iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2026 **Issue:** Conference **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82973

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com
National Conference on Innovation in Engineering and Technology-(NCIET2026)

Quantum-Resistant AI Model for Intrusion Detection

Avadhut Shivaji Patil[1], Mr. Vikas A Patil[2]
Computer Science and Engineering,Ashokrao Mane Group Of Institutions Vathar Tarf Vadgaon, India

Abstract: ***With the rapid growth of quantum computing technology, conventional encryption and cybersecurity methods have become vulnerable and require quantum-proof alternatives. Custom-made Intrusion Detection Systems (IDSs) should be designed to identify the presence of malicious actions within the network; however, most of them lack quantum-resistant capabilities. In this research, a quantum-resistant AI model is developed to detect intrusion in computer networks using post-quantum security combined with advanced machine learning and deep learning techniques. The proposed system emphasizes the importance of strong feature extraction, safe storage of data, and intelligent threat detection capabilities in order to provide protection against all types of threats, including both known and novel attacks. Through implementation of these methods, the adaptability and resiliency of intrusion detection will be enhanced to ensure effective operation in future quantum-enabled security networks.***

Index Terms: Intrusion Detection System (IDS), Quantum-Resistant Security, Post-Quantum Cryptography, Artificial Intelligence, Deep Learning, CNN–LSTM, Quantum Machine Learning, Cybersecurity, Zero-Day Attack Detection, Network Security

I. INTRODUCTION

The dynamics of digital technology and the widespread use of network systems have caused a great increase in the volume and intensity of cyber threats. One of the crucial components in today's cybersecurity systems is the Intrusion Detection System (IDS), which involves the active monitoring of network traffic and system activity in order to discover any malicious behavior. Traditional systems for intrusion detection, such as signature-based and rule-based approaches, are often limited in their ability to identify sophisticated or new types of cyber-attacks. As a result, significant attention is now being paid to AI-based models of intrusion detection.

On the other hand, quantum computing represents a revolution in computation power, and there is a real possibility that quantum systems could break widely used cryptographic algorithms such as RSA, ECC, and Diffie-Hellman. Quantum algorithms — specifically Shor's and Grover's algorithms — pose serious threats to the fundamental security mechanisms that ensure the privacy, integrity, and authenticity of data. Consequently, even existing cybersecurity systems, including AI-based IDS, will require redesigning to remain functional in the post-quantum era.

Artificial Intelligence techniques employing machine learning and deep learning have demonstrated strong performance in recognizing complex attack patterns by learning high-dimensional data from extensive networks. However, AI-enabled IDS systems rely on conventional security models and do not account for threats posed by attackers using quantum computing. This necessitates the development of novel AI models that leverage post-quantum security principles while retaining efficiency in real-time threat detection. The current project integrates quantum-resistant and AI-powered intrusion detection system models to improve their performance against future cybersecurity threats. The proposed concept provides a sustainable and forward-looking perspective for intrusion detection in next-generation networks through the use of a secure feature extraction process, a resilient learning architecture, and a quantum-resistant design. This research ultimately aims to create cybersecurity infrastructure capable of handling new attack vectors as well as challenges associated with quantum computing.

A. Key Contributions of the Research

1) Quantum-Resistant Intrusion Detection Framework: This study proposes a hybrid AI-based intrusion detection system integrated with post-quantum cryptographic techniques to ensure long-term security against quantum-enabled cyber threats.

2) Efficient Feature Extraction and Preprocessing: The system applies advanced preprocessing and feature selection methods to handle large-scale network traffic data, reducing computational complexity and improving detection efficiency.

©IJRASET: All Rights are Reserved

3) Hybrid AI Model for Accurate Detection: Multiple machine learning and deep learning algorithms — including CNN, LSTM, and ensemble methods — are utilized to accurately detect both known and zero-day cyber-attacks.
4) Integration of Post-Quantum Cryptography: The framework incorporates quantum-resistant algorithms such as Kyber and Dilithium to secure data transmission and enhance end-to-end system security.
5) Scalable and Real-Time Detection System: The proposed model is optimized for real-time performance, scalability, and deployment in resource-constrained and next-generation network environments.

II. LITERATURE REVIEW

A comprehensive review of prior studies on quantum-based intrusion detection systems was conducted to understand the state of the art and identify research gaps. The following summarizes the key contributions and limitations of relevant prior work.

