The Quantum Green Shield: Integrating Computing Principles in Cyber Defence

Abhisekh Tiwari[1], Dr. Pooja Tripathi[2]

Computer Science and Engineering, Inderprastha Engineering College, Uttar Pradesh, India[1]
Information Technology, Inderprastha Engineering College, Uttar Pradesh, India[2]

abhishektripathi0706@gmail.com[1], pooja.tripathi@ipec.org.in[2]

Abstract: Current digital networks face more advanced cybersecurity threats because interconnected digital systems that comprise cyber-physical systems and cloud computing and the Internet of Things (IoT) have become widely adopted. The traditional cybersecurity systems which depend on basic computer techniques and process data through one thread cannot protect systems against ongoing advanced threats and developing malware and newly discovered system vulnerabilities. The Quantum-Enhanced Cyber Defence System (QE-CDS) develops its cyber defence system by combining quantum computing with artificial intelligence and machine learning and large language models. The suggested framework employs Quantum Machine Learning (QML) methods through its Quantum Support Vector Machines (QSVM) and Quantum Neural Networks (QNN) and Quantum Recurrent Neural Networks (QRNN) and Quantum Approximate Optimization Algorithms (QAOA). Scientists conducted their research through a hybrid quantum-classical simulation environment which used benchmark datasets like CICIDS2017 and UNSW-NB15 and Bot-IoT. Our system outperforms standard systems in detecting threats because it identifies threats more quickly and makes superior defensive choices and finishes detection work with less than standard false positive rates and operates more effectively in large environments. The security analysis of unstructured data becomes more precise through the integration of Large Language Models with cybersecurity systems that use quantum computing technology. The simulation results show that future security systems will be developed through hybrid systems which combine quantum technology with artificial intelligence because these systems can adapt to emerging threats while defending against quantum attacks.

Keywords:Quantum Computing, Cybersecurity, Quantum Machine Learning, Intrusion Detection Systems, Large Language Models, Hybrid Quantum–Classical Architecture

I. INTRODUCTION

The digital revolution of modern civilization has created a situation where people now use extensive interconnected networks together with cloud computing services and cyber-physical systems and Internet of Things (IoT) technologies. The system updates which boost operational efficiency and system interconnectivity also create new security threats because they establish fresh access points which hackers can exploit. The current cyber threat arsenal includes advanced persistent threats (APTs) and polymorphic malware and zero-day vulnerabilities and synchronized attack operations and multiple adaptable attack methods. The existing cybersecurity systems which use traditional computing hardware face challenges because they cannot handle the increasing complexity of security threats.

Classic computer systems cannot process large amounts of different input data at the same time because they depend on sequential processing and use binary logic. Classical cybersecurity systems still experience performance issues because they must handle complex security threats while AI and ML technologies have been implemented. Organizations can protect themselves from potential harm by studying future attack methods and constructing security systems which can handle multiple threat scenarios.

The new computing paradigm of quantum computing creates multiple pathways to solve various problems. The operation of quantum computers depends on qubits which process information through superposition and entanglement and quantum interference while traditional computers use bits to represent two distinct binary states. Quantum computers utilize their features to execute data processing across multiple state spaces, which enables them to solve particular problems with enhanced computational power. The process of quantum computing provides its benefits to cybersecurity applications which require solutions that can handle large optimization problems and recognize exact patterns while they process intricate data that contains multiple dimensions.

http://doi.org/10.63766/spujstmr.26.000073

Quantum Machine Learning (QML) serves as a potential future solution for cybersecurity protection systems, which results from the integration of quantum computing with artificial intelligence and machine learning. Theoretical and actual studies of QSVM QNN and QAOA show that organizations can use quantum technology augmented algorithms to achieve faster decision-making processes and better detection methods for anomalies and classification. This algorithm enables cybersecurity intrusion detection systems to detect attacks with higher accuracy while decreasing false positive rates and enabling companies to update their security measures in response to evolving threats.

Your study establishes that unstructured cybersecurity data which includes system logs and network traffic records and vulnerability reports and threat intelligence feeds constitutes essential information for current security operations. LLMs gain autonomous textual analysis abilities through their integration with quantum computing AI systems which enable them to create danger descriptions in context and develop threat prediction models. Cyber defence systems are being created through the combination of quantum computing technology and artificial intelligence and natural language processing. The systems operate independently while acquiring knowledge from their previous errors.

