Shodh Sari-An International Multidisciplinary Journal

@2025 International Council for Education Research and Training
ISSN: 2959-1376

2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

Quantum Machine Learning for Anomaly Detection in Cyber Security Audits

Ganapathy, Venkatasubramanian

Faculty in Auditing Department, Southern India Regional Council of the Institute of Chartered Accountants of India (SIRC of ICAI), Chennai, Tamil Nadu, Bharat

Abstract

Quantum Machine Learning (QML) is emerging as a transformative technology in cybersecurity, particularly in anomaly detection for cyber security audits. Traditional machine learning models are effective but face scalability and efficiency limitations as cyber threats grow more sophisticated. QML, leveraging quantum computing's ability to process and analyze large datasets in parallel, offers potential breakthroughs in identifying anomalous patterns that could signify cyber threats such as data breaches, insider threats, or unauthorized access. Content Analysis Research Methodology used in this research work. This paper explores the integration of QML into anomaly detection systems for cyber security audits, where detecting deviations from normal behavior is crucial. Quantum algorithms, particularly those based on Quantum Support Vector Machines (QSVM), Quantum Neural Networks (QNN), and Quantum Principal Component Analysis (QPCA) can enhance the detection of subtle anomalies that classical algorithms may overlook due to noise or the complex, high-dimensional nature of cyber data. The inherent properties of quantum computing, such as superposition and entanglement, allow for more efficient feature selection and optimization, potentially leading to faster and more accurate anomaly detection. The impact of implementing QML in cyber security audits is profound. First, it enhances detection capabilities by identifying anomalies with greater precision, reducing false positives, and improving response times to cyber incidents. Second, quantum algorithms' ability to manage exponentially large datasets makes them ideal for environments with extensive data logs, such as enterprise networks and cloud infrastructures. Third, as cyber threats become increasingly adaptive and stealthy, QML offers a dynamic solution that evolves alongside these threats by continuously learning from new patterns of attack. However, practical challenges remain, including the need for quantum hardware advancements, the development of hybrid

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

quantum-classical models, and ensuring the interpretability of quantum models in audit scenarios. Despite these challenges, early research and experimental implementations demonstrate the potential of QML to revolutionize anomaly detection in cybersecurity audits. This paper concludes that while QML is still in its early stages, its application to anomaly detection holds promise for significantly enhancing the effectiveness of cyber security audits. The impact of this technology, when fully realized, could redefine how organizations protect their networks and data from ever-evolving cyber threats, making QML a critical area for future research and development in cybersecurity.

Keywords: Quantum Machine Learning (QML), Cyber Security Audit, Quantum Support Vector Machines (QSVM), Quantum Neural Networks (QNN), Quantum Principal Component Analysis (QPCA), Anomaly Detection.

INTRODUCTION

Quantum computing is a revolutionary type of computing that leverages the principles of quantum mechanics to perform computations in ways that classical computers cannot. While classical computers use bits as the basic unit of information, which can be either 0 or 1, quantum computers use quantum bits, or qubits, which can exist in a state of 0, 1, or both simultaneously due to a property called superposition. This allows quantum computers to process multiple possibilities at once**.** Quantum computing also takes advantage of entanglement, a phenomenon where qubits become linked, and the state of one qubit can instantly influence the state of another, even across vast distances. This enables highly efficient parallel processing and complex problem-solving.

Quantum Artificial Intelligence: Quantum AI refers to the integration of quantum computing and artificial intelligence (AI), combining the principles of quantum mechanics with the computational techniques of AI to create more efficient and powerful systems**.** In the context of AI, quantum computing could enhance various areas, including: Optimization, Machine Learning, Data Processing and Simulations. While quantum AI is still in its early stages, research

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

is advancing rapidly, and it holds promise for transforming how AI systems are developed and deployed in the future.

Quantum Machine Learning: Quantum Machine Learning integrates quantum algorithms within machine learning programs to improve computational speed and data storage capabilities. It leverages the unique properties of quantum mechanics, such as superposition and entanglement, to process massive datasets and solve complex problems at high speeds. The primary goal of QML is to expedite and enhance the machine learning processes that are traditionally performed on classical computers.

Cyber Security Audits: A cybersecurity audit is a comprehensive assessment and analysis of an organization’s cybersecurity posture and cyber risks. It involves a detailed examination of the organization's information systems, policies, and procedures to ensure they are effective in protecting against cyber threats and comply with relevant laws and regulations. The audit aims to proactively identify vulnerabilities, threats, and associated mitigation options to prevent weaknesses from being exploited

Quantum machine learning (QML) is an emerging field that combines the computational power of quantum computing with machine learning techniques to solve complex problems more efficiently than classical approaches. In the context of cybersecurity audits, anomaly detection plays a critical role in identifying unusual patterns that may indicate security breaches or system vulnerabilities. Traditional machine learning methods for anomaly detection face limitations in processing large datasets and handling high-dimensional spaces. Quantum machine learning offers the potential to accelerate these tasks by leveraging quantum algorithms, which can process vast amounts of data in parallel and explore multiple solutions simultaneously. By integrating QML into cybersecurity audits, organizations can enhance their ability to detect sophisticate d anomalies, potentially improving the detection of threats and reducing response times.

RESEARCH QUESTION

How can quantum machine learning techniques, specifically Quantum Support Vector Machines (QSVM), Quantum Neural Networks (QNN), and Quantum Principal Component Analysis (QPCA), enhance the accuracy and efficiency of anomaly detection in cybersecurity audits compared to classical machine learning methods?

TARGETED AUDIENCE

1. **Researchers and Academics**: Those studying quantum computing, machine learning, cyber security, and related fields.
2. **Cyber Security Professionals**: Experts and practitioners in the field of cyber security looking for advanced methods to improve anomaly detection.
3. **Industry Professionals**: Individuals working in technology sectors where cyber security is a concern, including IT, finance, healthcare, and critical infrastructure.
4. **Students and Educators**: Graduate students and educators in computer science, data science, and cyber security programs.
5. **Policy Makers**: Officials and decision-makers interested in understanding emerging technologies and their implications for national security.
6. **Investors and Business Leaders**: Individuals in leadership roles who may be interested in the commercial applications of quantum machine learning in improving cyber security measures.

