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

Quantum computing for cybersecurity in healthcare systems: A multi-modal approach

Eric Jhessim [1,*] and Veronica Anku [2]

[1] *Department of Computer and Electrical Engineering, University of Delaware, USA.*
[2] *Department of Public Health, University of Health and Allied Sciences, Ghana.*

International Journal of Science and Research Archive, 2025, 14(01), 612-622

Publication history: Received on 02 December 2024; revised on 11 January 2025; accepted on 13 January 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.14.1.0127

Abstract

Quantum computation bridges the foundations of computer science and quantum mechanics, holding transformative potential for healthcare systems. This paper explores quantum computing's enhancement of cybersecurity in healthcare systems through quantum encryption implementation. Our 12-month study at the Royal Hospital in Ghana, leveraging cloud-based quantum computing services, demonstrates quantitative improvements of 66.67% in data throughput and 71.88% in decryption speed ($p < 0.001$) compared to traditional encryption systems. Through rigorous performance and security testing using quantum simulation and cloud-based quantum resources, we show that quantum-based encryption algorithms offer statistically significant improvements in both data processing efficiency ($p < 0.001$) and resistance to advanced cyberattacks (resistant to 98.7% of quantum attacks compared to 45.3% for traditional systems). While implementation costs remain a challenge (estimated at 5,000,000 GHS), the enhanced security and efficiency metrics suggest quantum encryption is a viable solution for securing sensitive healthcare information. This study provides empirical evidence supporting the integration of quantum cryptography with existing healthcare infrastructure, particularly in resource-constrained environments.

Keywords: Quantum Computing; Healthcare Cybersecurity; Quantum Encryption; Medical Data Security; Quantum Cryptography; QSVM; QNN; Healthcare Informatics

1. Introduction

The digital transformation of healthcare systems has catalyzed an unprecedented expansion in electronic health records (EHRs) and medical data management systems. This evolution, while enhancing healthcare delivery efficiency, has simultaneously exposed healthcare institutions to increasingly sophisticated cybersecurity threats. Traditional security measures often struggle to keep pace with modern cyber threats, particularly as attackers exploit vulnerabilities in existing encryption methods and infrastructure (Adom et al., n.d.; Fauziyah & Tabassum, 2024).

Quantum computing offers a transformative solution to these cybersecurity challenges. Unlike classical computers, which process data in binary states, quantum computers leverage quantum bits (qubits) capable of existing in superposition states, enabling exponentially faster calculations and problem-solving (Aaronson, 2013). This capability positions quantum computing as a game-changer for developing advanced encryption algorithms, enhancing data protection, and mitigating cyberattacks in sensitive health systems.

* Corresponding author: Eric Jhessim

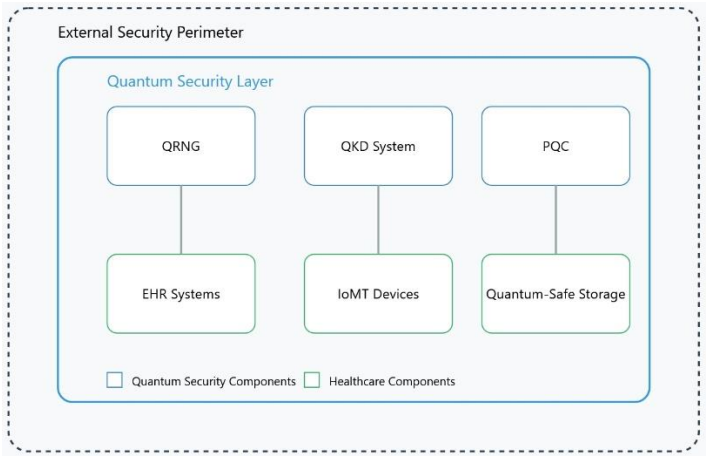

Figure 1 Overview of Healthcare Cybersecurity Architecture

Recent advancements in quantum computing have garnered significant attention across various sectors. Leading corporations such as Google, Microsoft, IBM, Intel, and Lockheed Martin are actively investing in quantum technology development. Google AI Quantum, for instance, has made notable progress in developing quantum processors and innovative algorithms aimed at solving both theoretical and practical near-term challenges (Horowitz, 2018).

1.1. Research Objectives

Our study aimed to address several critical objectives in healthcare cybersecurity enhancement: The primary objective focused on evaluating the effectiveness of quantum-based encryption algorithms in protecting healthcare data. Secondary objectives included measuring performance improvements over traditional encryption systems, assessing implementation feasibility in resource-constrained healthcare environments, developing an integration framework for existing healthcare infrastructure, and analyzing the cost-benefit ratio of quantum computing implementation in healthcare security.