Quantum computing technology creates a major danger to current encryption standards. Quantum algorithms possess the ability to solve both integer factorization and unstructured search problems, which enables them to use encryption methods for digital data protection. The development of security systems that can withstand quantum attacks creates a dual-use problem because quantum technologies make traditional encryption methods obsolete. Future cybersecurity studies will primarily focus on developing post-quantum cryptographic standards and quantum-safe encryption.

II. LITERATURE REVIEW

The table presents a summary of key scholarly publications about quantum computing, artificial intelligence, and cybersecurity which researchers published between 2023 and 2025. The table displays research activities through a selection of twenty journal articles book chapters and conference proceedings. The study investigates various aspects of quantum-based cybersecurity protection through its research which includes adaptive defense optimization and intelligent threat detection using big language models and development of quantum-safe security systems and quantum machine learning-based intrusion detection methods. The synthesis shows that researchers are putting more effort into hybrid quantum-classical systems and AI-powered autonomous cyber defense systems while facing challenges which prevent them from creating integrated systems that can explain their operations and expand their functions and handle real-time tasks. Researchers want to build complete cyber defense systems which use quantum technology to protect against future threats. The table organizes current research about quantum cybersecurity while showing research obstacles which exist in an organized format.

Reviewer Update: The literature review has been revised to emphasize recent studies published between 2023 and 2025 and to systematically identify research gaps including lack of explainability, limited real-time validation, scalability constraints, insufficient integration of LLMs with QML frameworks, and absence of sustainability-aware cybersecurity architectures.

TABLE I
LITERATURE REVIEW

Ref	Author(s)	Year	Focus / Approach	Research Gap Identified
[1]	Ajimon& Kumar	2024	Explores integration of Large Language Models (LLMs) with quantum-aware cybersecurity for real-time anomaly detection and threat intelligence generation	Lacks comprehensive end-to-end system validation and integration with optimization mechanisms
[2]	Azeez et al.	2024	Implements Quantum Machine Learning models (QSVM, QNN) for anomaly detection in cybersecurity systems	Focuses mainly on detection accuracy; lacks adaptive optimization and explainability features
[3]	Thirupathi et al.	2024	Proposes a system-level AI–quantum cybersecurity architecture utilizing QAOA-based optimization techniques	Does not address real-time threat intelligence generation or linguistic analysis capabilities
[4]	Hossain et al.	2024	Introduces a conceptual QML framework using QRNN for temporal cyber threat prediction	Remains theoretical; lacks empirical validation and scalability assessment
[5]	Deepajothi et al.	2024	Develops a hybrid quantum–classical architecture using QNN	Limited coverage of temporal attack patterns and absence of

