Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/IN05.20250391
Published: November 6, 2025

A Comprehensive Study on Intrusion detection System using Quantum Computing

Vidhyashree M
School of Computer Science Engineering and Information Systems
Vellore Institute of Technology, Vellore
Vellore, Tamil Nadu, India
vidhyashree.m2023@vitstudent.ac.in

Subhashini R
Associate Professor
School of Computer Science Engineering and Information Systems
Vellore Institute of Technology, Vellore
Vellore, Tamil Nadu, India
rsubhashini@vit.ac.in

Abstract

Technology development has made cyber-security threats more sophisticated, to the point where the detection mechanisms in place are unable to handle the problem. Therefore, the key to solving this issue would be the deployment of a clever and potent intrusion detection system. They monitor computer networks by gathering and evaluating data and information, recognizing user activity and automatically defending against attacks. There is an increasing need for countermeasures for prevention, detection, and protection due to the complexity of computer networks and harmful attacks. The problem of incorrect judgment, incorrect detection, and unsuccessful lack of a consistent response to the attack is one of the essential tests for intrusion detection. The conventional cryptographic security protocols are seriously threatened by the emergence of large-scale quantum computing. They become useless due to quantum assaults, which specifically target the mathematical underpinnings of existing asymmetric cryptography techniques. Longer keys or longer hash function outputs could potentially improve security, making even basic symmetric key cryptography vulnerable, if only slightly. As a result, the cryptographic techniques currently used to protect data will no longer be sufficiently safe and will be exposed to new risks posed by quantum technology.

Keywords
Intrusion Detection, Cyber security, Quantum Computing

1. Introduction
Cyber security is a difficult problem in the modern cyberspace, and its prevalence has been rising sharply in response to computerization in many vital fields, such as banking, business, medicine, and many more. Increasing the amount of interconnection and interoperability in computer systems has become essential for enhancing our daily lives. In the same way, it opens the door for vulnerabilities that are far outside the control of humans. Cyber security methods are necessary in order to communicate because of the weaknesses. Reliable connectivity requires security methods to fend off worries, as well as advancements in protection measures to manage escalating security issues (Rahman, et al. 2023). The increasing interconnectedness and interoperability of computer systems have turned into essential requirements to improve our day-to-day operations. In addition, it creates an avenue for

weaknesses to be exploited that are well beyond the reach of human control. Because of these weaknesses, cyber-security measures are necessary to ensure communication. Security measures must be taken to counteract threats, and security measures must be updated to counter new security risks. The collection of actions taken with the goal of getting around the security measures included in computer networks and systems is referred to as a "intrusion". It is not possible to implement corrective measures without first identifying any breaches that have happened. Intrusion Detection Systems (IDS) are the systems in charge of identifying intrusions from network traffic. Intrusion detection is the process of keeping an eye on a network connection to find any potential intrusions. The goal of intrusions is to compromise one or more of the confidentiality, availability, and integrity—the three main security goals of the network system. In order to get access to the system, an unauthorized user may initiate an intrusion; authorized users may also do so in order to obtain further rights; and authorized users may misuse the authority that has been bestowed upon them. These undesirable behaviors typically involve the utilization of network resources meant for other purposes. Moreover, they nearly always endanger the security of the network and/or its data. In academic literature, the phrases "intrusion" and "attack" are frequently used interchangeably when addressing network security (Ambika et al. 2024)

More and more people are turning to quantum computing as an inventive answer to challenges that conventional computer methods are unable to solve. Compared to conventional computers, quantum computers operate in a different computing environment. Particularly with quantum computers, superposition and entanglement are not present in traditional computing environments and allow for extraordinarily fast operations due to qubit parallelism. The term "qubit" refers to the quantum bit, which is essentially a quantum information unit (Dai et al. 2010). These advantages make quantum computing a desirable option for resolving difficult algorithmic problems. Many studies using quantum computing models are also being conducted in the field of machine learning. Moreover, since the optimisation of quantum devices using gradient descent technique has been studied, hyperparameters can be used to train quantum machine learning quickly (Mu et al.2004). Essentially, the difficulty of executing quantum operations on classical computers stems from the fact that the resources needed increase exponentially with the number of qubits. The new and developing regime of noisy intermediate-scale quantum (NISQ) devices provides us with a good platform to create quantum machine learning and deep learning models, while providing a thorough picture of the errors that take place. Qiskit Aer is used in conjunction with Qiskit Terra to provide a highly configurable noisy model for doing calculations, hence forming a simulation backend that Qiskit provides (Liu and Li 2023).

2. Literature Review

In the healthcare sector, intrusion detection systems (IDSs) are critical for data protection. This study introduces a hybrid classical-quantum neural architecture that utilizes a quantum-assisted activation function, demonstrating improved efficiency using the KDD99 dataset. Additionally, it addresses cyber vulnerabilities in vehicular networks through a new classification-based approach that merges federated learning with the Extra Trees Classification algorithm for enhanced response times and reduced server load. A Geographical Dynamic Intrusion Detection system, leveraging Micro-Blockchain for vehicle-to-everything (V2X) networks, is proposed, showing promising accuracy via simulations (K. et al. 2023) The performance of quantum systems is highlighted, as they may surpass traditional systems in identifying attack patterns, utilizing quantum generative adversarial networks (qGAN) for enhanced pattern recognition (Almutairi et al. 2023). Furthermore, the research illustrates an experimental side-channel attack on superconducting quantum computers, emphasizing the necessity for further examination of quantum hardware robustness. The quantum evolutionary algorithm is suggested for optimizing network intrusion detection tasks, displaying effective optimization in simulations. The study also evaluates both classical and quantum detection techniques, indicating hybrid models achieve superior accuracy rates. Lastly, the Quantum Dwarf Mongoose Optimisation technique is introduced for the classification of intrusions in Cyber-Physical Systems, employing various deep learning models for improved detection accuracy (Kalinin and Krundyshev 2021). Table.1 analysis the journal papers and categorize their methods and datasets. And further we list the observations found in these paper for further understanding of Quantum Intrusion Detection Systems (QIDS).

