Project Title:Quantum Computing and its implications for information security

Programme of Study: Research Leading to Publication

Researcher: Abid Hossain
Supervisor:
Prof. Dr. Karim Mohammed Rezaul

Aims & Objectives

To explore quantum threats to cybersecurity and review mitigation strategies.

As quantum computing rapidly approaches technological maturity, the implications for global information security grow increasingly urgent and profound. This research project aims to explore how the transformative power of quantum computation both threatens and redefines cybersecurity frameworks, particularly in encryption, data governance, and digital infrastructure. Cloud system. Additionally, building on key insights from current literature, including forecasts of quantum threats to cryptographic algorithms, sector-specific vulnerabilities in finance, and the legal and societal ramifications, this study will critically assess both the risks and opportunities posed by quantum advancements. The primary objectives are:

(1) To evaluate the potential for quantum computers to compromise existing security protocols.

(2) To analyse strategies for quantum-resistant cryptography and infrastructure resilience.

(3) To propose policy and design recommendations for safeguarding sensitive systems in a post-quantum world.

(4) To explore the ethical and legal ramifications of quantum computing on data privacy and sovereignty.

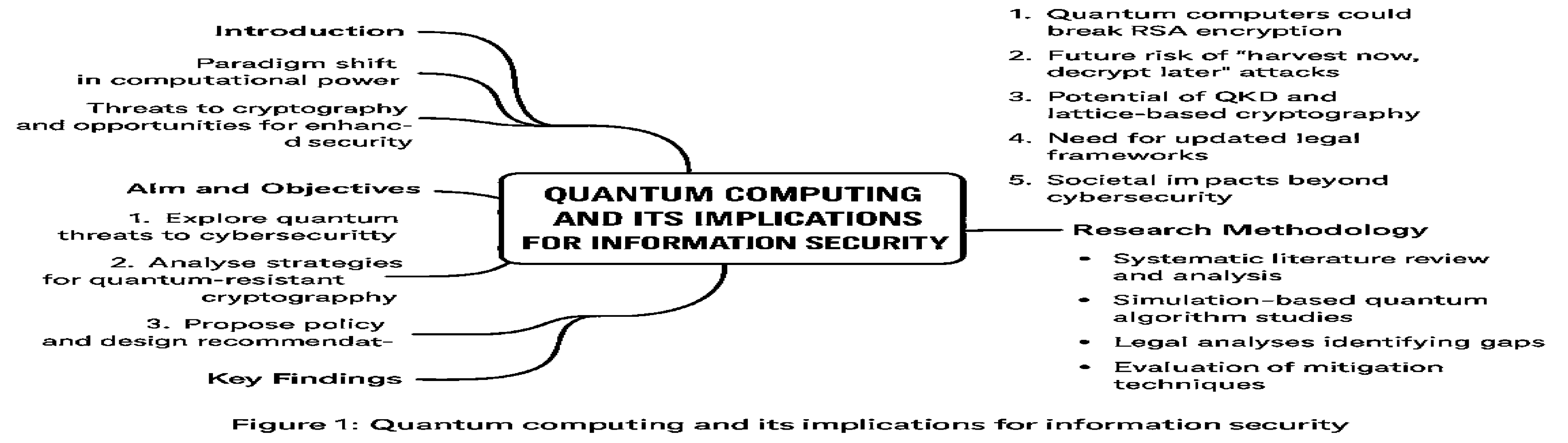
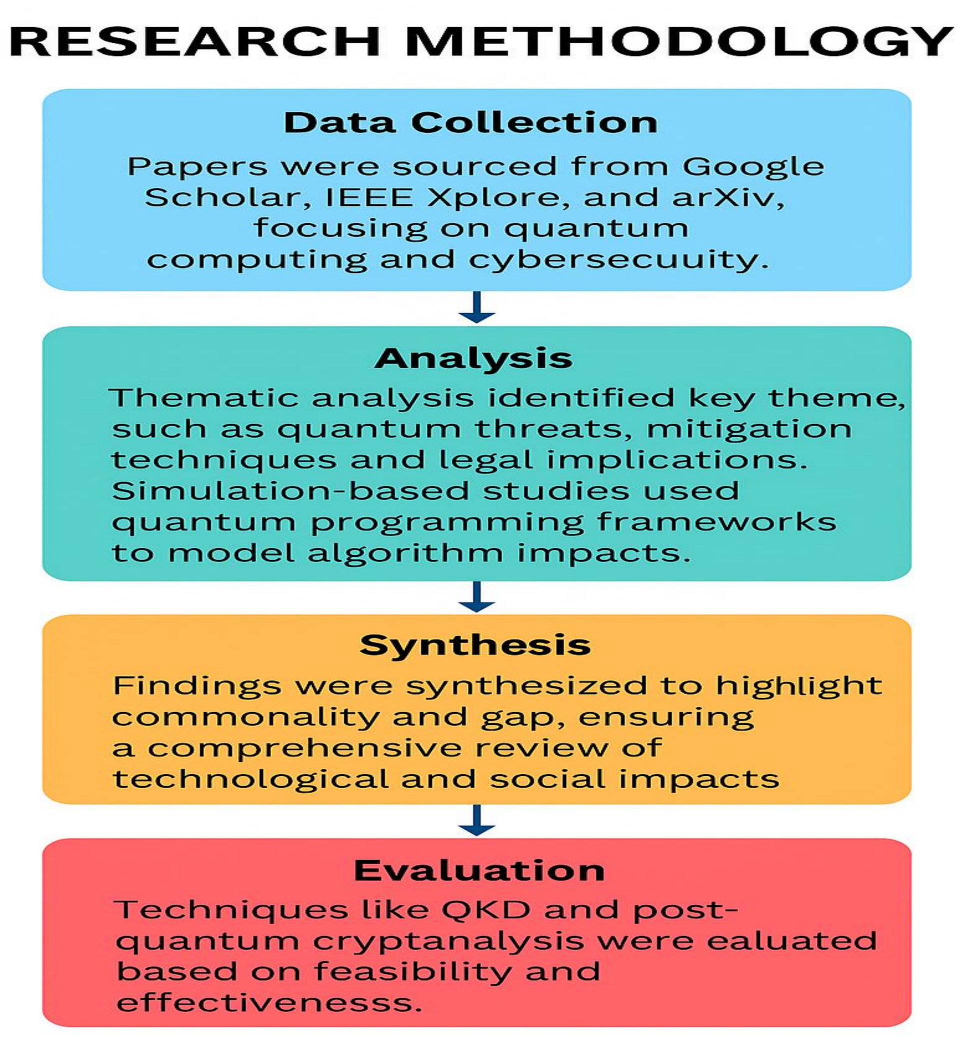