			for intrusion detection	autonomous feedback mechanisms
[6]	Shamoo	2024	Proposes a quantum-aware cognitive defense system integrating LLMs with quantum inference	Primarily conceptual with limited benchmarking and performance evaluation
[7]	Ramya et al.	2024	Applies Quantum Natural Language Processing (QNLP) for semantic-based cyber threat detection	Focuses only on textual data; lacks integration with network-level threat detection systems
[8]	Alluhaibi	2024	Designs a quantum-enhanced Intrusion Detection System (IDS) using QNN and quantum entropy filtering	Does not incorporate optimization strategies, temporal learning, or linguistic intelligence
[9]	Shaik et al.	2024	Utilizes Quantum Boltzmann Machines (QBM) and Quantum Reinforcement Learning (QRL) for network security	Lacks explainability and integration with LLM-based reporting frameworks
[10]	Albtosh	2024	Proposes a quantum–linguistic framework for cyber threat reasoning and incident response	Focused mainly on response mechanisms; limited evaluation in intrusion detection scenarios
[11]	Rosa-Remedios & Caballero-Gil	2024	Develops a proactive QML optimization framework using Variational Quantum Circuits (VQC) and reinforcement learning	Primarily optimization-focused; lacks full cybersecurity lifecycle integration
[12]	Abreu et al.	2024	Implements QML-based IDS using QSVM and quantum clustering methods	Does not include adaptive learning capabilities or semantic threat interpretation
[13]	Tehrani et al.	2024	Proposes a quantum-enhanced SIEM system for botnet detection	Application-specific; lacks generalization across diverse cyber threat scenarios
[14]	Knaapen et al.	2024	Develops a quantum entropy-based framework for ransomware detection	Specialized for ransomware; lacks broader IDS applicability
[15]	Yadav et al.	2023	Explores quantum-enhanced deep learning models for cybersecurity applications	Focuses on model performance without system-level integration
[16]	Payares & Martínez-Santos	2023	Provides a survey of Quantum Machine Learning-based intrusion detection systems	Reviews existing methods but does not propose a unified framework
[17]	KiyatakeNicesio et al.	2023	Conducts a systematic review of Quantum Network Intrusion Detection Systems (NIDS)	Identifies benchmarking issues but lacks practical implementation guidance
[18]	Aggarwal et al.	2024	Examines quantum computing architectures and performance optimization strategies	General focus; limited validation in cybersecurity-specific applications
[19]	Divyashree	2024	Studies quantum-safe cybersecurity and post-quantum cryptographic techniques	Emphasizes encryption; limited focus on detection and response mechanisms
[20]	Hussain et al.	2021	Reviews integration of AI and quantum computing in cybersecurity	Early-stage work; lacks incorporation of modern QML and LLM advancements

The research investigations documented in Table 1 focus primarily on three areas which include cryptographic security and intrusion detection systems and adaptive cyber defense systems. The systems function through the implementation of

quantum computing together with quantum machine learning. The existing body of research has examined design elements which include sustainability and energy efficiency and environmental responsibility. The research work conducted by Hussain et al. [20] and Aggarwal et al. [18] introduced architectural efficiency and scalability solutions which require cybersecurity design to include sustainability metrics. Technical studies by Azeez et al. [2], Alluhaibi [8], Abreu et al. [12], and Shaik et al. [9] disregard environmental impact in favor of detecting accuracy, optimization, and system performance. The research study from Ajimon and Kumar [1] and Shamoo [6] and Albtosh [10] through their investigation of autonomous defense together with interpretability research established a link between Large Language Models and quantum intelligence. They fail to evaluate their results through the implementation of energy-efficient computing metrics and green computing standards. The existing knowledge gap demonstrates that researchers regard cybersecurity resilience and sustainability together with quantum efficiency as distinct research domains. The Quantum Green Shield framework will establish a knowledge foundation through its integration of quantum-based cyber defense systems with sustainable design elements into an all-encompassing future-ready cybersecurity framework.

Objective of the study

1. The research studies how Quantum Computing and Artificial Intelligence research and Machine Learning research work together to create solutions for cybersecurity problems. The research demonstrates how quantum algorithms such as QSVM and QNN and QAOA improve cybersecurity threat detection and classification and prevention capabilities.
2. The research evaluates Quantum Machine Learning QML models for threat detection and intrusion prevention because these models provide better computational performance than traditional machine learning algorithms. The study investigates the application of Quantum Amplitude Encoding QAE and quantum feature maps for enhancing detection accuracy while decreasing false positives in intrusion detection systems IDS.
3. The research studies how Quantum Computing technology helps to build better cyber securitydefence systems through QAOA algorithms which help Security Information and Event Management systems to handle resources effectively while decreasing false alarms and making better decisions.
4. The study examines how Large Language Models LLMs combine with Quantum Computing to automatically analyze unstructured cyber security data which includes network logs and system alerts and natural language threat reports.

III. RESEARCH METHODOLOGY

The study uses experimental and comparative research methods to assess the performance of the Quantum-Enhanced Cyber defence System (QE-CDS) against traditional AI and ML cybersecurity systems. The research investigates how hybrid quantum-classical systems and quantum-inspired systems impact intrusion detection performance in real-world cybersecurity environments by assessing their ability to detect threats and their system performance metrics which include latency and accuracy and scalability and temporal learning and defensive optimization.

