iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

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

DOI:

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, Mr.Vikas A Patil
Computer Science and Engineering ASHOKRAO MANE GROUP OF INSTITUTIONS Vathar Tarf Vadgaon, India

Abstract: ***Because of the rapid growth of quantum computing technology, conventional encryption and cyber security methods havebecomevulnerableandrequirequantum-proofalternatives. Custom-madeIDSsshouldbedesignedinordertoidentifythe presenceofmaliciousactionswithinthenetwork,butmostofthemlackquantum-resistantcapabilities.Inthisresearch, quantum-resistantAIwillbedevelopedinordertodetectintrusionincomputersusingpost-quantumsecuritycombined withnewmachinelearninganddeeplearningtechniques.The proposedsystememphasizesimportanceofstrongfeatureex-traction, safestorageof dataandintelligentthreatdetection capabilitiesinordertoprovideprotectionagainstanytypes ofthreats,including knownandnovelattacks. Itisexpected that through implementation of these methods, adaptability and resiliencyofintrusiondetectionwillbeenhancedandensure effectiveoperationinfuturequantum-enabledsecuritynetworks.***

IndexTerms: ***IntrusionDetectionSystem(IDS),Quantum-ResistantSecurity,Post-QuantumCryptography,ArtificialIntel-ligence, Deep Learning, CNN–LSTM, Quantum Machine Learn-ing,Cybersecurity,Zero-DayAttackDetection,NetworkSecurity***

I. INTRODUCTION

Thedynamicsofdigitaltechnologyandthewidespread use of network systems have caused a great increase in the volume and intensity of cyber threat levels. One of the crucial components in today's cyber security systems is the Intrusion DetectionSystem(IDS),whichinvolvestheactivemonitoring ofnetworktrafficandsystemactivityinordertodiscover anymaliciousbehavior.Sometraditionalsystemsforintrusion detection, such as signature-based and rule-based, are often limited regarding their ability to identify sophisticated or new types of cyber-attacks, so much attention is paid now to AI-based models of intrusion detection.

On the other hand, quantum computing is a revolution as faras computation power is concerned, and there is a possibility that these can crack the widely used cryptographic algorithms (RSA,ECC,andDiffie-Hellman)too.Thealgorithmsofquan-tum computing, specifically the Shor and Grover algorithms, can be considered threats to the fundamental security of the systems that ensure the privacy, integrity, and authenticity of data. Consequently, even the existing cybersecurity systems, including AI-IDSs, will require redesigning to make them functional in the post-quantum era.

ArtificialIntelligencetechniquesthatemploymachinelearning
algorithms and deep learning have been found to exhibit similar performance standards in recognizing complicated attack patterns through learning high dimensional data from extensivenetworks.However,AI-enabledIDSsystemsrelyon conventional security theories and do not account for threats posedbyattackersusingquantumcomputing.Thisnecessitates the development of novel AI models that utilize post-quantum security theories but still retain their efficiency in real-time detection of threats.

The current project is going to include the integration of quantum-resistant and AI-powered intrusion detection system models to improve their performance in the future amid cy-bersecurity threats. In general, the suggested concept will pro-vide a sustainable and futuristic perspective for the intrusion detection process within the next generation network through the use of a safe feature extraction process, resilient learning architecture, and quantum-resistant design. The research pa-per will result in the creation of cybersecurity infrastructure capable of handling any new vectors of attacks as well as any issues associated with quantum computers.

A. KeyContributionsoftheResearch

1) Quantum-ResistantIntrusionDetectionFramework: This study proposes a hybrid AI-based intrusion de-tection system integrated with post-quantum crypto-graphic techniques to ensure long-term security against quantum-enabled cyber threats.
2) Efficient Feature Extraction and Preprocessing: The system applies advanced preprocessing and feature se-lection methods to handle large-scale network traffic data, reducingcomputational complexityand improving detection efficiency.

3) Hybrid AI Model for Accurate Detection: Multiple machine learning and deep learning algorithms (CNN, LSTM,andensemblemethods)areutilizedtoaccurately detect both known and zero-day cyber-attacks.
4) Integration of Post-Quantum Cryptography: The framework incorporates quantum-resistant algorithms suchasKyberandDilithiumtosecuredatatransmission and enhance end-to-end system security.
5) Scalable and Real-Time Detection System: The pro-posedmodelisoptimizedforreal-timeperformance, Scalability, and deployment in resource-constrained and next-generation network environments.

