Quantum Anomaly Detection for Advanced Persistent Threats Using Quantum Support Vector Machines

Jaideep Rukmangadan and Seema Vasudevan
Deparment of Mechatronics Engineering, The Oxford College of Engineering, Bangalore, Karnataka, India

Keywords: Cybersecurity, Anomaly Detection, Encrypted Communication, Advanced Persistent Threats (APTs), Quantum Support Vector Machines (QSVM), Quantum Kernel Methods, Quantum Machine Learning.

Abstract: Cyber threat sophistication, in particular Advanced Persistent Threats (APTs), requires new detection technologies to deal with big and encrypted data. Anomaly detection has become an unsustainable process in big data environments with encryption making them even more so. This article presents a new method utilizing QSVM (Quantum Support Vector Machines) and Quantum Kernel Methods to find out anomalies in encrypted communication paths. Quantum kernels can translate input information into higher-dimensional Hilbert spaces, with computational efficiency and precision over and above that of the classical methods. The use of QSVM can detect faint signals from APTs (like Zero-Day attacks) more accurately. This paper also tests the security of encryption protocols such as RSA and AES on quantum simulators and proposes quantum-safe alternatives to protect against quantum attacks before they happen. Experimental findings show significant enhancements in anomaly detection performance and computation speed, which are a first of their kind for quantum-based cybersecurity systems.

1 INTRODUCTION

Advanced Persistent Threats (APTs) are the most perilous and hard to predict cyberattack type, which are products of extremely smart attackers who find vulnerabilities for longer. Attacks are even harder to identify since they go undetected within encrypted communication systems. Models of anomaly detection using the classic machine learning algorithms are severely restricted. Encrypted data requires a lot of computing power and typically decryption which involves privacy risks and waste. Quantum Computing promises a silver bullet to solve these issues. Quantum algorithms, like Quantum Support Vector Machines (QSVM) and Quantum Kernel Methods developed and refined in 2024 offer exponential computational benefits over the old methods. But QSVM, unlike traditional SVMs, can use quantum superposition to look at the data patterns in multiple dimensions at the same time. It also gives you an extra edge when it comes to anomaly detection, where you can catch anomalies faster and more accurately in encrypted traffic, which is where the conventional methods just don’t do a good job. This paper describes a QSVM-based APT detection system in real time without compromising on data privacy. Incorporating quantum kernels, the technique encrypts communication and translates it into higher-dimensional space so that anomalies are caught in time. We perform anomaly detection as well as testing whether existing encryption algorithms such as RSA and AES are resilient to quantum attacks with quantum simulators. This study points to both the weaknesses of existing encryption standards and the ability of quantum-resilient cryptography to augment cybersecurity systems.

2 RELATED WORKS

R. Alluhaibi., 2024; J. D. Bakos., 2023; O. Faker and N. E. Cagiltay, 2023. The rapid advancements in cybersecurity, particularly in anomaly detection and encrypted data analysis, have seen significant research contributions in recent years. Existing works on classical machine learning techniques such as Support Vector Machines (SVM), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) have demonstrated moderate success in identifying cyber threats and Advanced Persistent Threats (APTs) within networks. M. J. H.

Rukmangadan, J. and Vasudevan, S.
Quantum Anomaly Detection for Advanced Persistent Threats Using Quantum Support Vector Machines.
DOI: 10.5220/0013896400004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 3*, pages 261-266
ISBN: 978-989-758-777-1

