iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

TOWARD QUANTUM-ENHANCED INTRUSION DETECTION: UNIFIED EVALUATION OF LEARNING MODELS

V R Srividhya
Assistant Professor, RV Institute of Technology and Management, Bengaluru,
Affiliated to Visvesvaraya Technological University, Belagavi
Gali Akshata
Mamata Balesh Kamagoudar
Neha Shakari
Sampreeth N Ganganagoudar
UG Students, RV Institute of Technology and Management, Bengaluru,
Affiliated to Visvesvaraya Technological University, Belagavi

ABSTRACT
Intrusion Detection Systems (IDS) rely on intelligent learning techniques to identify complex and evolving attack patterns within network traffic. This paper presents a comparative study of Support Vector Machines (SVM), Quantum Support Vector Machines (QSVM), and Variational Quantum Classifiers (VQC) in the context of intrusion detection. A unified evaluation framework is employed to compare these models based on feature representation, computational complexity, scalability, hardware requirements, and deployment feasibility. The analysis examines how QSVM and VQC utilize quantum feature mapping and parameterized quantum circuits to improve data representation capabilities. Nevertheless, their practical adoption remains limited by the constraints of current Noisy Intermediate-Scale Quantum (NISQ) devices, including hardware noise, restricted qubit resources, and scalability limitations. Conversely, SVM continues to be a dependable and scalable solution for present-day intrusion detection systems. The study further identifies the absence of a standardized framework for evaluating classical and quantum approaches as an important research gap. Overall, the findings suggest that hybrid quantum–classical learning frameworks provide the most realistic path toward adopting quantum machine learning for future cybersecurity solutions

Keywords:
Quantum Machine Learning, Intrusion Detection, QSVM, VQC, Comparative Analysis

INTRODUCTION

Intrusion Detection Systems (IDS) serve a vital function in safeguarding modern network environments from increasingly advanced cyber threats. As network traffic continues to grow and attack patterns become more complex, traditional detection techniques often face limitations in maintaining both accuracy and adaptability. Machine learning approaches have improved IDS performance by allowing systems to learn from large-scale data and identify anomalies more effectively [1], [2]. Among the various machine learning techniques employed for intrusion detection, Support Vector Machines (SVM) have become a preferred choice because of their robust classification capability and their ability to handle high-dimensional network traffic efficiently [1], [2].

The rapid progress of quantum computing has opened new opportunities for improving conventional machine learning approaches [3], [4]. This advancement has led to the emergence of Quantum Machine Learning (QML), which combines quantum computing concepts with classical learning techniques to develop more efficient predictive models [3], [4]. Approaches such as Quantum Support Vector Machines (QSVM) and Variational Quantum Classifiers (VQC) utilize quantum phenomena, including superposition and entanglement, to construct enhanced feature representations and improve learning performance [6]–[9]. These capabilities make quantum-based models particularly suitable for identifying intricate and evolving intrusion patterns in cybersecurity applications.

Although QML has demonstrated considerable promise, its application to intrusion detection is still in the early stages of development. Existing research primarily investigates individual quantum models, with comparatively few studies providing a systematic comparison against well-established classical techniques.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Furthermore, the practical adoption of these models is limited by the constraints of current Noisy Intermediate-Scale Quantum (NISQ) hardware, including quantum noise, limited qubit resources, and scalability challenges [10]–[12]. Consequently, a comprehensive evaluation framework is required to assess both classical and quantum learning models using consistent performance criteria.

For practical evaluation, benchmark datasets such as NSL-KDD and UNSW-NB15 are widely used [1], [2]. These datasets represent a range of network behaviors and provide a common basis for testing classification models in IDS scenarios. Using such standardized datasets helps connect theoretical research with real-world applications. To address these challenges, this study presents a comprehensive comparative assessment of classical and quantum machine learning techniques for intrusion detection. The proposed evaluation examines SVM, QSVM, and VQC using a common analytical framework based on feature representation, computational complexity, scalability, hardware requirements, and deployment feasibility. By systematically examining the advantages and limitations of each model, this work aims to provide deeper insights into the potential role of quantum machine learning in the development of next-generation cybersecurity solutions.

