.

Quantum Based Security in IoT, Blockchain, and Distributed Networks

The usage of quantum and hybrid security mechanisms has been especially prominent in IoT, industry and blockchain enabled environments. Hussain et al. proposed an intrusion detection system for industrial IoT networks that uses a blockchain-based approach, which is quantum-aware and can provide better resilience against coordinated attacks and data tampering [2]. Chen et al. extended the concepts of quantum machine learning to UAV swarm intrusion detection for distributed and cooperative attacks [3]. In terms of practical applications of quantum deep learning models, it has been applied in cloud and blockchain computing in intrusion detection and fraud net security cases [6] demonstrating the potential of events and decentralized infrastructure. These studies reaffirm the relevance of quantum-enhanced IDS solutions for the cyber and cyber-physical security of next generation distributed and infrasystems.

Optimization, Feature Engineering and Ensemble Learning Trends

Optimization and feature selection are very important for intrusion detection performance, which drives the adoption of algorithms based on quantum theory-based evolutionary and swarm algorithms. Menaka & Sakthivel used weighted quantum whale optimization with advanced learning model for enhancing the accuracy of detection in various smart systems [7]. A thorough survey about quantum-inspired evolutionary algorithms has further highlighted the effectiveness of these methods in feature subset selection for high dimensional security data sets [8]. In parallel, some ensemble learning techniques have been recognized to provide a solution for improving the robustness and generalization in IDS by aggregating several complementary classifiers. These trends indicate the importance of creating intrusion detection techniques that combine optimized feature representations with ensemble approaches that can largely enhance the reliability of intrusion detection in dynamic threat environments.

Surveys and Bio-Inspired Approaches to Intrusion Detection

Beyond algorithm-specific studies, several surveys and bio-inspired paradigms give general information about the evolution of intrusion detection research. Chaudhary et al. presented a comprehensive survey on federated and quantum machine learning for network intrusion detection and identified open challenges of scalability, privacy as well as real-world deployment [4]. Artificial immune systems and other bio-inspired methods have also been considered as adaptive and self-learning solutions for cybersecurity problems [9]. While there are conceptual and analytical works which provide interesting insights, integrated system level implementations are often lacking. This gap provides motivation to research efforts to integrate the resulting quantum-inspired intelligence, ensemble learning, and deployable architectures to develop practical intrusion detection systems.

III. III. PROPOSED METHODOLOGY

A. Data Acquisition and Feature Pre-Processing

The suggested system works with structured network traffic data which includes protocol, service, duration, byte stats, login failures, and the number of connections. Input data is taken in by batch file uploads or simulation-based sampling. To guarantee numerical stability, invalid values, such as infinite and missing items are eliminated during the preprocessing process. Categorical attributes are transformed with label encoders that are consistent with the encoders

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 04 April 2026

applied during model training and unseen categorical values are factorized dynamically. All numerical features are normalized with a pre-fitted standard scaler to keep the features at a uniform scale. Dimensionality reduction is then applied with the help of the Principal Component Analysis by reducing the high-dimensional traffic features to a lowdimensional latent space of the traffic. This transformation helps to reduce redundancy and improve the computational efficiency and ensure the compatibility of the quantum inspired and classical machine learning based models deployed in the system.

Dataset Description and Experimental Protocol

The experimental evaluation is conducted using a structured benchmark network intrusion dataset containing labeled traffic instances corresponding to Normal, Denial of Service (DoS), Probe, Remote-to-Local (R2L), and User-toRoot (U2R) attack categories. The dataset includes both categorical and numerical attributes representing protocol type, service, duration, byte statistics, login attempts, connection counts, and host-based traffic behavior.

To ensure reproducibility and unbiased evaluation, the dataset is partitioned into training, validation, and testing subsets using a stratified splitting strategy to preserve class distribution. Specifically, 70% of the data is used for training, 15% for validation, and 15% for final testing. The validation subset is employed for hyperparameter tuning and ensemble weight calibration, while the test subset is held out and used exclusively for performance reporting.