1) Kumar et al. (2020) introduced a quantum-based intrusion detection system for IoT using the Quantum Support Vector Machine (QSVM). The authors aimed to improve cyber-attack detection performance by applying quantum computing concepts. While the approach led to comparatively high detection accuracy, notable drawbacks include reliance on quantum computer simulators, inability to handle large datasets, high computational costs, and difficulty implementing the method in practice due to the current immaturity of quantum computing technologies [1].
2) Nguyen et al. (2021) discussed an effective IDS strategy using deep learning designed for intrusion detection in the post-quantum era. The authors employed advanced deep learning algorithms including CNN and LSTM to enhance detection performance. A key highlight of this work is the development of a framework that integrates an AI-based IDS with post-quantum security concepts. Despite strong performance on benchmarked datasets, limitations include increased system complexity and limited evaluation against real quantum attacks [2].
3) Cirillo et al. (2022) proposed the implementation of a Hybrid Quantum Generative Adversarial Network (QGAN) for anomaly detection by integrating principles of quantum computing with classical machine learning. The study demonstrated impressive accuracy rates, suggesting better performance compared to classical algorithms. However, multiple constraints remain, including extremely high computational costs, the need for integrated quantum-classical hardware, instability of GAN training processes, and unsuitability for big data [3].
4) Chaudhary et al. (2023) conducted a detailed survey on federated learning and quantum machine learning in network intrusion detection. The study presents a taxonomy and comparative analysis of existing federated IDS methods with quantum computing, along with suggestions for future work. While the presented techniques provide higher precision and protect data privacy, limitations include high communication costs, delays in distributed learning, susceptibility to model poisoning attacks, and deployment challenges related to quantum computing [4].
5) Zhang et al. (2024) proposed a quantum-aware secure intrusion detection framework for Industrial IoT (IIoT), integrating deep learning models such as CNN–LSTM with post-quantum cryptographic techniques to enhance security against emerging quantum threats. The model achieved high detection accuracy on industrial network datasets. However, the system faces notable limitations including high computational complexity, increased training time, resource consumption, and challenges in deploying the framework in real-time and resource-constrained environments [5].
6) Kim et al. (2024) introduced an Intrusion Detection System based on quantum-inspired outlier analysis for anomaly detection. The core idea involves using quantum-based algorithms for outlier detection to improve detection accuracy. Limitations include high computational cost and practical impracticality [6].
7) Elsedimy et al. (2024) created a novel IDS combining the QSVM algorithm with enhanced grey wolf optimization. The work focuses on enhancing feature selection and classification through quantum learning. Despite achieving high classification accuracy, the hybrid model faces challenges such as dependency on quantum simulation, prolonged computation time, and scalability limitations [7].
8) Abreu et al. (2024) proposed QML-IDS, an intrusion detection system based on quantum machine learning. The concept highlights the advantages of a hybrid quantum-classical approach for improved attack detection. Drawbacks are associated with simulation-only environments and high implementation complexity [8].
9) Nalayini et al. (2025) introduced a novel adaptive transformer-based quantum intrusion detection system applicable to software-defined networks (SDN). The work incorporates transformer architecture and quantum concepts into the detection process to achieve efficient detection of new threats. The model's weaknesses include high computational cost, latency, and complexity of implementation [9].

10) Nagarjun et al. (2025) proposed a quantum deep learning-assisted blockchain-based intrusion detection system. The approach uses blockchain technology to ensure data security and quantum deep learning techniques to detect intrusions. Significant advantages include enhanced data security and integrity. Drawbacks are associated with system complexities and processing overheads [10].

11) Hussain et al. (2025) designed a quantum-enabled secure blockchain-based intrusion detection system for IIoT. The approach combines quantum security with blockchain and artificial intelligence for effective intrusion detection. Despite enhancing security and trustworthiness in IIoT networks, the proposed scheme faces challenges including expensive computation, scalability concerns, and complex implementation [11].

12) Cirillo et al. (2026) conducted a benchmarking study of quantum machine learning techniques for IDS in noisy quantum computing environments. The study provides a comprehensive analysis of the strengths and limitations of quantum-based IDS models. Limitations include reliance on noisy intermediate-scale quantum (NISQ) devices, limited availability of large-scale training data, and reduced applicability to current real-world systems [12].