OBJECTIVES

- This study proposes a comprehensive framework for comparing classical and quantum machine learning techniques applied to intrusion detection, with emphasis on SVM, QSVM, and VQC.
- A systematic evaluation of these learning models is carried out by considering feature representation, computational complexity, scalability, hardware requirements, and deployment feasibility.
- The work examines the advantages and limitations of quantum learning approaches, including quantum kernel based methods and variational quantum circuits, for intrusion detection applications.
- Key barriers affecting the practical adoption of quantum computing are analyzed, including hardware noise, limited qubit availability, and scalability constraints associated with current quantum platforms.
- The study identifies existing research gaps and outlines hybrid quantum–classical architectures as a promising direction for advancing future cybersecurity solutions.

BACKGROUND

Figure 1 illustrates the proposed hybrid quantum–classical intrusion detection framework. Initially, network traffic is collected and preprocessed before relevant features are extracted and transformed into a quantum representation. The encoded information is then processed by a quantum learning model, which classifies the traffic as either normal or malicious to produce the final intrusion detection outcome [11], [12].

I. Support Vector Machine (SVM)

Support Vector Machine (SVM) is a supervised classification technique that separates data into distinct classes by determining an optimal decision boundary with the maximum possible margin between them [1], [2]. To address non-linear classification problems, SVM employs kernel functions that transform the input data into a higher-dimensional feature space, enabling effective separation of complex patterns [1]. Because of its strong performance on high-dimensional datasets and reliable classification capability, SVM has become a widely adopted approach for network intrusion detection [1], [2]. Nevertheless, its effectiveness is influenced by the choice of kernel function, and computational scalability can become a concern when processing large-scale datasets [1]. The proven success of SVM has also inspired the development of quantum-based variants, including the Quantum Support Vector Machine (QSVM) [5], [6].

II. Quantum Computing Fundamentals

Quantum computing uses qubits that exploit superposition and entanglement to process information beyond classical capabilities [3], [4]. Quantum circuits can represent complex data relationships, making them attractive for classification and optimization tasks [3], [5]. However, current NISQ hardware is limited by noise, qubit availability, and scalability constraints [10], [11], leading most QML approaches to adopt hybrid quantum– classical architectures [7], [8].

III. Quantum Support Vector Machine (QSVM)

Quantum Support Vector Machines (QSVM) extend SVM by employing quantum feature maps and quantum kernels to encode and compare data in quantum feature spaces [5], [6]. This enables richer feature representations that may improve classification of complex network traffic patterns [5], [6]. However, practical deployment remains limited by hardware constraints, including noise and restricted qubit resources [10], [11].

IV. Variational Quantum Classifier (VQC)

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Variational Quantum Classifiers (VQC) are hybrid quantum–classical learning models that perform classification using parameterized quantum circuits, whose parameters are iteratively optimized through classical optimization algorithms [7]–[9]. Their ability to generate expressive quantum feature representations makes them well suited for complex classification tasks [7]–[9]. However, the practical implementation of VQC continues to face several challenges, including barren plateaus during training, hardware-induced noise, and scalability constraints associated with current quantum computing platforms [9]–[11].

Fig. 1 Intrusion Detection using Quantum Classifier

LITERATURE REVIEW AND GAP

By incorporating the principles of quantum computing into conventional machine learning, Quantum Machine Learning (QML) aims to develop models capable of learning richer data representations and improving classification effectiveness [3], [4].The advancement of quantum feature spaces and quantum kernels has enabled models such as Quantum Support Vector Machines (QSVM), which have been investigated for classification and intrusion detection tasks [5], [6], [11], [12]. Similarly, Variational Quantum Classifiers (VQC) and other hybrid quantum–classical architectures have demonstrated promising performance in classification and anomaly detection applications [7]–[9], [13]. However, practical deployment remains constrained by hardware limitations, scalability challenges, and the lack of standardized evaluation protocols [10]–[12].

Despite these recent developments, most studies focus on individual models, while direct comparisons of SVM, QSVM, and VQC under common evaluation criteria remain limited. Differences in datasets, evaluation metrics, and experimental settings further hinder meaningful comparison. To enable a consistent assessment of existing approaches, a unified evaluation of these models is carried out based on feature representation, computational complexity, scalability, hardware requirements, and practical deployment feasibility. Through a systematic comparison of SVM, QSVM, and VQC, this work aims to provide insights into their effectiveness and future potential for intrusion detection systems.

COMPARATIVE ANALYSIS OF SVM, QSVM, AND VQC

Table I compares SVM, QSVM, and VQC in terms of feature representation, computational requirements, scalability, and practical deployment. SVM has established itself as a reliable baseline for intrusion detection by consistently delivering strong generalization performance and effective classification across diverse network traffic datasets [1], [2]. In contrast, QSVM leverages quantum feature maps and quantum kernels to capture complex data relationships, while VQC employs trainable parameterised quantum circuits that offer greater flexibility and expressive feature representations [5]–[9].