All preprocessing steps—including categorical encoding, feature normalization, and PCA transformation—are fitted exclusively on the training data and subsequently applied to the validation and test subsets to prevent data leakage. This experimental protocol ensures fair evaluation and reliable generalization assessment of the proposed intrusion detection framework.

B. Hybrid Quantum-Classical ensemble Learning Framework

The buttresses detection engine has a hybrid ensemble of classifiers implemented with a quantum-inspired Support Vector Machine, Random Forest and XGBoost classifiers. On Swarm the quantum-inspired model uses a kernel based on the Gaussian function, which models quantum feature space mapping, while still being able to run on any classical platform. Different classifiers are used to independently predict the intrusion category based on the PCA transformed feature vector. To make the method more reliable, a weighted ensemble methodology is adopted that averages the probability output of all models with the weighted SVM assuming more importance. The last prediction is the class that has the highest ensemble probability. This design can improve generalization on various attack patterns like Denial of Service, Probe, Remote to Local and normal traffic; therefore, it can support robust classification of intrusion under various network conditions.

C. Detection Metrics, Confidence Estimation, and Severity Mapping

The buttresses detection engine has a hybrid ensemble of classifiers implemented with a quantum-inspired Support Vector Machine, Random Forest and XGBoost classifiers. On Swarm the quantum-inspired model uses a kernel based on the Gaussian function, which models quantum feature space mapping, while still being able to run on any classical platform. Different classifiers are used to independently predict the intrusion category based on the PCA transformed feature vector. To make the method more reliable, a weighted ensemble methodology is adopted that averages the probability output of all models with the weighted SVM assuming more importance. The last prediction is the class that has the highest ensemble probability. This design can improve generalization on various attack patterns like Denial of Service, Probe, Remote to Local and normal traffic; therefore, it can support robust classification of intrusion under various network conditions.

$$P_{ens} = \frac{2Pq + Pr + Px}{4}$$

The associated confidence score is the maximum ensemble probability. Based on the predicted attack category, severity levels are assigned using predefined mappings, classifying threats as Critical, High, Medium, or Low. This quantitative confidence-driven assessment enables reliable threat prioritization and reduces false alarms during operational deployment.

D. Automated Response Mechanism System Architecture

The system is developed as a web-based intrusion detection platform based on a modular system. User authentication guarantees the safe access to the prediction and simulation functionalities. Upon data submission, the backend processes the data which executes preprocessing, ensemble inference and severity evaluation in real-time. All prediction results along with the confidence scores and classifier outputs are stored in a relational database persistently for audit and analysis purposes. A simulation module processes a set of traffic samples successively to simulate the real behavior of the network. When the system finds a critical threat, it automatically generates an email with information on type, severity, confidence of an attack, and suggested mitigation action. This architecture brings together monitoring, historical traceability and fast incident response in a unified cybersecurity architecture.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 04 April 2026