TABLE I
Literature Survey of Quantum-Based Intrusion Detection Systems

Sr. No.	Author & Year	Algorithm Used	Cryptographic Technique	Limitations
1	Zhang et al. (2024)	CNN–LSTM	Lattice-based cryptography	High system complexity; increased training time; high resource consumption; difficult real-time deployment.
2	Chaudhary et al. (2023)	FL + QML	Secure aggregation + Post-quantum encryption	High communication overhead; latency issues; vulnerable to model poisoning attacks.
3	Cirillo & Esposito (2022)	Hybrid QGAN	Not explicitly defined	High computational cost; unstable training; limited scalability.
4	Nguyen et al. (2021)	AI-based IDS	PQ cryptographic pipelines	Limited real quantum attack evaluation; increased system complexity.
5	Kumar & Swarnkar (2020)	QSVM	Not explicitly used	Requires quantum hardware; scalability issues; high implementation cost.

A. Research Gaps

1) Existing studies mainly focus on quantum-enhanced or quantum-inspired models, with limited emphasis on true quantum-resistant AI-based intrusion detection frameworks.

2) Integration of post-quantum cryptographic mechanisms with AI-driven IDS is insufficient, leaving data transmission and model security vulnerable to quantum attacks.

3) Most approaches rely on benchmark datasets and lack validation against real-world and zero-day attack scenarios, reducing practical applicability.

4) Scalability and computational overhead of quantum or hybrid IDS models remain significant challenges for real-time and large-scale deployment.

5) There is an absence of standardized evaluation metrics to measure quantum resilience, robustness, and long-term security of IDS models.

6) Lightweight and explainable quantum-resistant IDS models suitable for edge and resource-constrained environments are largely unexplored.

B. Problem Statement

It is essential to create a quantum-resistant AI-based IDS that is efficient and scalable enough to address the constraints of existing cryptographic and AI-based IDS approaches, and to provide reliable detection of both known and emerging cyber-attacks in order to ensure the future quantum-resistant security of networks.

III. PROPOSED SYSTEM

To address the identified problem, the proposed system develops a hybrid quantum-resistant AI-based intrusion detection framework that integrates advanced machine learning models with post-quantum security mechanisms. The system employs efficient preprocessing and feature selection techniques to handle large-scale network traffic data, followed by the implementation of hybrid AI models — such as CNN–LSTM and ensemble methods — for accurate detection of both known and zero-day attacks.

To overcome the limitations of traditional systems, quantum-inspired algorithms are incorporated to enhance pattern recognition and improve the detection of complex attack behaviors. Additionally, post-quantum cryptographic techniques are integrated to ensure secure data transmission and protection against quantum-enabled threats. The model is further optimized for scalability, reduced computational complexity, and real-time performance, making it suitable for deployment in next-generation and resource-constrained network environments.