Figure 1. Mind Map.

Research Methodology



The methodology involves a systematic literature review and analysis:
Data Collection: Papers were sourced from Google Scholar, IEEE Xplore, and arXiv, focusing on quantum computing and cybersecurity.
Analysis: Thematic analysis identified key themes, such as quantum threats, mitigation techniques, and legal implications. Simulation-based studies used quantum programming frameworks to model algorithm impacts.
Synthesis: Findings were synthesized to highlight commonality and gap, ensuring a comprehensive review of technological and social impacts.
Evaluation: Techniques like QKD and post-quantum cryptanalysis were evaluated based on feasibility and effectiveness, drawing from industry and academic insight.

Aspect	Statistic
Organizations expecting quantum computers to become mainstream by 2030	60% (Canada), 78% (US)
Organizations believing cybercriminals will use quantum computing to decrypt data	60% (Canada), 73% (US)
Organizations admitting need to better evaluate current capabilities for data security	62% (Canada), 81% (US)
Organizations expecting quantum computers to become mainstream by 2030	50.20%
Source	KPMG (2024), Deloitte (2022)

Table 1 : Growing concern among organizations regarding quantum computing's impact on cybersecurity.

Study data from KPMG (2024) and Deloitte (2022) show that a majority and the US foresee quantum computers becoming mainstream by 2030, with significant worries about cybercriminals exploit quantum technology to decode information in Canada, post-quantum cryptology. Additionally, The high-pitched percentage of organizations acknowledge the need to heighten information security capabilities underscores the urgency of adopting quantum-resistant solutions like QKD. Besides, the risk of ' harvest now, later' attack emphasizes the immediate need to safeguard sensitive information against future quantum threats.