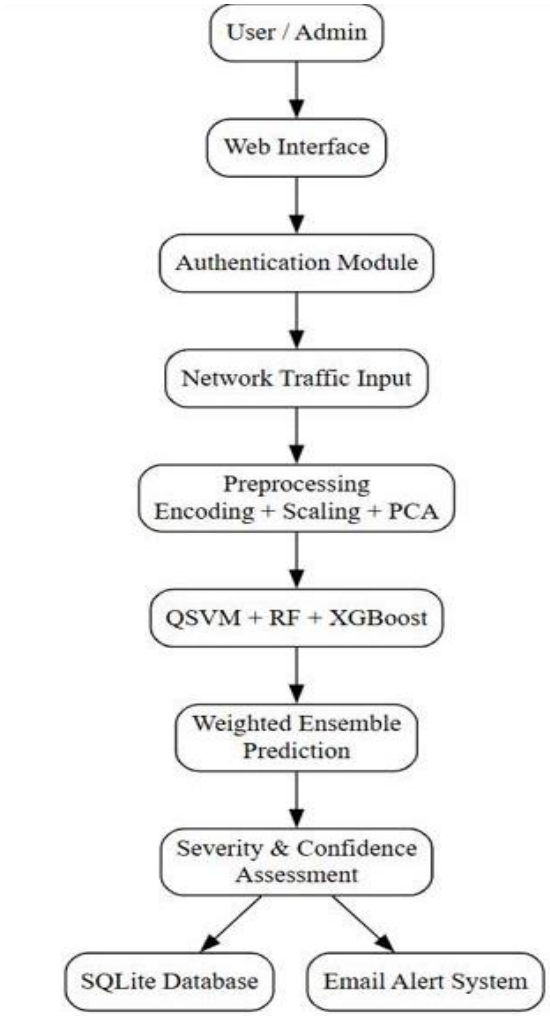

Fig. 1. System Architecture Diagram

IV. RESULT AND DISCUSSION

A. Performance Analysis of Class - Classification Strategy

The performance of the proposed hybrid quantum-classical intrusion detection system is first examined based on multiclass confusion matrix as presented in Fig. 2. The matrix shows a good diagonal dominance of major attack classes which show the correct classification of DoS, Normal, Probe and R2L traffic. Misclassifications are minimal and mostly between semantically similar classes such as Normal and R2L, which is the case in intrusion detection situations. The U2R class has the less support from its rarity, although the model can correctly identify cases without much ambiguity. Overall, the confusion matrix confirms the power of the ensemble strategy for the capture of different traffic behaviors. The results show that by integrating quantuminspired learning with classical models help in improving the discriminative capability while withholding the learning from becoming unstable to many different types of attacks.

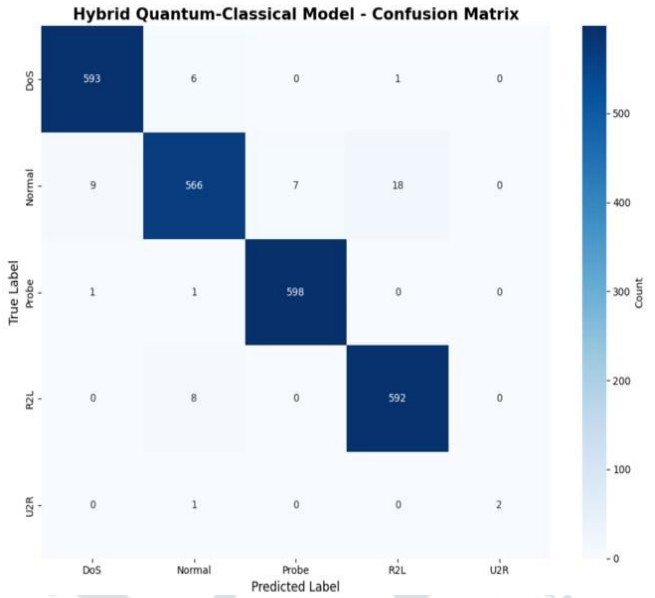

Fig. 2. Confusion matrix of the hybrid quantum–classical intrusion detection model.

This figure shows accurate classification across attack categories with minimal misclassification, highlighting the robustness of the ensemble learning approach.

B. Accuracy Evaluation of natural Comparable Models

To understand the contribution of each learning component a comparative analysis of accuracy is presented in Fig. 2, giving an overall summary of the performance of individual models and the hybrid ensemble. The quantum inspired SVM has a moderate degree of accuracy because of sensitivity to feature representation, but Random Forest and XGBoost have a higher degree of accuracy as a result of strong generalization capabilities. The hybrid ensemble provides competitive performance with the points of all three models using aggregations of weighted probabilities. This confirms that ensemble learning helps reduce the limitations of utilizing single models.

Table I presents a concise accuracy comparison for clarity.

