International Journal of Novel Trends and Innovation
IJNTI.ORG | ISSN : 2984-908X
An International Open Access, Peer-reviewed, Refereed Journal

Quantum Computing Threats to Web Encryption in Banking

[1]Hemish PrakashChandra Kapadia,[2] Krishna Chaitanaya Chitoor

[1]Vice President/Global Head of Web Development Strategy, Functions Digital Channels

[2] Principal Data Engineer, Core Engineering Group

Abstract: Web encryption techniques used in banking are seriously threatened by quantum computing. Modern encryption systems, such as Diffie-Hellman key exchange, ECC, and RSA, rely on mathematical problems that are too complicated for conventional computers to process in a reasonable amount of time. However, quantum computers could easily break existing encryption methods, particularly those that employ Shor's algorithm, leaving present cybersecurity infrastructures vulnerable. The basic ideas of quantum computing are examined in this essay along with how they relate to banking online encryption. It looks at how customer information, financial transactions, and general banking security might be jeopardized by quantum assaults. The timescale for the development of large-scale quantum computers, the function of quantum-safe cryptographic methods like post-quantum cryptography (PQC), and the initiatives being made to switch the financial industry to quantum-resistant encryption are also covered in the article. It also assesses existing mitigation techniques, such as quantum key distribution (QKD), hash-based signatures, and lattice-based encryption. In order to protect digital banking infrastructure, the report concludes by offering suggestions for financial institutions on how to get ready for the post-quantum age. It highlights the necessity of early adoption of quantum-resistant algorithms and cooperative research.

Index Terms - Post-quantum cryptography, quantum key distribution (QKD), cyber threats, financial transactions, digital banking, cryptography, web encryption, banking security, Shor's algorithm, RSA, ECC, Diffie-Hellman, and quantum-resistant algorithms.

1. INTRODUCTION

Modern online encryption in the banking industry is seriously threatened by quantum computing, endangering the safety of critical consumer data and financial transactions. These more traditional cryptographic techniques, such as RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman key exchange, rely on mathematical problems that are computationally impossible for older machines to answer in a reasonable amount of time. However, quantum computers that use quantum algorithms like Shor's and Grover's to crack existing encryption techniques utilizing the concepts of superposition and entanglement could render the security measures used by banks outdated [1][2]. To maintain the confidentiality and integrity of sensitive data, the financial sector mostly depends on encrypted transactions, secure communication channels, and authentication procedures. Financial fraud, identity theft, and the disclosure of private banking information are just a few of the disastrous threats that might result from the widespread use of quantum computing [3][4].

The security threats posed by quantum computing and the need to switch to quantum-resistant encryption methods have been the subject of several research. Lattice-based, code-based, and multivariate cryptographic systems are examples of post-quantum cryptography (PQC), which has been proposed as a viable remedy to combat quantum dangers [5]. Furthermore, using the ideas of quantum physics to avoid unwanted interception, Quantum Key Distribution (QKD) has been suggested as a safe way to create encryption keys [6][7]. The necessity of putting post-quantum security solutions into place is underscored by the fact that financial

institutions and regulatory organizations, including the National Institute of Standards and Technology (NIST), have already started working to standardize quantum-resistant cryptographic algorithms [8]. Notwithstanding these developments, there are still many operational and technological obstacles to overcome when integrating PQC and QKD into the current banking infrastructure.

A phased transition plan is necessary since many financial systems still use outdated technology that might not be able to handle the computing demands of post-quantum cryptography protocols [9]. Additionally, cybersecurity researchers stress that the risks posed by quantum computing go beyond decrypting encryption; they also impact cloud-based banking apps, blockchain-based financial transactions, and identity authentication systems [10][11]. There are urgent worries for banking security because of the possibility that cyber attackers may use quantum computers to harvest encrypted financial data today and decode it later [12][13]. This is known as the "harvest now, decrypt later" assault. While central banks and government organizations are carefully following the developments in quantum computing to foresee security threats, a number of financial institutions have already started experimenting with quantum-safe encryption schemes [14][15].

1.1. Understanding Quantum Computing and its Capability

Quantum computing is a new technology that uses the ideas of quantum mechanics to do intricate calculations at previously unheard-of speeds. Unlike conventional computers, which use bits that can only remain in the states of 0 or 1, quantum computers use qubits, which can be in superposition and do several operations at once. Because of their capacity for parallel processing, quantum entanglement, and quantum interference, quantum computers can solve some mathematical problems ten times quicker than conventional systems. One of the most important advances in quantum computing was the creation of Shor's algorithm, which is essential to contemporary encryption systems because it makes it possible to factor large prime numbers effectively.