II. LITERATURE REVIEW

1) :A. Kumar et al. (2020) introduced the concept of a quantum-based intrusion detection system for IoT through the useofQuantumSupportVectorMachine(QSVM).Inparticu-lar, the authors aimed at improving the cyber-attack detection performance by utilizing quantum computing concepts. The main idea of the research was to implement quantum machine learning into the IDS design for IoT in order to gain higher efficiency and flexibility. It appears that the approach led to increasedaccuracyofdetection(accuracyofthealgorithmwas comparatively high according to experimental results). At the same time, there are numerous drawbacks of the algorithmthat should be considered, namely reliance on quantum com-puter/simulator,inabilitytohandlelargeamountsofdata,high computing costs, and difficulty implementing the method in practice due to lack of development of quantum computing technologies [1].
2) : T. T. Nguyen et al. (2021), have discussed an ef-fective IDS strategy using deep learning, which is designedfor intrusion detection in the post-quantum age. In this paper, the authors have used advanced deep learning algorithms like CNN and LSTM to enhance intrusion detection. The key highlightofthispaperisthedevelopmentofaframework thatintegratesAI-basedIDSwiththeconceptofpost-quantum security, which can be helpful in developing a more robust IDS. It has been found that the model performs very well in detecting cyber-attacks using benchmarked datasets. Despite several merits, there are certain limitations associated withthe use of deep learning for intrusion detection in the post-quantum age [2].
3) :A. Cirillo et al. (2022) suggested the implementa-tion of a Hybrid Quantum Generative Adversarial Network (QGAN) that can be employed for detecting anomalies by integrating principles of quantum computing and classical machine learning techniques. This paper mainly discusses the application of quantum-based generative models to improve the performance of anomaly detection due to the superiorityofsuchamethodoverclassicalones.Theprimaryinnova-tionprovidedinthisstudyisthatquantum-basedfeatures canenhancetheperformanceofanomalydetectiontasks. Theexperimentsperformedshowedimpressiveaccuracyrates achieved by this technique, implying the possibility of better performance than classical algorithms. Nonetheless, there are multipleconstraintsassociatedwiththeimplementationofthis algorithm, namely extremely high computational costs, need for integration of quantum and classical computers, instability of the training process inherent in GANs, and unsuitability for big data [3].
4) :A detailed survey conducted by R. Chaudhary et al. (2023) on federated learning and quantum machine learningin network intrusion detection is analyzed in the followingpart of the discussion. This study examines the use of fed-eratedlearningandquantum-basedmodelsforIDSsystems to enhance the security and accuracy of data processing. The main contribution of this paper is that it presents a taxonomy and comparative analysis of existing FL-IDS methods with quantum computing, along with suggestions for future work. Althoughthepresentedtechniquesarefoundtoprovidehigher precision and protect the privacy of data processing, several limitations should be mentioned, including high communica-tion costs because of frequent updates of the model, delays in theprocessofdistributedlearning,susceptibilitytomodelpoi-soning, and deployment issues related to quantum computing applications [4].
5) : Y. Zhang et al. (2024) proposed a quantum-aware secure intrusion detection framework for Industrial IoT (IIoT) thatintegratesdeeplearningmodelssuchasCNN–LSTMwith post-quantum cryptographic techniques to enhance security against emerging quantum threats. The study focuses on securingindustrialnetworksbycombiningintelligentintrusion detection with quantum-resistant encryption mechanisms. The maincontributionofthisworkisthedevelopmentofa hybridframeworkthatensuresbothaccurateattackdetec-tion and secure data transmission in IIoT environments. The model achieved high detection accuracy on industrial network datasets,demonstratingimprovedperformanceovertraditional IDS approaches. However, the system has notable limitations, includinghighcomputationalcomplexityduetotheintegration ofdeeplearningandcryptographicmodules,increasedtraining time, resource consumption, and challenges in deploying the frameworkinreal-timeandresource-constrainedenvironments [5].

6) :Kim et al. (2024) introduced an Intrusion Detection System based on the concept of quantum inspired outlier analysis for detecting anomalies. In this model, the core idea lies in making use of quantum-based algorithms for outlier detection in order to improve detection accuracy. The main contribution in this case is high performance detection that results from a combination of quantum based models and outliers.Limitations of the paper include high computational cost and impracticality [6].

7) :In this study, Elsedimy et al. (2024) have created a novel approach of intrusion detection system that is a combi-nation of the QSVM algorithm and enhanced grey wolf opti-mization.Theidearevolvesaroundenhancingfeatureselection and classification techniques through quantum learning. The core innovation includes achieving high-classification accuracy and feature optimization over other classical systems. Despite these benefits, the hybrid model faces several challenges such asdependencyonquantumsimulation,prolongedcomputation time, and scalability [7].