Table 1. Literature Review

Paper (Title)	Year	Method	Dataset	Observations
"A Novel Intrusion Detection System based on a Hybrid Quantum Support Vector Machine and Improved Grey Wolf Optimizer (QSVM-IGWO)"	2024	Hybrid QSVM + metaheuristic optimization (IGWO), quantum kernel features	BoT-IoT Dataset	BoT-IoT has a lot of capabilities and is a fantastic way to test the impact of quantum kernels. They probably need sampling or dimension reduction due to their size.
"Intrusion Detection System Based on Quantum Generative Adversarial Network"	2025	Quantum generator + Classical discriminator	NSL-KDD	A common benchmark that is useful for comparability is NSL-KDD. Their usage of QGAN implies that they require sufficient data for discriminator training.
"Quantum deep learning-based anomaly detection for enhanced network security"	2024	Quantum / hybrid deep learning anomaly detection	KDD-999, IoT-23, CIC IoT-23	Evaluation of generalizability is aided by the use of mixed datasets, which demonstrate a readiness to test on both traditional network intrusion data and more recent IoT traffic. However, when using quantum circuits, huge sizes may require robust preprocessing and sampling.
"Quantum-Neural Network Model for platform Independent DDoS Attack Classification in Cyber Security"	2024	RNNs + feature selection (not fully quantum, but hybrid)	UNSW-NB15	The UNSW-NB15 has a good range of assault kinds and is more realistic and current. In these situations, quantum feature selection or embedding techniques are particularly helpful.
"Quantum Epigenetic Algorithm for Adaptive Cybersecurity Threat Detection"	2025	Quantum inspired multi-objective feature selection (QEA) + classifiers	UNSW-NB15, CIC-IDS2017, CSE-CIC-IDS2018, TON-IoT	Having both IoT and non-IoT datasets in the same evaluation boosts confidence. Additionally, it suggests the need for methods to handle a variety of characteristics, as including a large number of features into quantum circuits can become resource-intensive.
"Quantum-Inspired Feature Engineering for Intrusion Detection Systems"	2022	Feature Engineering using quantum-inspired optimization (QPSO) + ML models	NSL-KDD, CIC-IDS2017	Reducing overhead by using quantum-inspired (as opposed to complete quantum) approaches also works with more recent datasets (CIC-IDS2017).

3. Methodology

Advances in technologies like cloud computing, Internet of Things (IoT), vehicle networks, Blockchain, Wireless sensor networks, Quantum Computing etc. have led to a jump in the amount of information carried across communication infrastructures in recent years. Attackers have therefore increased their efforts in an attempt to weaken network systems (Gong et al. 2011). Consequently, strengthening the security of those network systems is crucial. The development of post-quantum cryptography (PQC) aims to create cryptographic algorithms resistant to

quantum computer attacks. Current cryptographic methods are predicted to remain secure against quantum threats until 2023, but cryptographers are proactively designing new algorithms for the anticipated Y2Q or Q-Day. Post-quantum symmetric cryptography requires minimal adjustments, as many existing symmetric algorithms are considered relatively secure against quantum attacks. The research focuses on six main approaches: lattice-based, multivariate, hash-based, code-based, isogeny-based cryptography, and the quantum resistance of symmetric keys. Security reductions are also important in PQC, showing the equivalence between a cryptographic method and a hard mathematical problem, indicating the method's security level. Researchers continue to explore ways to enhance the robustness of post-quantum encryption systems. A shared random secret key used in quantum key distribution (QKD) is generated through quantum mechanics, enabling secure communication by allowing parties to detect potential eavesdroppers due to measurable disturbances in a quantum system. Unlike traditional public key cryptography which hinges on computation's complexity, QKD is rooted in quantum mechanical principles and necessitates a verified conventional communication channel. This key can be employed with various encryption algorithms, including the one-time pad, which is theoretically secure with a truly random key. Quantum Neural Networks (QNN) combine quantum information with classical artificial neural network models, aimed at leveraging properties such as interference and quantum parallelism, although they remain largely theoretical. They operate by processing information across qubit layers with three variations: classical with quantum data, quantum with quantum data, and quantum with classical data.