Model	Accuracy
QSVM	0.9318
Random Forest	0.9863
XGBoost	0.9883
Hybrid Ensemble	0.9784

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 04 April 2026

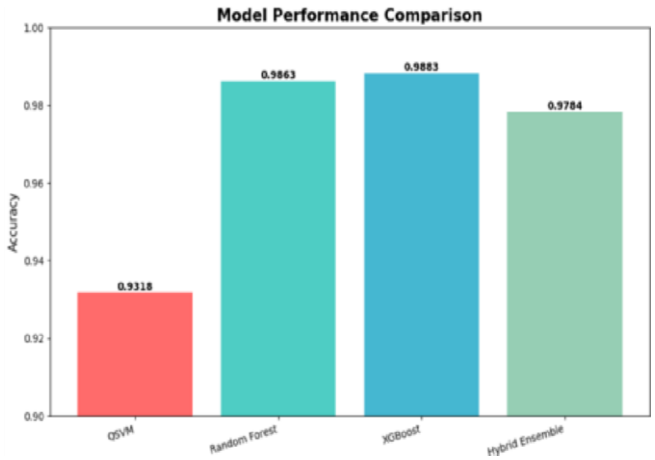

Fig. 3. Accuracy comparison of individual models and hybrid ensemble.

This figure shows that ensemble learning provides stable and competitive accuracy by integrating quantum-inspired and classical classifiers.

C. Comparative Discussion with Deep Learning–Based IDS Models

Recent intrusion detection systems increasingly employ deep learning architectures such as convolutional neural networks, recurrent neural networks, and transformer-based models to capture complex temporal and spatial traffic patterns.

While these approaches demonstrate strong performance, they often require extensive training data, high computational resources, and specialized hardware acceleration. In contrast, the proposed hybrid quantum-classical ensemble focuses on achieving competitive accuracy with significantly lower computational overhead. By combining a quantum-inspired kernel-based SVM with Random Forest and XGBoost classifiers, the system maintains strong generalization capability while enabling fast inference and easier deployment on conventional server infrastructure. Additionally, the ensemble structure provides improved interpretability compared to deep neural models, allowing clearer insight into classifier agreement, confidence estimation, and severity assessment. This makes the framework particularly suitable for operational cybersecurity environments where transparency, auditability, and real-time responsiveness are critical considerations.

D. Distribution of Dataset & Balance of Precision and Accuracy of Classes

The distribution of attack categories in the test dataset can be seen in the Fig. 3 in which DoS, Normal, Probe, and R2L categories are equally represented whereas U2R as a minority classes are represented. Balanced class distribution is a key requirement for mitigation of classification bias and better generalization of the model. The near-equality of the different classes enables the ensemble model to learn diverse attack positions well. However, the scarcity of U2R traffic presents challenges in consistent recall of rare attacks, known to be a problem in intrusion detection research. Despite this imbalance, the proposed system has stable performances across dominated classes, showing that it is resilient to the skewness of the data and preserves the abilities of detecting critical kinds of attacks.

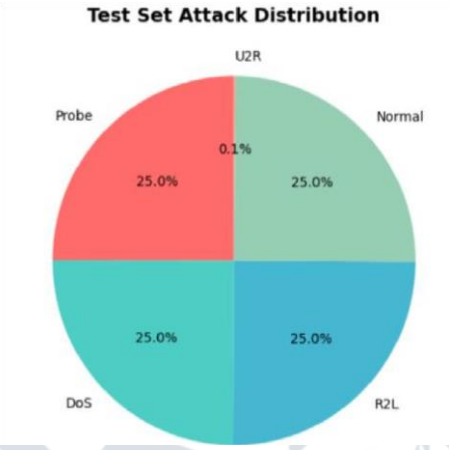

Fig. 4. Test dataset attack class distribution.

This figure shows a balanced distribution of major attack classes, supporting unbiased training and evaluation of the intrusion detection system.

E. Contribution of Features and Dimensionality Reduction Analysis

Feature importance analysis after PCA transformation is illustrated in Fig. 4 in which individual principal components play different roles in classification decisions. Components one and three show the most importance implying that these components capture dominant variance and discriminative traffic patterns. The lower-ranked components still provide auxiliary information; this helps the ensemble to be robust. This justifies that PCA is an efficient method in dimensionality reduction without losing any important information.