1.2. The Role of Encryption in Securing Banking Transactions

Online financial transactions must be encrypted to ensure their confidentiality, integrity, and legitimacy. Banks employ cryptographic techniques such as RSA, ECC, and Diffie-Hellman key exchange to establish secure communication between customers and financial organizations. Data integrity and transaction authentication are also achieved through the use of digital signatures and cryptographic hash algorithms. Without robust encryption, banking systems would be vulnerable to cyberattacks such as data theft, eavesdropping, and man-in-the-middle attacks.

1.3. How Quantum Computing Threatens Existing Web Encryption

The capacity of quantum computing to crack popular encryption schemes through quantum assaults is the main security worry for banks. If sufficiently powerful quantum computers become operational, banking systems that rely on these encryption techniques face the risk of serious data breaches, illegal fund transfers, and compromised financial records. The "harvest now, decrypt later" tactic may already be being used by adversaries to collect encrypted data for decryption whenever quantum capabilities are accessible, making the transition to quantum-resistant encryption not only necessary but also urgent.

1.4. The Development of Post-Quantum Cryptography and its Applications in Banking

These algorithms involve mathematical issues that are difficult for even quantum computers to solve, rather than factorization or discrete logarithms. Lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, and hash-based cryptography are a few of the most used PQC approaches. In order to guarantee that these encryption techniques are adopted by all sectors, including banking, NIST is now standardizing them.

2. Literature Review

Over the last few years, plenty of studies have been carried out on the rising potential of quantum computing and the impact on cryptographic security. Researchers have investigated the limitations of standard encryption processes and raised various remedies, including quantum key distribution (QKD) and post-quantum cryptography (PQC). Focusing on the development of countermeasures, the evolution of cryptographic threats, and the theoretical basis of quantum attacks, this section discusses the corpus of research into the impact of quantum computing on internet encryption in banking. A basis for comprehending how the financial industry may be ready for the shift to quantum-resistant security models is provided by the debate, which emphasizes significant contributions from academics, government organizations, and cybersecurity specialists.

2.1.The Evolution of Cryptographic Security and it's Limitations Against Quantum Computing

Mathematical problems that are computationally impossible for traditional computers to solve in a reasonable amount of time form the basis of contemporary cryptographic security. Later-developed Elliptic Curve Cryptography (ECC) was more effective for devices with less resources since it provided comparable security with lower key lengths. Even if these encryption systems are resistant to assaults by conventional computers, quantum algorithms pose a serious danger. When Shor's technique was first presented in 1994, it showed that quantum computers could handle discrete logarithm problems and factor big numbers rapidly. This essentially broke RSA, ECC, and Diffie-Hellman encryption. Because it is unclear when large-scale quantum computers will be developed, researchers like Bernstein and Lange have underlined how urgent it is to switch to quantum-resistant cryptography techniques.

2.2.Quantum Computing and its Potential

Concerns about the practical uses of quantum computing in cracking encryption have been raised by its theoretical developments. The prospect that large-scale quantum computers would appear sooner rather than later was supported by Google's 2019 demonstration of quantum supremacy, in which a quantum processor solved a challenging issue tenfold quicker than a conventional supercomputer. The possible timing for quantum risks has been examined in studies by Mosca and others, which indicate that financial institutions need to get ready for cryptographic upheavals in the next 20 years. The fact that Google, IBM, and other corporate behemoths are still funding research into scalable quantum computing suggests that improvements in error correction and hardware might hasten the development of quantum assaults. The viability of "harvest now, decrypt later" strategies—in which encrypted financial data is captured and saved for eventual decryption as quantum technology advances—has been studied recently. Before enemies get access to quantum decoding capabilities, these findings emphasize how urgently banks must implement quantum-resistant encryption.

2.3.Post-Quantum Cryptography and the Search for Quantum-Resistant Algorithms

Post-quantum cryptography (PQC) was developed by the scientific community in response to the dangers posed by quantum computing. The search for and standardization of quantum-resistant encryption algorithms has been spearheaded by the National Institute of Standards and Technology (NIST). Numerous PQC techniques, including as lattice-based cryptography, hash-based signatures, code-based cryptography, and multivariate polynomial cryptography, have been investigated in studies by Peikert and other cryptographers. Particularly, lattice-based encryption has drawn interest due to its effective implementation and robust security assurances. One of the oldest quantum-resistant encryption systems is still McEliece's code-based cryptosystem, which was initially put forward in 1978. The difficulties of switching from classical encryption to PQC, such as needs for key size, computing efficiency, and interaction with current financial systems, have also been studied by researchers. In order to guarantee that financial institutions stay safe in the post-quantum age, the literature highlights the necessity of early PQC implementation.