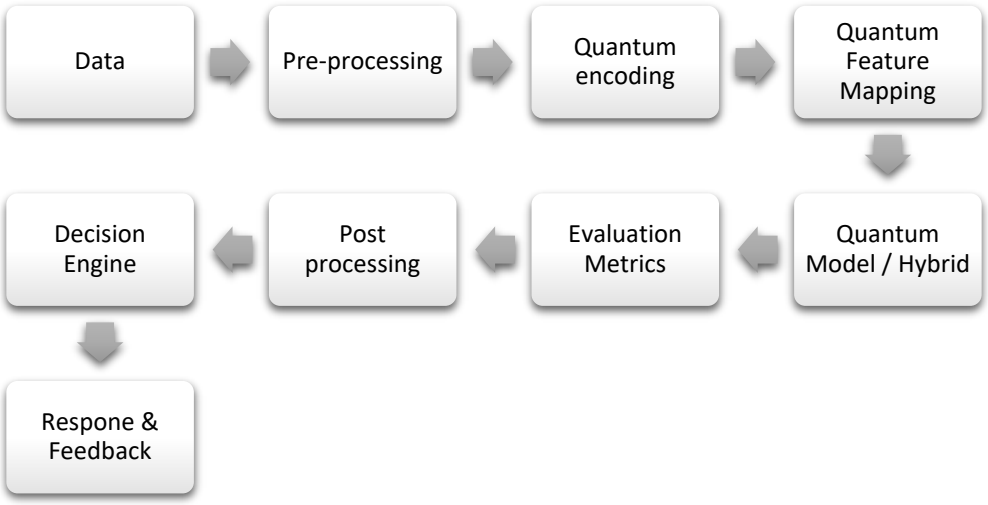

Figure 1. Analyzed Basic Architecture for Quantum Intrusion Detection System (QIDS)

Figure.1 is the basic architecture where it explains the process flow of Quantum intrusion detection system. Quantum Generative Adversarial Networks (qGAN) utilize quantum systems in machine learning, capitalizing on their potential to identify patterns better than classical systems. The loading of classical data into quantum states, necessary for enhancing quantum capabilities, is typically resource-intensive. A hybrid quantum-classical approach for efficient quantum state loading is proposed, using implicit data samples and qGANs to learn probability distributions, with performance demonstrated on IBM Q Experience quantum processors (Cirillo and Esposito 2025). Quantum Machine Learning (QML) refers to the application of quantum algorithms in machine learning, enhancing speed and data handling by utilizing qubits. QML also explores the convergence of classical AI methodologies with quantum processes. The Quantum Genetic Algorithm (QGA) innovatively melds genetic algorithms with quantum principles, using quantum bits and efficient crossover mechanisms for superior search capabilities and faster convergence compared to traditional genetic algorithms. Quantum Support Vector Machines (QSVM) address classification tasks where kernels cannot efficiently segregate data by leveraging non-linear transformations. This supervised learning method faces challenges due to its exponential resource requirements. Quantum Annealing (QA) applies quantum fluctuations to optimize functions, particularly effective for discrete combinatorial problems, through state superposition and tunneling to reach optimal solutions, demonstrating utility in solving NP-complete issues. Lastly, the Quantum Convolutional Neural Network (QCNN) adapts CNN structures to quantum environments, using qubit gates for convolution and pooling, thereby managing the exponentially

growing complexity associated with quantum data, employing techniques like the Multiscale Entanglement Renormalisation Ansatz (MERA) for state simulation and size reduction of quantum systems.

4. Results and Discussion

Intrusion Detection Systems (IDS) are crucial in this security preservation environment because they monitor system activity and proactively identify possible threats. The very basic initial generation of intrusion detection systems (IDS) merely collected system events and compared them to manually updated signature database tuples. But it was soon discovered that these techniques had serious drawbacks, chief among them being their lack of flexibility. Their main lack of proactivity was their inability to identify novel threats outside of the signature database. Second, there was a chance that a considerable amount of time would pass between the discovery of an attack and the creation and updating of fresh signatures in the intrusion detection system (IDS), leaving systems open to vulnerability. The strain on network intrusion detection is expanding as network intrusion continues to develop. Cyberspace security is particularly vulnerable due of concerns with unbalanced network traffic, which make it harder for intrusion detection systems to foresee the dispersion of damaging attacks. Many datasets containing superfluous and useless information are available to address IDS. As a result, the standard techniques have very large computational costs. Feature selection techniques can be used to address this problem. Our research indicates that quantum upgrades to network security systems look very promising.

4.1 Descriptive Analysis of Datasets

The assessment of the efficacy of intrusion detection systems (IDS) hinges significantly on the selection of appropriate data for collection. Observational data from networks is vital, though developers tend to favor existing datasets due to the high costs associated with data collection. This summary reviews several prominent datasets utilized in attack detection systems, emphasizing the need for frequent updates and benchmarking due to the dynamic nature of malware and evolving attack strategies. NSL-KDD, KDD'99, UNSW-NB15, CIC-IDS2017/2018, BoT-IoT, IoT-23, are the most frequently used datasets. These characteristics (tens-~80 features) deal with supply flow / connections. In order to reduce dimensionality to a scale that is practical for quantum encoding, authors usually subsample or use feature selection / PCA for quantum experiments.

The KDDCup-'99 dataset, containing approximately 4.9 million unique connections with 41 features, is widely recognized for comparing various IDSs. It is classified into three attack types: Denial-of-Service (DoS), User-to-Root (U2R), Remote-to-Local (R2L), and Probing attacks, each characterized by distinct methods of intrusion. The NSL_KDD dataset is the enhanced version of the KDD'99 dataset addresses biases by removing redundant connection records, resulting in 136,489 test records. It includes numerous network intrusion techniques such as R2L and U2R attacks, proving to be superior for identifying misuse in IDS.

