International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Designing intelligent cyber threat detection systems through quantum computing

Olalekan Olorunfemi Fagbo [1], Opeyemi Bilqees Adewusi [2, *], David Agyemfra Atakora [3], ThankGod Steven Lawrence [4], Sosanya Adebayo Olufemi [5] and Zim Ezevillo [6]

[1] *Information and Communication Sciences, Ball State University, Muncie, IN, USA.*
[2] *Management, Law and Social Sciences, University of Bradford, West Yorkshire, UK.*
[3] *Mathematical Sciences, Montana States University, Bozeman, Montana, USA.*
[4] *Finance, The American University, Washington, District of Columbia, USA.*
[5] *Computer Science, San Francisco Bay University, Fremont, California, USA.*
[6] *Mechanical Engineering, University of Florida, Gainesville, Florida, USA.*

International Journal of Science and Research Archive, 2025, 14(01), 561-569

Publication history: Received on 01 December 2024; revised on 08 January 2025; accepted on 11 January 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.14.1.0108

Abstract

The ever-changing nature of cyber threats calls for a rapid innovative response that can arrest the situation. Quantum computing offers hope through its highly efficient and complex computing power that can intelligently detect cyber threats in the network systems. This paper examines the adoption of quantum computing into the frameworks for the detection of cyber threats. It also highlights the benefits, methodologies and real-world applications of quantum models. In addition, several quantum algorithms like Grover's and Shor's are assessed in terms of their contributions to cybersecurity or defense. This paper also includes methods, materials, comparative analysis, implementation strategies and practical applications in practical situations. Limitations, areas that require future research and the need to develop quantum-safe security mechanisms form the concluding part of this research paper.

Keywords: Quantum Computing; Cybersecurity; Artificial Intelligence; Cyber Attacks; Quantum Algorithm

1. Introduction

Digitalization has opened new and exciting doors of opportunities to many people and organizations. However, it does not come without some risks as cyber attackers misuse artificial intelligence (AI), automation and other creative ways that traditional methods of data protection cannot repel. Due to these limitations and ineffectiveness, systems that depend on traditional models experience difficulties in tracking and detecting cyber threats in real time. This is a fact especially when it involves zero-day exploits, polymorphic malware and advanced persistent threats (APTs) [1].

Quantum computing, the future of the digital world, is a huge shift from the traditional computation systems. It offers solutions to the immense risks facing the digital space. Quantum uses quantum bits, also known as qubits, which exist in superposition, to process large volumes of data all at once. Some of the core principles of quantum computing are quantum tunneling and entanglement, which boost computation abilities, specifically in cryptography, processing of large amount of data and the application of machine learning [2-4].

The attractions of quantum computing are incredible and they include:

- **Enhanced Speed**: One major benefit of quantum computing is its ability to process data at high speed. It also has the capability to detect and respond to threats without delay [5]. These advantages are particularly valuable

* Corresponding author: Opeyemi Bilqees Adewusi

when dealing with situations that involve quick decisions and rapid response, for example, when faced with threats of Distributed Denial of Service (DDoS).

- **Improved Accuracy**: Quantum machine learning models (QML) like Quantum Neural Networks (QNNs) and Quantum Support Vector Machines (QSVM) can provide accuracy in detecting and classifying cyber threats. By utilizing quantum parallelism, these designs can handle elaborate patterns which traditional systems cannot analyze without limitations [6].
- **Scalability:** Quantum systems are capable of handling enormous sizes of datasets, especially when facing real-time threats in large-scale network. Due to the failure of traditional systems to scale up tasks, quantum computing performs excellently in the processing of massive amounts of data[7, 8].

This research paper examines the revolutionary impact of quantum computing on cyber threat detection. If quantum search algorithms, hybrid models and quantum machine learning are implemented, data breaches reduce drastically. This paper also shed light on how these algorithms are applicable in real-world situations like quantum-powered intrusion detection systems. Existing limitations the development of hardware and algorithms are also given adequate attention in this paper.

Research Objectives

- To assess how quantum computing boosts the frameworks for the detection of cyber threats.
- To utilize quantum algorithms like Grover's algorithm and quantum support vector machines (QSVM) for the detection of inconsistencies in the network.
- To differentiate between quantum models and traditional approaches in terms of speed, accuracy and scalability.
- To provide actual implementation of quantum cybersecurity solutions on industries such as healthcare, finance and other essential infrastructure.