8) : The intrusion detection system based on quantum machine learning, known as QML-IDS, was proposed by Abreu et al. (2024). This concept highlights the idea of a hybrid quantum-classical approach for improved attack detec-tion. The important point here is that the researchers have shown theadvantages of QML-IDS comparedto conventional MLtechniques.Thedrawbacksareassociatedwithsimulations only and high implementation complexity [8].

9) :The research by Nalayini et al. (2025) introduced a novel adaptive transformer-based quantum intrusion detection system that can be applied on software-defined networks (SDN). The strength of this proposal is in incorporating the transformer architecture and quantum concepts into the detec-tion process to achieve efficient detection of new threats. The weakness associated with the model is its high computation cost, delay, and complexity in implementation [9].

10) :Nagarjun et al. (2025) that proposed a quantum deep learning-assistedblockchain-basedintrusiondetectionsystem. The idea revolves around using blockchain technology to ensure security of data and utilizing quantum deep learning techniques to detect any intrusions. The significant advantage offered by this approach is enhanced data security and in-tegrity. The drawbacks are associated with complexities and processing overheads [10].

11) : Hussain et al. (2025) have designed a quantum-enabled secure blockchain-based intrusion detection system for IIoT. The key idea behind the approach lies in the combi-nationofquantumsecuritywithblockchainandartificialintel-ligence for effective intrusion detection. The core innovation includes security enhancement and increased trustworthiness in the network of IIoT, alongside efficient attack detection. Nevertheless, the proposed scheme faces challenges like ex-pensivecomputation,scalability,andcomplexiimplementation [11].

TABLEI
LITERATURESURVEYOFQUANTUM-BASEDINTRUSIONDETECTION SYSTEMS

Sr. No.	Author &Year	Algorithm Used	Cryptographic TechniqueUsed	DetailedLimita-tion
1	Zhang et al. (2024)	CNN–LSTM	Lattice-based cryptography	High system complexity;increasedtraining time;high resourceconsumption ;difficult real-timedeployment.
2	Chaudhary et al. (2023)	FL + QML	Secure aggregation +Post-quantumencryption	High communicationoverhead; latency issues;vulnerable tomodel poisoningattacks.
3	Cirillo &Esposito(2022)	Hybrid QGAN	Notexplicitlyde-fined	High computationalcost; unstabletraining;limitedscalability.
4	Nguyen et al. (2021)	AI-basedIDS	PQcryptographic pipelines	Limited real quantumattackevaluation;increasedsystemcomplexity.
5	Kumar &Swarnkar(2020)	QSVM	Not explicitly used	Requires quantumhardware;scalability issues; highimplementationcost.

*12) :*Cirillo et al. (2026) conducted a benchmarkingstudy of quantum machine learning techniques for intrusion detection systems (IDS) in noisy quantum computing envi-ronments. The approach evaluates the performance of various quantum machine learning algorithms under realistic quantum constraints.Themaincontributionofthisworkisproviding a comprehensive analysis of the strengths and limitations of quantum-based IDS models. However, the study has several limitations, including reliance on noisy intermediate-scale quantum (NISQ) devices, limited availability of large-scale training data, and reduced applicability to current real-world systems [12].

A. Research Gaps

1) Existing studies mainly focus on quantum-enhanced or quantum-inspiredmodels,withlimitedemphasisontrue quantum-resistant AI-based intrusion detection frame-works.
2) Integration of post-quantum cryptographic mechanisms withAI-drivenIDSisinsufficient,leavingdatatransmis-sion and model security vulnerable to quantum attacks.
3) Most approaches rely on benchmark datasets and lack validationagainstreal-worldandzero-dayattackscenar-ios, 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) Thereisanabsenceofstandardizedevaluationmetricsto 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 en-vironments are largely unexplored.

B. ProblemStatement

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 provide reliable detection of known and new cyber-attacks to ensure 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 de-tection framework that integrates advanced machine learning modelswithpost-quantumsecuritymechanisms.Thesys-tem employs efficient preprocessing and feature selection techniques to handle large-scale network traffic data, fol-lowed by the implementation of hybrid AI models (such as CNN–LSTMorensemblemethods)foraccuratedetection of both known and zero-day attacks. To overcome the lim-itations of traditional systems, quantum-inspired algorithms are incorporated to enhance pattern recognition and improve the detection of complex attack behaviors. Additionally, post-quantumcryptographictechniquesareintegratedtoensure secure data transmission and protect against quantum-enabled threats.Themodelisfurtheroptimizedforscalability,reduced computationalcomplexity,andreal-timeperformance,making it suitable for deployment in next-generation and resource-constrained network environments.