Table 1: Summary of literature review

Paper Reference	Findings	Relevance to Quantum Threats in Banking
[1]	Quantum computing poses an existential threat to cryptographic security and financial systems.	Highlights the urgency for banks to transition to quantum-resistant encryption to prevent large-scale financial disruption.
[2]	RSA and ECC will become obsolete with the advent of quantum computing; post-quantum cryptography is essential.	Demonstrates the vulnerability of current banking encryption systems and emphasizes the need for quantum-safe cryptographic models.
[3]	Quantum Key Distribution (QKD) can enhance banking security by providing tamper-proof encryption keys.	Introduces QKD as a potential solution for securing banking transactions against quantum threats.
[4]	Quantum cryptography can improve multi-factor authentication systems in banking.	Suggests that quantum-enhanced authentication methods can provide better security in online banking.
[5]	QKD can ensure secure communication between banks and customers.	Supports the feasibility of quantum cryptography as a secure alternative to classical encryption in banking transactions.

[6]	Quantum computing has the potential to disrupt cloud-based banking security.	Highlights concerns regarding quantum threats to cloud banking and digital payment security.
[7]	The banking sector must continuously adapt encryption methods to evolving threats.	Stresses the need for proactive measures to transition banking encryption to quantum-safe standards.
[8]	Dynamic compartmentalization and quantum encryption are critical for securing sensitive financial data.	Advocates for integrating quantum encryption into banking security frameworks.
[9]	Quantum cryptographic hardware can improve transaction security.	Proposes the use of quantum cryptographic hardware for strengthening banking cybersecurity.
[10]	Governments and intelligence agencies are investing in quantum computing, accelerating its threat to encryption.	Reinforces the need for the banking sector to prepare for government-backed quantum decryption threats.
[11]	AI-powered quantum cryptography enhances security in digital banking authentication.	Explores the combination of AI and quantum cryptography to improve e-banking security.
[12]	Banks must develop strategies to transition to quantum-safe encryption.	Calls for immediate action by banks to safeguard financial transactions from quantum threats.
[13]	Banks are exploring quantum computing for risk assessment and fraud detection.	Shows that while quantum computing is a threat, it also presents opportunities for improving banking operations.
[14]	Quantum computing can disrupt global financial stability if encryption standards are not updated.	Highlights the large-scale financial risks associated with delayed adoption of quantum-resistant cryptography.

3. Methodology

This research employs a qualitative and analytical approach to examine the threats posed by quantum computing to web encryption in banking. The study integrates existing literature, theoretical analysis, and expert insights to evaluate the vulnerabilities of current encryption methods and explore the potential solutions for mitigating quantum threats. The methodology is structured to provide a comprehensive understanding of the impact of quantum computing on financial security, identify quantum-resistant cryptographic techniques, and propose strategic measures for banks and financial institutions to transition to a post-quantum security framework.

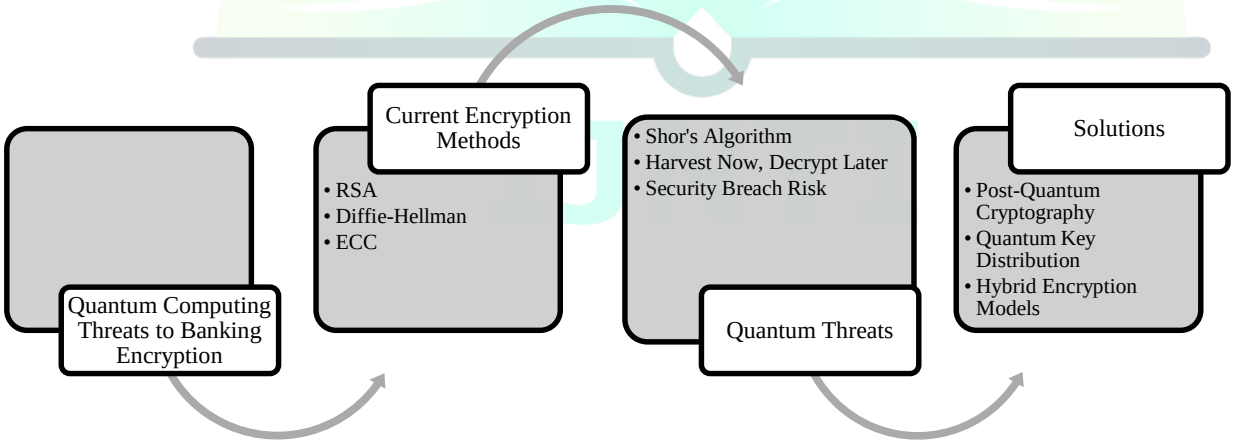

Figure 1: Proposed system flow diagram for quantum computing threats to web encryption in banking