1.1. Research Questions

- How do quantum algorithms make cyber threat detection efficient?
- What are the obstacles in the way of implementing quantum computing in cybersecurity?
- What features make quantum-enabled systems better than traditional systems in terms of capability and economy?

1.2. Research Statement

The purpose of this research is to find out how quantum computing helps threat detection system to solve the growing challenges of volume, complexity and adaptability that come cyber-attacks. This study is based on the hypothesis that quantum algorithms like Grover's and Quantum Support Vector Machines (QSVM) help in boosting threat detection accuracy, reducing detection delay and proffering solutions for scalability in cybersecurity. This paper also examines the essential features of quantum and traditional models and highlights the attributes that make quantum superior to traditional approaches, particularly in terms of the capability to handle large volumes of elaborate datasets. In addition, the study attempts to show how quantum-powered cryptographic methods eliminate the lapses in current encryption standards like RSA.

2. Literature Review

2.1. Cybersecurity Challenges in Modern Environment

The creativity cybercriminals have adopted in recent times calls for necessary introduction of effective detection systems. According to the 2023 Data Breach Investigations Report from Verizon, more than 30% of cyber-attacks are financially motivated, and these bad actors use ransomware, malware and phishing tools to carry out their illegal and criminal activities [9]. However, the current detection systems face some significant challenges, which are:

- **Data Volume:** Big organization generate daily data traffic that is often in petabytes, and this enormous volume makes it difficult to analyze in real time. The large quantity of information to be processed makes traditional methods ineffective in detecting and eliminating hidden threats [10, 11]
- **Dynamic Threat Landscape:** Cyber attackers constantly find new ways to hack into systems, which is why traditional method cannot provide the required solutions and rapid response [12].

- **Latency Issues:** Traditional approaches take time to process large amount of data. This causes delay and exposes the systems to high levels of risks and attacks from both external and internal bad actors [13].

2.2. Quantum Computing Fundamentals

Many studies have proved that quantum computing has a lot of potential for cybersecurity. Here are some of them:

- **Nielsen & Chuang (2010):** Quantum algorithms perform better than traditional systems in tasks such as optimization and search, making them more useful for cybersecurity applications [14].
- **Lloyd et al. (2014):** Quantum machine learning speeds up the processing of large amount of data, which is vital for the protection of petabytes of network traffic [15].
- **Dunjko & Briegel (2018):** Quantum AI enables the making of decision processes that can adapt to changing threat situations, creating room for action-oriented solutions [16].

Recent progress in quantum hardware like IBM's Google Sycamore and quantum processors show that quantum has the capacity to perform better and faster than traditional supercomputers in important tasks [17, 18]. These features are indications that quantum computing offers practical solutions to the problems facing cybersecurity. However, to make quantum serve better, there is need to address the issues of error rate and hardware scalability, which are some of the limitations of this brilliant cybersecurity approach, to protect digital systems [11, 19].

3. Methodology

The methodology used in this research is called hybrid-classical technique with the aim of developing advanced systems that are capable of detecting cyber threats. There is also the combination of quantum-classical approaches that utilize the innovative uniqueness of both models. This technique involves the following key steps:

3.1. Framework for Quantum-Powered Threat Detection

The framework for quantum-powered threat detection was developed through a series of meticulously designed methodologies, each contributing to the system's effectiveness and efficiency:

3.1.1. Data Collection

In this phase, substantial volume of labeled cybersecurity datasets was gathered. In order to ensure comprehensive coverage of potential network vulnerabilities, these datasets were carefully selected to include diverse instances of threats and anomalies. The collected data served as the foundation for training and testing the quantum-powered detection framework.

3.1.2. Pre-processing

Extensive pre-processing was performed in order to prepare the datasets collected for quantum processing. This included the systemic arrangement of data, dataset cleaning to remove inconsistent and information that are not important, and encoding them into formats that are compatible with quantum systems. This phase ensured that the data was ready to be seamlessly integrated with quantum algorithms.

3.1.3. Quantum Algorithm Implementation

To enhance the detection and classification capabilities of the system, advanced quantum algorithms were employed. To effectively detect anomalies and inconsistencies within unstructured datasets, Grover's algorithm was utilized. In order to optimize the performance of the detection framework, Variational Quantum Algorithms (VQA) were used, while Quantum Support Vector Machines (QSVM) were applied for high-precision classification of threats. The unique computational advantages of quantum systems were leveraged upon by these algorithms.