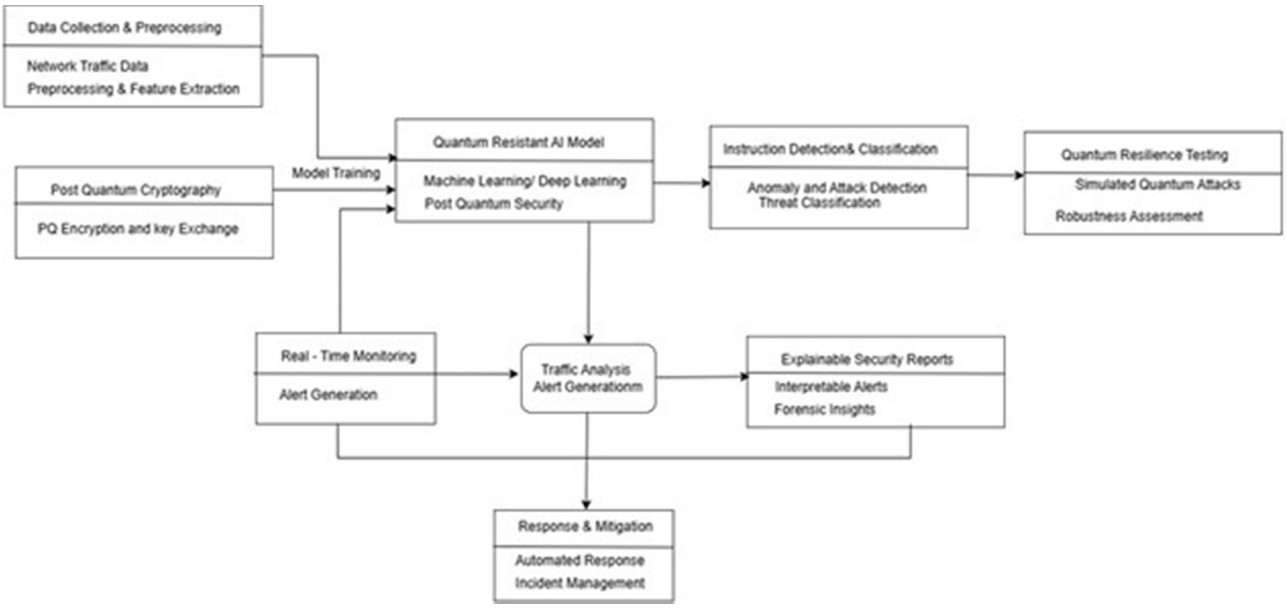


Fig.1.ProposedSystemArchitecture

Figure 1 represents the architecture of the proposed quantum-resistant AI-based intrusion detection system. Network traffic data is first collected and preprocessed. The data is then secured using post-quantum cryptographic techniques before being passed to a hybrid AI model for analysis. The system performs intrusion detection and classification to identify both normal and malicious activities, followed by real-time monitoring and traffic analysis to generate alerts. It also provides explainable security reports for better understanding of detected threats and initiates response and mitigation actions to handle attacks. Finally, the system undergoes quantum resilience testing to ensure robustness against future quantum-enabled threats.

The inputs for the proposed quantum-resistant AI-based IDS consist of raw network traffic data obtained through different sources, including packets, flows, and communication records. The characteristics included in the inputs are IP address, ports, protocol used, packet size, flow time, and connection statistics. Security parameters and encrypted streams of data using post-quantum cryptography algorithms are also considered as inputs. Preprocessing of input data is carried out to clean, normalize, and extract features to make it ready for processing by the AI model.

Output data consist of classification results and security reactions. The model decides whether the traffic is malicious or normal, and further determines the nature of the attack. In addition, the model issues real-time alerts in case of any intrusion, while providing insights in security reports that explain how the threats were handled.

The model also automates the reaction and mitigation process, which could include blocking of malicious connections. The results generated by the system also include the evaluation of robustness through quantum resilience testing, ensuring that the system remains secure in the event of any quantum-based attacks.

The proposed system adopts hybrid AI models such as CNN-LSTM, in addition to SVM, Random Forest, and anomaly detection algorithms. Quantum computing algorithms such as QSVM and post-quantum cryptographic algorithms including Kyber and Dilithium, together with symmetric algorithms like AES-256 and SHA-3, are used for security. The role of each cryptographic component is as follows:

1) Kyber: Used for secure key exchange; protects data communication from quantum attacks.
2) Dilithium: Used for digital signatures; ensures data authenticity and integrity.
3) SPHINCS+: Hash-based signature scheme; provides strong quantum-resistant authentication.
4) AES-256: Symmetric encryption; secures data during transmission with high security.
5) SHA-3: Hash function; ensures data integrity by generating unique hash values.

TABLE II
Algorithms Used in Proposed Quantum-Based IDS

Sr. No.	Module	Algorithms Used	Purpose
1	Data Preprocessing & Feature Extraction	PCA, Min-Max Normalization, TF-IDF	Data cleaning, normalization, and feature selection
2	AI-Based Intrusion Detection Model	CNN, LSTM, CNN–LSTM (Hybrid), Random Forest, SVM	Detect and classify normal and malicious network traffic
3	Anomaly Detection	Isolation Forest, One-Class SVM	Identify unknown and zero-day attacks
4	Quantum-Based Techniques	Quantum SVM (QSVM), Quantum Feature Mapping	Improve pattern recognition and classification accuracy
5	Post-Quantum Cryptography	Kyber, Dilithium	Secure data transmission and key exchange
6	Optimization & Ensemble	Gradient Boosting, Ensemble Learning	Improve accuracy and reduce false positives

A. Dataset Description

The proposed system utilizes multiple publicly available benchmark datasets to ensure robust evaluation across diverse network environments:

1) NSL-KDD: An improved version of the KDD Cup 1999 dataset, addressing redundancy issues and providing labeled records for normal and attack traffic.
2) CICIDS2017: Contains realistic modern network traffic with various attack types such as DDoS, brute force, and infiltration, suitable for evaluating real-world intrusion scenarios.
3) UNSW-NB15: Includes contemporary synthetic network traffic with diverse attack categories and rich feature sets.