UNSW NB15 dataset is Collected by the Australian Centre for Cyber Security, this dataset encompasses over 2.5 million records and 49 features derived from simulated network traffic attacks, including DoS and various types of exploits. It categorizes data into labels for normal and abnormal traffic, encompassing nine distinct attack types. CICIDS2018 is Developed by the Canadian Institute of Cyber Security in 2018, this dataset represents the largest and most current publicly available intrusion dataset. It consists of six attack scenarios and provides 83 features per sample, representing real-world attack simulations, thus improving upon previous datasets like CSE-CIC-IDS2017.

Table 2. Analysis of Datasets

Datasets	Common Use	Strengths in QIDS Context	Limitations
KDD'99	Large classical dataset that serves as a standard for comparison and anomaly identification	Very Large, Plenty of connections and historically very popular	Unless sampled or compressed, known problems, redundancy, overfitting risk, excessive size can be a challenge for quantum experiments.
NSL-KDD	Quantum and hybrid models, baseline classification , anomaly	Small enough for simulators, excellent comparability due to	Not recent, some classes are under-represented, traffic patterns and attack kinds can

	detection and QGANs	broad use, basic feature count (about 41)	be out of date.
UNSW-NB15	More realistic, modern mixed attacks, and are utilized to evaluate sophisticated techniques, feature selection	More varied attacks, more recent features and included are IoT and non-IoT traffic	Larger feature sets, more intricate, it takes a lot of resources to incorporate numerous characteristics into quantum circuits; more pre processing required.
CSE-CIC-IDS2018	Multiple attack vectors and real-world traffic and also widely used for comparison	High relevance, useful for monitoring false positives, etc,: in validating techniques on realistic traffic	Large size, a lot of features, the potential need to reduce dimensionality, high traffic values, computational resources and class imbalance.

The significance of dataset selection either extensive classical pre-processing (feature selection / PCA) or the creation of compact encodings (angle / amplitude encodings) are required by quantum circuits (actual devices or simulators with restricted qubits). As a result, many research test on synthetic or sampled copies of big datasets or smaller subsets.

4.2 Descriptive Analysis of Evaluation metrics

We assess the performance of the experimental model through several metrics: F1-Score, Accuracy, Precision, and Recall, while considering the false alarm rate of the intrusion detection system and the flow recognition accuracy rate. There are four categories based on true labels and model predictions: False Negative (FN), where a positive sample is incorrectly identified as negative; False Positive (FP), where a negative sample is misclassified as positive; True Negative (TN), correctly identified negative samples; and True Positive (TP), correctly identified positive samples (Li et al. 2022).

Table 3. Analysis of Evaluation metrics

Metric	Purpose	Formula	Observed Range	Trend Across Papers	Analytical Observation
Accuracy	Calculates the overall percentage of correctly classified traffic, including attack and routine traffic	Accuracy = $\frac{TP+TN}{TP+TN+FP+FN}$	92% - 99.9%	Relatively high; >95% is demonstrated by Quantum SVM (QSVM), QNN, and QEA techniques.	Due to the fact that quantum feature space separation allows QML models to reach high accuracy, hybrid QSVM models frequently outperform classical baselines. Due to generating noise, slightly lesser for QGAN-based IDS.
Precision	Displays the proportion of predicted attacks that really occurred (i.e., True Positives / All Positives).	Precision = $\frac{TP}{TP+FP}$	97.9% - 98.8%	Fewer studies has reported it, however when it is observed, it is consistently high.	By enhancing precision, quantum-enhanced optimizers (IGWO, QEA) lessens false alarms. Demonstrates a high level of confidence in positive detections.
Recall	Calculates the number of real	Recall = $\frac{TP}{TP+FN}$	94.4% - 98.6%	Robust and steady in	High recall scores indicate that attacks

	attacks that were accurately identified.			hybrid and QSVM-based models.	are rarely missed by QIDSs. By enhancing separability, quantum models with adaptive encoding (like QSVM-IGWO) optimize recall.
F1-Score	Balances false positives and false negatives by taking the harmonic mean of precision and recall.	$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$	93.8% - 98.5%	Resilient and well-balanced across the majority of hybrid QIDS architectures.	Indicates a good balance between the rate of classification and the accuracy of detection; models based on quantum kernels work best.
False Positive Rate(FPR)	The rate at which regular traffic mistakenly categorized as attacks.	$FPR = \frac{FP}{FP+TN}$	0.1% - 1.3% (reported in only a few of studies)	Quiet low for QSVM and Quantum anomaly models.	High reliability is indicated, which is important for lowering false alarms in networks that are operating. However, FPR is not clearly reported in the majority of QIDS articles.
AUC (ROC Area)	Class Separability is indicated by the area under the receiver operating characteristic curve.	$AUC = \int_0^1 TPR\ (FPR), dFPR$	-(rarely reported)	At present, there are only few publications in the field of QIDS research	Very minimum number of publications in the field of research today. AUC be used in future research to represent model robustness in the face of class imbalance.
Detection Latency	Time needed for model inference / detection.	-	- (qualitative reports only)	Not often measured	Although more current research rather than hardware-tested, Quantum circuits may theoretically Speed up
Quantum Circuit Depth (D)	Determines the complexity of the quantum model; deeper circuits are more capable of learning but are difficult to operate on NISQ devices.	Number of quantum gate layers that are put in the circuit one after the other.	20-180 layers	Increasing relatively between (2022 – 2025) as models become more expressive.	Deeper circuits had a better detection rate but a higher risk of decoherence; the optimal range $\approx 50 - 100$.
Quantum Gate Count (G)	Calculates the hardware execution time and computational cost	Total number of gates with one or two qubits.	10^3-10^5 gates	Rapid growth with hybrid models; Richer encodings	The cost of execution was lowered by 20-30% using gate optimization (QEA, IGWO).