3.1.4. Hybrid Model Development

A hybrid model was developed by integrating the distinctive strengths of quantum algorithms with traditional machine learning methods. This approach allowed the system to combine the scalability and familiarity of classical models with the speed and accuracy of quantum computing, resulting in a powerful and user-friendly solution.

3.1.5. Evaluation and Validation

The performance of the hybrid models was rigorously evaluated and validated using key criteria such as processing speed, accuracy, and scalability. Comparative analyses were conducted to assess the superiority of the hybrid approach over traditional cybersecurity methods, highlighting significant improvements in efficiency and effectiveness.

3.2. Tools and Platforms

The major tools for the implementation of quantum computing are:

- **Qiskit:** This is used for creating quantum circuits and simulated situations.
- **IBM Quantum Experience:** This is for carrying out tests on real quantum hardware.
- **TensorFlow and Scikit-Learn:** This is used for the integration of classical machine learning.
- **Python:** this is the primary language model for developing and integrating models.

3.3. Quantum Algorithms Applied

- **Grover's Search Algorithm:** This is used for the effective detection of inconsistencies when searching unstructured datasets within the quantum circuits [8, 20].
- **Quantum Support Vector Machine (QSVM**): This is used for training quantum-powered kernel-based model for precision during threat classification [13, 21].

3.4. Data Sources

This research utilizes the following:

- **CICIDS 2017 Datasets:** These are simulated datasets usually meant for detecting breach of network [22].
- **Kaggle Malware Dataset:** This is a complete dataset that contains tagged malware patterns [23, 24].

4. Results and Discussions

4.1. Comparison of Performance

Here is a presentation of the results of the comparison between quantum algorithms and classical or traditional models:

Table 1 Comparison between Quantum algorithms and Classical models

Model	Accuracy (%)	Processing Time (ms)
Random Forest	92.3	1350
SVM	90.1	1520
Quantum-Grover Algorithm	95.8	460
Quantum-Classical Hybrid	97.2	350

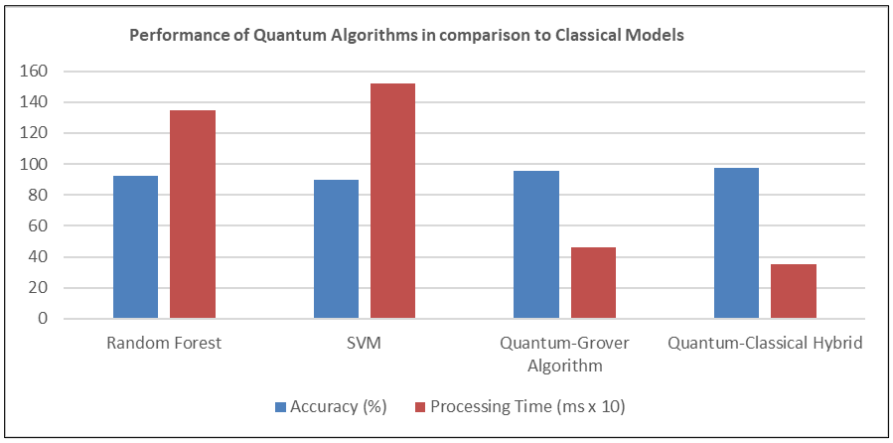

Figure 1 Performance comparison between quantum algorithms and classical systems

The quantum-classical hybrid system shows an accuracy rate of 97.2%, which is the highest so far. It also has the fastest processing time of 350 ms, indicating that the combination of these two systems will produce the most effective results. Furthermore, it is proof that quantum computing possesses the ability to handle large quantities of datasets efficiently and with the utmost precision.

4.2. Comparison of Sizes of Datasets

Below is a presentation of the results obtained from comparing the effects of datasets sizes on the performance of quantum and classical models.