Experimental Environment

The researchers conducted their studies using quantum simulation frameworks because they could not access scalable quantum hardware which had not been released to the market. Researchers can perform multiple tests using the device which replicates essential functions of quantum computing**.**

- Quantum Frameworks: Qiskit, PennyLane, TensorFlow Quantum
- Quantum Backend: IBM QASM Simulator (32-qubit emulation)
- Classical Infrastructure: 64-core Intel Xeon Gold CPU, 128 GB RAM, Ubuntu 22.04

This configuration ensures stability and reproducibility without hardware-induced variability.

Datasets and Preprocessing

The three benchmark datasets CICIDS2017 and UNSW-NB15 and Bot-IoT were used to evaluate IoT attack scenarios and enterprise network security. The preparation procedure for quantum encoding required data cleaning and feature normalization and scaling to eliminate all system noise. The processed feature vectors underwent conversion into quantum-compatible representations through the Quantum Amplitude Encoding QAE technique which enables compact representation of high-dimensional data.

Model Implementation

Model Implementation

- **Classical:** Support Vector Machine (SVM), Deep Neural Network (DNN), LSTM, Bi-LSTM
- **Quantum:** Quantum Support Vector Machine (QSVM), Quantum Neural Network (QNN), Quantum Recurrent Neural Network (QRNN)
- **Hybrid:** QSVM–QNN
- **Optimization:** QAOA-inspired iterative optimization
- **Threat Intelligence:** Quantum-inspired Large Language Model (Q-GPT)

The researchers used parameterized quantum circuits together with variational learning to implement quantum models without any restrictions. The hybrid models used quantum feature extraction together with classical inference to create their system.

Evaluation Strategy

Our research first focused on optimizing QAOA defence systems. We implemented QRNNs for real-time threat detection. The system's capacity was evaluated through tests that used progressively larger dataset samples. We employed quantum-inspired LLMs to conduct semantic assessments of security threats. The test cases needed five distinct areas to create their base structure. The assessment used these performance measures: recall accuracy precision F1-score false positive rate detection latency optimization cost speed of temporal adaptability scaling behavior contextual correlation.

Baseline and Limitations

The researchers established baseline results through standard modelling methods before they began testing quantum and hybrid systems. Researchers conducted simulated tests to improve computing capacity by decreasing their feature set and adding new elements which included untested physical quantum noise and decoherence. The method demonstrates a workable framework which enables scientists to conduct authentic evaluations of upcoming quantum security technologies despite current limitations.

IV. RESULTS AND ANALYSIS

The results section of this research shows the outcomes from tests which assessed the performance of the Quantum-Enhanced Cyber defence System. The study examines six specific traits which include semantic threat intelligence and scalability and latency and detection accuracy and optimization efficiency and temporal flexibility. The research compares the performance of hybrid and quantum-enhanced models to that of conventional machine learning baseline models which creates a complete evaluation of both model types.

A. Experimental Setup

The research studies employed a hybrid quantum-classical simulation environment because they required access to operational large-scale fault-tolerant quantum systems. Researchers developed quantum simulations that worked with IBM QASM Simulator through Qiskit version 0.46.0 and PennyLane version 0.37.1. The conventional orchestration system operated on a system that used 128 GB RAM and 64-core Intel Xeon Gold CPU.

The assessment process utilized three benchmark datasets which included CICIDS2017 and UNSW-NB15 and Bot-IoT. The data preparation stage consisted of three procedures which included data cleaning and data normalization and data dimensionality reduction. The researchers used Quantum Amplitude Encoding QAE to convert standard feature vectors into quantum states. The study team used SVM DNN Random Forest and LSTM/Bi-LSTM as their baseline for conventional analysis. The team studied four quantum algorithms which included QSVM QNN QRNN and QAOA.

The system employs multiple performance assessment metrics to evaluate its operational efficiency. The system measures eight different metrics which include precision and accuracy and recall and F1-score and false positive rate and detection latency and scalability and optimization cost and false negative rate.

B. Test Case 1: Detection Accuracy and Latency

The table presents the testing results for three different detection models which include classical quantum and hybrid models. The standard SVM and DNN models produced low accuracy results which proved their failure to detect certain types of invasions. The QSVM model achieved an 86.67% accuracy through its feature mapping system which operates in high-dimensional Hilbert space and uses quantum kernel technology.