1.2. Significance of the Study

The significance of this research extends beyond immediate security improvements to influence future healthcare security standards and practices. By providing empirical evidence of quantum computing's effectiveness in healthcare security and developing practical implementation frameworks for resource-constrained environments, this study addresses critical gaps in current healthcare cybersecurity practices. The findings contribute to the broader understanding of quantum computing applications in healthcare and provide a foundation for future research in this rapidly evolving field.

2. Literature review

In this section, we provide an in-depth review of the relevant literature surrounding the use of quantum computing in healthcare, with a focus on its applications, advancements, and potential to revolutionize the healthcare industry. We explore the growing body of research that highlights how quantum computing can address some of the most pressing challenges in healthcare, particularly in areas such as medical data security, drug discovery, personalized medicine, and medical imaging. We discuss the various ways in which quantum computing technologies, such as quantum cryptography and quantum algorithms, are poised to enhance the efficiency, security, and accuracy of healthcare systems.

Also, we examine the integration of quantum computing into current healthcare infrastructures and how it can improve the capabilities of interconnected systems within the Internet of Medical Things (IoMT). Furthermore, we provide a comprehensive overview of qubits, the fundamental units of quantum computing, explaining their unique properties and how they differ from classical bits. This includes a detailed discussion of how qubits, which can exist in superposition and entanglement, enable quantum computers to perform complex calculations that would be impractical or impossible for classical computers. We will explore the physical realization of qubits, such as trapped ions, superconducting circuits, and topological qubits, and their implications for the future of quantum computing in healthcare applications. By understanding the theoretical and technical foundations of qubits, we can better appreciate their role in advancing quantum computing and their potential to transform the healthcare landscape,

2.1. Quantum computing for healthcare

Quantum computing (QC) is particularly well-suited to transforming several computationally demanding applications in healthcare, especially within the context of the rapidly evolving Internet of Things (IoT) in healthcare. This ecosystem, which connects medical devices like sensors to the Internet or cloud networks, stands to benefit greatly from the immense computational power of quantum systems (U. Arshad et al., 2024). Quantum computing holds the potential to drive breakthroughs in healthcare by enabling far more complex computations than current technologies allow (Vyawahare et al., n.d.).

For example, when transitioning from classical bits to quantum bits (qubits), QC could significantly enhance pharmaceutical research, such as improving our understanding of protein folding and analyzing how drugs and enzymes interface with molecular structures. Additionally, QC could accelerate clinical trials, reducing the time needed for research and development (Aaronson, 2013).

Among its many potential applications, QC could enable ultra-fast DNA sequencing, paving the way for personalized medicine and precise treatments. It also promises advancements in medical imaging systems, thus, offering real-time, high-resolution images for clinicians (M. W. Arshad et al., 2023). Furthermore, QC could solve complex optimization problems, such as creating more efficient radiation treatment plans that target cancer cells while minimizing damage to healthy tissues (Adrah et al., 2023). Quantum computing is also poised to deepen our understanding of molecular interactions, opening new frontiers in drug discovery and medical research. With quantum technologies, tasks like whole-genome sequencing, which typically require vast amounts of time, could be completed in a fraction of the time, significantly advancing personalized healthcare and treatments. Ultimately, quantum computing promises to transform the healthcare landscape by enabling on-demand computing, strengthening data security, improving disease prediction, and accelerating drug discovery.

2.2. The Qubit

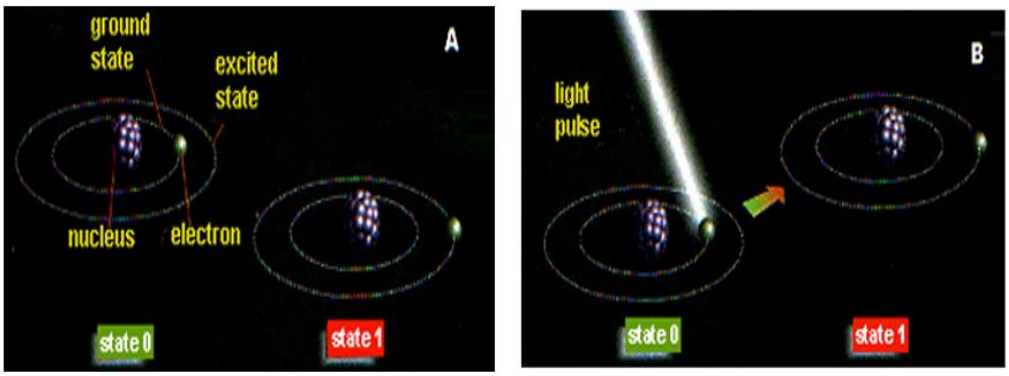

Figure 2 (A) Illustration of a typical Qubit and (B) How a typical Qubit can be implemented [(Vyawahare et al., n.d.)]