Despite their considerable potential, the practical deployment of QSVM and VQC is constrained by the inherent limitations of current quantum hardware, including noise, limited qubit availability, and challenges associated with scalability [10]–[12]. Overall, the comparison highlights a trade-off between the practicality of classical methods and the emerging capabilities of quantum learning models, making hybrid quantum–

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

classical approaches the most feasible direction for near-term intrusion detection applications.

Feature	SVM	QSVM	VQC
Model Type	Classical	Hybrid Quantum	Quantum
Feature Mapping	Kernel Trick	Quantum Feature Map	Parameterized Circuits
Learning Approach	Convex Optimization	Kernel-based	Variational Optimization
Performance	Stable and reliable	High for small datasets	Still developing
Scalability	Moderate	Limited	Simulation-based
Hardware Requirement	Not required	Quantum hardware/simulator	Quantum hardware/simulator
Computational Cost	Moderate	High	High
Limitations	Kernel selection	Noise, hardware constraints	Noise, barren plateaus

Table 1: COMPARISON OF SVM, QSVM, AND VQC

Overall, the comparison highlights a trade-off between the maturity and robustness of classical machine learning and the emerging capabilities of quantum learning models. While SVM remains the most feasible approach for current intrusion detection systems, QSVM and VQC offer promising feature representation capabilities for handling complex cybersecurity data. However, hardware limitations, noise, and scalability challenges continue to restrict their widespread adoption, making hybrid quantum–classical approaches the most feasible direction for near-term deployment.

CONCLUSION AND FUTURE WORK

This study presented a systematic comparative analysis of SVM, QSVM, and VQC in intrusion detection systems. The analysis indicates that SVM remains the most feasible approach for current IDS deployments, while QSVM and VQC offer promising quantum-enhanced feature representation capabilities. However, hardware limitations, noise, and scalability challenges continue to restrict the widespread implementation of quantum models. Future studies should concentrate on advancing quantum hardware, improving noise-resilient algorithms and optimizing quantum feature encoding methods, and establishing standardised evaluation frameworks. Until fault-tolerant quantum systems become available, hybrid quantum–classical architectures are likely to remain the most feasible approach for quantum-enabled intrusion detection.

REFERENCES

1) M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the NSL-KDD dataset," in Proc. IEEE Symp. Comput. Intell. Secur. Def. Appl., 2009.
2) N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive dataset for network intrusion detection systems," in Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS), 2015.
3) J. Biamonte et al., "Quantum machine learning," Nature, vol. 549, pp. 195–202, 2017.
4) V. Dunjko and H. J. Briegel, "Machine learning and artificial intelligence in the quantum domain," Rep. Prog. Phys., vol. 81, 2018.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

5) M. Schuld and N. Killoran, "Quantum machine learning in feature Hilbert spaces," Phys. Rev. Lett., vol. 122, no. 4, 2019.
6) V. Havlíček et al., "Supervised learning with quantum enhanced feature spaces," Nature, vol. 567, no. 7747, pp. 209–212, 2019.
7) M. Benedetti, E. Grant, L. Wossnig, and S. Severini, "Parameterized quantum circuits as machine learning models," Quantum Sci. Technol., vol. 4, no. 4, 2019.
8) K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii, "Quantum circuit learning," Phys. Rev. A, vol. 98, 2018.
9) E. Farhi and H. Neven, "Classification with quantum neural networks on near-term processors," arXiv preprint arXiv:1802.06002, 2018.
10) T. H. Kim and S. Madhavi, "Quantum intrusion detection system using outlier analysis," Scientific Reports, vol. 14, Art. no. 27114, 2024.
11) E. I. Elsedimy, H. Elhadidy, and S. M. M. Abohashish, "A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer," Cluster Computing, vol. 27, pp. 9917–9935, 2024.
12) D. Abreu, C. E. Rothenberg, and A. Abelem, "QML-IDS: Quantum machine learning intrusion detection system," arXiv preprint arXiv:2410.16308, 2024.
13) Cong, S. Choi, and M. D. Lukin, "Quantum convolutional neural networks," Nature Physics, vol. 15, 2019.
14) IBM, "Qiskit: An open-source framework for quantum computing." [Online]. Available: https://qiskit.org
15) S. Lloyd, M. Mohseni, and P. Rebentrost, "Quantum algorithms for supervised and unsupervised machine learning," arXiv preprint arXiv:1307.0411, 2013.