TABLE III
Datasets for Quantum-Resistant AI-Based Intrusion Detection System

Dataset Type	Dataset Name	Access Link
Benchmark IDS Dataset	NSL-KDD Dataset	https://www.unb.ca/cic/datasets/nsl.html
Real-World Network Traffic	CICIDS2017 Dataset	https://www.unb.ca/cic/datasets/ids-2017.html
Modern Synthetic Dataset	UNSW-NB15 Dataset	https://research.unsw.edu.au/projects/unsw-nb15-dataset

B. Novelty of Research

1) Integration of AI with Post-Quantum Cryptography: The proposed system combines advanced AI models with quantum-resistant cryptographic algorithms such as Kyber and Dilithium to ensure end-to-end secure intrusion detection.

2) Quantum-Enhanced Detection Capability: Quantum-inspired techniques such as QSVM and quantum feature mapping are utilized to improve the detection of complex and zero-day cyber-attacks.

3) Hybrid AI Architecture: A novel hybrid model combining CNN–LSTM and ensemble learning methods is proposed to enhance detection accuracy and reduce false positives.

4) End-to-End Secure Framework: Unlike traditional intrusion detection systems, the proposed framework ensures both accurate intrusion detection and secure data transmission.

5) Scalable and Real-Time Design: The system is optimized for scalability and real-time performance, making it suitable for next-generation and resource-constrained environments.

6) Explainable and Robust System: Explainable AI techniques are incorporated to improve transparency, interpretability, and trust in intrusion detection decisions.

IV. CONCLUSION

This review highlights the growing importance of integrating artificial intelligence with quantum-resistant techniques for developing secure and future-ready intrusion detection systems. Existing approaches, including machine learning and deep learning-based IDS, have demonstrated strong capabilities in detecting known cyber-attacks; however, they face significant challenges such as high computational complexity, lack of scalability, limited detection of zero-day attacks, and absence of quantum-resilient security mechanisms.

Recent advancements in quantum computing pose serious threats to traditional cryptographic systems, emphasizing the need for post-quantum cryptography and quantum-aware security frameworks. The literature also reveals that while some studies have explored quantum machine learning and hybrid approaches, there remains a lack of fully integrated, efficient, and scalable solutions for real-world deployment.

Therefore, there is a critical need to develop a hybrid quantum-resistant AI-based intrusion detection system that combines robust detection capabilities with secure data transmission. Such systems must focus on improving accuracy, reducing false positives, ensuring real-time performance, and enhancing explainability. This review provides a foundation for future research in designing next-generation IDS that are resilient to both classical and quantum-enabled cyber threats.