OBJECTIVES OF THE STUDY

1. To explain the impact of implementing Quantum Machine Learning (QML) in Cyber Security Audits
2. Explore the capabilities and limitations of quantum machine learning (QML) techniques, specifically Quantum Support Vector Machines (QSVM), Quantum Neural Networks (QNN), and Quantum Principal Component Analysis (QPCA), in the context of anomaly detection for cybersecurity.
3. Benefits and Practical challenges of implementing Quantum Machine Learning in Cyber Security Audits.
4. To provide recommendations for improvement of cyber security audits using quantum computing machine learning.

RESEARCH METHODLOLOGY AND DATA COLLECTION METHOD

Content Analysis Research Methodology used in this research work, Secondary Data used for research work, collected from e-journals, e-magazines, e-books and website of Quantum Computing, Cyber Security Audit domains.

REVIEW OF LITERATURE

@2025 International Council for Education Research and Training 2025, Vol. 04, Issue 01, 127-154
ISSN: 2959-1376 DOI: https://doi.org/10.59231/SARI7784

S.No.	Author(s)	Year	Focus of Study	Algorithms/Tools used	Key Findings	Research Gap
1	Shor et al.	2000	Quantum algorithms for cybersecurity anomaly detection and their potential use in auditing.	Shor's Algorithm, Grover's Algorithm for Search and Optimization.	Grover's algorithm was shown to reduce search times for large datasets in anomaly detection tasks.	Focused on algorithmic complexity; no direct testing on cybersecurity audit datasets.
2	Lloyd et al.	2014	Quantum algorithms for supervised machine learning and anomaly detection.	Quantum Principal Component Analysis (QPCA), Quantum Support Vector Machine (QSVM).	Demonstrated faster training and prediction in machine learning using quantum algorithms.	Lack of practical applications for large-scale cybersecurity systems; limited real-world implementation .
3	Li et al.	2018	Application of Quantum Machine Learning (QML) in cybersecurity and anomaly detection.	Quantum Neural Networks (QNN), Quantum Random Access Memory (QRAM).	Found significant speedup in detecting anomalies in simulated data, offering a	Lack of real-time application in cybersecurity audit scenarios; scalability issues not explored.

					quantum advantage.	
4	Schuld et al.	2019	Quantum machine learning: A classical perspective.	Hybrid Quantum-Classical Algorithms (Variational Circuits, Quantum Kernels),	Provided a theoretical overview of how quantum resources can improve machine learning tasks, including anomaly detection.	Focused on theoretical improvements; no detailed exploration of specific cybersecurity uses cases.
5	Lu and Wang	2020	Quantum-inspired anomaly detection for cybersecurity.	Quantum-Inspired Optimization Algorithm (QIOA), Quantum Approximate Optimization Algorithm (QAOA).	Applied QIOA to detect anomalies in network traffic, leading to improved efficiency in small datasets.	Limited experiments with small datasets; real-world complexities in network traffic were not considered.
6	Housley et al.	2021	Quantum-enhanced anomaly detection for network security audits.	Quantum K-Means, Quantum Decision Trees.	Demonstrated improved anomaly detection accuracy and speed	Lacked integration with actual cybersecurity audit tools; scalability with

					compared to classical algorithms, though still in simulation.	big data not fully explored.
7	Patel et al	2022	Exploring quantum neural networks for anomaly detection in cybersecurity.	Quantum Neural Networks (QNN), Quantum Variational Autoencoders (QVAE).	Showed potential for anomaly detection using QNNs in synthetic cybersecurity datasets, with faster convergence.	Focus on synthetic data limits generalizability; real-world deployment issues like noise in quantum computers ignored.
8	Chatterjee et al.	2023	Quantum-enhanced machine learning models for cybersecurity auditing anomaly detection.	Quantum Support Vector Machines (QSVM), Quantum Boltzmann Machines.	Achieved notable speedup and higher accuracy in detecting cybersecurity anomalies compared to classical models.	Lack of exploration of hybrid classical-quantum models; insufficient exploration of cybersecurity audit integration.

11	Ngairangbam et al.	2023	QML for anomaly detection in network security.	Quantum Autoencoders,	Quantum autoencoders provided accurate detection in high-dimensional data, highlighting quantum advantages in handling extensive network logs while reducing false positives.	Need for optimized quantum data encoding techniques to further improve efficiency.
13	Vyas et al.	2024	Hybrid quantum-classical models in threat detection.	Q-SVM, Hybrid Quantum Neural Networks (QNNs).	Hybrid models showed competitive performance, balancing execution time with accuracy in detecting anomalies. They achieved higher accuracy by	Optimization strategies for quantum layer configurations and qubit allocation.

					combining quantum and classical layers.	
14	Schuhmacher et al.	2024	Application of QML for cybersecurity in adaptive IDS.	Quantum Principal Component Analysis (QPCA), Quantum Layered Network.	QPCA proved effective in detecting adaptive anomalies in evolving cyber environments, suggesting quantum algorithms can adapt more readily to emerging cyber threats.	Further work needed on adaptive IDS integration and real-time anomaly handling across different network conditions.

Key findings from Review of Literature:

- **Scalability and Large-Scale Datasets**: Most studies show quantum algorithms' potential in small-scale or simulated settings, but practical use in large, real-world cybersecurity audits is underdeveloped.
- **Real-Time Application**: Real-time applicability of quantum algorithms in cybersecurity audits, where speed is crucial, is still a challenge.
- **Hybrid Models**: The potential of hybrid quantum-classical models remains underexplored, despite their promise to enhance performance while dealing with large datasets and noise.
- **Practical Integration**: Few studies examine practical integration with existing cybersecurity audit tools, focusing mainly on theoretical aspects or simulations.
- **Quantum Noise and Error Correction**: Quantum noise and error

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

correction, critical to real-world quantum applications, are not adequately explored in cybersecurity anomaly detection.