				require more gates.	
Qubit Utilization (Q)	Represents the IDS's quantum resource footprint.	Numbers of qubits that are actively employed in computation or model encoding.	4-64 qubits (simulated)	Scaling up gradually as simulators develop.	Although multi-attack type detection is made possible by higher qubit counts, noise bottlenecks still exist.
Quantum State Fidelity (F)	Evaluates how closely ideal and real quantum states resemble one another.	$F(\rho, \sigma) = (\mathrm{Tr}\sqrt{\sqrt{\rho\sigma}\sqrt{\rho}})^2$	0.92-0.999	Steadily getting better (because of improved error mitigation).	Stable encoding is ensured by fidelity > 0.98, which is a crucial measure of hardware quality.
Entanglement Entropy (S)	Measures the level of entanglement between qubits, or subsystems.	$S = -\mathrm{Tr}(\rho \log_2 \rho)$	0.6-1.2 bits	Slightly increasing with model complexity.	Better nonlinear separation is correlated with higher entanglement.
Quantum Accuracy (QAcc)	Purely in the quantum kernel or QNN output space, accuracy is measured.	$QAcc = \frac{Correct\ Quantum\ Predictions}{Total\ Samples}$	94.5-99.8%	Growing steadily since 2022.	Quantum-enhanced models perform about 3-5% better than classical SVMs.
Quantum Feature Overlap (QFO)	Calculates the degree of similarity between two quantum-encoded data points in the feature space (Hilbert).	$QFO(xi, xj) = \lvert\langle \emptyset(xi) \rvert \emptyset(xj)\rangle\rvert^2$	0.05 – 0.35	Between 2022-2025, QFO decreased by almost 70%, indicating a steady improvement in attack detection accuracy and quantum class separability.	A lower QFO suggests that a richer, more separable feature space is produced by the quantum model.
Quantum Advantage Ratio (QAR)	Ratio of resource or time efficiency in relation to traditional IDS	$QAR = \frac{T_{classical}}{T_{quantum}}$	1.3x – 6x	Growing with hybrid optimization since the mid-2023.	Feature extraction shows a quantum advantage, but it is not yet full-pipeline.
Decoherence Rate(δ)	Probability of noise causing a quantum state to lose coherence.	$\delta = 1 - F$	0.01 - 0.05	Gradual decrease through layers of error correction.	Robust QML inference is ensured via lower decoherence.

From the Table.2 and Table.3 we can understand that several datasets and metrics are available to enhance the quality of our findings. In most of the papers, Accuracy and occasionally F1 are frequently mentioned. In the BoT-IoT subset, for instance, QSVM-IGWO reported an overall accuracy ≈ 99.11% with precision ≈ 97.99%, recall ≈ 98.67%, and F1 ≈ 98.45% (Elsedimy et al. 2024). on NSL-KDD, QGAN work showed accuracy ≈ 93.7% and F1≈ 93.84% (Cirillo and Esposito 2025). Extremely high DDoS detection accuracy (≈99.9%) was reported by QIDS-OA (Kim et al. 2024) for the studied situations. Complete confusion matrix breakdowns, ROC-AUC per-class recall / precision (important for uncommon attack types), or system- level parameters like detection delay and throughput are sometimes absent. Cross-paper comparison is difficult as a result.

Quantum Specific metrics which contributes to measure Quantum Intrusion Detection Systems (QIDS) or any quantum machine learning (QML) based security model. Theses metrics measures more than just detection performance like quantum circuit efficiency, fidelity, and entanglement quality and so on which are important for real world quantum intrusion detection system implementations.

4.3 Descriptive Analysis of Limitations and challenges

Although Quantum-based intrusion detection system architectures provide exponential speedups in pattern recognition and anomaly detection, their actual implementation is limited by present technological immaturity, ranging from hardware to algorithmic stability. To overcome these obstacles, advancements must be made in: resilient quantum techniques for noise, benchmark datasets that are standardized, quantum-classical hybrid orchestration, quantum error correction and quantum data protocols that protect privacy. Future research could concentrate on the following to address these issues: Creating quantum IDS algorithms that can withstand noise, Developing hybrid cloud architectures for QIDS in real time, Creating quantum benchmark datasets to assess security, Improving stable model inference with quantum error correction (QEC), Using QIDS pipelines to incorporate quantum-safe cryptography.