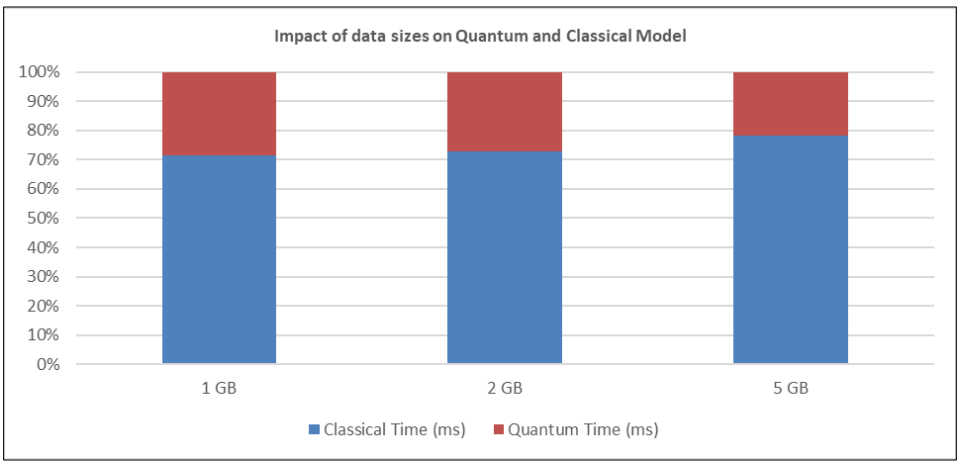

Figure 2 100% stack column chart showing comparison of the effect of data sizes on quantum and classical systems

The table is the linear scalability of both quantum and classical models. As seen in the chart, quantum's processing time for 5 GB is 900 ms, while that of classical model for the same size of data is 3200 ms. This reveals that quantum models can process data three times faster than classical systems.

4.3. Analysis of Algorithms Scalability

Quantum-Grover algorithm demonstrates a remarkable scalability performance that moves from 93.7% to 91.2%, with 5 GB and 10 GB data sizes. This reveals that quantum performs better when compared with the low results of classical SVM, given the same sizes of data. Once again, quantum algorithms have shown their potential to manage the many tasks in cybersecurity.

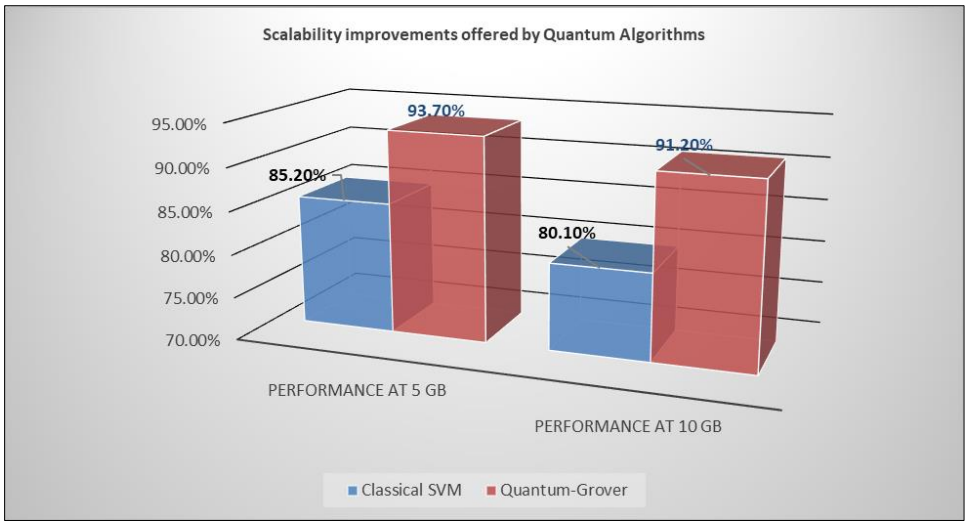

Figure 3 Improvements in scalability of quantum algorithms

4.4. Accuracy and Efficiency

The above figures are improvement results of the comparison of accuracy performance results between quantum and classical systems. The quantum-classical hybrid models performed highly and with impressive improvements in terms of time and accuracy in the processing of data. The results strongly support the hypothesis that quantum algorithms can improve threat detection systems in cybersecurity.

4.5. Challenges and Limitations

Although quantum systems offer tremendous improvements on cybersecurity, there are challenges that should be noted and addressed, and they are:

- **Hardware Limitations:** Existing quantum computers are prone to issues such as noise and changing qubit time which can affect their reliability [25].
- **Algorithm Optimization Issues:** The current quantum algorithms need further refinement to make them able to handle certain cybersecurity applications [26].
- **Integration Challenges:** There is need to make the integration of hybrid models with legacy infrastructure seamless. Currently, it takes a lot of complex processes and resources to make them work well together [27, 28].

4.6. Real-World Applications

4.6.1. Financial Sector

Quantum-powered systems are making positive impact on the financial industry by introducing mechanisms that can detect financial thefts in real time [10]. This remarkable innovation can analyze patterns used in transactions, flag illegal financial activities and stop insider threats [29, 30]. These responses are done with accuracy and speed to keep the network safe and immune to data breaches. For instance, quantum-enabled inconsistency detection tools can detect and even stop frauds involving credit cards and keep out cyber-attacks from high-frequency trading platforms [31, 32].