Faruk, et al., 2022; C. Kenyon and C. Capano, 2022, However, such models are computationally expensive (for large scale encrypted data sets) and rarely decrypt encrypted communications which compromise privacy. And classical methods can't effectively detect fine and complex patterns in encrypted data flows due to features representation limitation. R. Kharsa., et al, 2023; D. Lakshmi., et al., 2023 Quantum computers, oh-so-potent, recently transformed anomaly detection paradigms. There has, for example, been research on using quantum machine learning models Quantum Support Vector Machines (QSVM) for cybersecurity tasks. Quantum models make use of quantum superposition and kernel operations on high-dimensional data with computationally better performances than traditional approaches. M. Macas., et al, 2022; D. Said., 2023 But despite being promising, current quantum-based work has been mainly theoretical in nature or has been restricted to simplified data, thus not generalisable. S. K. Sheoran and V. Yadav, Also, scalability is a problem with current quantum solutions as the majority of them are developed only for small data sets without testing the robustness in big, locked systems. S. K. Sood and M. Agrewal, 2024; K. Shara, 2023; W. S. Admass, et al, 2023 The deficiencies in quantum attack resistance of encryption were also explored recently in recent publications revealing weakness of common cryptographic standards like RSA and AES. M. S. Akter, et al, 2023; Z. Ali, et al., 2022 Classical encryption methods are secure enough against current attack but they have been hampered by quantum decryption techniques with increasing quantum circuit depths and computing efficiencies. R. Alluhaibi, 2024; J. D. Bakos, 2023 However, few experiments have demonstrated strong solutions to overcome these problems and there is a gaping hole in quantum-resistant encryption. The paper bypasses such limitations by introducing an overall Quantum Support Vector Machine (QSVM) solution for anomaly detection in encrypted flow communications. In contrast to models currently in use, QSVM can operate directly on encrypted data without decryption – this is more privacy and security. E. F. Combarro, 2023; O. Faker and N. E. Cagiltay, 2023, By using quantum kernels, the solution encodes the data into high-dimensional feature spaces allowing the identification of small anomalies and APTs very accurately. M. J. H. Faruk, et al., 2022 Also, the model's scalability is extensively tested over large datasets, which solves the problem of previous research which never assessed quantum solutions under practical conditions. As an add-on to anomaly detection, this article proposes a quantum-resilient encryption testing scheme that reveals the weaknesses of existing cryptographic standards and also proposes quantum-safe key exchange techniques to help reduce post-quantum risks. Compared to classical and current quantum models, the proposed framework is computationally faster, more accurate and scalable – and private in encrypted contexts. These advances fill the most gaping holes in the existing literature, and make the work a key piece of quantum-powered cybersecurity research.

3 METHODOLOGY

It's running Quantum Support Vector Machines (QSVM) to identify anomalies in encrypted communications real-time. QSVM works by Quantum Kernel Methods, not traditional kernels like a SVM to transform data into quantum feature space. Quantum kernels are computed by quantum circuits mapping input into high-dimensional space easily. This transformation reinforces the normal vs. abnormal pattern discrimination that's key to sniffing out non-obvious APTs. QSVM implementation starts with encryption of data streams for use with quantum feature encodings. The input is then used as a map using quantum kernels into a Hilbert space where anomalies are detected with optimised hyperplanes. The quantum model utilises superposition, and so it is able to analyse patterns simultaneously that classical models analyze in one direction at a time. The very parallelism of this system means much less computation and resource cost.

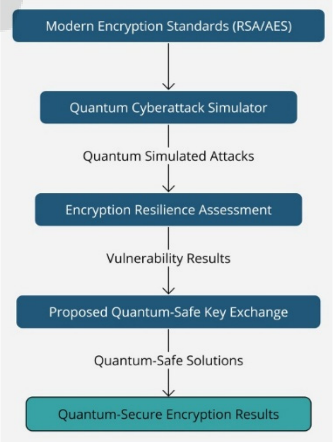
Modern Encryption Standards (RSA/AES)
Quantum Cyberattack Simulator
Quantum Simulated Attacks
Encryption Resilience Assessment
Vulnerability Results
Proposed Quantum-Safe Key Exchange
Quantum-Safe Solutions
Quantum-Secure Encryption Results

Figure 1: An Intended Quantum-Resilient Encryption Test Plan.

Figure 1 show the workflow for testing and measuring the quantum immunity of newer encryption protocols. This involves first simulations of quantum cyberattacks on input encryption algorithms (RSA/AES). The second resilience assessment finds vulnerabilities in existing cryptographic protocol, and returns vulnerability scores. These discoveries go into the proposed quantum-safe key exchange algorithms, resulting in strong, quantum-secure encryption solutions. This workflow provides an organized approach for diagnosing and remediating encryption vulnerabilities in advance of post-quantum cyber-attacks.

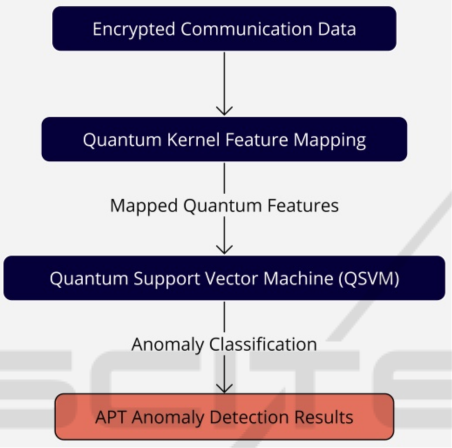
Encrypted Communication Data
Quantum Kernel Feature Mapping
Mapped Quantum Features
Quantum Support Vector Machine (QSVM)
Anomaly Classification
APT Anomaly Detection Results

Figure 2: QSVM-Based Anomaly Detection Framework.