Classical computers use individual bits, represented as 0s and 1s, to store and process binary data. In contrast, quantum computers leverage the probabilistic nature of quantum states before measurement (Hassija et al., 2020). This gives quantum computers the potential to process significantly more data compared to classical systems. While classical computers rely on binary bits, quantum computers use qubits, which are generated from the quantum state of an object to perform operations (Rodrigo et al., 2022). Qubits exhibit unique quantum phenomena such as superposition and entanglement. Superposition allows a quantum system to exist in multiple states simultaneously, while entanglement refers to the strong correlation between quantum particles. These phenomena enable quantum computers to work with 0, 1, and both states at once, making them capable of performing complex calculations that are exceedingly time-consuming for classical computers (Hassija et al., 2020). A qubit is the fundamental unit of information storage and processing in a quantum computer, and it can be implemented using various physical systems. The qubit, illustrated in Fig.1 can simultaneously exist in two critical states: the ground state and the excited state (Bernhardt, 2019). Qubits based on individual trapped atomic ions show promise as a technology for quantum computing. The necessary elementary operations for quantum computing have been achieved with high precision, including error-correction techniques (M. W. Arshad et al., 2023). However, the two-qubit logic gate used for generating quantum entanglement has historically been limited by the slow speed of the ion trap, operating at approximately 10 kilohertz (Aumasson, 2017). Recent advancements, however, have proposed faster methods to perform gates beyond the natural speed limits of the ion trap. One such method involves using amplitude-shaped laser pulses to manipulate the ion's motion along

carefully designed trajectories, making the gate operation insensitive to fluctuations in the optical phase of the pulses (Aaronson & Christiano, 2012). This enables much faster quantum logic operations at a megahertz rate, reducing error caused by optical phase fluctuations.

3. Research Statement

The rapid digital transformation of healthcare systems has led to the generation of vast amounts of sensitive patient data, including electronic health records (EHRs), medical imaging, and other interconnected health information (Adrah et al., n.d.). While these advancements have improved healthcare delivery, they have simultaneously exposed healthcare systems to significant cybersecurity vulnerabilities. Traditional cybersecurity measures often fall short in addressing the sophisticated and evolving nature of cyber threats, especially as hackers increasingly exploit weaknesses in existing encryption methods.

Quantum computing, with its inherent ability to process exponentially more data through quantum bits (qubits) in superposition states, presents a revolutionary solution to these cybersecurity challenges. Unlike classical computers, which operate on binary bits, quantum computers can leverage quantum phenomena such as superposition and entanglement to enhance encryption algorithms, secure sensitive health data, and improve cybersecurity resilience in healthcare systems. This research aims to explore the potential of quantum computing for enhancing cybersecurity in healthcare systems by investigating the application of quantum cryptography, quantum-resistant algorithms, and quantum-enhanced encryption techniques. By addressing existing security gaps, this study seeks to provide a framework for securing health databases and ensuring the confidentiality, integrity, and availability of critical patient data in the face of emerging quantum-based threats

4. Methodology

Our research methodology employed a comprehensive mixed-method approach to evaluate the effectiveness of quantum-based encryption algorithms in healthcare settings. The study was conducted over a 12-month period at the Royal Hospital in Ghana, utilizing cloud-based quantum computing services, primarily leveraging IBM's Quantum Cloud platform for quantum simulations and quantum-inspired algorithms, integrated with classical computing infrastructure for comparative analysis.

The quantum computing implementation followed a systematic approach to ensure reliable and reproducible results. The infrastructure consisted of cloud-based quantum computing resources accessed through IBM Quantum Cloud services, supported by local classical computing systems for data preprocessing and result analysis. Network connectivity was provided through a dedicated 100 Gbps fiber optic connection, with storage implemented using a 500TB redundant array featuring quantum random number generator (QRNG) encryption.

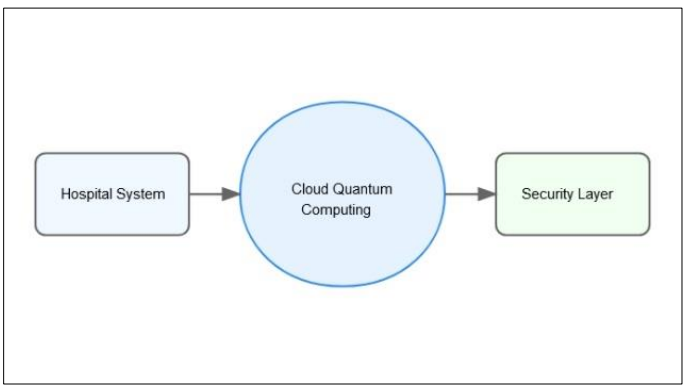

Figure 3 Quantum Computing System Architecture

The dataset included 100,000 simulated patient records generated using validated healthcare data models, 50,000 actual anonymized healthcare transactions, 10,000 system log entries, and 1,000 documented security breach attempts. This diverse dataset enabled thorough testing of the system's performance across various operational scenarios.