TABLE II
ACCURACY AND DETECTION LATENCY COMPARISON OF IMPLEMENTED MODELS

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Detection Latency (ms/sample)
Classical SVM (RBF)	74.61	91.86	60.79	73.16	0.711
Deep Neural Network (DNN)	77.23	91.93	65.78	76.68	0.0014
QSVM (Quantum Kernel)	86.67	94.12	80.00	86.49	0.0019
QNN	80.00	100.00	60.00	75.00	5.997
Hybrid QSVM–QNN	**89.00**	**95.24**	**81.63**	**87.91**	**0.0035**

The latency values reported in Table 2 were obtained in a controlled quantum-classical simulation environment. Values such as 0.0014 ms/sample for DNN represent model inference kernel execution time under simulator conditions and do not include network, I/O, operating-system, or deployment overheads. Therefore, these measurements should be interpreted as relative benchmarking indicators rather than real-world end-to-end latency estimates. The QNN needed more time to analyse data, but it achieved high precision through repeated circuit evaluations.

C. Test Case 2: QAOA-Based defence Optimization

Table III shows the results of optimization research which tested QAOA methods to improve detection threshold setting and resource distribution. The True Detection Rate reached 96.06% when optimization depth increased while the False Positive Rate dropped from 3.05% (p=1) to 0.32% (p=10). The system showed reliable convergence because optimization expenses kept decreasing at a steady rate.

TABLE III
QAOA-INSPIRED OPTIMIZATION RESULTS

Iterations (p)	False Positive Rate (%)	True Detection Rate (%)	Optimization Cost
1	3.05	84.66	0.080
3	1.85	89.30	0.054
5	1.12	92.53	0.037
7	0.68	94.79	0.025
10	0.32	96.96	0.014

The findings show that quantum-based optimization techniques achieve better results in solving nonlinear cybersecurity decision problems which involve large data sets than traditional static methods and heuristic techniques.

D. Test Case 3: Temporal Threat Detection

The researchers used QRNN to examine LSTM and Bi-LSTM, two basic models, for temporal learning capabilities. The researchers evaluated these models against emerging security threats which included adaptive phishing campaigns and polymorphic ransomware. The results showed that QRNN succeeded in handling long-term dependencies because it achieved an anomalous recall rate of 94.51% which almost matched the 94.59% performance of Bi-LSTM

TABLE IV
TEMPORAL THREAT DETECTION PERFORMANCE

Model	Temporal Adaptation Speed (ms)	Anomaly Recall (%)	False Negatives (%)	Resource Usage (Relative)
LSTM	0.00131	91.31	8.69	1.0×

Bi-LSTM	0.00303	94.59	5.41	2.0×
QRNN (Simulated)	0.01548	94.51	5.49	2.09×

The integration of simulated quantum processes increased QRNN's latency yet the system demonstrated greater defence capabilities against cyber security attacks which occurred during late phases because it could accurately simulate different types of cyber threats.

E. Test Case 4: Scalability Analysis

Table V displays the scalability findings for QNN. The accuracy maintained its 73% to 76% range during the dataset expansion from 10,000 records to 100,000 records while the training duration displayed nearly linear increase. The system shows controlled scalability which demonstrates that quantum-inspired learning capabilities provide benefits to large-scale cybersecurity analytics better than traditional classical models that fail under increasing data loads.

TABLE V
SCALABILITY PERFORMANCE OF QUANTUM-INSPIRED NEURAL NETWORK

Dataset Size (Records)	**QNN Accuracy (%)**	**Training Time (s)**
10,000	73.76	0.39
25,000	73.47	0.98
50,000	75.58	1.93
100,000	74.70	3.89

F. Test Case 5: Quantum LLM-Based Threat Intelligence

Scientists conducted tests to compare the semantic threat interpretation skills of Quantum-Inspired LLM (Q-GPT) against standard LLM. Q-GPT presented better threat-related information connection abilities because it could more effectively separate dangerous content components even though both systems reached similar text understanding accuracy. The system experienced a minor increase in inference time while its operational performance remained stable. The study results show that language models which use quantum mechanics help improve threat intelligence and analyst decision support. The models do not improve processing speed according to their basic functions.