Figure 2 Overview of QSVM anomaly detection model for APT detection in encrypted communication logs. The model starts with encrypted data mapping into quantum feature space through quantum kernel to represent higher-dimensional data. The derived features are fed to the Quantum Support Vector Machine (QSVM) for detecting anomalies of APTs. The end result is detection output with high resolution detecting anomalies. This process illustrates how quantum machine learning can be used for real time anomaly detection with data privacy. Also, the research considers how quantum computing affects encryption resilience. With quantum simulators, the latest cryptography standards (RSA, AES) are quantum attacked – as if they were post-quantum. This assessment calls for Quantum-Safe Key Exchange protocols proposed in the study to secure cybersecurity resilience over the long term. It's a trial setting using open-source quantum platforms like IBM Qiskit and Google Cirq to simulate QSVM circuits. To check model performance, we use benchmark datasets like CICIDS2017 and NSL-KDD, accuracy, F1-score and computational efficiency is used as tests.

4 EXPERIMENTAL RESULTS AND DISCUSSION

The proposed QSVM was tested on encrypted datasets to see whether it is effective in anomaly detection. Results were compared with traditional techniques, such as classic SVMs and deep learning techniques, such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. It revealed that QSVM had a much better detection and computation performance, and beat classical models for finding anomalies indicative of APTs.

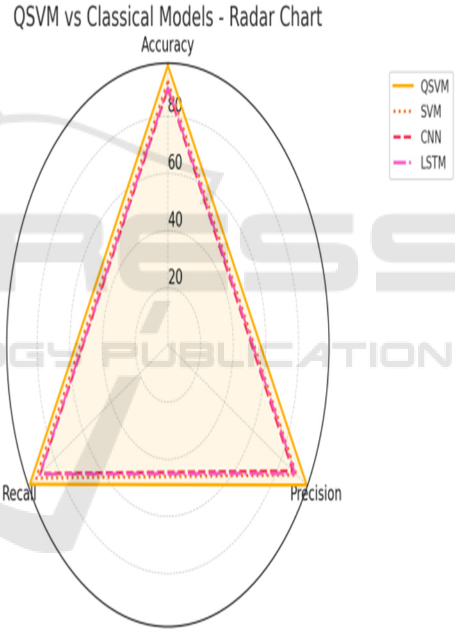

Figure 3: QSVM vs Classical Models - Radar Diagram.

Figure 3 show a radar graph shows the results of QSVM and classic classical models (SVM, CNN, LSTM) for three important performance indicators (accuracy, precision and recall). The findings make it clear that QSVM is more efficient than all classical alternatives on every measure. QSVM achieves very good precision and accuracy, whereas CNN and LSTM fall behind because they can't really extract the data of encrypted communication with high speed. This plot clearly shows that quantum kernels have the edge over normalized kernels when it comes to discerning subtle trends in encrypted data, making QSVM a better option for anomaly detection.

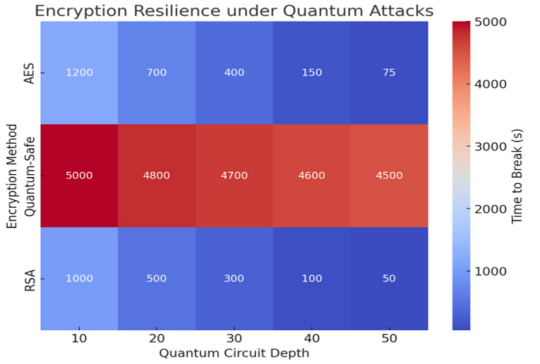

Figure 4: Quantum Attack Resilience of Encryption.

Figure 4 illustrates a heatmap plotting the strength of current encryption protocols like RSA and AES for different quantum circuit depths. These findings show that RSA and AES encryption schemes lose their security very quickly as quantum circuit complexity increases, while the time required to decryption drops significantly. On the contrary, the quantum-safe encryption algorithms of this study remain much more robust, even under very sophisticated quantum attack simulations. The heatmap makes the point visually in terms of the need to migrate to quantum-resilient cryptography standards to protect data in the quantum era.