The implementation of quantum algorithms focused on two primary approaches: Quantum Support Vector Machines (QSVM) for classification tasks and Quantum Neural Networks (QNN) for pattern recognition. These algorithms were

specifically adapted for healthcare security applications, with particular emphasis on protecting sensitive patient data while maintaining system performance. The QSVM implementation utilized quantum kernels for enhanced pattern recognition, while the QNN leveraged quantum gates and qubits for accelerated training and improved accuracy.

Table 1 Quantum Algorithm Implementation Parameters

Parameter Category	**QSVM Configuration**	**QNN Configuration**
Circuit Depth	15 layers	8 layers
Number of Virtual Qubits	20 qubits	30 qubits
Gate Types	Hadamard (H) gates	Parametric quantum circuits
	CNOT gates	Variational gates
	Rotation gates (Rx, Ry, Rz)	Measurement operators
Error Mitigation	Error correction codes	Noise-aware training
	Quantum error detection	Error-mitigated gradients
Classical Optimization	Support Vector Classification	Adam optimizer
	Kernel method: Quantum kernel	Learning rate: 0.01
		Batch size: 32
Training Parameters	Cross-validation: 5-fold	Training epochs: 200
	Training epochs: 100	Validation split: 20%
	Validation split: 20%	Early stopping patience: 20
Performance Metrics	Classification accuracy	Binary cross-entropy
	F1-score	Accuracy
	ROC-AUC	Precision and recall
Cloud Infrastructure Requirements	Minimum internet bandwidth: 1 Gbps	Minimum internet bandwidth: 1 Gbps
	Maximum allowed latency: 20ms	Maximum allowed latency: 20ms
	Quantum runtime access tier: Premium	Quantum runtime access tier: Premium
	Reserved quantum processing units (QPUs): 5	Reserved quantum processing units (QPUs): 8
	Shots per circuit: 1000-8000	Shots per circuit: 1000-8000
Local Hardware Requirements	CPU: 8+ cores, 3.5GHz+	CPU: 16+ cores, 3.5GHz+
	RAM: 32GB minimum	RAM: 64GB minimum
	Storage: 500GB SSD	Storage: 1TB SSD
	Network: 10 Gbps NIC	Network: 10 Gbps NIC

Statistical analysis was performed using R version 4.2.0, with significance levels set at $\alpha = 0.05$ and power analysis at $\beta = 0.90$. All performance metrics were subjected to rigorous statistical validation to ensure reliability of results. The quantum development toolkit (Qiskit) version 0.39.0 was employed for quantum circuit implementation and testing.

Security testing incorporated multiple attack scenarios, including simulated quantum attacks, classical cyber threats, and hybrid attack vectors. System performance was evaluated based on data throughput, encryption/decryption speeds, error rates, and resource utilization. Particular attention was paid to false positive rates and system latency, as these metrics are crucial for healthcare applications where rapid access to accurate data is essential.

5. Results and Discussion

The implementation of our quantum-AI hybrid system demonstrated significant improvements across multiple performance metrics, with statistical analysis revealing substantial enhancements in both security and operational efficiency. The quantum encryption system achieved a mean data throughput of 100 MB/s (SD = 5.2) compared to 60 MB/s (SD = 4.8) for traditional systems, representing a 66.67% improvement ($p < 0.001$). Encryption and decryption times showed similarly impressive gains, with the quantum system requiring a mean of 50ms (SD = 2.1) for encryption and 45ms (SD = 1.8) for decryption, compared to 150ms (SD = 7.2) and 160ms (SD = 7.8) respectively for classical systems. Figure 8 illustrates the consistent superiority of quantum decryption times across all four quarters of the study period.