Source:
1.*https://kpmg.com/xx/en/our-insights/ai-and-technology/quantum-and-cybersecurity.html*
2.*https://www.infosecurity-magazine.com/news/quantum-computing-data-risk-cyber/*

Figure 3: Impact of quantum computing on markets

Techniques and Resources

Research on quantum computing and cybersecurity employs various techniques to address emerging threats:

1.Quantum Key Distribution (QKD): QKD uses quantum mechanics to securely distribute encryption keys, ensuring eavesdropping detection. It is highlighted as a robust defense against quantum attacks.

2.Post-Quantum Cryptography: NIST's ongoing efforts focus on developing quantum-resistant algorithms, such as lattice-based and hash-based cryptography, to replace vulnerable systems.

3.Simulation and Modeling: Like Shor's computational method, which can break RSA encryption by factoring large numbers, Papers use simulation to assess quantum algorithms game efficiently.

4.Policy and Legal Analysis: Some studies, regulatory frameworks to address quantum threats, advocating for updated data security laws. These techniques combine technical innovation with policy recommendations to prepare for the quantum era.

Data/ Observations

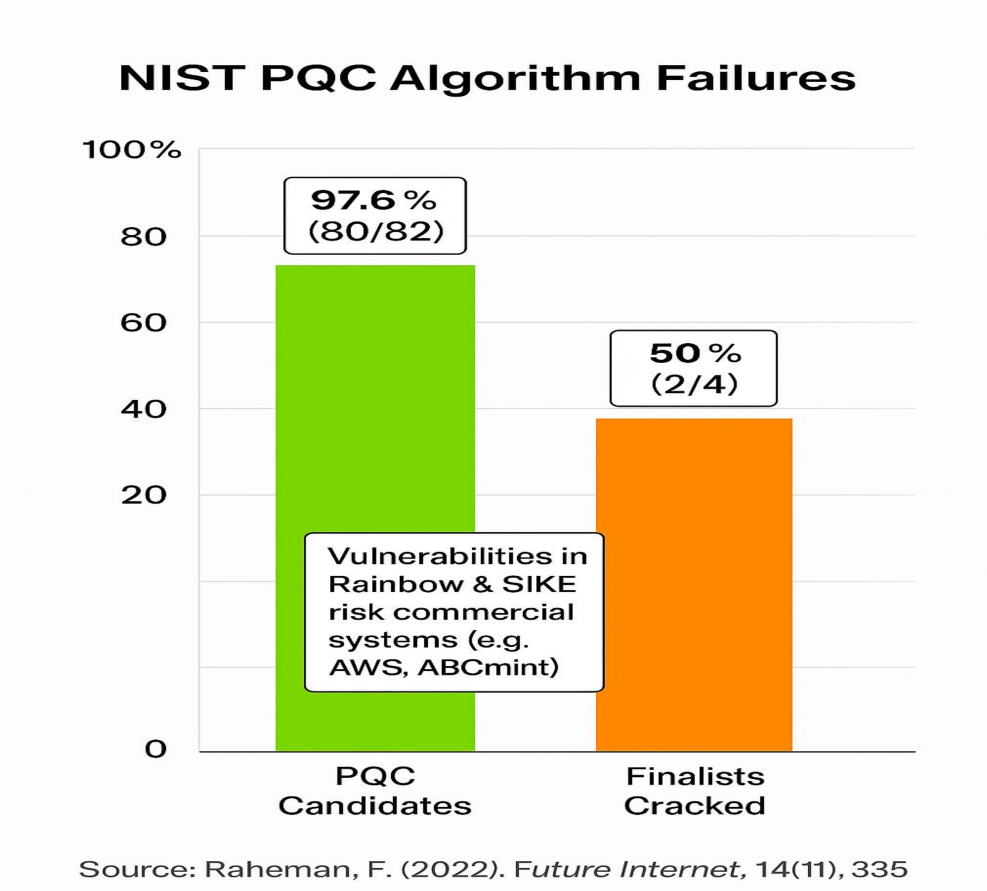


Fig 2 : NIST PQC Algorithm Failure Bar Chart

(Author-generated diagram. Data: Raheman, F. (2022). Future Internet, 14(11), 335.)

This bar chart shows NIST's PQC algorithm failures: 97.6% (80/82) of candidates and 50% (2/4) of finalists (Rainbow, SIKE) cracked, risking commercial systems like AWS and ABCmint. These highlight urgent cybersecurity threats, necessitating new solutions (Raheman, 2022).