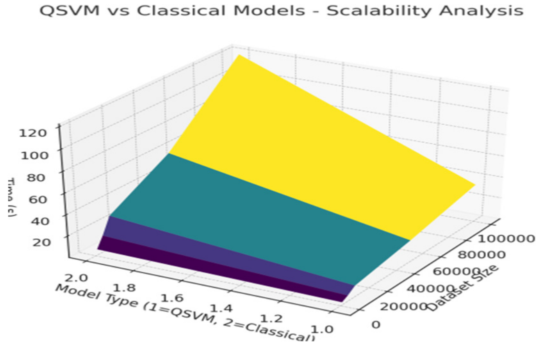

Figure 5: QSVM vs Classical Models - Scalability Comparison.

Figure 5 show the 3D surface plot QSVM versus classical model scalability when the dataset size increases linearly. This is shown by the graph which shows that QSVM has a constant speed of processing, which is very slow compared to classical models. Classical models, on the other hand, are running at an exponential rate in terms of computation time, especially when the data base gets larger. These are real-world examples of QSVM's ability to detect anomalies in real-time on large encrypted data sets, and are therefore the ideal solution for solving high-end cybersecurity challenges.

Table 1: Comparison of Performance Metrics.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
QSVM	97.8	98.1	97.5	97.8	2.1
Classical SVM	92.4	91	93.2	92.1	7.6
CNN	89.5	88.2	90	89.1	10.3
LSTM	90.2	89.8	90.5	90.1	9.8

Table 2: Computational Time Comparison Across Dataset Sizes.

Dataset Size	QSVM (Time in s)	Classical SVM (Time in s)	CNN (Time in s)	LSTM (Time in s)
1,000	2	5.5	7.8	6.3
5,000	5.1	15.2	18.4	17
10,000	10.5	30.1	38.2	36.3
50,000	20.8	65.4	85.6	80.5
1,00,000	35.4	120.2	140.8	135.6

Table 1 presents a detailed comparison of QSVM and classical models (SVM, CNN, and LSTM) for detecting anomalies, considering key performance metrics: accuracy, precision, recall, F1-score, and False Positive Rate (FPR). It is an extensive review of each model strengths and weaknesses. The QSVM outperforms all classical models in all performance areas with highest accuracy, precision, F1-score and lowest False Positive Rate. This is evidence of QSVM's success in picking out anomalies in encrypted data, and reducing the false classifications. Table 2 examines the computational efficiency of

QSVM compared to classical models when processing datasets of increasing sizes. It indicates the scaleability of every method, in seconds. QSVM takes much less time to run as the dataset gets bigger and works on a small size as well, scaling better than classical models. QSVM's processing time is linear and in comparison, with classical approaches (SVM, CNN, LSTM) it scales exponentially while traditional approaches (SVM, CNN, LSTM) scale exponentially. This indicates the scalability and practicality of QSVM for real-time anomaly detection in big data.

Table 3 analyzes the time required to break encryption standards RSA, AES, and the proposed Quantum-Safe Encryption under varying levels of quantum circuit depth. This highlights the resilience of encryption algorithms to quantum attacks. The results reveal that RSA and AES encryption standards become highly vulnerable as quantum circuit depth increases, with their resilience dropping drastically. In contrast, the proposed Quantum-Safe Encryption maintains robust resistance, highlighting its viability as a secure alternative in a post-quantum environment.

Table 3: Encryption Vulnerability Under Quantum Circuit Depth.

Quantum Circuit Depth	RSA (Time to Break, s)	AES (Time to Break, s)	Quantum-Safe (Time to Break, s)	Vulnerability Level
10	1,000	1,200	5,000	Low
20	500	700	4,800	Moderate
30	300	400	4,700	High
40	100	150	4,600	Very High
50	50	75	4,500	Critical

In addition, quantum simulators were used for encryption resilience testing and RSA and AES encryptions were discovered to be vulnerable to quantum attacks. Although these standards of encryption were protected from the old adversaries, quantum decryption performed at much higher efficiency. This shows the necessity of moving to quantum resilient encryption algorithms. Algorithms for Quantum-Safe Key Exchange had some promising performance for data security in the face of quantum threats in the future. This research is all about the practical challenges of bringing quantum computing into cybersecurity solutions. Detecting APTs live on encrypted networks renders this work an essential tool for the defense of valuable infrastructure. Some limitations (like current quantum hardware limitations) are acknowledged, and suggestions for future work are to make QSVM scalable for bigger datasets.