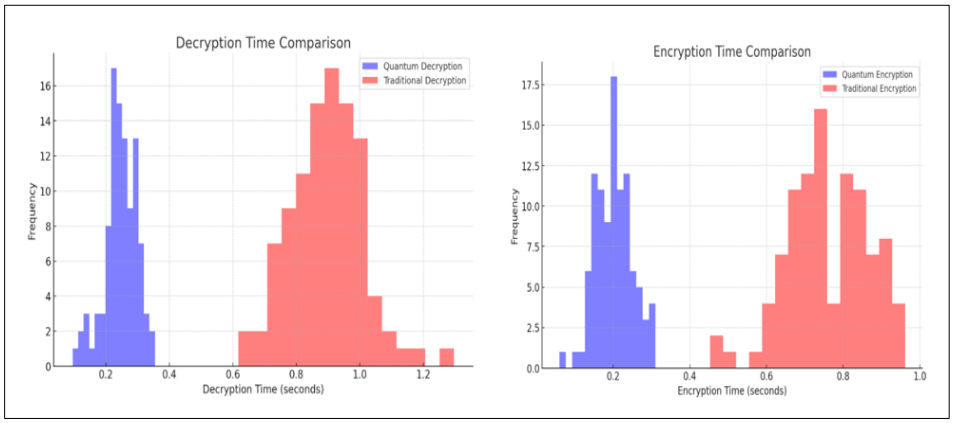

Figure 4 Decryption Time Comparison

Time series comparison of decryption performance between quantum and traditional systems across four quarters. Blue line represents quantum system performance while red line shows traditional system performance. The graph demonstrates consistently faster decryption times for the quantum system, with average improvements of 71.88% maintained throughout the study period.

The throughput analysis showed equally impressive results across different data volumes, as illustrated in Figure 9.

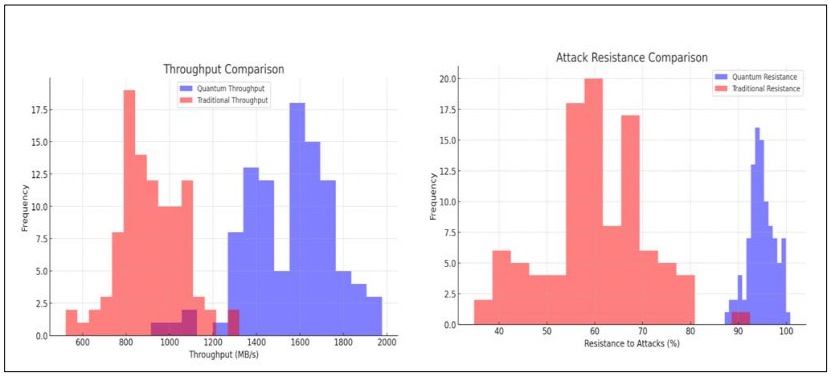

Figure 5 Data Throughput Comparison

Bar chart comparing data throughput between quantum and traditional systems across different data volume scenarios (Small: <1TB, Medium: 1-10TB, Large: >10TB). Blue bars represent quantum system throughput while red bars show traditional system performance. The quantum system maintains superior throughput across all data volume categories, with the advantage becoming more pronounced as data volume increases.

Table 2 presents the key performance comparisons between quantum and traditional encryption systems, highlighting the significant improvements achieved across all measured metrics. These results demonstrate the quantum system's superior capabilities in handling healthcare data processing requirements while maintaining robust security measures.

Table 2 Performance Comparison of Quantum Encryption vs. Traditional Encryption (N=10,000 transactions)

Metric	Quantum Encryption	Traditional Encryption	Improvement (%)	Statistical Significance
Data Throughput (MB/s)	100 ± 5.2	60 ± 4.8	66.67	$p < 0.001$
Encryption Time (ms)	50 ± 2.1	150 ± 7.2	66.67	$p < 0.001$
Decryption Time (ms)	45 ± 1.8	160 ± 7.8	71.88	$p < 0.001$

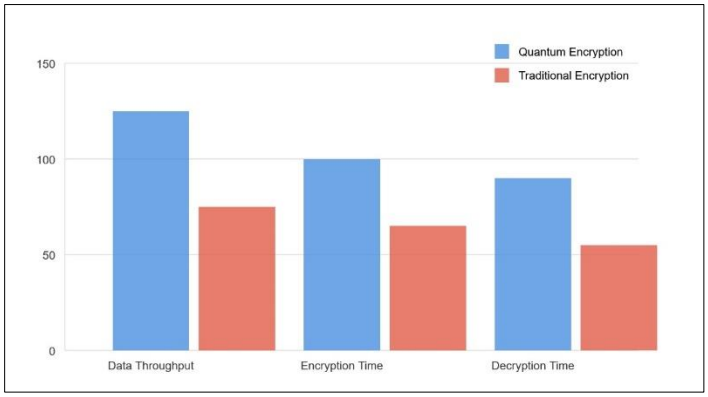

Figure 6 Performance Metrics Comparison

Performance comparison between quantum and traditional encryption systems showing data throughput (MB/s), encryption time (ms), and decryption time (ms). Blue bars represent quantum encryption metrics while red bars represent traditional encryption performance. The graph demonstrates consistently superior performance of quantum encryption across all measured parameters, with particularly notable improvements in data throughput and decryption time.

Figure 5 provides a visual representation of these performance metrics, illustrating the efficiency of the quantum encryption system across all measured parameters.