IMPLEMENTATION OF QUANTUM MACHINE LEARNING IN CYBER SECURITY AUDITS

Use Cases for QML in Cybersecurity Audits

a. Anomaly Detection: - Quantum machine learning can be used to detect anomalous patterns or irregularities in network data, which could indicate potential security threats or policy violations.

b. Malware Detection: - QML models trained on vast datasets could identify malware signatures, even those that are obfuscated, by finding complex patterns in data.

c. Behavioural Analysis: - QML can model behavioural data to detect unusual activities, which could help identify insider threats or compromised user accounts.

d. Risk Scoring and Prediction: - By analyzing historical data, QML models can assign risk scores to various network components, predicting potential vulnerabilities.

Requirements to Implement QML in Cybersecurity Audits

- **Access to Quantum Computing Hardware:**

Since QML requires quantum computing resources, organizations need access to quantum processors. This could be through cloud-based quantum computing services like IBM Quantum, Amazon Braket, or Google's Quantum AI, or by investing in on-premise quantum computers (though costly).

- **Data Preprocessing Infrastructure:**

Data preparation is critical since QML models are highly sensitive to data quality. Quantum-ready data requires large, clean datasets and often quantum-specific encoding (like amplitude encoding, angle encoding, etc.).

- **Quantum Machine Learning Algorithms:**

Familiarize with or develop algorithms suited to cybersecurity use cases. Variational Quantum Classifiers (VQC), Quantum Support Vector Machines (QSVM), and Quantum Neural Networks (QNN) are popular algorithms.

- **Cybersecurity Data Science Expertise:**

Skilled data scientists with cybersecurity knowledge and an understanding of quantum computing are essential. They need to know about quantum algorithms and how they can be applied to detect cybersecurity threats.

- **Hybrid Classical-Quantum System:**

Quantum resources are still limited, so a hybrid approach (quantum and classical) is often necessary. Some computations will be performed on classical hardware, with specific high-complexity tasks offloaded to quantum processors.

- **Integration with Cybersecurity Platforms:**

QML systems must be able to integrate with existing security information and event management (SIEM) tools and other cybersecurity platforms for effective audits and threat monitoring.

Implementation Steps

Step 1: Problem Identification and Feasibility Study - Determine which cybersecurity audit tasks could benefit from quantum speed-ups and conduct a feasibility analysis.

Step 2: Data Collection and Preprocessing Collect, clean, and encode data for quantum algorithms. Focus on high-quality, high-volume datasets for training and testing.

Step 3: Model Development - Develop QML models using libraries like Qiskit (IBM), TensorFlow Quantum, or PennyLane that provide frameworks for QML.

Step 4: Hybrid Model Integration - Implement a hybrid approach where quantum models are trained on quantum processors, while other tasks are managed by classical processors.

Step 5: Model Testing and Validation - Evaluate the models' performance against classical models in terms of accuracy, speed, and anomaly detection capabilities.

Step 6: Deployment and Monitoring - Integrate QML models with cybersecurity audit tools. Continuously monitor the system, retrain models as necessary, and ensure ongoing optimization.

Challenges and Considerations

- **Current Limitations of Quantum Hardware:**

Noise, decoherence, and limited qubits can impact QML model performance. Near-term quantum systems may not outperform classical models consistently.

- **Data Security and Compliance:**

Quantum systems need to be compliant with data security protocols, as they will handle

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

sensitive information in a cybersecurity audit context.

APPLICATION OF QUANTUM MACHINE LEARNING ALGORITHMS IN CYBER SECURITY AUDIT

Quantum Support Vector Machine (QSVM): A Quantum Support Vector Machine (QSVM) is a machine learning model adapted from classical Support Vector Machines (SVMs) and tailored to harness the unique computational advantages of quantum computing. QSVMs are particularly valuable for tasks that require efficient processing of large datasets, such as anomaly detection in cybersecurity audits, where identifying subtle patterns and outliers in complex data is essential.

Components of QSVM

QSVM is built upon several key quantum computing concepts and components that distinguish it from classical SVMs:

1. **Quantum Kernel Estimation**:

i) The kernel function is central to both classical SVMs and QSVMs, as it enables the transformation of input data into a higher-dimensional feature space where classes (e.g., normal vs. anomalous) become more separable. Quantum-enhanced kernels, however, allow QSVMs to process much more complex data by leveraging quantum superposition and entanglement.

ii) The quantum kernel leverages a feature map that encodes classical data into quantum states. The inner product of these quantum states forms a high-dimensional space for better separation of the data classes. This mapping allows the QSVM to classify data with high accuracy, even with slight variations in complex data, such as those in cybersecurity logs.

2. **Quantum Circuits**:

i) Quantum circuits are used to implement the quantum kernel and perform the necessary computations for classification. In QSVMs, these circuits create a unique quantum state for each data point and then compare these states to calculate similarities between data points.

ii) Quantum gates within these circuits, such as Hadamard or Pauli gates, manipulate qubits (quantum bits) to create the desired feature space. These operations allow QSVMs to handle high-dimensional feature spaces without the exponential increase in computational costs that would occur on classical systems.

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

3. **Hyperplane Creation and Margin Optimization**:

i) Similar to classical SVMs, QSVMs use a hyperplane to separate different classes within the high-dimensional feature space. In cybersecurity, this hyperplane could separate “normal” behavior from “anomalous” behavior. The algorithm finds the hyperplane that maximizes the margin between classes, which enhances classification accuracy.

ii) However, in a QSVM, this hyperplane exists within a quantum-enhanced feature space, allowing for the separation of more complex data that might overlap or present non-linear boundaries.

How QSVMs are used in Cybersecurity Audits

In cybersecurity, QSVMs enhance the detection of anomalies and threats by classifying vast amounts of data, such as network traffic logs, user access patterns, and event logs, to pinpoint abnormal patterns that may indicate security risks.