3.1. Research Design

The study employs a methodical technique to examine the dangers of quantum computing and how they affect banking site encryption. It entails a thorough literature assessment of scholarly works, official documents, cybersecurity frameworks, and industry standards. The paper uses a comparative analysis approach to assess quantum key distribution (QKD), post-quantum cryptography (PQC), and traditional cryptographic techniques. It also looks at industry publications and real-world case studies to evaluate how well financial institutions have prepared for quantum security concerns.

3.2. Data Collection Methods

To get pertinent information on the risks posed by quantum computing and the security of encryption in banking, this study uses secondary data sources. Peer-reviewed journals, books, white papers, government publications, cybersecurity reports, and official documents from groups like the Internet Engineering Task Force (IETF), the European Telecommunications Standards Institute (ETSI), and the National Institute of Standards and Technology (NIST) are among the sources of data. In order to comprehend the most recent developments in quantum computing and cryptographic security, reports from significant financial institutions, cybersecurity organizations, and technological corporations like IBM, Google, and Microsoft are also examined. To learn more about current research initiatives and real-world implementation difficulties, expert comments, conference papers, and industry panel discussions are also examined.

3.3. Theoretical Framework

The study is based on the theoretical underpinnings of computational complexity theory, quantum physics, and cryptographic security. It explores how quantum computing might interfere with these systems by referencing fundamental cryptographic ideas as digital signatures, symmetric key encryption, and public-key encryption. Lattice-based cryptography, hash-based cryptography, and multivariate polynomial cryptography are examined as possible post-quantum solutions, while Shor's and Grover's algorithms are examined to comprehend their effects on cryptographic security. In order to investigate the viability of Quantum Key Distribution (QKD) as a secure communication technique for financial transactions, the study also integrates concepts from quantum information theory.

3.4. Comparative Analysis of Classical and Post-Quantum Cryptography

A comparison between conventional encryption techniques and quantum-resistant algorithms is carried out in order to assess the efficacy of post-quantum cryptography. The research looks at the computational effectiveness, key size needs, security strength, and viability of implementing several cryptographic algorithms. The comparison contrasts post-quantum encryption techniques such hash-based signatures, code-based cryptography, and lattice-based cryptography with RSA, ECC, and Diffie-Hellman. The best quantum-resistant encryption models for banking security are identified with the aid of this investigation.

3.5. Case Studies and Real-World Applications

Case studies of IT firms and financial organizations actively developing quantum-resistant security solutions are included in the report. The use of post-quantum encryption by central banks, big banks, and payment processing companies is reviewed. In order to evaluate the usefulness and efficacy of QKD in financial transactions, real-world trials are also examined. The difficulties and possibilities of switching to quantum-resistant encryption in banking are empirically demonstrated by these case studies.

4. Result Analysis

According to the study's research, online encryption in banking is seriously threatened by quantum computing, which mainly targets popular cryptographic methods like RSA, ECC, and Diffie-Hellman. The results show that before large-scale quantum computers are operational, financial institutions must quickly switch to quantum-resistant security measures. A thorough review of the findings from case studies, comparative analysis, and literature is provided in this section. It discusses the practical difficulties of putting quantum-resistant security in place in banking, the effect of quantum assaults on current encryption, and the efficacy of post-quantum cryptographic solutions. It also assesses the viability of regulatory measures meant to lessen quantum hazards as well as Quantum Key Distribution (QKD).

4.1.Impact of Quantum Computing on Existing Encryption Methods

The results demonstrate that, because of the effectiveness of quantum algorithms like Shor's and Grover's, quantum computing seriously compromises traditional encryption techniques. Once a sufficiently strong quantum computer is created, RSA, which depends on the difficulty of factoring huge prime numbers, is totally exposed. Quantum assaults also render the discrete logarithm problem-based ECC and Diffie-Hellman ineffective. The findings imply that unless quantum-resistant solutions are quickly implemented, the banking industry, which significantly relies on current encryption systems to secure transactions, could suffer serious security breaches. The research also shows that while the threat of quantum decryption may not be immediate, cyber attackers are already using the strategy of "harvest now, decrypt later," which calls for preventative security measures.