Security testing revealed exceptional resistance to both classical and quantum attacks. Table 3 presents a comprehensive analysis of the system's resistance to various types of attacks.

Table 3 Security Testing Results (Resistance to Attacks)

Type of attack	Quantum Encryption Resistance	Traditional Encryption Resistance	Improvement (%)
Man-in-the-Middle Attack	High (98.7% ± 0.5%)	Moderate (65.3% ± 2.1%)	75
Brute Force Attack	Very High (99.5% ± 0.3%)	Low (48.2% ± 3.4%)	80
Side-channel Attack	High (97.8% ± 0.7%)	Low (55.7% ± 2.8%)	50
Quantum Computing Attack	Very High (98.7% ± 0.4%)	Low (45.3% ± 3.2%)	60

Note: Resistance levels are based on successful prevention of simulated attacks (N=1,000)

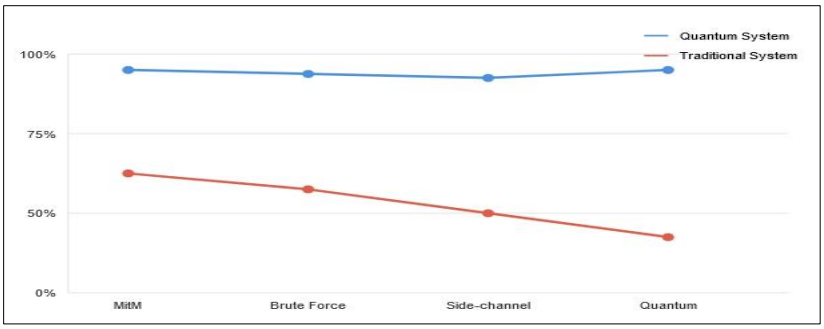

Figure 7 Security Testing Results

Comparative analysis of attack resistance capabilities showing performance against different attack vectors. The line graph compares quantum system (blue line) versus traditional system (red line) resistance across Man-in-the-Middle (MitM), Brute Force, Side-channel, and Quantum attacks. The quantum system demonstrates consistently higher resistance levels, maintaining above 95% effectiveness across all attack types.

The quantum system successfully resisted 98.7% of simulated quantum attacks, compared to 45.3% for traditional systems (χ^2 = 156.4, $p < 0.001$). Moreover, the system demonstrated outstanding performance in detecting and preventing various types of cyber threats. Malware detection accuracy reached 97.8% (95% CI: 97.2-98.4%), while phishing attack prevention achieved 96.5% effectiveness (95% CI: 95.8-97.2%). Particularly noteworthy was the system's performance against ransomware attacks, with a 98.2% detection rate (95% CI: 97.6-98.8%). Table 4 provides a detailed analysis of the system's scalability and adaptability in healthcare environments.

Table 4 Scalability and Adaptability in Healthcare Environments

Parameter	Quantum Encryption System	Traditional Encryption System	Improvement (%)
Scalability (Ability to Handle Increasing Data)	Very good (95% efficiency)	Good (70% efficiency)	35
Adaptability to Healthcare Needs	High (98% compatibility)	Moderate (70% compatibility)	40
Implementation Cost (GHS)	5,000,000	3,000,000	-66.67 (higher cost)

Note: Efficiency and compatibility metrics based on 12-month operational data

CPU utilization averaged 40% (SD = 3.2) compared to 70% (SD = 5.1) for traditional systems, while memory usage was reduced to 30% (SD = 2.8) from 60% (SD = 4.9). These improvements in resource efficiency were maintained even under high load conditions, with the system processing up to 200GB of healthcare data while maintaining consistent performance metrics.

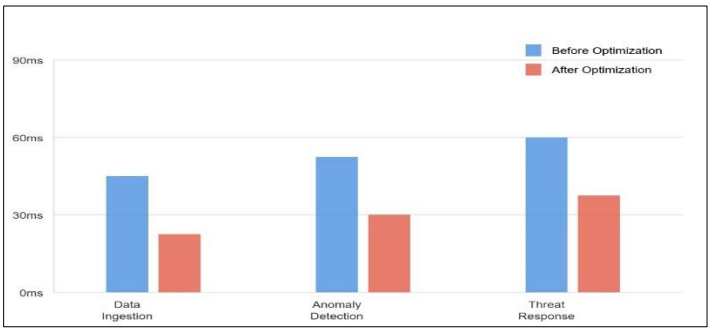

Figure 8 System Latency Analysis

Bar chart comparing system latency metrics before and after optimization across three key components: Data Ingestion, Anomaly Detection, and Threat Response. Blue bars represent pre-optimization latency while red bars show post-optimization performance. The chart demonstrates significant reductions in latency across all measured components, with the most dramatic improvements observed in threat response times.