1. **Intrusion Detection**:

i) QSVMs can be employed to classify incoming network traffic as normal or malicious based on learned patterns of historical data. By mapping network traffic data into a quantum-enhanced feature space, QSVMs improve accuracy in identifying subtle deviations from normal behavior, which can signal the presence of intruders or anomalous activity.

ii) QSVMs, in this case, benefit from their high-dimensional processing capabilities, which allow them to differentiate between benign and potentially harmful traffic even when the differences are subtle.

2. **User Behavior Analysis**:

i) User behavior monitoring is crucial in detecting insider threats or compromised accounts. QSVMs can classify user activities by analyzing login times, access patterns, and resource usage. Any deviation from a user’s typical behavior profile can be flagged as anomalous.

ii) The high-dimensional mapping provided by QSVM allows for a nuanced representation of user behavior patterns, capturing even minor variations that might escape detection in classical models.

3. **Malware and Phishing Detection**:

i) QSVMs can classify file patterns or URL data to detect potential malware or phishing attempts. By analyzing data characteristics, such as URL structure or file attributes, QSVMs identify atypical patterns associated with known malware or phishing techniques.

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

ii) This application leverages QSVM's efficiency in handling high-dimensional data, processing vast numbers of URLs or files quickly to distinguish normal items from those with malicious characteristics.

4. **Financial Fraud Detection**:

i) In financial sectors, QSVMs can monitor transaction patterns to flag fraudulent behavior. By mapping each transaction into a high-dimensional feature space, the QSVM model can detect outlier patterns indicative of fraud with greater precision.

ii) This is particularly beneficial in real-time applications, where rapid and accurate classification of transactions can help prevent fraud before it affects users or organizations.

Step-by-Step process of QSVM

Advantages:

- **Speed and Efficiency**: QSVMs have the potential to classify large, high-dimensional datasets faster than classical SVMs due to quantum parallelism.
- **Improved Accuracy**: Quantum-enhanced kernels allow QSVMs to identify complex, non-linear boundaries between classes, which is critical for cybersecurity where threats may exhibit nuanced behavior.
- **Scalability**: As quantum hardware develops, QSVMs will increasingly be able to handle larger datasets, making them ideal for scaling cybersecurity applications.

Challenges:

@2025 International Council for Education Research and Training
ISSN: 2959-1376

2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

- **Quantum Hardware Limitations**: Currently, quantum computers are in the NISQ (Noisy Intermediate-Scale Quantum) stage, which limits the stability and number of qubits available, impacting QSVM's real-world applications.
- **Complexity and Cost**: Developing and maintaining quantum algorithms requires specialized expertise, and running QSVMs on quantum hardware can be expensive.
- **Integration with Existing Systems**: Adopting QSVMs within cybersecurity infrastructure requires seamless integration with existing tools, which can be challenging, given the early stage of quantum computing technology.

Quantum Neural Networks:

Quantum Neural Networks (QNNs) combine principles from quantum computing with artificial neural networks to create a hybrid approach, leveraging quantum properties like superposition and entanglement to improve data processing capabilities. This integration holds particular promise in the cybersecurity field, especially for enhancing security audits.

Key Features of QNNs:

- **Superposition**: Qubits can exist in multiple states simultaneously, allowing QNNs to explore multiple paths in a network at once. This boosts parallel processing capabilities.
- **Entanglement**: QNNs can make use of qubits that are entangled, meaning that changing the state of one affects the others, allowing efficient data correlation and pattern recognition.
- **Interference**: Quantum interference allows QNNs to strengthen or cancel out certain states, guiding computations toward the optimal solution path.

Applications of QNNs in Cybersecurity Audits

a) Anomaly Detection

- **Enhanced Pattern Recognition**: The entanglement and superposition properties of QNNs can analyze vast amounts of network traffic data simultaneously, identifying anomalies or deviations from normal patterns quickly.
- **Real-Time Threat Detection**: Quantum processing speeds up the analysis of real-time network data. QNNs can compare vast amounts of current and historical data to detect unusual behavior, which is crucial in identifying advanced persistent threats (APTs) and zero-day vulnerabilities.

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

b) Improved Malware and Intrusion Detection

- **Complex Pattern Recognition**: Traditional neural networks may struggle to detect sophisticated attack patterns, especially polymorphic malware that frequently changes its code. QNNs, however, are better at spotting subtle, multidimensional data patterns.

- **Adaptive Learning**: QNNs can adapt to new attack vectors more rapidly by leveraging quantum algorithms to generalize knowledge gained from prior cybersecurity threats, making them more efficient in detecting evolving malware strains.

c) Quantum-Enhanced Encryption Testing

- **Quantum-Resistant Cryptography (QRC)** QNNs can aid in assessing and testing quantum-resistant cryptographic algorithms. Cybersecurity audits increasingly focus on assessing cryptographic protocols against quantum attacks.

- **Quantum Key Distribution (QKD)**: QNNs can evaluate the security of QKD systems, which use quantum mechanics for secure communication, making it difficult for adversaries to intercept information undetected.

d) Risk Assessment and Threat Prediction

- **Predictive Analysis**: With superposition and entanglement, QNNs can process multiple potential threat scenarios simultaneously, making them well-suited to perform predictive analytics. This is valuable for proactive cybersecurity measures, as it can help anticipate and mitigate risks before they materialize.

- **Scalability**: QNNs can handle large, complex datasets, making them suitable for enterprise-scale cybersecurity audits. They can process data across multiple systems and networks, identifying interconnected threats that may go unnoticed with traditional auditing methods.