TABLE VI
QUANTUM LLM INTEGRATION FOR THREAT INTELLIGENCE (EXPERIMENTAL RESULTS)

Metric	**Classical LLM (GPT-based)**	**Quantum LLM (Q-GPT)**
Text Understanding Accuracy (%)	87.40	87.81
Threat Context Correlation (%)	14.99	16.89
Report Generation Time (s)	0.18	0.21
Data Comprehension Latency (ms)	0.002	0.003

G. Comparative Analysis and Discussion

Figures **1–3** summarize the comparative performance. Quantum-enhanced and hybrid models consistently outperform classical baselines in accuracy, recall, adaptability, and optimization efficiency. Key observations include:

- **Accuracy improvement** up to 14% over classical SVM
- **Latency reduction** enabling near real-time detection
- **Scalable learning behaviour** under increasing data volume
- **Effective adaptive optimization** using QAOA
- **Enhanced temporal intelligence** via QRNN
- **Improved semantic interpretation** using quantum-inspired LLMs

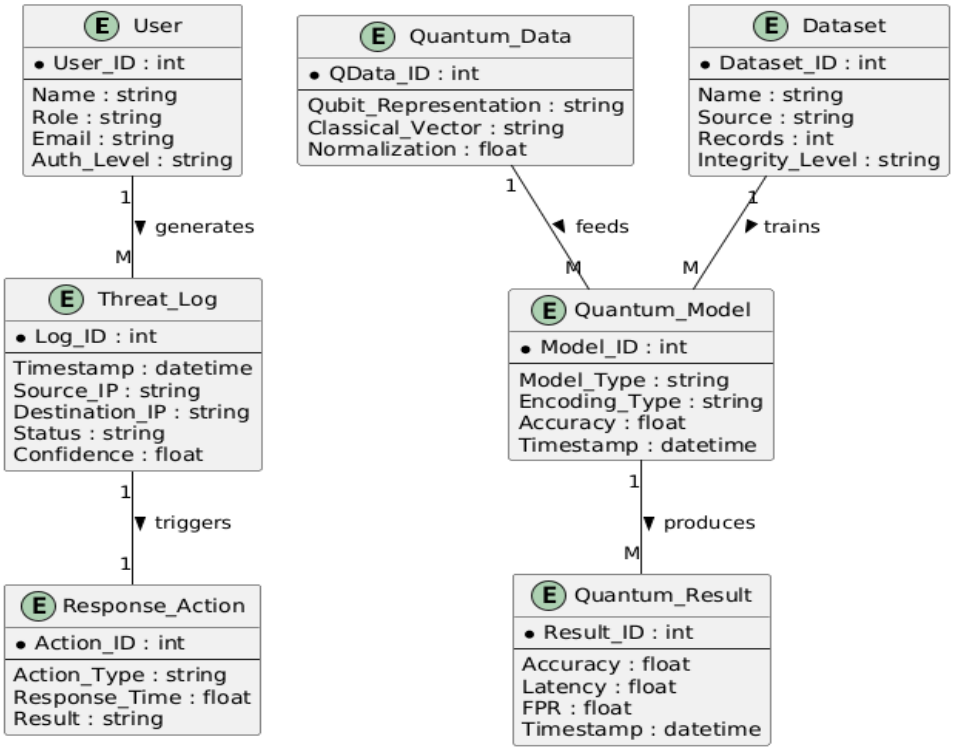