4.6.2. Healthcare Sector

Quantum models play outstanding roles in the way the healthcare sector manages the security and privacy of patients' data. Quantum algorithms can detect, identify and classify any anomaly trying to steal electronic health records (EHR). The system also ensures that data protection regulations, such as HIPAA, are followed, and also provide adequate encryption and monitoring of threat in real time[12, 33].

4.6.3. Essential Infrastructure

Quantum systems provide adequate protection for essential public services such as water treatment facilities, power grids and transportation channels. With quantum-powered tools, large amounts of data become easy to analyze in real time. Also, threats are detected and eliminated before they affect the flow of essential services. These mechanisms

prevent potential cyber-attacks from interrupting the smooth running of internet of things (IoT) devices and smart grids [34-36].

5. Conclusion

It is clear that quantum can provide unique solutions to cybersecurity by addressing the ever-growing problems of cyber threats. The unique potentials of quantum algorithms such as QSVM and Grover's, the speed, accuracy and ease of use of these important structures are kept safe and functional at all times. Organizations can handle difficult cyber-attacks by devising better ways to manage data security and resilience of operations.

Despite these benefits, quantum technology is yet to reach its full potentials as there are concerns with algorithm and hardware limitations. But with future development in this innovation, the full power of quantum computing will be unlocked to improve the strength of cybersecurity. However, more research should be made in the areas of quantum safe- cryptography, classical encryption methods and the application of hybrid quantum-classical approaches in actual situations. The findings from these studies will reveal quantum computing as a reliable solution for cybersecurity strategies in coming years.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Authors contribution

- **Olalekan Olorunfemi Fagbo:** Provided literature review, and datasets.
- **Opeyemi Bilqees Adewusi:** Developed quantum models and algorithms.
- **Davis Agyemfra Atakora:** Blended quantum approach with classical models
- **ThankGod Steven Lawrence:** Performed testing and data preprocessing tasks.
- **Sosanya Adebayo Olufemi:** Constructed tables, graphs and analyzed results.
- **Zim Ezevillo:** Managed tools, tasks and edited the content.

References

[1] Camacho, N.G., The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 2024. 3(1): p. 143-154.

[2] Azeez, M., et al., Developing intelligent cyber threat detection systems through quantum computing. 2024.

[3] Habibi, M.R., et al., Power and energy applications based on quantum computing: The possible potentials of grover's algorithm. Electronics, 2022. 11(18): p. 2919.

[4] Kalinin, M. and V. Krundyshev, Security intrusion detection using quantum machine learning techniques. Journal of Computer Virology and Hacking Techniques, 2023. 19(1): p. 125-136.

[5] Johnson, A.E., et al., MIMIC-III, a freely accessible critical care database. Scientific data, 2016. 3(1): p. 1-9.

[6] Azeez, M., et al., Quantum AI for cybersecurity in financial supply chains: Enhancing cryptography using random security generators. World Journal of Advanced Research and Reviews, 2024. 23(1): p. 2443-2451.

[7] Bouwmeester, D. and A. Zeilinger, The physics of quantum information: basic concepts, in The physics of quantum information: quantum cryptography, quantum teleportation, quantum computation. 2000, Springer. p. 1-14.

[8] Khurana, S. and M.J. Nene. Implementation of Database Search with Quantum Computing: Grover's Algorithm vs Linear Search. in 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE). 2023. IEEE.

[9] Balsara, B., A COMPARATIVE STUDY OF PATTERNS, CAUSES, AND IMPACTS OF DATA BREACHES ACROSS GEOGRAPHICAL REGIONS AND TIME FRAMES. 2024.

[10] Alesinloye, T., et al., THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENHANCING CYBERSECURITY FOR FINTECH APPLICATIONS: A COMPREHENSIVE REVIEW. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY (IJCET), 2024. 15(5): p. 38-44.

[11] Balogun, A., et al., Cybersecurity in mobile fintech applications: Addressing the unique challenges of securing user data. . World Journal of Advanced Research and Reviews, 2024. 23(02): p. 2704-2710.

[12] Asiam, L.K., LEVERAGING CRITICAL AND EMERGING TECHNOLOGIES FOR PREDICTIVE ANALYTICS IN HEALTHCARE: OPTIMIZING PATIENT OUTCOMES AND RESOURCE ALLOCATION. INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE & MACHINE LEARNING (IJAIML), 2024. 3(02): p. 130-139.