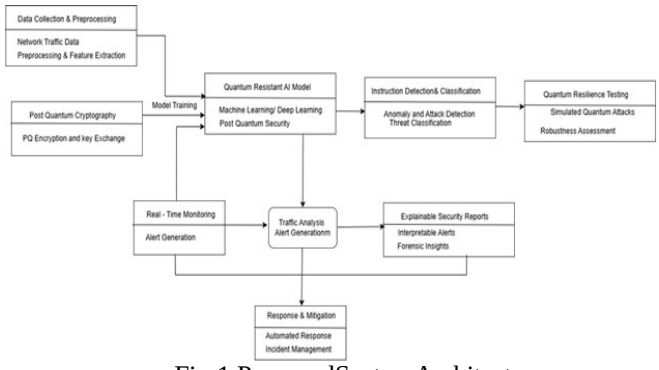


Fig.1.ProposedSystemArchitecture

The figure 1 represents a quantum-resistant AI-based in-trusion detection system where network traffic data is first collected and preprocessed.

The data is 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 normal and malicious activities, followed by real-time monitoring and traffic anal-ysis to generate alerts. It also provides explainable security reportsforbetterunderstandingofdetectedthreatsandinitiates responseandmitigationactionstohandleattacks.Finally, the system undergoes quantum resilience testing to ensure robustness against future quantum-enabled threats.

TABLEII
ALGORITHMSUSEDINPROPOSEDQUANTUM-BASEDIDS

Sr. No.	Module	AlgorithmsUsed	Purpose
1	Data Pre-processing & FeatureExtraction	PCA,Min-MaxNor-malization,TF-IDF	Datacleaning,nor-malization,andfea-ture selection
2	AI-Based IntrusionDetectionModel	CNN,LSTM,CNN–LSTM(Hybrid),Ran-dom Forest, SVM	Detectandclassify normalandmaliciousnetwork traffic
3	Anomaly Detection	IsolationForest,One-ClassSVM	Identifyunknownand zero-dayattacks
4	Quantum-BasedTechniques	Quantum SVM (QSVM), QuantumFeature Mapping	Improve pattern recognition andclassificatio naccuracy
5	Post-QuantumCryptogra-phy	Kyber,Dilithium	Secure data transmission andkey exchange
6	Optimization &Ensemble	Gradient Boosting, EnsembleLearning	Improveaccuracyand reducefalsepositives

The inputs for the proposed quantum-resistant AI-basedIDSconsistoftherawnetworktrafficdatasetthatcanbe Obtained through different sources, including packets, flows, communication records, etc. The characteristics included inthe inputs are IP address, ports, protocol used, packet size, flow time, connections statistics, etc. Security parameters and encrypted streams of data using post-quantum cryptography algorithms are also considered as inputs.Preprocessing ofinput 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 and security reactions. The model decides if it is malicious or normal, and even determines the nature of the attack. In addition, the model issuesreal-timealertsincaseofanyintrusion,whileproviding insights to the security reports that explain how the threats were handled. Besides, the model automates the reaction and mitigation process, which could be blocking of malicious connections. The results generated by the system also include the evaluation of robustness in the light of quantum resilience testing, ensuring that the system would still be secure in the event of any quantum-based attacks. The proposed system adopts hybrid AI models such as CNN-LSTM in addition to SVM,RandomForest,anomalydetectionalgorithms,quantum computing algorithms such as QSVM, and post-quantum cryptography. Post-quantum cryptographic algorithms suchas Kyber and Dilithium, together with symmetric algorithms like AES-256 and SHA-3, are used for security.

1) Kyber:Usedforsecurekeyexchange;protectsdata communication from quantum attacks.
2) Dilithium:Usedfordigitalsignatures;ensuresdata authenticity and integrity.
3) SPHINCS+:Hash-basedsignaturescheme;provides strong quantum-resistant authentication.
4) AES-256:Symmetricencryption;securesdataduring transmission with high security.