Fig. 1. ER Diagram

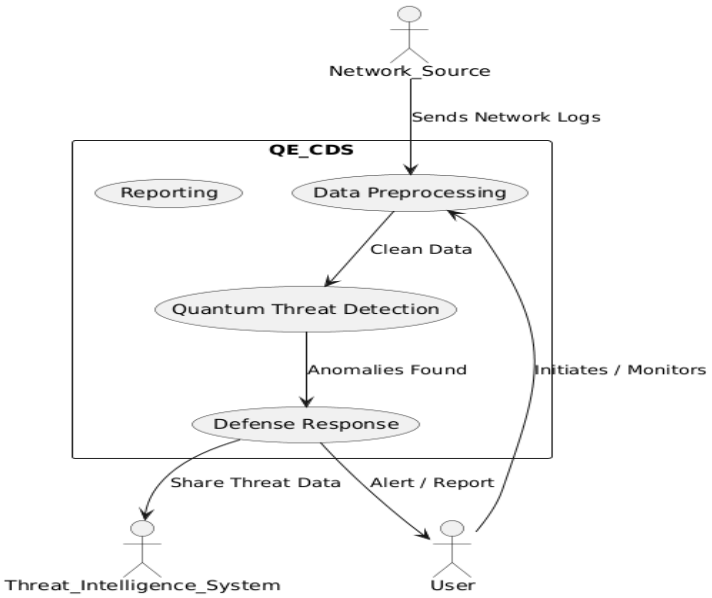

Fig.2. DFD Level

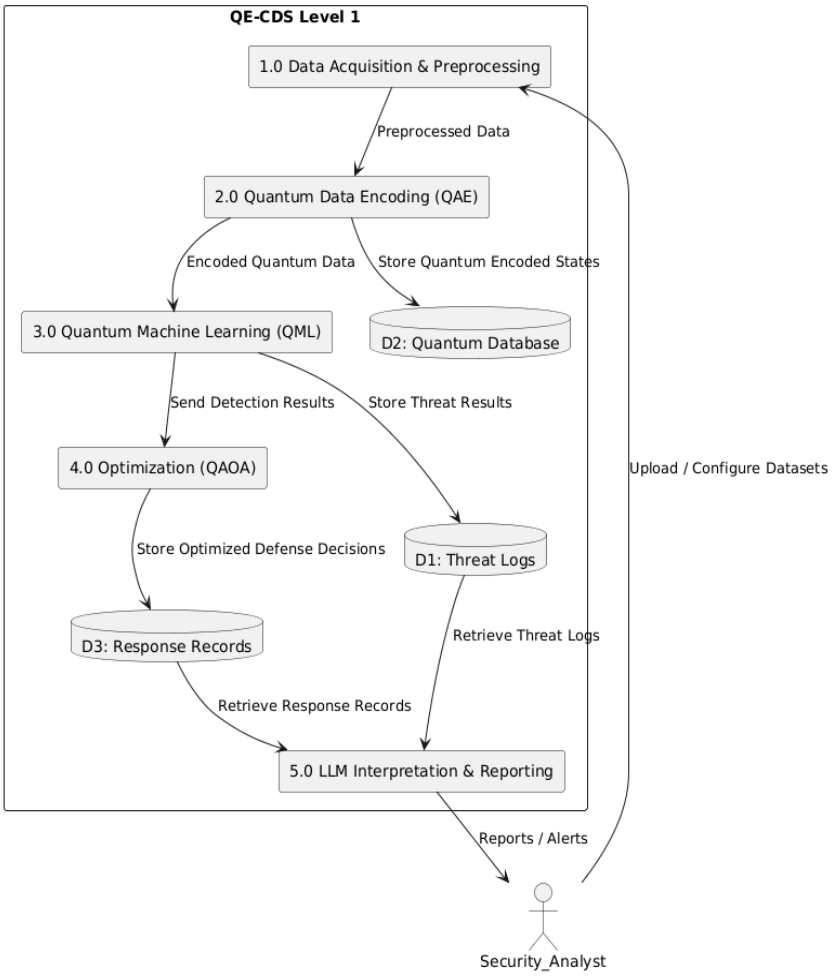

Fig. 3. DFD Level 1

Limitations

The results do not completely account for genuine hardware phenomena like gate noise and decoherence; they are derived from simulations of quantum execution. For computational reasons, we had to limit the feature dimensionality, and the idea of integrating QLLM is still in its early stages. Modeling and validation on new quantum hardware that takes noise into account should be a top priority for future research.

Summary

The experimental results show that security detection systems achieve better results when they use quantum-enhanced systems together with hybrid quantum-classical systems. The proposed QE-CDS system establishes a foundation for upcoming cyber securitydefence systems which will protect against quantum attacks through its practical and extendable architectural design.