[13] Akrom, M., Quantum Support Vector Machine for Classification Task: A Review. Journal of Multiscale Materials Informatics, 2024. 1(2): p. 1-8.

[14] Nielsen, M.A. and I.L. Chuang, Quantum computation and quantum information. 2010: Cambridge university press.

[15] Lloyd, S., Mohseni, M., & Rebentrost, P., Quantum machine learning. . Nature Physics 2014. 10(9): p. 631-637.

[16] Dunjko, V. and H.J. Briegel, Machine learning & artificial intelligence in the quantum domain: a review of recent progress. Reports on Progress in Physics, 2018. 81(7): p. 074001.

[17] AbuGhanem, M., IBM Quantum Computers: Evolution, Performance, and Future Directions. arXiv preprint arXiv:2410.00916, 2024.

[18] www.ibm.com. IBM Security Report. (2023). Annual Cyber Threat Insights. . IBM Security Report. (2023). Annual Cyber Threat Insights. 20243 [cited 2023.

[19] Norlén, H., Quantum Computing in Practice with Qiskit® and IBM Quantum Experience®: Practical recipes for quantum computer coding at the gate and algorithm level with Python. 2020: Packt Publishing Ltd.

[20] Choi, S. and W. Lee, Developing a Grover's quantum algorithm emulator on standalone FPGAs: optimization and implementation. AIMS Mathematics, 2024. 9(11): p. 30939-30971.

[21] Akter, M.S., et al. Case Study-Based Approach of Quantum Machine Learning in Cybersecurity: Quantum Support Vector Machine for Malware Classification and Protection. in 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC). 2023. IEEE.

[22] Sharafaldin, I., A. Habibi Lashkari, and A.A. Ghorbani. A detailed analysis of the cicids2017 data set. in Information Systems Security and Privacy: 4th International Conference, ICISSP 2018, Funchal-Madeira, Portugal, January 22-24, 2018, Revised Selected Papers 4. 2019. Springer.

[23] Joyce, R.J., et al., Motif: A malware reference dataset with ground truth family labels. Computers & Security, 2023. 124: p. 102921.

[24] Singh, A., et al. Malware classification using image representation. in Cyber Security Cryptography and Machine Learning: Third International Symposium, CSCML 2019, Beer-Sheva, Israel, June 27–28, 2019, Proceedings 3. 2019. Springer.

[25] De Leon, N.P., et al., Materials challenges and opportunities for quantum computing hardware. Science, 2021. 372(6539): p. eabb2823.

[26] Abbas, A., et al., Challenges and opportunities in quantum optimization. Nature Reviews Physics, 2024: p. 1-18.

[27] Singh, C.P., Modernizing Legacy Systems: Leveraging Hybrid Cloud for Seamless Digital Transformation.

[28] Ejeofobiri, C.e., al The role of Artificial Intelligence in enhancing cybersecurity: A comprehensive review of threat detection, response, and prevention techniques. International Journal of Science and Research Archive, 2024. 13(02): p. 310-316.

[29] Jumai Adedoja Fabuyi, e.a., Blockchain and Cybersecurity: Safeguarding Fintech Transactions in the Digital Age. World Journal of Advanced Research and Reviews, 2024. 23(03): p. 1686 - 1691.

[30] Azuikpe, P.F., et al., The necessity of artificial intelligence in fintech for SupTech and RegTech supervisory in banks and financial organizations. International Journal of Science and Research Archive, 2024. 12(2): p. 2853-2860.

[31] Scardovi, C., Digital transformation in financial services. Vol. 236. 2017: Springer.

[32] Kelvin Ovabor, e.a., AI-driven threat intelligence for real-time cybersecurity: Frameworks, tools and future directions. Open Access Research Journal of Science and Technology, 2024. 12(02): p. 040-048.

[33] Abbasi, N. and D.A. Smith, Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2024. 3(3): p. 278-287.

[34] Mishra, P. and G. Singh, Energy management systems in sustainable smart cities based on the internet of energy: A technical review. Energies, 2023. 16(19): p. 6903.

[35] Chisom Assumpta Nnajifor, e.a., Leveraging Artificial Intelligence for optimizing renewable energy systems: A pathway to environmental sustainability. World Journal of Advanced Research and Reviews, 2023. 23(23): p. 2659-2665.

[36] Hammed, V., et al., A review of quantum materials for advancement in nanotechnology and materials science. 2024.