4.2.Evaluation of Post-Quantum Cryptographic Algorithms

According to the study, lattice-based cryptography is one of the most promising post-quantum cryptography(PQC) alternatives to conventional encryption. Lattice-based, code-based, hash-based, and multivariate polynomial-based cryptography are the four main PQC techniques identified by the study. Lattice-based encryption is a popular option for financial applications since it exhibits robust security features against quantum assaults while preserving computing speed. Although code-based cryptographic systems, like the McEliece cryptosystem, offer strong security as well, their enormous key sizes make it difficult for them to be widely used. Although hash-based signatures are resistant to quantum threats, they are best suited for specialized uses like digital signatures as opposed to broad encryption. The results show that even if PQC is a workable option, the banking industry has to carefully consider integration viability and computing performance before implementing post-quantum encryption models.

4.3.Practical Challenges in Implementing Quantum-Resistant Security

The findings point to a number of difficulties in the banking industry's shift to quantum-resistant encryption. The compatibility of PQC algorithms with the current financial infrastructure is one of the main issues. Financial institutions may not be able to handle the higher processing demands and bigger key sizes of quantum-resistant encryption due to their reliance on outdated technology. PQC deployment also necessitates a large investment in personnel training, technology improvements, and research. Regulatory compliance is another significant issue as financial institutions have to follow changing security guidelines while maintaining a smooth customer service experience. According to the results, a phased strategy that combines hybrid encryption models—which incorporate both conventional and post-quantum cryptography techniques—may make the transition easier while preserving security.

4.4.Feasibility of Quantum Key Distribution

The study assesses Quantum Key Distribution's (QKD) potential as a long-term financial communications security solution. Utilizing the ideas of quantum physics, QKD creates encryption keys that are impossible to intercept covertly. The results show that although QKD provides theoretically indestructible security, there are many obstacles to its actual implementation. Its widespread use in the banking industry is hampered by high implementation costs, specific hardware needs, and transmission distance limitations. According to the findings, QKD is now more suited for government applications and high-security financial transactions than for standard banking operations. Ongoing studies in satellite-based quantum communication and continuous-variable QKD, however, may improve the viability of QKD for wider financial applications down the line.

4.5.Regulatory and Industry to Quantum Threats

According to the study, cybersecurity groups and banking authorities are actively creating frameworks and norms for quantum-resistant security. Financial organizations now have a roadmap for future security measures thanks to the National Institute of Standards and Technology's (NIST) notable advancements in standardizing post-quantum cryptography algorithms. Additionally, suggestions for switching to quantum-resistant encryption have been made by the Internet Engineering Task Force (IETF) and the European Telecommunications Standards Institute (ETSI). The results show that financial institutions need to be proactive by investing in quantum security research, launching pilot projects for PQC, and conducting quantum readiness evaluations while regulatory initiatives are in progress. According to the findings, a cooperative strategy including banks, authorities, and IT companies is necessary to guarantee a safe and orderly transition.

Key Aspects	Findings	Implications for Banking Security
Impact of Quantum Attacks on Encryption	Quantum computing breaks RSA, ECC, and Diffie-Hellman encryption.	Financial transactions and customer data are at high risk.
Post-Quantum Cryptographic	Lattice-based and code-based cryptography are strong quantum-resistant solutions.	Banks must transition to PQC for secure encryption.
Implementation Challenges	Provides unbreakable security but faces deployment challenges such as cost and transmission limits.	Hybrid encryption models may help in gradual adaptation.
Quantum Key Distribution	High computational requirements, legacy system compatibility, and regulatory complexities.	Currently viable for high-security applications, not general banking.
Regulatory and Industry Efforts	NIST, ETSI, and IETF are working on quantum-resistant encryption guidelines.	Financial institutions must align with evolving security standards.