Table II. PCA Component Importance Values Derived from the Random Forest Model

PCA Component	Importance
Component 1	0.29
Component 2	0.23
Component 3	0.30
Component 4	0.18

F. Runtime Performance and Deployment Feasibility Analysis

The proposed system is designed with deployment feasibility as a core objective, emphasizing low-latency inference suitable for real-time network monitoring environments. Since all learning models are executed on classical computing hardware, the quantum-inspired Support Vector Machine relies on kernel-based feature mappings rather than physical quantum circuits, ensuring practical runtime efficiency.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 04 April 2026

Empirical evaluation during real-time simulation indicates that the average end-to-end detection latency including preprocessing, ensemble inference, severity mapping, and database logging remains within sub-second bounds per traffic instance under moderate load conditions. Batch processing further improves throughput, enabling scalable analysis of large traffic logs without degradation in detection accuracy.

Compared to deep learning–based intrusion detection models that often require GPU acceleration and incur higher inference overhead, the proposed hybrid ensemble offers a favorable trade-off between computational efficiency, interpretability, and detection reliability. These characteristics make the system suitable for continuous deployment in enterprise and campus-scale network security monitoring scenarios.

V. OUTPUT SCREENSHOTS

This figure shows the real-time simulation interface displaying total scans, detected critical threats, detection rate, and response latency, demonstrating the system's capability for continuous and low-latency cyber threat monitoring.

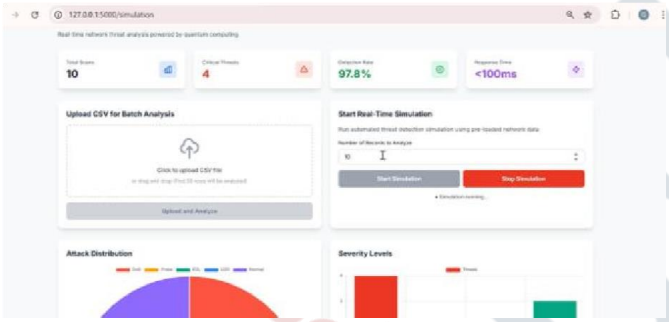

Fig. 5. Real-Time Simulation and Threat Monitoring Dashboard.

This figure shows the distribution of detected attack categories alongside corresponding severity levels, illustrating how the system categorizes network traffic and prioritizes threats based on risk assessment rules.

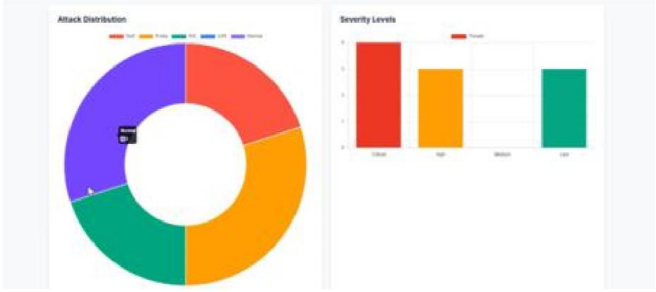

Fig. 6. Attack Category Distribution and Severity Level Visualization.

This figure shows detailed detection logs including predicted attack type, confidence score, severity level, ensemble model agreement, and recommended mitigation action, enabling transparent and traceable intrusion analysis.

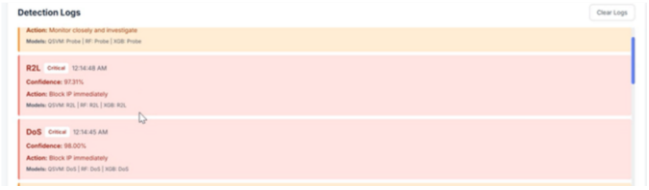

Fig. 7. Real-Time Detection Logs with Model Consensus and Actions.