5) SHA-3: Hash function; ensures data integrity by gener-ating unique hash values

A. DatasetDescription

The proposed quantum-resistant AI-based intrusion detec-tion system utilizes multiple publicly available benchmark datasets to ensure robust evaluation across diverse network environments. The NSL-KDD dataset is used as an improved version of the KDD Cup 1999 dataset, addressing redundancy issues and providing labeled records for normal and attack traffic. The CICIDS2017 dataset contains realistic modern networktrafficwithvariousattacktypessuchasDDoS, brute force, and infiltration, making it suitable for evaluating real-worldintrusionscenarios.Additionally,theUNSW-NB15 dataset is employed, which includes contemporary synthetic network traffic with diverse attack categories and rich feature sets.Thesedatasetscollectivelyenablecomprehensivetraining and testing of the system for detecting both known and zero-dayattackswhileensuringscalabilityandadaptabilityinnext-generation network environments.

TABLEIII
DATASETSFORQUANTUM-RESISTANTAI-BASEDINTRUSIONDETECTION SYSTEM

DatasetType	DatasetName	AccessLink
BenchmarkIDS Dataset	NSL-KDD Dataset	https://www.unb.ca/cic/datasets/nsl.html
Real-WorldNet-workTraffic	CICIDS2017 Dataset	https://www.unb.ca/cic/datasets/ids-2017.html
Modern SyntheticDataset	UNSW-NB15 Dataset	https://research.unsw.edu.au/projects/unsw-nb15-dataset

B. Noveltyofresearch

- Integration of AI with Post-Quantum Cryptography: The proposed system combines advanced artificial in-telligence models with quantum-resistant cryptographic algorithmssuchasKyberandDilithiumtoensureend-to-end secure intrusion detection.
- Quantum-Enhanced Detection Capability: Quantum-inspired techniques such as Quantum Support Vector Machine (QSVM) and quantum feature mapping are utilized to improve the detection of complex and zero-day cyber-attacks.
- Hybrid AI Architecture: A novel hybrid model com-bining CNN–LSTM and ensemble learning methods is proposed to enhance detection accuracy and reduce false positives.
- End-to-End Secure Framework: Unlike traditional in-trusion detection systems, the proposed framework en-sures both accurate intrusion detection and secure data transmission.
- Scalable and Real-Time Design: The system is opti-mized for scalability and real-time performance, making it suitable for next-generation and resource-constrained environments.
- Explainable and Robust System: Explainable AI tech-niques are incorporated to improve transparency, inter-pretability, and trust in intrusion detection decisions.

IV. CONCLUSION

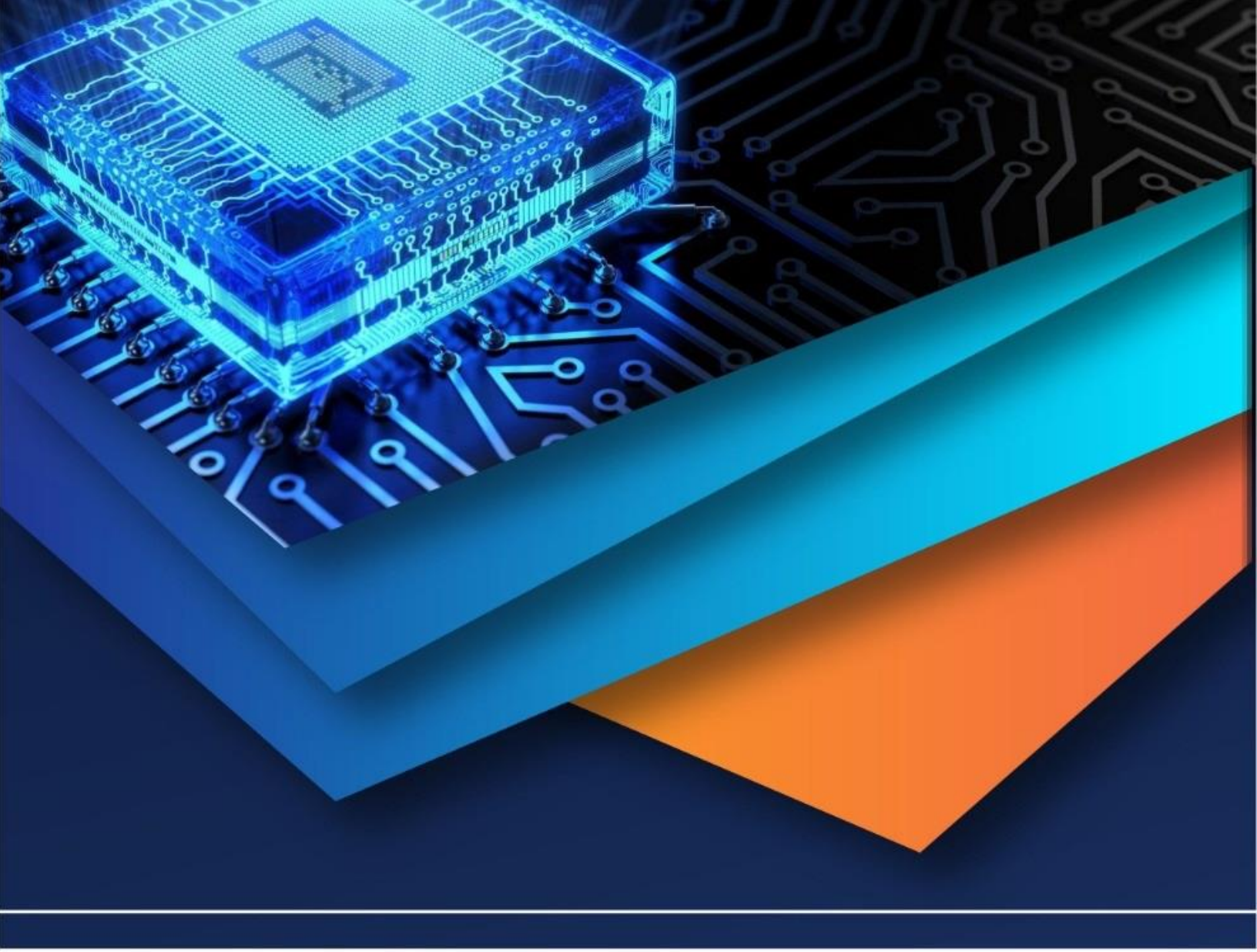
This review highlights the growing importance of integrating artificial intelligence with quantum-resistant techniquesfor developing secure and future-ready intrusion detection systems. Existing approaches, including machine learning and deep learning-based IDS, have demonstrated strong capabilities 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,thereisacriticalneedtodevelopahybridquantum-resistant AI-based intrusion detection system that combines robust detection capabilities with secure data transmission.