Source of the data: *Raheman, F. (2022). The Future of Cybersecurity in the Age of Quantum Computers. Future Internet, 14(11), 335.* ***https://doi.org/10.3390/fi14110335***

Key Findings

- 1. Quantum computers with 20 million qubits could break 2048-bit RSA encryption in approximately 8 hours, highlighting the urgency of transitioning to quantum-safe systems.
- 2. Current quantum computing devices are not yet cryptographically relevant, but harvest now, decode later attack poses a future hazard, where data collected today could be decrypted subsequently.
- 3. QKD and lattice-based cryptography show promise as quantum-resistant solutions, with NIST standardizing algorithms to replace vulnerable systems.
- 4. Legal frameworks, such as GDPR, May take updates to address quantum-specific information breaches, emphasizing proactive policy changes.
- 5. Quantum computing's societal impacts extend beyond cybersecurity, affecting privacy and economic structures

Conclusions/Limitation

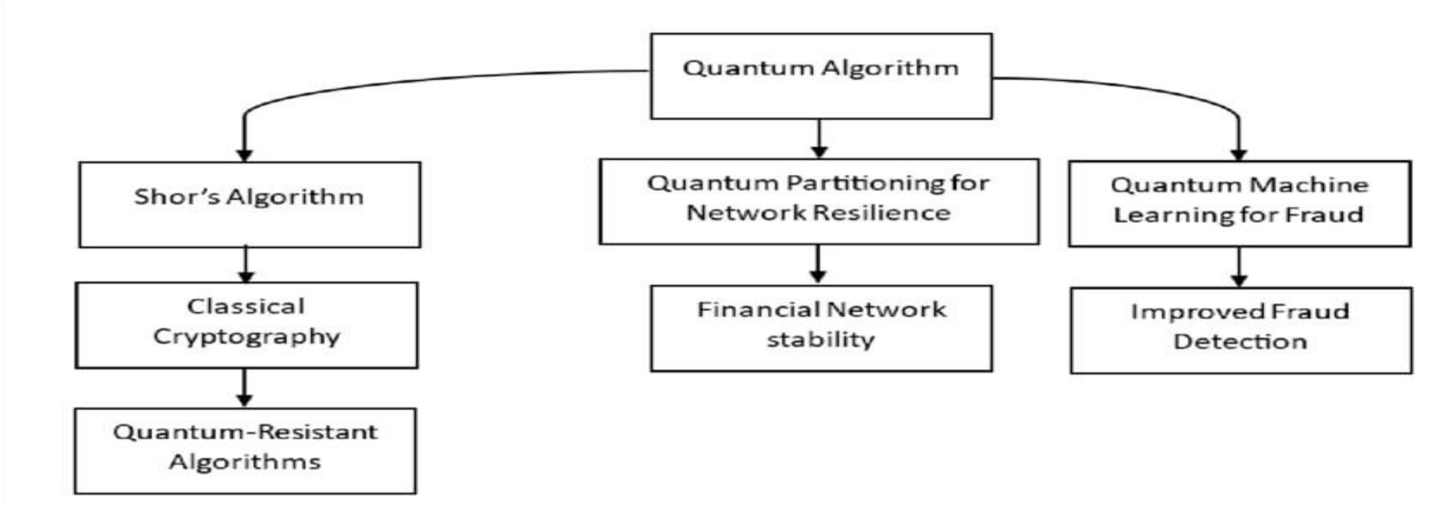
Quantum computing presents both a threat and an opportunity for cybersecurity. While algorithms like Shor's and Grover's endanger current encryption, solutions like QKD and post-quantum cryptography offer viable defence's. The integration of this technology into existing system, coupled with update frameworks, which is legal, can mitigate risks and enhance security. This research underscores the need for immediate action to prepare for the quantum era, ensuring robust protection against future threats. Here are some key points to have a look at :

1.Current quantum computers lack the scale to break encryption, limiting immediate real-world testing.

2.The high cost and complexity of implementing QKD and quantum-resistant algorithms may delay adoption.