Advantages of QNNs in Cybersecurity

QNNs offer unique benefits that can be particularly valuable for cybersecurity audits:

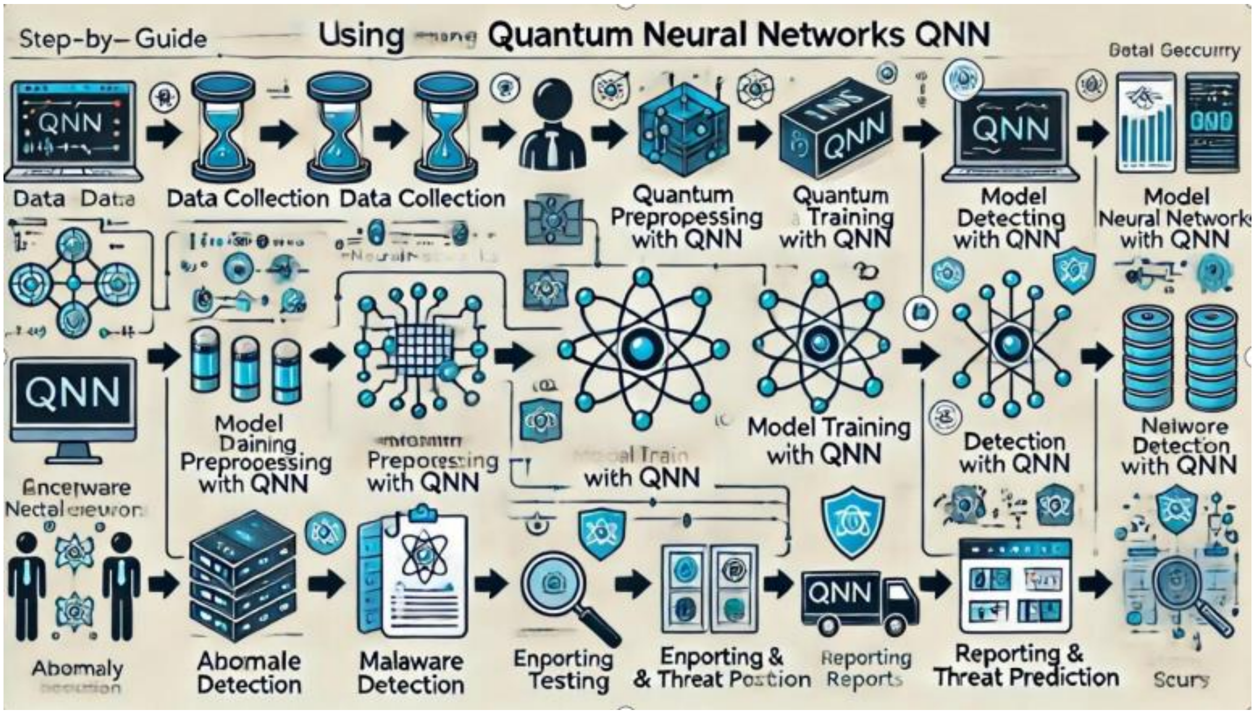
- **Processing Efficiency**: Due to quantum parallelism, QNNs can potentially operate faster and more efficiently than classical neural networks.

- **Improved Accuracy**: QNNs excel in high-dimensional data processing, improving accuracy in threat detection, particularly for identifying complex, multi-step cyber-attacks.

- **Adaptability**: The adaptability of

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

QNNs can reduce the time needed for system training and can respond more quickly to new types of threats.



Challenges of QNNs in Cybersecurity

Quantum Hardware Limitations: Current quantum hardware lacks the qubit stability (coherence time) and error rates needed for large-scale QNNs.

Complexity in Implementation: Quantum algorithms are complex and require expertise in both quantum mechanics and neural network design, making their implementation challenging for many organizations.

Security Risks: As quantum computing progresses, there are potential risks of new vulnerabilities, particularly if QNNs are used without adequately secured quantum infrastructure.

Quantum Principal Component Analysis (QPCA):

Quantum Principal Component Analysis (QPCA) is a quantum computing approach to **Principal Component Analysis (PCA)**, a

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

standard technique used in data science for dimensionality reduction and feature extraction. PCA is widely used to analyze complex datasets, finding the main components (or "principal components") that capture the most variance in the data. By focusing on these components, PCA can simplify data analysis without losing significant information.

How QPCA Works:

- **Quantum State Encoding**: In QPCA, data is encoded into quantum states. Each data vector is represented as a quantum state, and QPCA operates on these states.
- **Eigenvalue Estimation**: QPCA uses quantum algorithms, such as the Quantum Phase Estimation (QPE), to find eigenvalues and eigenvectors, which represent the principal components.
- **Dimensionality Reduction**: Using these eigenvalues, QPCA reduces data dimensions while retaining meaningful patterns, just like classical PCA but with potential speed advantages.

Applications of QPCA in Cybersecurity Audits

In a cybersecurity audit, the goal is to identify weaknesses, irregularities, and potential vulnerabilities across an organization’s digital infrastructure. QPCA can enhance cybersecurity audits in the following ways:

a) Threat Detection and Anomaly Identification:

- With the high dimensionality of cybersecurity data, QPCA could help auditors detect anomalies at scale.
- Rapidly detecting patterns associated with known or unknown threats would allow auditors to flag issues in real-time and recommend mitigations.

b) Behavioral Analysis of Network Activity:

- Quantum-enhanced PCA can aid in recognizing patterns in user behavior across large datasets, identifying any suspicious or abnormal activity.
- This could be particularly helpful for identifying insider threats or unusual access patterns, which are hard to detect using traditional methods.

c) Real-Time Data Analysis and Compliance Checks:

- QPCA can accelerate real-time data analysis, allowing auditors to continuously monitor systems and ensure compliance with cybersecurity standards.
- By improving the ability to process and analyze data in real-time, organizations can be