5. Conclusion

Nowadays, Cyber security is a must to prevent data breaches, hostile invasions, denials of service, and other issues. In a never-ending arms race, the field of information security is unpredictable and requires ongoing readjustment to keep up with the introduction of new attack patterns. The quantity of computers was negligible and they were only used for business purposes when cyber security originally emerged. Back then, there was no such thing as a completely sensorized device that would become commonplace, generate massive amounts of network traffic, and hold a ton of sensitive data. Intrusion detection using quantum and hybrid techniques is a dynamic and rapidly evolving field. The majority of the work is in its early stages, relying on simulators or small subsampled datasets, rarely evaluating on real quantum hardware at scale, and frequently omitting full metric breakdowns (per-class recall, FPR, and AUC). However, recent papers demonstrate promising performance detection (many report high accuracy on benchmark IDS datasets). Quantum Neural Networks (QNN / VQCs), Quantum SVMs (QSVM), Quantum GANs (QGAN), QCNN variations, and quantum-inspired feature-selection / optimizers are important methods. Quantum-Enhanced Intrusion Detection Systems (QIDS) and quantum secure communications systems have high detection accuracy, with extremely low false positive rates. These values reveal the possibility that quantum technologies may increase network security in terms of both precision and reliability. The interdisciplinary work was an important factor in the success of our research, as described in methodology. Cross-field convergence of expertise in quantum physics, cryptography and network security enhances the research process to deepen understanding and bring forth integrated solutions.

References

Abreu, D., Rothenberg C. E. and Abelém, A., QML-IDS: Quantum Machine Learning Intrusion Detection System, *2024 IEEE Symposium on Computers and Communications (ISCC)*, Paris, France, 2024, pp. 1-6,

Akshai, A., Anushri, M. and Sonu, P., A New Systematic Network Intrusion Detection System Using Deep Belief Network, *2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS)*, KOTTAYAM, India, 2023, pp. 1-7,

Al-E'mari, S., Sanjalawe, Y., and Fraihat, S., A Novel Quantum Epigenetic Algorithm for Adaptive cybersecurity Threat Detection. *AI(Switzerland),* 6(8), Article165.(2025)

Almutairi, L., Daniel, R., Khasimbee, S., Lydia, E. L., Acharya, S. and Kim, H. -I., Quantum Dwarf Mongoose Optimization With Ensemble Deep Learning Based Intrusion Detection in Cyber-Physical Systems, in *IEEE Access*, vol. 11, pp. 66828-66837, 2023

Alomari, A. and Kumar, S. A. P., DEQSVC: Dimensionality Reduction and Encoding Technique for Quantum Support Vector Classifier Approach to Detect DDoS Attacks, in *IEEE Access*, vol. 11, pp. 110570-110581, 2023,

Ambika, S., Balaji, V., Rajasekaran, R. T., Periyasamy P. N. and Kamal, N., Explore the Impact of Quantum Computing to Enhance Cryptographic Protocols and Network Security Measures, *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, Greater Noida, India, 2024, pp. 1603-1607,

Anupama, A. and Prasad, R. R., Hybrid Intrusion Detection System, *2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS)*, KOTTAYAM, India, 2023, pp. 1-6,

Belavagi, M. C., & Muniyal, B.. Improved Intrusion Detection System using Quantal Response Equilibrium-based Game Model and Rule-based Classification. *International Journal of Communication Networks and Information Security (IJCNIS)*, *13*(1). (2022)

Bell, B., and Trügler, A., Reconstructing quantum circuits through side-channel information on cloud-based superconducting quantum computers, *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Broomfield, CO, USA, 2022, pp. 259-264,

Chao, S., Yang, G., Nie, M, Liu, Y. and Zhang, M., Full-Rotation Quantum Convolutional Neural Network for Abnormal Intrusion Detection System. *In Proceedings of the 2022 5th International Conference on Artificial Intelligence and Pattern Recognition (AIPR '22). Association for Computing Machinery,* New York, NY, USA, 852–859. 2023.

Cirillo, F. and Esposito, C., Intrusion detection using quantum generative adversarial networks:a federated approach with noisy simulators, *IET and communications Conference 2025*, London, uk, , pp. 31-35, 2025

Cui, A., Li, Y., Gao, Y. and Guo, R., Intrusion Detection Approach of Power Information Network Based on DNSAE and IQPSO-SVM, *2022 9th International Forum on Electrical Engineering and Automation (IFEEA)*, Zhuhai, China, pp. 596-601, 2022.

Dai, Z., Huang, L., Zhu, Y. and Yang, W., Privacy Preserving Density-Based Outlier Detection, *2010 International Conference on Communications and Mobile Computin*g, Shenzhen, China , pp. 80-85, 2010

Dhote, V., Sadim, M., Tanna, P. and Tiwari, A. N., Machine Learning Strategies in Quantum-Resistant Network Security Protocols, *2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, India, pp. 1-6, 2023

Dong, Y., Hu, W., Zhang, J., Quantum beetle swarm algorithm optimized extreme learning machine for intrusion detection, *Quantum Inf Process* 21, 9 (2022).

Elsedimy, E.I., Elhadidy, H. & Abohashish, S.M.M. A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer. *Cluster Comput* **27**, 9917–9935 (2024)

Francis E, G., and Sheeja, S., *A* Novel RDAE Based PSR-QKD Framework for Energy Efficient Intrusion Detection, *2022 International Conference on Knowledge Engineering and Communication Systems (ICKES)*, Chickballapur, India, , pp. 1-6, 2022. doi: 10.1109/ICKECS56523.2022.10060298.

Ghanbarzadeh, R., Hosseinalipour, A. & Ghaffari, A., A novel network intrusion detection method based on metaheuristic optimisation algorithms, *J Ambient Intell Human Comput* 14, 7575–7592 (2023).