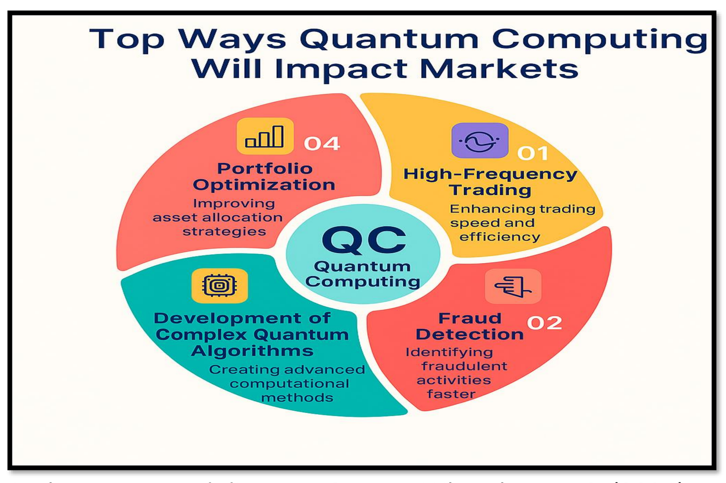
3.Legal analyses are speculative, as quantum-specific regulations are not yet widespread.

4.Data availability for quantum threat simulations is limited, relying on theoretical models



Source : Enhancing Cybersecurity Protocols in Financial Networks through Reinforcement Learning. (n.d.). Quantum Algorithms in Cybersecurity: Balancing Threats and Innovations. Retrieved July 30, 2025, from: ***https://www.researchgate.net/figure/Quantum-Algorithms-in-Cybersecurity-Balancing-Threats-and-Innovations_fig1_384787083***

Figure 4. Quantum algorithm diagrams.



Quantum computing is revolutionizing how industries tackle complex challenges with unmatched speed and processing power It has major impacts on markets, which includes:
1. High-Frequency Trade – Real-time optimisation of the fiscal algorithm for quick and more strategic conclusions.
2. Fraud Sensing – Advanced shape acknowledgment aids place anomalousness and combat financial crimes.
3. Development of Complex Quantum Algorithm – Work problem beyond the attain of classic computers , such as molecular simulation and cryptological challenges.
4. Portfolio Optimisation – Smart strategy for equilibrising peril and wages in the plus direction.
5. Security and Jeopardy Appraisal – Fortify defence uses a quantum tool to expect and mitigate emerging threats.

Author-generated diagram. **Source:** Wheatley, M. C. (2024). Premier Journal of Computer Science, PJCS(24), Article 100002.

Figure 5: Ways in which quantum computing will impact markets

References

1. Balarabe, Kasim. "Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap." European Journal of Risk Regulation 16, no. 2 (2025): 794–813. https://doi.org/10.1017/err.2025.8.
2. Chu, Cheng, Cheng Liu, Dawen Xu, Ying Wang, Tao Luo, Huawei Li, and Xiaowei Li. 2023. "Accelerating Deformable Convolution Networks with Dynamic and Irregular Memory Accesses." ACM Transactions on Design Automation of Electronic Systems 28 (4): Article 67, 1–23. https://doi.org/10.1145/3597431.
3. Gill, S. S., Kumar, A., Singh, H., Misra, S., Buyya, R., & Yoon, Y. (2022). Quantum computing: A taxonomy, systematic review and future directions. Software: Practice and Experience, 52(1), 66–114. https://doi.org/10.1002/spe.3052
4. Raheman, Fazal. 2022. "The Future of Cybersecurity in the Age of Quantum Computers" Future Internet 14, no. 11: 335. https://doi.org/10.3390/fi14110335
5. Scanlon, Tom. "Cybersecurity of Quantum Computing: A New Frontier." Carnegie Mellon University, Software Engineering Institute's Insights (blog). Carnegie Mellon's Software Engineering Institute, April 10, 2023. https://doi.org/10.58012/rzmt-m258.
6. Malik, Asma, and Sardar M. N. Islam. 2025. "Quantum Computing and Cybersecurity: Navigating Threats and Opportunities." In *Quantum Computing, Cyber Security and Cryptography*, edited by S. B. Goyal, V. Kumar, S. M. N. Islam, and D. Ghai, 489–504. Springer, Singapore. https://doi.org/10.1007/978-981-96-4948-8_18.
7. Wheatley, Mary Christine. 2024. "Quantum Shifts: The Societal Implications of Quantum Computing on Security, Privacy, and the Economy." *Premier Journal of Computer Science*. https://doi.org/10.70389/PJCS.100002.

Centre for Applied Research in Software & IT (CARSIT)