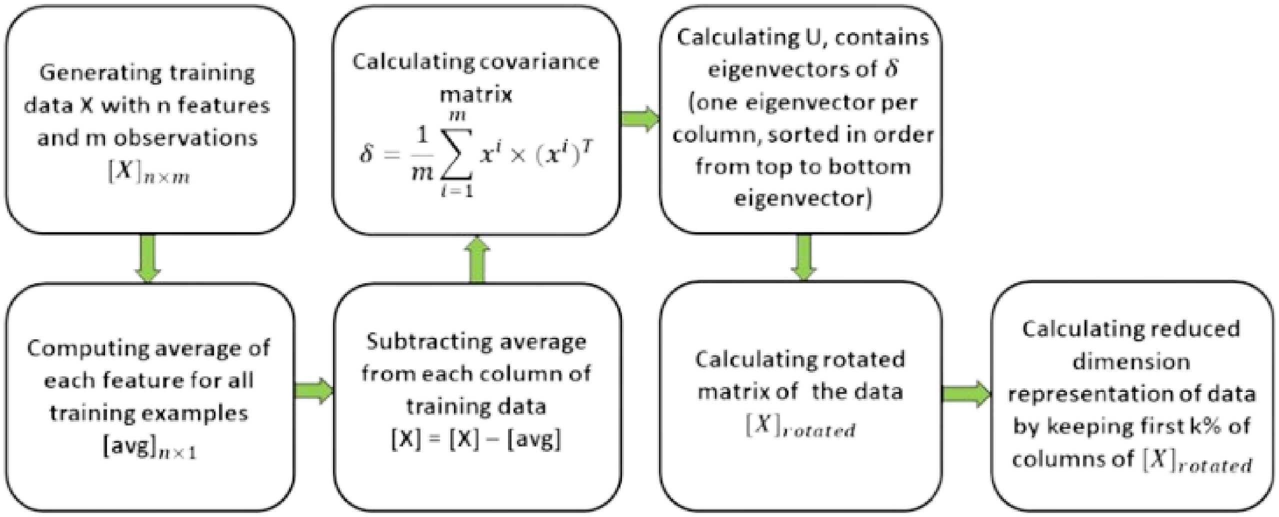
@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

alerted to potential compliance issues or breaches as they arise.

4. Challenges in Applying QPCA to Cybersecurity Audits

- **Quantum Hardware Limitations**: Current quantum computers are in their early stages and may not yet handle complex, high-dimensional datasets efficiently.
- **Data Encoding Costs**: Encoding large datasets into quantum states can be challenging and may limit real-world applications.
- **Expertise and Infrastructure**: Organizations need quantum specialists and infrastructure, which could be a barrier to practical implementation in cybersecurity audits.

The Proposed dimension reduction Algorithms using QPCA


Generating training data X with n features and m observations $[X]_{n\times m}$
Calculating covariance matrix $\delta = \frac{1}{m}\sum_{i=1}^{m} x^i \times (x^i)^T$
Calculating U, contains eigenvectors of δ (one eigenvector per column, sorted in order from top to bottom eigenvector)
Computing average of each feature for all training examples $[\text{avg}]_{n\times 1}$
Subtracting average from each column of training data [X] = [X] – [avg]
Calculating rotated matrix of the data $[X]_{rotated}$
Calculating reduced dimension representation of data by keeping first k% of columns of $[X]_{rotated}$

Comparison between Quantum Support Vector Machine (QSVM), Quantum Neural Network (QNN), and Quantum Principal Component Analysis (QPCA)

No	Feature	QSVM	QNN	QPCA
1	**Purpose**	Classification and regression.	Modeling complex patterns in data.	Dimensionality reduction and feature extraction.

2	**Concept**	Quantum analogue of classical SVM.	Quantum adaptation of classical neural networks.	Quantum version of PCA leveraging quantum states
3	**Architecture**	Kernel-based method.	Layered network with weights and activation.	Eigenvalue decomposition using quantum circuits.
4	**Quantum Advantage**	Uses quantum kernel functions for efficiency.	Parallel processing via superposition and entanglement.	Handles high-dimensional data faster than classical PCA.
5	**Applications**	Image recognition, financial predictions.	Image classification, quantum chemistry.	Data compression, denoising, cybersecurity.
6	**Strengths**	Effective for high-dimensional feature spaces.	Adaptable to complex nonlinear patterns.	Reduces noise and dimensionality in large datasets.
7	**Weaknesses**	Limited scalability in current quantum hardware.	High computational resources required.	Sensitive to noise in quantum measurements.
8	**Complexity**	Moderate	High	Moderate
9	**Learning Mechanism**	Support vectors and quantum kernels.	Backpropagation through quantum gates.	Eigen decomposition on quantum states.
10	**Performance**	Enhanced in large feature spaces with quantum speedup.	Can surpass classical NNs on complex data.	Effective in compressing data with fewer components.
11	**State of Research**	Actively researched	Emerging, highly experimental	Moderate research focu especially in big data.

BENEFITS OF QML IN CYBER SECURITY AUDITS:

Enhanced Threat Detection and Anomaly Detection: QML algorithms, such as

Quantum Support Vector Machines (QSVM) and Quantum Neural Networks (QNN), can quickly analyze vast amounts of data to identify subtle anomalies or deviations that signal potential cyber threats.

- Quantum models can improve the accuracy of intrusion detection systems by detecting even minor behavioral anomalies, which can often be challenging to identify with classical methods.

Rapid Data Encryption and Decryption:

- Quantum computing offers high-speed encryption and decryption, using complex quantum algorithms such as Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNG).
- Quantum cryptographic methods can create theoretically unbreakable encryption, offering protection against potential quantum hacking threats that could decrypt classical encryption.

Efficient Pattern Recognition for Malware Detection:

- Quantum-enhanced machine learning techniques can recognize patterns and correlations within large, complex datasets, aiding in detecting malware and new types of viruses faster and more efficiently than classical machine learning models.
- This rapid pattern recognition can identify and mitigate zero-day vulnerabilities by detecting previously unseen malware strains.

Improved Risk Assessment and Threat Forecasting:

- Quantum Principal Component Analysis (QPCA) can reduce data dimensionality, enabling faster and more effective analysis of risk patterns within a system.
- By processing vast threat intelligence data, QPCA can enhance threat forecasting models to anticipate potential risks and prioritize cybersecurity defenses accordingly.

Strengthening Password Security and Access Control:

- Quantum-enhanced algorithms can handle the analysis of complex biometric data, improving user authentication and access control by reducing the chance of false positives or negatives in identity verification.
- Additionally, QML can be used in behavior-based access control systems, monitoring for unusual access patterns in real-time to prevent unauthorized access.