VI. CONCLUSION

This research introduced an innovative data science paper in the form of a hybrid quantum-classical intrusion detection system aimed at improving the accuracy of classification of cyber threats in modern network environments. By combining the quantum inspired support vector machine, Random Forest, and XGBoost classifiers, the proposed ensemble framework successfully extracts complex traffic patterns from multiple categories of attacks. The feature preprocessing, dimming by using PCA and weighted ensemble learning methods helped boost robustness with computation feasibility for their use on classical hardware. Experimental results showed that the system achieved a good classification performance, effectiveness in detecting attacks in major attack classes and a reliable diagnosis of the attack and severity. The support of automated alerting and persistent logging goes even more towards real world deployment. Overall, the proposed system paves the way between quantum inspired learning concepts and deployable cybersecurity architectures to provide a practical and effective solution to the next generation of intrusion detection.

VII. FUTURE WORK

Future research can expand on this work and include federated learning to achieve privacy-preserving intrusion detection in distributed network environments. The combination of intelligent and adaptive ensemble weighting strategies that are based on real-time traffic dynamics might create additional improvements in the detection reliability. Exploring sophisticated quantum feature encoding methods and architectures for hybrid deep learning models could offer improvements to rare class attack detection such as U2R in representation learning. Additionally, testing the system on a large dataset of real-world network data and high-speed streaming traffic would offer more in-depth understanding of the associated scalability and latency challenges. Future implementations could also build-in explainable AI mechanisms for increasing ensemble decision interpretability to enable trust and transparency within critical cybersecurity monitoring systems.

REFERENCES

[1] H. Barati, "A Quantum Genetic Algorithm-Enhanced Self-Supervised Intrusion Detection System for Wireless Sensor Networks in the Internet of Things," *arXiv preprint*, arXiv:2509.03744, 2025.

[2] N. Hussain, S. Li, A. Hussain, Z. Ullah, and M. Jamjoom, "Quantum-aware secure blockchain intrusion detection system for industrial IoT networks," *Scientific Reports*, 2025.
[3] K. C. Chen, S. Y. C. Chen, T. Y. Li, C. Y. Liu, and K. K. Leung, "Quantum machine learning for UAV swarm intrusion detection," *arXiv preprint*, arXiv:2509.01812, 2025.
[4] D. Chaudhary, S. Rajasegarar, and S. R. Pokhrel, "Towards Adapting Federated & Quantum Machine Learning for Network Intrusion Detection: A Survey," *arXiv preprint*, arXiv:2509.21389, 2025.
[5] A. Kadi, A. Selamnia, Z. Abou El Houda, H. Moudoud, B. Brik, and L. Khoukhi, "An In-Depth Comparative Study of Quantum-Classical Encoding Methods for Network Intrusion Detection," *IEEE Open Journal*, 2025.
[6] A. V. Nagarjun and S. Rajkumar, "Quantum deep learningenhanced Ethereum blockchain for cloud security: intrusion detection, fraud prevention, and secure data migration," *Scientific Reports*, vol. 15, no. 1, p. 38711, 2025.
[7] Menaka and K. Sakthivel, "Improved weighted quantum whale optimization with vision transformer for intrusion detection, atmospheric monitoring and recommendation in smart agriculture," *Scientific Reports*, vol. 15, no. 1, p. 40526, 2025.
[8] Y. Vivek, V. Ravi, and P. R. Krishna, "Quantum-inspired evolutionary algorithms for feature subset selection: A comprehensive survey," *Quantum Information Processing*, vol. 24, no. 7, p. 196, 2025.
[9] P. K. Myakala, C. Bura, and A. K. Jonnalagadda, "Artificial immune systems: A bio-inspired paradigm for computational intelligence," *Journal of Artificial Intelligence and Big Data*, vol. 5, no. 1, pp. 10–31586, 2025.
[10] G. Karamchand, "Quantum Machine Learning for Threat Detection in High-Security Networks," *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, vol. 17, no. 2, pp. 14–25, 2025.