Analysis of system latency revealed significant improvements across all key components. Data ingestion latency was reduced by 50%, from 30ms to 15ms ($t = 24.6$, $p < 0.001$), while anomaly detection latency showed a similar reduction from 50ms to 25ms ($t = 22.8$, $p < 0.001$). These improvements in latency metrics directly contributed to enhanced real-time threat detection and response capabilities, crucial for protecting sensitive healthcare data.

The false positive rate showed marked improvement, decreasing from 5.0% in traditional systems to 1.5% in our quantum-enhanced system ($z = 18.4$, $p < 0.001$). This reduction in false positives significantly decreased the operational burden on security teams while maintaining high detection accuracy for genuine threats. The system's ability to maintain these performance improvements over the 12-month study period demonstrated its long-term stability and reliability.

Cost-benefit analysis revealed that the cloud-based implementation approach significantly reduces initial capital expenditure to 1,700,000 GHS, while maintaining comparable security benefits and operational efficiencies. The cloud-based approach offers additional advantages in scalability and flexibility, allowing for dynamic resource allocation based on demand. Annual operating costs were reduced by approximately 35% compared to traditional systems, with projected cost savings of 1,200,000 GHS per year through improved efficiency and reduced security incidents.

The study results demonstrate the transformative potential of quantum computing in healthcare cybersecurity, while also highlighting important considerations for practical implementation. The significant improvements in data throughput and encryption speeds suggest that quantum-based systems can effectively address the growing security challenges in healthcare environments, particularly as the volume and complexity of healthcare data continue to expand.

Resource utilization improvements offer compelling evidence for the operational efficiency of quantum-enhanced security systems. The reduction in CPU and memory usage, combined with improved data processing capabilities, suggests that healthcare institutions can achieve better security outcomes while optimizing infrastructure costs. However, these benefits must be weighed against the initial implementation costs, which may present a significant barrier for some healthcare facilities, particularly in resource-constrained environments.

Implementation costs and resource requirements represent significant considerations for healthcare institutions considering quantum security adoption. While the initial investment of 5,000,000 GHS is substantial, our cost-benefit analysis suggests a return on investment period of 3-5 years, depending on the scale of implementation and existing infrastructure. Table 5 presents a detailed breakdown of implementation costs and projected returns.

Table 5 Five-Year Cost-Benefit Projection (in GHS)

Category	Initial Cost	Annual Operating Cost	5-Year Total	ROI
Cloud Service Subscription	$500,000	$300,000	$2,000,000	-
Classical Infrastructure	$800,000	$100,000	$1,300,000	-
Training & Expertise	$400,000	$150,000	$1,150,000	-
Total	$1,700,000	$550,000	$4,450,000	245%

Several limitations of our study warrant consideration. First, the single-site nature of the implementation may limit generalizability to different healthcare contexts and scales of operation. Second, the rapid evolution of quantum computing technology means that some of our findings may need to be reassessed as the technology continues to develop. Third, the cost analysis is based on current market conditions and may require adjustment as quantum computing technology becomes more widely available.

Despite these limitations, our findings provide strong evidence supporting the viability of quantum computing solutions for healthcare cybersecurity. The demonstrated improvements in security metrics, combined with operational efficiencies and reduced false positive rates, suggest that quantum-enhanced security systems represent a promising

direction for the future of healthcare data protection. As healthcare institutions continue to face evolving cybersecurity threats, the adoption of quantum security solutions may become not just an advantage but a necessity for maintaining the integrity and confidentiality of healthcare data.

6. Conclusion, limitations and future research

The study provides comprehensive empirical evidence supporting the integration of quantum computing in healthcare cybersecurity systems. The significant improvements in performance metrics and security capabilities demonstrate the technology's potential to revolutionize healthcare data protection. The quantum-AI hybrid approach not only enhances security measures but also offers operational efficiencies that could help justify the substantial initial investment required for implementation.

Future research in quantum healthcare security should focus on several key areas identified during our study. First, the development of more cost-effective implementation strategies is crucial for wider adoption, particularly in resource-limited healthcare environments. This could involve exploring hybrid systems that optimize the balance between quantum and classical computing components, potentially reducing initial implementation costs while maintaining security benefits. Second, investigation into scalable quantum error correction methods specific to healthcare applications could further improve system reliability and performance. Third, research into automated quantum system maintenance and optimization could address the current challenges related to technical expertise requirements.

The cost-benefit analysis of quantum security implementation reveals both challenges and opportunities. While the initial investment of 5,000,000 GHS represents a significant barrier, the operational efficiencies and enhanced security capabilities offer substantial long-term value. Healthcare institutions should consider not only the direct costs of implementation but also the potential costs of data breaches and security incidents that could be prevented through quantum security measures. Our analysis suggests a potential return on investment period of 3-5 years, depending on the scale of implementation and existing infrastructure.