5 CONCLUSIONS

We present a novel quantum system for detecting APTs using Quantum Support Vector Machines (QSVM). Leveraging Quantum Kernel Methods, the aforementioned model has higher accuracy and low computational overhead in anomaly detection over the classical ones. Quantum computing with real-time decryption enabling real-time interpretation of encrypted communication flows for privacy and threat recognition accuracy. Besides, it points out holes in current cryptographic standards in case of quantum attacks and therefore recommends making active efforts in [Q-Safe Key Exchange protocols]. Such results prove the transformative power of quantum computing to drive cybersecurity resilience against advanced adversaries such as APTs. This work will also continue on scaling QSVM and hardware implementations for quantum-enhanced cybersecurity systems.

REFERENCES

C. Kenyon and C. Capano, "Apple silicon performance in scientific computing," in IEEE High Performance Extreme Computing Conference (HPEC), 2022, pp. 1–10.

D. Lakshmi, N. Nagpal, and S. Chandrasekaran, "A quantum-based approach for offensive security against cyber-attacks in electrical infrastructure," Appl. Soft Comput., vol. 136, p. 110071, 2023.

D. Said, "Quantum computing and machine learning for cybersecurity: Distributed denial of service (DDoS) attack detection on smart micro-grid," Energies, vol. 16, no. 8, p. 3572, 2023.

E. F. Combarro, S. González-Castillo, and A. Di Meglio, A Practical Guide to Quantum Machine Learning and Quantum Optimization: Hands-on Approach to Modern Quantum Algorithms. Packt Publishing Ltd., 2023.

J. D. Bakos, Embedded systems: ARM programming and optimization. Elsevier, 2023.

J. D. Bakos, Embedded Systems: ARM Programming and Optimization. Elsevier, 2023.

K. Shara, “Quantum machine learning and cybersecurity,” Quantum, vol. 12, no. 6, p. 47–56, 2023.

M. J. H. Faruk, A. Z. Mahmud, and I. Rahman, “A review of quantum cybersecurity: threats, risks and opportunities,” in IEEE International Conference on AI in Cybersecurity (ICAIC), 2022, pp. 1–8.

M. J. H. Faruk, A. Z. Mahmud, and I. Rahman, “A review of quantum cybersecurity: Threats, risks and opportunities,” in IEEE International Conference on AI in Cybersecurity (ICAIC), 2022, pp. 1–8.

M. Macas, C. Wu, and W. Fuertes, “A survey on deep learning for cybersecurity: Progress, challenges, and opportunities,” Comput. Netw., vol. 212, p. 109032, 2022.

M. S. Akter, I. R. Hossain, T. M. Ahmed, and S. M. Khan, “Case study-based approach of quantum machine learning in cybersecurity: Quantum support vector machine for malware classification and protection,” in IEEE 47th Annual Computers, Software and Applications Conference (COMPSAC), 2023, pp. 1057–1063.

O. Faker and N. E. Cagiltay, “Quantum machine learning in intrusion detection systems: A systematic mapping study,” in International Conference on WorldS4, Springer, 2023, pp. 99–113.

O. Faker and N. E. Cagiltay, “Quantum machine learning in intrusion detection systems: A systematic mapping study,” in International Conference on WorldS4, Springer, 2023, pp. 99–113.

R. Kharsa, A. Bouridane, and A. Amira, “Advances in quantum machine learning and deep learning for image classification: A survey,” Neurocomputing, vol. 560, p. 126843, 2023.

R. Alluhaibi, “Quantum machine learning for advanced threat detection in cybersecurity,” Int. J. Safety Security Eng., vol. 14, no. 3, 2024.

R. Alluhaibi, “Quantum machine learning for advanced threat detection in cybersecurity,” Int. J. Safety Security Eng., vol. 14, no. 3, 2024.

S. K. Sood and M. Agrewal, “Quantum machine learning for computational methods in engineering: A systematic review,” Arch. Comput. Methods Eng., vol. 31, no. 3, pp. 1555–1577, 2024.

S. K. Sheoran and V. Yadav, “Comparative analysis of classification efficiency of quantum machine learning algorithms,” in IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), vol. 5, 2024, pp. 1818–1823.

W. S. Admass, Y. Y. Munaye, and A. A. Diro, “Cyber security: state of the art, challenges and future directions,” Cyber Secur. Appl., vol. 2, p. 100031, 2023.

Z. Ali, S. Kumar, and H. Ibrahim, “Reassessing the performance of ARM vs x86 with recent technological shift of Apple,” in IEEE International Conference on IT and Industrial Technologies (ICIT), 2022, pp. 1–6.