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

Improved Scalability in Security Solutions:

▪ QML algorithms can handle increasingly large and complex data sets, making them suitable for real-time monitoring in large networks, cloud-based environments, and IoT systems**.**

▪ QML's scalability supports adaptive, real-time cybersecurity measures that grow with the network or system's needs, crucial in a rapidly evolving threat landscape.

Enhanced Data Privacy and Compliance:

▪ Quantum algorithms can be used in privacy-preserving computations (like federated learning) where data does not need to be centralized. This reduces exposure to data breaches and complies with data privacy regulations.

▪ Quantum-secured data sharing can ensure that sensitive data, once shared, is safe from interception or unauthorized access.

Increased Speed and Efficiency in Security Analytics:

▪ Quantum models can dramatically accelerate processing times in tasks like log analysis, traffic monitoring, and event correlation, allowing cybersecurity teams to respond more quickly to emerging threats.

▪ Faster analysis can significantly reduce the time it takes to analyze large-scale breaches, aiding in rapid incident response and recovery.

CHALLENGES OF QML IN CYBER SECURITY AUDIT

Hardware Limitations:

● Current quantum hardware, especially Noisy Intermediate-Scale Quantum (NISQ) devices, lacks the capacity and reliability to handle complex, large-scale cybersecurity audit tasks.

● Quantum systems are sensitive to environmental noise, requiring sophisticated error correction techniques and stable environments, which increases resource demands and complexity.

Algorithm Scalability and Complexity:

● QML algorithms used for cybersecurity audit require a high level of precision and scalability. However, quantum algorithms for real-world, large-scale audit applications often struggle with scalability due to qubit constraints.

● Many QML algorithms are experimental and may not yield reliable results when applied to vast cybersecurity data, such as logs and traffic data from large networks.

Data Privacy and Compliance Concerns:

- Quantum computing poses new challenges to data privacy regulations (e.g., GDPR, HIPAA) because of its potential to break existing encryption standards. Handling sensitive data for audits can thus pose a risk if quantum decryption becomes feasible.
- Quantum systems may need tailored privacy-preserving methods, which are still under development and add additional complexity to cybersecurity audits.

Limited Availability of Skilled Professionals:

- The field of QML, especially in cybersecurity, is highly specialized, and there is a shortage of professionals skilled in both quantum computing and cybersecurity.
- Organizations may face challenges in finding qualified personnel who can design, implement, and interpret QML algorithms for cybersecurity audits effectively.

Integration with Classical Systems:

- Most existing cybersecurity frameworks and audit systems are built on classical computing infrastructure. Integrating quantum systems with these classical frameworks is complex and may lead to compatibility issues.
- Developing hybrid quantum-classical systems that leverage the strengths of both for cybersecurity audits is still in its infancy and can result in high development costs.

High Computational and Resource Costs:

- Quantum computing resources, such as qubits and cryogenic cooling, are costly and require substantial physical and operational resources, making the cost of QML audits higher than conventional methods.
- The energy-intensive nature of quantum systems further adds to operational costs, especially for regular audits that demand consistent computational power.

Error Rates and Quantum Decoherence:

- Quantum systems are prone to high error rates and decoherence, meaning that algorithms running on quantum systems may produce unreliable or inconsistent results, which is critical in security audits where precision is essential.
- Error correction techniques are under development but consume substantial resources, further limiting the effective use of QML in audits.

Standardization and Benchmarking Challenges:

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

- There is a lack of standardized metrics and benchmarks to evaluate the effectiveness of QML algorithms in cybersecurity contexts. Without clear standards, it's challenging to assess the validity and reliability of QML audit results.
- Developing industry standards and best practices for quantum-based cybersecurity audits is necessary to achieve widespread adoption, but this is still in its early stages.

Vulnerability to Quantum-Specific Attacks:

- QML systems themselves may be susceptible to quantum-specific attacks, including quantum malware or other exploits that target quantum vulnerabilities. This introduces additional security considerations that aren't typically encountered in classical systems.
- As quantum computing progresses, ensuring the resilience of QML algorithms in the face of quantum-specific threats becomes essential for secure audits.

Difficulty in Interpretability and Transparency:

- QML algorithms can be highly complex and less interpretable than classical methods, making it harder for cybersecurity auditors to understand or justify their decisions.
- In sensitive areas like cybersecurity audits, interpretability is crucial for accountability, and the "black-box" nature of some QML models presents a challenge to achieving this transparency.

KEY FINDINGS

❖ **Quantum Support Vector Machines (QSVM):** Studies show QSVM's utility in malware classification, with high accuracy rates of up to 95% for malware detection. QSVM benefits from quantum properties like superposition, enhancing classification performance over classical methods in some cases. However, hardware constraints mean QSVMs sometimes struggle to maintain accuracy on larger datasets due to qubit limitations, which also increases the need for data pre-processing steps like PCA to reduce dimensionality before quantum processing can begin.

❖ **Quantum Neural Networks (QNN):** QNNs have been applied in areas such as threat intelligence and anomaly detection. They leverage quantum parallelism to analyze large volumes of data and identify subtle patterns associated with potential threats more quickly than classical neural networks. However, QNNs are currently affected by issues related to noise and decoherence in near-term quantum devices, which impacts their precision.

❖ **Quantum Principal Component Analysis (QPCA):** QPCA is commonly used in cybersecurity audits to preprocess and compress data, making it manageable for QSVMs and QNNs on quantum hardware with limited qubits.

By identifying essential features, QPCA allows cybersecurity models to achieve higher efficiency and lower latency, although current implementations are still experimental and best suited for hybrid quantum-classical models to offset quantum limitations.

RECOMMENDATIONS

➢ **Combine Quantum and Classical Models**: Hybrid approaches, blending QML algorithms like QSVM and QNN with classical models, help mitigate hardware limitations in current quantum systems, such as qubit decoherence and noise. For example, QSVM can handle initial anomaly detection and filtering, while classical models can manage post-detection processing for decision-making. This synergy also allows quantum models to handle feature extraction efficiently without compromising accuracy due to current hardware constraints.