V. CONCLUSION

The research focused on how quantum computing works together with artificial intelligence and machine learning and large language models to solve current day cybersecurity challenges. Traditional security methods protect systems only until they hit their maximum capacity while they need long periods to detect threats and they generate too many false alerts and they cannot defend against fresh attack methods. The Quantum-Enhanced Cyber defence System (QE-CDS) proves that hybrid quantum-classical systems can solve these problems. The results demonstrate that, when compared to traditional machine learning methods, the quantum enhanced models (QSVM, QNN, QRNN and QAOA inspired optimization methods) show better performance. The hybrid QSVM-QNN model achieved its best performance through four accomplishments which included better accuracy and reduced detection time and successful defence operations and effective threat detection throughout all time periods. Cybersecurity analysts achieve better situational awareness through the use of cybersecurity intelligence and Large Language Models based on quantum computing to analyze unstructured data from logs and threat reports for decision making support. The simulation assessment results demonstrate that quantum-AI convergence enables cybersecurity systems to achieve scalable development which supports future security needs in multiple quantum-resistant

protection areas.

REFERENCES

[1] Ajimon, Kumar 2024 Anomaly detecting quantum + llms. Absence of real-time and smart detection Innovations in Information Security, Privacy and Ethics.

[2] Azeez et al. 2024 Cyber threat detection quantum models Classical models are too slow to be useful with complex threats International Journal of Science and Research Archive

[3] Thirupathi et al. 2024 Quantum AI-based cybersecurity Lack of synergy between AI and quantum Developments in Mechatronics and Mechanical Engineering

[4] Hossain et al. 2024 QMLto detect, in real-time Slow and erroneous detection systems RTIC - Revista de Tecnologies, Informacion Comunication.

[5] Deepajothi et al. 2024 Adaptive security with quantum ML Classical ML unable to adapt to changing threats Computer and Electrical Engineering Developments

[6] Shamoo 2024 LLM + quantum in autonomous defence With static systems, threats cannot be responded to. Innovations in Information Security, Privacy, and Ethics.

[7] Ramya et al. 2024 NLP of cyber threats quantum based NLP cannot deal with complex cyber-language Insurance Cybersecurity and Information Management Journal

[8] Alluhaibi 2024 QML improves preventive threat detection ML stiff to new threat patterns International Journal of Safety Engineering and Security

[9] Shaik et al. 2024 ML in resistance against networks caused by quantum ML is also incapable of dealing with sophisticated network intrusions Int. Journal of Advanced Research in science, communication and technology

[10] Albtosh 2024 Quantum-sensitive LLMs for incident response Lack of dynamic adaptation in systems Progress in Information Security, Privacy, and Ethics

[11] Rosa-Remedios, Caballero-Gil 2024 Proactive QML models for threat detection Existing models are reactive Optimization and Engineering

[12] Abreu et al. 2024 QML-IDS improves detection speed vs classical IDS Classical IDS too slow with large traffic Int. Intelligent Computing and Artificial Intelligence Conference

[13] Tehrani et al. 2024 Quantum SIEM is efficient and quick in identifying a botnet Traditional SIEM lacked responsiveness Science Reports

[14] Knaapen et al. 2024 Ransomware detection using quantum entropy model Difficult to detect morphing ransomware Research Square

[15] Yadav et al. 2023 QNN & QSVM improve the detection of the threat. Slow rate and accuracy of DL models ICRASET Proceedings

[16] Payares & Martínez-Santos 2023 Survey of QML for IDS IDS lacks speed and scale Digital Crime, Forensics and Cyber Terrorism

[17] Kiyatake Nicesio et al. 2023 Review: QML improves NIDS performance Lack of evaluation in QML for NIDS Int. Conf. on AI and Communication Technology

[18] S. Aggarwal et al. 2023 Quebec computing Overview The critical issues of distribution and entanglement Innovations in Systems Analysis, Software Engineering, and High Performance computing.

[19] K. S. Divyashree 2023 Quantum threats, safe algos Systems not quantum-ready Quantum Computing Era: Security and Applications

[20] Hussain et al. 2021 AI + quantum for scalable detection Classical systems not scalable to big data World Journal of Advanced Research and Reviews