Gong, C., Guan, W., Gani, A., Network attack detection scheme based on variational quantum neural network, *J Supercomput* 78, 16876–16897 (2022).

Gong, C., Guan, W., Zhu, H., Network intrusion detection based on variational quantum convolution neural network, *J Supercomput* 80, 12743–12770 (2024).

Gong, C., Zhu, H., Gani, A., QGA–QGCNN: a model of quantum gate circuit neural network optimized by quantum genetic algorithm. *J Supercomput* 79, 13421–13441 (2023).

Gong, S., Gong, X., and Bi, X., Feature selection method for network intrusion based on GQPSO attribute reduction, *2011 International Conference on Multimedia Technology*, Hangzhou, China, pp. 6365-6368, 2011

Gouveia, A. and Correia, M., Towards Quantum-Enhanced Machine Learning for Network Intrusion Detection, *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, Cambridge, MA, USA, pp. 1-8, 2020

Guo, L., Research on Anomaly Detection in Massive Multimedia Data Transmission Network Based on Improved PSO Algorithm, in *IEEE Access*, vol. 8, pp. 95368-95377, 2020,

Hadib, M., Rajasegarar, S. and Pan, L., Quantum deep learning-based anomaly detection for enhanced network security. *Quantum Mach.Intell*.6,26(2024)

Heigl, M. S. and Fiala, D., A Lightweight Quantum-Safe Security Concept for Wireless Sensor Network Communication, *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Kyoto, Japan, pp. 906-911, 2019

K., S., C., R., Sermakani, A. M., Dhakshunhaamoorthiy, Menaga, P. and Maharasi, M., Quantum-Resistant Wireless Intrusion Detection System using Machine Learning Techniques," *2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA),* Pune, India, pp. 1-5, 2023

Kalinin, M. O. and Krundyshev, V. M., Computational intelligence technologies stack for protecting the critical digital infrastructures against security intrusions, *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*, London, United Kingdom, 2021, pp. 118-122,

Khatri, A.H., Gadag, V., Singh, S., Satapathy, S.K. and Mishra, S., Quantum Data Traffic Analysis for Intrusion Detection System. *In Evolution and Applications of Quantum Computing (eds S.N. Mohanty, R. Aluvalu and S. Mohanty)*. (2023).

Kim, T. and S, Madhavi,. Quantum intrusion detection system using outlier analysis. *Sci Rep* **14**, 27114 (2024).

Kumar G., G., U., Nagar, A, Patel, S, Jain, A, Quantum assisted machine learning for intrusion detection systems. *AIP Conf. Proc.* 29 July 2024; 3075 (1): 020280.

Kumar, R and Swarnkar, M, QuIDS: A Quantum Support Vector machine-based Intrusion Detection System for IoT networks, *Journal of Network and Computer Applications*, Volume 234, 2025, 104072, ISSN 1084-8045,

Kuo, S., Shen, J., Liu, C. and Chou, Y., Hybrid Quantum-inspired Evolutionary Neural Networks for Intrusion Detection System, *2024 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Kuching, Malaysia, 2024, pp. 2801-2806,

Lee, C., Sohn, I. and Lee, W., Eavesdropping Detection in BB84 Quantum Key Distribution Protocols, in *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2689-2701, Sept. 2022,

Li, M., Zhang, H., Fan, L. and Han, Z., "A Quantum Feature Selection Method for Network Intrusion Detection," *2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, Denver, CO, USA, 2022, pp. 281-289,

Liang, H., Wu, J., S., Mumtaz, Li, J., Lin, X. and Wen, M., MBID: Micro-Blockchain-Based Geographical Dynamic Intrusion Detection for V2X, in *IEEE Communications Magazine*, vol. 57, no. 10, pp. 77-83, October 2019,

Ling, Z. & Hao, Z. J., An Intrusion Detection System Based on Normalized Mutual Information Antibodies Feature Selection and Adaptive Quantum Artificial Immune System. *International Journal on Semantic Web and Information Systems (IJSWIS), 18*(1), 1-25. (2022).

Ling, Z. & Hao, Z. J., Intrusion Detection Using Normalized Mutual Information Feature Selection and Parallel Quantum Genetic Algorithm. *International Journal on Semantic Web and Information Systems (IJSWIS), 18*(1), 1-24. (2022).

Liu, J., Qin, X. and Jiang, F., A quantum inspired differential evolution algorithm with multiple mutation strategies, *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Wuhan, China, 2022, pp. 927-934,

Liu, W. -J. and Li, Z. -X., "Secure and Efficient Two-Party Quantum Scalar Product Protocol With Application to Privacy-Preserving Matrix Multiplication," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 70, no. 11, pp. 4456-4469, Nov. 2023,

Luitel, B., Venayagamoorthy, G. K. and Johnson, C. E., Enhanced wide area monitoring system, *2010 Innovative Smart Grid Technologies (ISGT)*, Gaithersburg, MD, USA, 2010, pp. 1-7,

Makopa, J., Christopher, A., Shah, R. and Mandela, N., Internet of Things (IoT) Network Forensic Analysis Using the Raspberry Pi 4 Model B and Open-Source Tools, *2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS)*, KOTTAYAM, India, 2023, pp. 1-7,

Ma, R., Liu, Y., and Lin, X., Hybrid QPSO based wavelet neural networks for network anomaly detection, *Second Workshop on Digital Media and its Application in Museum & Heritages (DMAMH 2007)*, Chongqing, China, 2007, pp. 442-447,

Mu X., Ding, Y., J., Wang, Z., Salamo, G. J. and Little, J., Coupling between InAs quantum dots and strained InGaAs/GaAs coupled quantum-wells: a novel type of quantum dots, *InternationalQuantum Electronics Conference, 2004. (IQEC)*., San Francisco, CA, USA, 2004, pp. 552-554.