➢ **Optimize Preprocessing with QPCA**: Using QPCA to preprocess data can make datasets more manageable and reduce computational requirements for QSVM and QNN. This preprocessing step effectively reduces the data's dimensionality, allowing the quantum models to operate more efficiently. QPCA, in particular, can help isolate key features from large volumes of network traffic data, which is valuable for cybersecurity applications where high-dimensional data is common.

➢ **Target Real-Time Anomaly Detection Applications**: Quantum algorithms can be particularly effective for real-time monitoring in cybersecurity. QSVM and QNN are recommended for scenarios where rapid anomaly detection is necessary, such as monitoring real-time network traffic for unusual patterns that might indicate a security threat. Implementing QML in real-time anomaly detection applications can help reduce response times and improve overall system resilience to cyber threats.

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

➢ **Optimize Model Parameters and Circuit Depth**: Regular fine-tuning of parameters and quantum circuit configurations is necessary to optimize QML models for anomaly detection. Adjustments to qubit count, quantum circuit layers, and feature mappings can significantly affect the accuracy and efficiency of QSVM and QNN algorithms. Iterative tuning and experimentation are essential for adapting models to the unique data patterns in cybersecurity, ensuring they maintain both speed and predictive accuracy.

➢ **Use QSVM for Pattern Recognition in Network Traffic**: QSVM is particularly recommended for applications where anomalies exhibit distinct patterns or outliers. For example, in network traffic analysis, QSVM can classify outliers effectively by leveraging quantum properties like superposition and entanglement, improving its detection capabilities over classical SVM. Researchers.

FUTURE RESEARCH

- **Quantum Algorithms for Anomaly Detection**: Developing specialized quantum algorithms designed to enhance the speed and accuracy of anomaly detection in large datasets. This can include leveraging quantum versions of classical algorithms like k-means, DBSCAN, or neural networks.
- **Hybrid Quantum-Classical Models**: Researching hybrid models that combine classical and quantum techniques to benefit from the strengths of both paradigms. This can involve using quantum computing for feature extraction or dimensionality reduction while employing classical systems for final anomaly detection.
- **Quantum Feature Selection**: Investigating quantum algorithms for efficient feature selection and dimensionality reduction, which could help in identifying relevant features in audit logs or network traffic data that are indicative of anomalies.
- **Quantum Simulation of Cyber Threats**: Utilizing quantum simulations to model potential cyber threats and their behaviors, allowing for a more robust understanding of what constitutes an anomaly in various contexts.
- **Benchmarking Quantum Anomaly Detection**: Establishing benchmarks for quantum anomaly detection methods against classical methods to evaluate performance improvements in speed, scalability, and accuracy in real-world scenarios.

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 01, 127-154
DOI: https://doi.org/10.59231/SARI7784

- **Privacy-Preserving Quantum Algorithms**: Exploring quantum algorithms that facilitate secure and privacy-preserving data processing, addressing concerns related to sensitive data in cybersecurity audits.
- **Quantum Reinforcement Learning**: Implementing quantum reinforcement learning techniques for anomaly detection, which could adapt to changing patterns in the data over time as new threats emerge.
- **Interdisciplinary Approaches**: Collaborating with fields such as cryptography, network theory, and complex systems to develop a more comprehensive understanding of anomalies in cybersecurity contexts.
- **Scalability Studies**: Conducting research on the scalability of QML techniques for anomaly detection with increasing sizes and complexities of datasets typical in cybersecurity.
- **Real-time Anomaly Detection Systems**: Developing real-time systems based on QML that can continuously monitor and analyze cybersecurity data to identify and respond to anomalies as they occur.
- **Ethical and Policy Implications**: Investigating the ethical implications of using QML in cybersecurity, including its impact on privacy, security, and accessibility.

CONCLUSION

Quantum Machine Learning (QML) holds transformative potential for anomaly detection in cybersecurity audits, enabling new levels of efficiency, precision, and adaptability in identifying and mitigating cyber threats. With advancements in Quantum Support Vector Learning (QSLV), Quantum Neural Networks (QNN), and Quantum Principal Component Analysis (QPCA), QML can address the unique demands of cybersecurity data, which is often high-dimensional, noisy, and complex. While current quantum hardware presents limitations, hybrid models that integrate classical and quantum systems can maximize immediate benefits, making QML solutions increasingly viable. As quantum hardware and algorithms evolve, QML-driven anomaly detection is poised to become a cornerstone in proactive cybersecurity, enhancing the ability to protect digital infrastructure from sophisticated attacks with speed and accuracy previously unattainable.

Reference:

1. Blog of the Fraunhofer institute for applied and integrated security AISEC. https://www.cybersecurity.blog.aisec.fraunhofer.de/en/
2. Dixit, A. (2024). Navigating the Future: Exploring the strategic integration of artificial intelligence in contemporary management practices. *Shodh Sari-An International Multidisciplinary Journal*, *03*(02), 295–303. https://doi.org/10.59231/sari7705
3. Tiwari, A. K. (2024b). Relevance of innovations in educational research technology of universities. *Edumania-An International Multidisciplinary Journal*, *02*(01), 235–254. https://doi.org/10.59231/edumania/9029
4. arXiv – (Cornell University) anomaly detection using QML. https://arxiv.org/search/?query=anomaly+detection+using+QML&searchtype=all&source=header
5. IBM. Quantum. https://securityintelligence.com/tag/quantum-computing/page/3/?mhsrc=ibmsearch_a&mhq=quantum%20computing%20comes%20to%20the%20cloud&_gl=1%2Ai68vs0%2A_ga%2AODk1MDE4MzYyLjE3MzAxOTczMjA.%2A_ga_FYECCCS21D%2AMTczMDE5NzMxOS4xLjEuMTczMDE5NzQ2Mi4wLjAuMA
6. International Information and Engineering Technology Association. https://www.iieta.org/
7. NSF (National Science Foundation) public access repository (NSF-PAR). https://par.nsf.gov/contact

Received on Oct 29, 2024
Accepted on Dec 05, 2024
Published on Jan 01, 2025