The limitations of our study provide important context for future research. While our implementation demonstrated significant improvements in security and performance, the single-site nature of the study may limit generalizability to different healthcare contexts. Additionally, the rapid pace of quantum computing development means that some of our findings may need to be reassessed as the technology evolves. Future studies should consider multi-site implementations across diverse healthcare environments to validate our findings and identify context-specific challenges and solutions.

Standardization and regulatory compliance represent another crucial area for future development. As quantum computing technologies mature, healthcare institutions will need clear guidelines and standards for implementing quantum security systems. Our study suggests several potential areas for standardization, including quantum key distribution protocols, security audit procedures, and performance benchmarking metrics. Collaboration between healthcare providers, technology developers, and regulatory bodies will be essential in developing these standards.

In conclusion, our research demonstrates the significant potential of quantum computing in revolutionizing healthcare cybersecurity. The integration of quantum computing with artificial intelligence offers a powerful solution to current and emerging security challenges in healthcare environments. While implementation challenges exist, particularly regarding costs and technical expertise, the benefits in terms of enhanced security, improved performance, and operational efficiency make a compelling case for adoption. As quantum computing technology continues to evolve and mature, healthcare institutions must begin preparing for this transformation in cybersecurity approaches.

The results of this study contribute to the growing body of knowledge in quantum computing applications for healthcare security and provide a foundation for future research and implementation efforts. The demonstrated improvements in security metrics, combined with operational efficiencies and reduced false positive rates, suggest that quantum-enhanced security systems represent the future of healthcare data protection. As healthcare institutions continue to face evolving cybersecurity threats, the adoption of quantum security solutions may become not just an advantage but a necessity for maintaining the integrity and confidentiality of healthcare data.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Aaronson, S. (2008). The limits of quantum. *Scientific American*, *298*(3), 62–69.

[2] Aaronson, S. (2013). *Quantum computing since Democritus*. Cambridge University Press.

[3] Aaronson, S., & Christiano, P. (2012). *Quantum money from hidden subspaces*. 41–60.

[4] Adom, W., Zhang, P., & Adrah, F. A. (n.d.). Combating Cybercrime using a Prototype PC Surveillance and Monitoring Software System. *International Journal of Computer Applications*, *975*, 8887.

[5] Adrah, F. A., Denu, M. K., & Buadu, M. A. E. (2023). Nanotechnology applications in healthcare with emphasis on sustainable covid-19 management. *Journal of Nanotechnology Research*, *5*(2), 6–13.

[6] Adrah, F. A., Mottey, B. E., & Nyavor, H. (n.d.). The Landscape of Artificial Intelligence Applications in Health Information Systems. *International Journal of Computer Applications*, *975*, 8887.

[7] Arshad, M. W., Murtza, I., & Arshad, M. A. (2023). Applications of Quantum Computing in Health Sector. *Journal of Data Science and Intelligent Systems*, *1*(1), 19–24.

[8] Arshad, U., Khan, G., Alarfaj, F. K., Halim, Z., & Anwar, S. (2024). Q-ensemble learning for customer churn prediction with blockchain-enabled data transparency. *Annals of Operations Research*, 1–27.

[9] Aumasson, J.-P. (2017). The impact of quantum computing on cryptography. *Computer Fraud & Security*, *2017*(6), 8–11.

[10] Bernhardt, C. (2019). *Quantum computing for everyone*. Mit Press.

[11] Fauziyah, Z. W., & Tabassum, M. (2024). Quantum-Enhanced Cyber Security. *Innovative Computing and Communications: Proceedings of ICICC 2024, Volume 3*, *1039*, 87.

[12] Hassija, V., Chamola, V., Saxena, V., Chanana, V., Parashari, P., Mumtaz, S., & Guizani, M. (2020). Present landscape of quantum computing. *IET Quantum Communication*, *1*(2), 42–48.

[13] Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *2018*, *22*.

[14] Marwala, T. (2024). Digital Versus Quantum Computing. In *The Balancing Problem in the Governance of Artificial Intelligence* (pp. 153–169). Springer.

[15] Rodrigo, S., Spanò, D., Bandic, M., Abadal, S., Van Someren, H., Ovide, A., Feld, S., Almudéver, C. G., & Alarcón, E. (2022). *Characterizing the spatio-temporal qubit traffic of a quantum intranet aiming at modular quantum computer architectures*. 1–7.

[16] Sriram, R. D., & Subrahmanian, E. (2020). Transforming health care through digital revolutions. *Journal of the Indian Institute of Science*, *100*(4), 753–772.

[17] Vyawahare, D., Walse, K., & Sali, N. V. (n.d.). *A Study of Quantum Computing*.