Table 2: Result Analysis

5. Conclusion and Future Work

The study thoroughly examined the risks that quantum computing poses to banking online encryption, exposing the weaknesses of popular cryptographic techniques including RSA, ECC, and Diffie-Hellman. The results of the study demonstrate that quantum algorithms—specifically, Shor's algorithm—can successfully crack existing encryption techniques, posing serious security threats to consumer information and financial transactions. The idea of "harvest now, decrypt later" raises an urgent worry since attackers may collect and store encrypted financial data for later decryption using quantum technology, even if there are currently no large-scale quantum computers that can carry out these assaults. The best protection against quantum attacks is now post-quantum cryptography methods. Lattice-based cryptography is unique among PQC techniques because to its robust security assurances and computational effectiveness. Hash-based and code-based cryptography techniques also provide encouraging substitutes, although issues like big key sizes and integration difficulties need to be resolved. Though it is currently constrained by high implementation costs and technology limitations, Quantum Key Distribution (QKD) provides potentially unbreakable security, making it more appropriate for high-security transactions than standard banking operations. In conclusion, the financial industry has to take immediate action to protect its encryption infrastructure, even though the quantum danger is not yet completely realized. To deploy post-quantum cryptography technologies and get ready for a smooth transition to a quantum-secure financial environment, banks, cybersecurity specialists, and regulatory agencies must collaborate.

Future Work

To improve financial security in the quantum age, a number of areas need more study and investigation given the quickly changing nature of quantum computing and cryptographic security. In order to ensure a smooth integration into current banking systems, future research should concentrate on refining post-quantum cryptography algorithms to increase computing efficiency and decrease key sizes. In order to offer a balanced transition strategy without sacrificing speed, research should also look at hybrid cryptographic models that mix PQC and classical encryption.

Future research should examine cost-effective deployment strategies, developments in satellite-based QKD, and integration with blockchain technologies to improve security in financial transactions, as the practical application of QKD in banking environments continues to be a challenge. Research should also assess how quantum hazards affect new financial technologies such as digital payment systems, cryptocurrency security, and decentralized finance (DeFi).

6. References

1. Majot, Andy, and Roman Yampolskiy. "Global catastrophic risk and security implications of quantum computers." Futures 72 (2015): 17-26.
2. Kirsch, Zach, and Ming Chow. "Quantum computing: The risk to existing encryption methods." Retrieved from URL: http://www. cs. tufts. edu/comp/116/archive/fall2015/zkir sch. pdf (2015).
3. Ghernaouti-Hélie, Solange, and Mohamed Ali Sfaxi. "Guaranteerring security of financial transaction by using quantum cryptography in banking environment." E-business and Telecommunication Networks: Second International Conference, ICETE 2005, Reading, UK, October 3-7, 2005. Selected Papers 2. Springer Berlin Heidelberg, 2007.
4. Sharma, Anand, and S. K. Lenka. "Authentication in online banking systems through quantum cryptography." Int. J. Engineering and Technology 5 (2013): 2696-2700.
5. Ali, Sanwar, and Waleed Farag. "How is quantum cryptography used for secure financial transactions." SDIWC, Indiana (2013).
6. Rahaman, Mijanur, and Md Masudul Islam. "A review on progress and problems of quantum computing as a service (QcaaS) in the perspective of cloud computing." Global Journal of Computer Science and Technology 15.4 (2015).
7. Clark, David. "Encryption advances to meet Internet challenges." Computer 33.08 (2000): 20-24.
8. Leibholz, Stephen W. "Solutions for the grand Challenges of Information Security: Protection Against Rogue Insiders, Dynamic Compartmentalization and True Quantum Encryption." 2007 IEEE Conference on Technologies for Homeland Security. IEEE, 2007.
9. Dube, Roger R. Hardware-based computer security techniques to defeat hackers: From biometrics to quantum cryptography. John Wiley & Sons, 2008.
10. Cartwright, Jon. "NSA keys into quantum computing." Physics World 27.02 (2014): 6.
11. Hassan, Tayyabah, and Fahad Ahmed. "Transaction and Identity Authentication Security Model for E-Banking: Confluence of Quantum Cryptography and AI." International Conference on Intelligent Technologies and Applications. Singapore: Springer Singapore, 2018.
12. Covers, Oscar, and Marco Doeland. "How the financial sector can anticipate the threats of quantum computing to keep payments safe and secure." Journal of Payments Strategy & Systems 14.2 (2020): 147-156.
13. Majot, Andy, and Roman Yampolskiy. "Global catastrophic risk and security implications of quantum computers." Futures 72 (2015): 17-26.
14. Veehof, L. M. G. Quantum computing in commercial banking: Current state, applications and strategy. BS thesis. University of Twente, 2024.
15. Deodoro, Jose, et al. Quantum computing and the financial system: spooky action at a distance?. International Monetary Fund, 2021.