Othmane F., Mohamed, A. F., Mohamed, B., Tarek, B., Burak, K., Kim-Kwang, R. C., 2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT, Computers & Security, Volume 127, 2023, 103097, ISSN 0167-4048,

Rahman, M. A., Shahriar, H., Clincy, V., Hossain, M. F. and Rahman, M., A Quantum Generative Adversarial Network-based Intrusion Detection System, *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, Torino, Italy, 2023, pp. 1810-1815

Raj, M.G., Pani, S.K. Intrusion detection system using combination of deep residual fuzzy network and white shark-dwarf mongoose optimization, *Soft Comput* (2023).

S, S., Doshi, S. and Joshi, A., Enhancing Security in Automobile Edge Computing through Federated Learning and Blockchain, *2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS)*, KOTTAYAM, India, 2023, pp. 1-6,

Salek, M. S. et al., A Novel Hybrid Quantum-Classical Framework for an In-Vehicle Controller Area Network Intrusion Detection, in *IEEE Access*, vol. 11, pp. 96081-96092, 2023,

Salvakkam, D.B., Saravanan, V., Jain, P.K. et al., Enhanced Quantum-Secure Ensemble Intrusion Detection Techniques for Cloud Based on Deep Learning, *Cogn Comput* 15, 1593–1612, 2023.

Shen, L. and Feng, L., An efficient architecture for Network Intrusion Detection based on Ensemble Rough Classifiers, *2013 8th International Conference on Computer Science & Education*, Colombo, Sri Lanka, 2013, pp. 1411-1415,

Shen, J. -Y. *et al*., An Efficient Quantum-inspired Computing Approach for Intrusion Detection System, *2024 IEEE 24th International Conference on Nanotechnology (NANO)*, Gijon, Spain, 2024, pp. 306-310,

Shen, S., Hu, K., Huang, L., Li, H., Han, R., Cao, Q., Quantal Response Equilibrium-Based Strategies for Intrusion Detection in WSNs, *Mobile Information Systems*, 2015, 179839, 10 pages, 2015.

Soliman, O. S., Rassem, A., A Network Intrusions Detection System based on a Quantum Bio Inspired Algorithm, *International Journal of Engineering Trends and Technology (IJETT)*, V10(8),370-379 April 2014. ISSN:2231-5381.

Thirumalairaj, A., and Jeyakarthic, M., Perimeter Intrusion Detection with Multi Layer Perception using Quantum Classifier, *2020 Fourth International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, 2020, pp. 348-352,

Venkatachalam, P. and Liu, D. Q., On Hybrid Artificial Neural Networks and Variational Quantum Classifier for Network Intrusion Detection, *2023 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Jiangsu, China, 2023, pp. 410-416,

Wu, X., Jin, Z., Zhou, J., Duan, C., Quantum walks-based classification model with resistance for cloud computing attacks, *Expert Systems with Applications*, Volume 232, 2023, 120894, ISSN 0957-4174

Yin, X., Quantum evolutionary algorithm based network intrusion detection, *2010 3rd International Conference on Computer Science and Information Technology*, Chengdu, China, 2010, pp. 683-685,

Yang, C., Yang, H. and Deng, F., Quantum-inspired immune evolutionary algorithm based parameter optimization for mixtures of kernels and its application to supervised anomaly IDSs, *2008 7th World Congress on Intelligent Control and Automation*, Chongqing, China, 2008, pp. 4568-4573

Yong, H. and Xue, f. Z., Quantum Self Organized Map-based intrusion detection system, *2010 International Conference on Artificial Intelligence and Education (ICAIE)*, Hangzhou, China, 2010, pp. 140-145,

Yong, H., and Xue, F. Z., Quantum Growing Hierarchical Self Organized Map-Based Intrusion Detection System, *2010 International Conference on System Science, Engineering Design and Manufacturing Informatization*, Yichang, China, pp. 110-115, 2010,

Biographies

Vidhyashree M is currently a Research Scholar who is pursuing PhD with the School of Computer Science Engineering and Information Systems, Vellore Institute of Technology (VIT), Vellore, India. She had completed her Integrated M.Tech Software Engineering in 2020 with the School of Computer Science Engineering and Information Systems, Vellore Institute of Technology (VIT), Vellore, India. Her research interests include Quantum computing, Cyber security, and Blockchain.

Subhashini R is currently an Associate Professor with the School of Computer Science Engineering and Information Systems, VIT. She received the Ph.D. degree from the Vellore Institute of Technology (VIT), Vellore, India, in 2018. She is In-Charge of the Artificial Intelligence Research Laboratory, IBM, where she is involved in consultancy industrial projects. She has more than 22 years of experience in teaching. She has published more than 46 international/national journals and conferences. Her research interests include artificial intelligence, machine and deep learning, and bio-inspired algorithms.