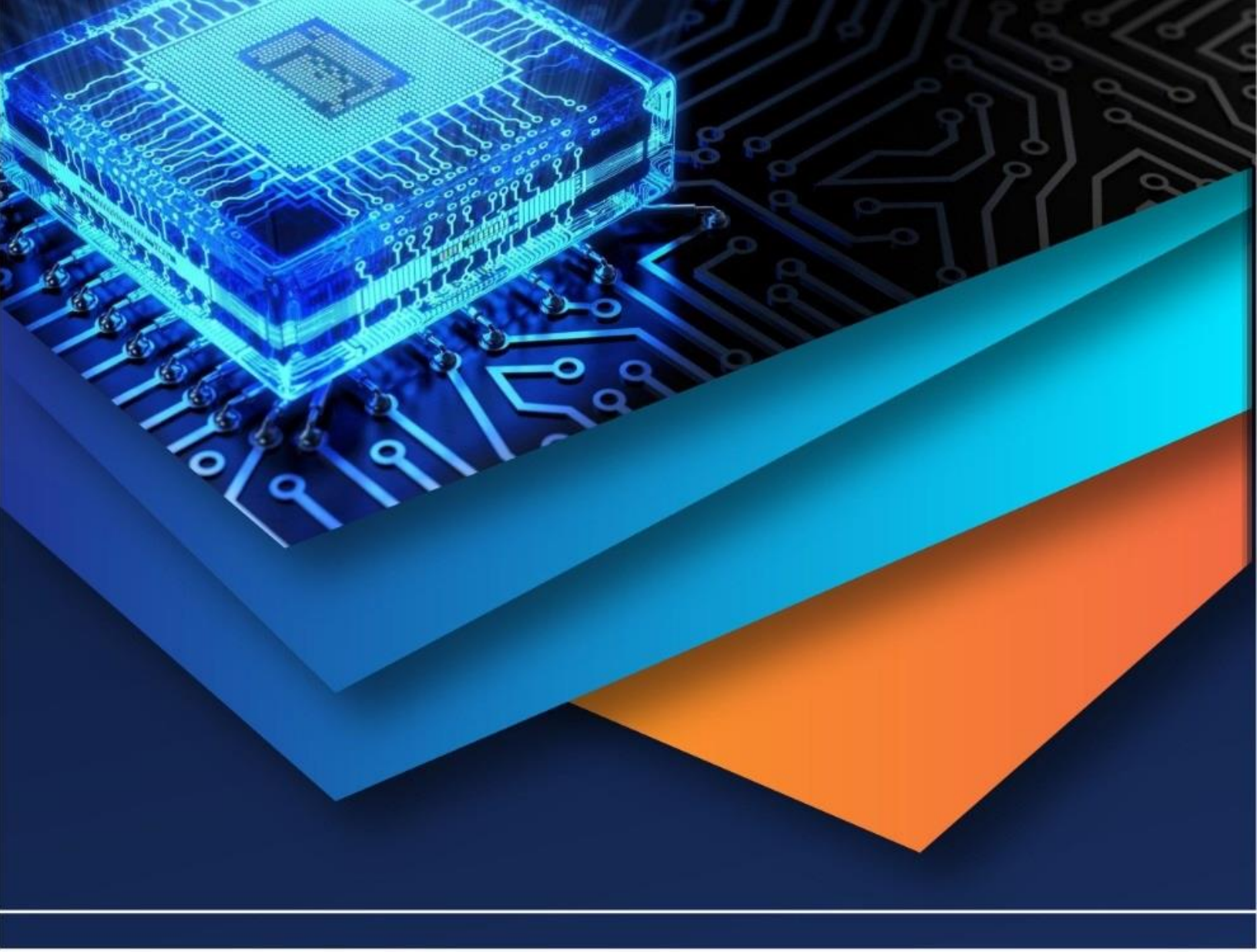
REFERENCES

[1] A. Kumar and R. Swarnkar, “Quantum-based intrusion detection system for IoT networks,” IEEE Internet of Things Journal, 2020.
[2] T. T. Nguyen et al., “Deep learning for cyber security: Preparing intrusion detection for the post-quantum era,” IEEE Access, 2021.
[3] A. Cirillo and C. Esposito, “Hybrid quantum generative adversarial networks for anomaly detection,” IEEE Transactions on Emerging Topics in Computing, 2022.
[4] R. Chaudhary et al., “Federated and quantum machine learning for network intrusion detection: A survey,” IEEE Communications Surveys & Tutorials, 2023.
[5] Y. Zhang et al., “Quantum-aware secure intrusion detection framework for industrial IoT,” IEEE Transactions on Industrial Informatics, 2024.
[6] T. H. Kim and S. Madhavi, “Quantum intrusion detection system using outlier analysis,” Scientific Reports, 2024.
[7] E. I. Elsedimy, H. Elhadidy, and S. M. M. Abohashish, “A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer,” Cluster Computing, 2024.
[8] D. Abreu, C. E. Rothenberg, and A. Abelem, “QML-IDS: Quantum machine learning intrusion detection system,” arXiv preprint arXiv: 2410.16308, 2024.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[9] C. M. Nalayini, T. R. Soumya, S. D. Lalitha, et al., "A novel adaptive transformer-based quantum intrusion detection system for software-defined networks," Scientific Reports, 2025.
[10] A. V. Nagarjun and S. Rajkumar, "Quantum deep learning-enhanced blockchain for cloud security: Intrusion detection and secure data migration," Scientific Reports, 2025.
[11] N. Hussain, S. Li, A. Hussain, et al., "Quantum-aware secure blockchain intrusion detection system for industrial IoT networks," Scientific Reports, 2025.
[12] F. Cirillo, C. Esposito, and J. T. Seo, "Benchmarking quantum machine learning methods for intrusion detection on noisy quantum computers," Quantum Machine Intelligence, 2026.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)