Such systems must focus on improving accuracy, reducing falsepositives,ensuringreal-timeperformance,andenhancing 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] Kumar, A., & Swarnkar, R. (2020). Quantum-based intrusion detectionsystem for IoT networks. IEEE Internet of Things Journal.
[2] Nguyen, T. T., et al. (2021). Deep learning for cyber security: Preparingintrusion detection for the post-quantum era. IEEE Access.
[3] Cirillo, A., & Esposito, C. (2022). Hybrid quantum generative adver-sarial networks for anomaly detection. IEEE Transactions on EmergingTopics in Computing.
[4] Chaudhary,R.,etal.(2023).Federatedandquantummachinelearn-ing for network intrusion detection: A survey. IEEE CommunicationsSurveys & Tutorials.
[5] Zhang, Y., et al. (2024). Quantum-aware secure intrusion detectionframework for industrial IoT. IEEE Transactions on Industrial Infor-matics.
[6] Kim, T. H., & Madhavi, S. (2024). Quantum intrusion detection systemusing outlier analysis. Scientific Reports.
[7] Elsedimy, E. I., Elhadidy, H., & Abohashish, S. M. M. (2024). A novelintrusion detection system based on a hybrid quantum support vectormachine and improved Grey Wolf optimizer. Cluster Computing.
[8] Abreu, D., Rothenberg, C. E., & Abelem, A. (2024). QML-IDS:Quantum machine learning intrusion detection system. arXiv preprintarXiv:2410.16308.
[9] Nalayini,C.M.,Soumya,T.R.,Lalitha,S.D.,etal.(2025).Anoveladaptivetransformer-basedquantumintrusiondetectionsys-tem for software-defined networks. Scientific Reports. :contentRefer-ence[oaicite:0]index=0
[10] Nagarjun, A. V., & Rajkumar, S. (2025). Quantum deep learning-enhanced blockchain for cloud security: Intrusion detection and securedata migration. Scientific Reports. :contentReference[oaicite:1]index=1
[11] Hussain, N., Li, S., Hussain, A., et al. (2025). Quantum-aware secureblockchain intrusion detection system for industrial IoT networks. Sci-entific Reports. :contentReference[oaicite:2]index=2
[12] Cirillo,F.,Esposito,C.,&Seo,J.T.(2026).Benchmarkingquan-tum machine learning methods for intrusion detection on noisyquantum computers. Quantum Machine Intelligence. :contentRefer-ence[oaicite:3]index=3



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY