TECHNIUM

Technium Vol. 5, pp.1-12 (2023)
ISSN: 2668-778X
www.techniumscience.com

Protection from A Quantum Computer Cyber-Attack: survey

Raya Jasim Easa [1], Asma Salim Yahya[2], Esraa Khalid Ahmad [3]

1 Department of Cyber Security, College of Computer Science and Mathematics, University of Mosul, MOSUL. IRAQ.

2 Department of Cyber Security, College of Computer Science and Mathematics, University of Mosul, MOSUL. IRAQ.

3 Department of Software, College of Computer Science and Mathematics, University of Mosul, MOSUL. IRAQ.

[1]raya.jassim@uomosul.edu.iq,[2]asma_alkhairi@uomosul.edu.iq,
[3]esraa@uomosul.edu.iq.

Abstract. Encryption is required to address the ongoing issue of information security within communication networks. In the second part of the 20th century, quantum computing was first utilized to crack encryption protocols with the SHOR algorithm's development. The transformation from traditional to computational has the possibility of jeopardizing the protection of the current transaction system, even though recent improvements in QC functionality have increased the privacy and security, integrity, and accessibility of networks by shielding them from attacks like eavesdropping. This research adopts a comprehensive literature review approach to clarify the effects of quantum computers on information security. In addition, the study provides a summary of current efforts to guard against quantum attacks. Examining all suggested information security and privacy safeguards, this study examines the additional issue that quantum computers would severely damage information security.

Keywords. Quantum Computing, Quantum Cyber-security, Quantum Threats, Quantum-safe cryptographic.

1. Introduction

Data, integrity, availability, security, authentication, and non-repudiation are all protected by cyber security, which guards against any harm to digital communication systems and services [1]–[4]. There has been a significant increase in cyber dangers due to the growth in available data volume; consequently, it is urgent to safeguard personal, commercial, and national information [5]–[7]. A quantum computer is an apparatus that use quantum physics to tackle difficult problems. It has a remarkable processing speed because of its two primary features, the superposition of states and entanglement [8]–[12]. Quantum physics' introduction and progress have undoubtedly been one of the most unanticipated dangers to cyber security [13]. Cryptography is one of the most significant domains adversely affected by quantum computers [14]–[16]. The encryption underlying contemporary Internet communications and e-commerce may one day be vulnerable to a quantum assault [17]. Researchers and experts in the field of cyber-security are legitimately concerned that a new form of computer based

on quantum physics rather than conventional electronics might compromise the majority of existing encryption [13], [18], [19]. The result would render communications as unsafe as if they had not been encrypted. Quantum-safe cryptographic solutions must be developed as quickly as possible to safeguard subtle and confidential information from possibly disastrous compromises [20]. And while true quantum-safe encryption is still in the future, you may use quantum-resistant technology to preserve the integrity of classified data and the security of operations now [21]–[23]. This research seeks to undertake a comprehensive literature review to understand the effects of quantum computers on information security and provide a quick summary of current efforts to guard against quantum attacks.

2. Quantum Cyber-Security: An Overview

Traditional computers have always worked in binary, employing bits to represent ones and zeros to calculate and process data [24]. Current computers are restricted because they can only handle a single set of inputs and a single computation simultaneously [25]. A century ago, a new set of physical principles known as quantum physics was established [26]. A quantum computer is a new form of computer that utilizes the power of quantum mechanics to tackle problems previously thought to be unsolvable on conventional computers. Quantum physics' introduction and progress have undoubtedly been one of the most unanticipated dangers to cyber-security [8]–[10], [27], [28]. Conventional computers manipulate data stored in a collection of bits, where each bit can hold one of two states that we call 0 and 1. As concepts progress toward functional technology and answer real-world issues, there is no unexpected worldwide competition for industrial leadership in quantum technologies [29], [30]. However, one unexpected effect of quantum computing is the destruction of some cryptographic techniques that now provide cyber security. A digital signature, for example, is a key prerequisite for online security [31].

2.1. Quantum Cyber-Security Impacts

Quantum computers, on a massive scale, will considerably increase computational power, giving new options for enhancing cyber-security [32]. Cyber-security in the quantum era will be able to identify and repel quantum-period cyberattacks before they damage [33]. Quantum computing may potentially introduce new vulnerabilities, such as the capacity to swiftly solve the challenging mathematical equations that form the basis of various kinds of encryption [34], [35]. While the standards for Post-Quantum Cryptography (PQC) are still being established, corporations and other organizations may begin preparations now [34]. No quantum computer can yet handle the vast quantity of qubits necessary to execute the required to compromise present safety. This will likely alter over the next 10 to 20 years, increasing the risk for organizations, especially the banking sector.

2.2. Quantum Cyber-Security Threats

Although many experts think quantum assaults won't happen for a few more years, there have been irregular and unexpected developments in the sector. With the advent of quantum computers, secure public-key techniques like RSA and DSA are now susceptible to compromise [36], [37]. One of the following maths equations will determine whether the approaches are secure: discrete logarithm, elliptic curve discrete logarithm, or integer factorization. Large quantum computers can effortlessly address these issues. Government entities, for instance, are preparing for the risk mitigation of existing cryptographic algorithm flaws [7], [38]. If a company stores sensitive information such as financial or medical data, it should take the same measures. As corporations continue to quicken their pace, however, the creation of the first quantum computers within the next decade cannot be ignored. The use of quantum computing to launch deception-based cyberattacks by threat actors is an additional cyber security concern relating to quantum computing. These quantum computing risks have distinct fingerprints and behaviours that the majority of current software cannot recognize [39]–[42].

2.3. Quantum-Safe Cryptography

In response to the quantum computer danger, the present cyber-security infrastructure must be replaced with one that is quantum-safe [43]. Innovators in cyber-security are utilizing several technologies for this goal. First, the present cryptographic methods, which cannot withstand the arrival of the quantum computer, can be replaced with a new set of quantum-resistant algorithms. The NIST has standardized the search for appropriate algorithms in the United States. Various candidates for cryptographic functions are presently being evaluated. There is, nevertheless, a definite chance that new quantum algorithms, i.e. algorithms that operate on quantum computers, might pose a danger to these [10]. The danger may be excessive for data with a high and lasting value. Alternately, and in an intriguing twist, one might employ quantum technology, including quantum cryptography, to combat the developing threat. For example, the development of quantum key generation and Quantum Key Distribution (QKD) is advancing rapidly [39], [44]–[46]. QKD is a revolutionary technology that uses a basic property of quantum physics to secure the confidentiality of encryption keys over an optical fibre network or in free space. Any effort to eavesdrop on the network would be noticed, preventing passive interception. Using QKD now will provide immediate protection for your data against current brute force attacks, safeguarding comprising in a post-quantum computation age against attacks, and shielding data with a lengthy shelf life.

3. Systematic Review Protocol

The procedure for the SLR set out to accomplish the goals of this review. The protocol was primarily comprised of the specifications for conducting the SLR. First, Sections 3.1 and 3.2 focus on identifying prospective bibliographic databases, creating inclusion/exclusion criteria, and selecting research papers. Each article was meticulously scanned in the second stage, and pertinent papers were extracted, as described in Section 3.3.

3.1. Conducting the SLR Method

This study was based on an SLR, which conducts the "Preferred Reporting Items for Systematic reviews and Meta-Analyses" (PRISMA) guideline [47]. The justification for undertaking this type of evaluation is to collect trustworthy studies from numerous databases. Between 2018 and 2022, a comprehensive search for English-language articles was conducted in the four major digital databases SD, IEEE, Scopus, and WoS. These indexes were selected due to their extensive coverage. Most of the studies were related to our research, considering that the cyber-security technique trends have been very active in quantum computing in recent years. This research employed query search using different keywords associated with information security (e.g., "Cyber-security" OR "Cyber-attack" OR "Cyber-security") and keywords that deliberated all these terms established under the concept of quantum computing (e.g., "Quantum Cyber-security" OR " Quantum Threats " OR " Quantum Computing "). As shown in Table 1, the query is used to support the search for various studies for protection from a cyber-attack within all these terms supporting quantum computing.

Table 1. Literature review query

Query Details Terms	Databases Result	Final Results
("Cyber-security" OR " Cyber-attack" OR " Cyber-security ") AND ("Quantum Cyber-security" OR " Quantum Threats " OR " Quantum Computing ")	IEEE=51 SD=262 Scopus=129 WoS=19	461 Articles

3.2. *Identifying Potential Research Articles*

To find relevant research publications, we established inclusion and exclusion criteria. The criteria for inclusion in the SLR were reviewed publications and analyzed the case-control context on quantum cyber-security authored in English and published in international conference proceedings and journals. In contrast, the criteria for exclusion from the SLR were publications related to cyber-security philosophy and not published in any conference proceedings or journals. The studies are in English full format language. Additionally, studies focusing on cyber-security but unrelated to the protection from quantum computing threads and vice versa are excluded. Throughout the study selection procedure, inclusion and exclusion criteria were evaluated.

3.3. *Systematic Review Results*

The earliest phases of the study's selection procedure began with around 461 articles culled from four databases. The procedure of removing duplicates resulted in the rejection of a total of (n = 167) papers. Therefore, the recollection is (n = 294) items. The second round of broadcast contained scanning titles and abstracts, obtaining 115 total articles. The next stage in the screening procedure was to recite the full texts of the identified articles. According to the criteria, a total of 22 types of research were evaluated and deemed pertinent to the evaluation. Fig.1 shows the schematic approach phase's flowchart.

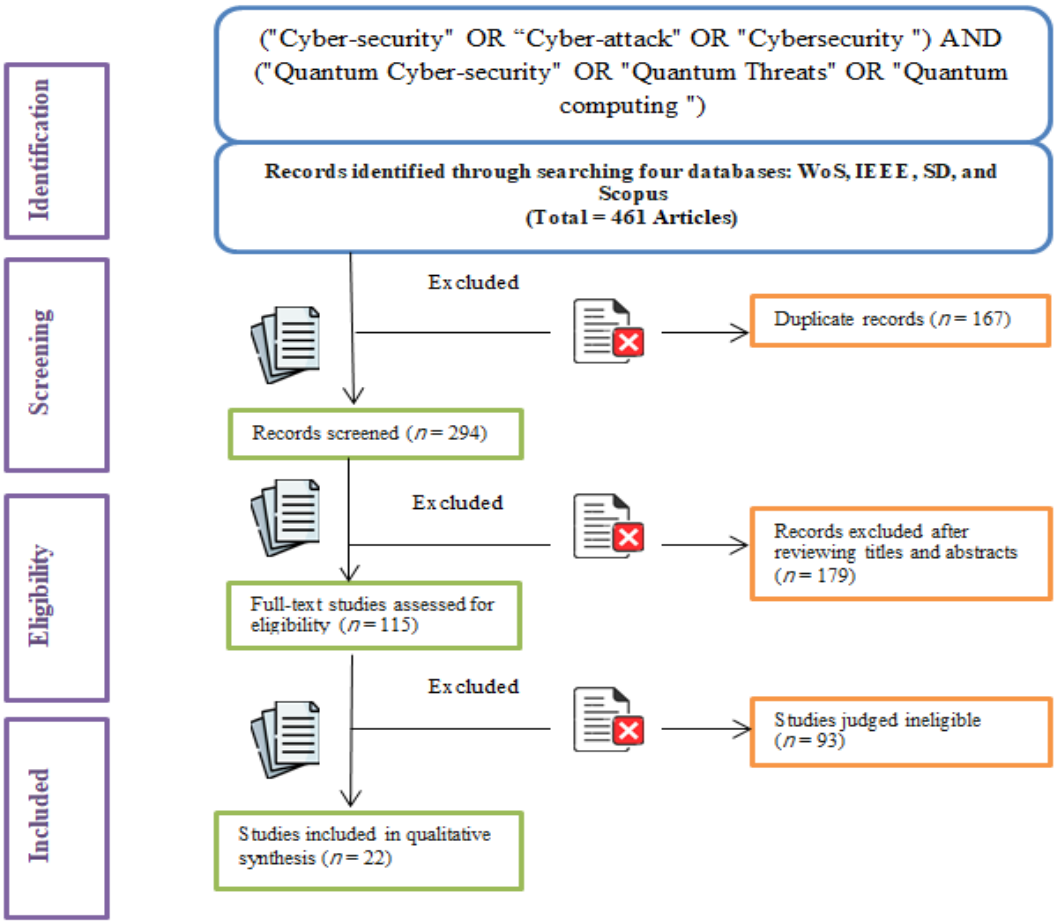

Figure 1: A schematic flowchart showing the methodology used for finding, screening, and including pertinent studies.

4. Discussion of Related Studies

The study [20] studied the situation of PQC at the moment and how distributed ledger technologies (such as blockchains) can use it (DLT). Grover's and Shor's algorithms may be significantly impacted by quantum computing attacks on public-key cryptography and hashing algorithms in the context of blockchain technology. Hash functions and general populace cryptography are at risk as a result of attacks using Grover's and Shor's algorithms, which have sped up the growth of quantum computing. The study uses post-quantum methods to overcome this issue and thoroughly contrasts public-key encryption and cryptographically signed for blockchain.

The study's authors [32] examined the relationship between classical technology and the Internet of Things, an emerging kind of networking that securely connects many Internet-connected devices. The study focuses on post-quantum IoT security methods and examines the architecture of 3GPP Security measures in a post-quantum environment. The researchers examined the methods that must be applied to protect IoT in the present and post-quantum eras from weaknesses in modern IoT architecture and implementation. The examination highlighted the current state of the Internet of Things security, including its protection of secrecy, authentication, and integrity, and how methods for identifying security threats in the IoT architecture are linked to specific data layering. The risks associated with IoT adoption include malware, direct channel attacks, and brute force attacks. Researchers developed potential lattice-driven cryptographic approaches as quantum-resistant security models ideal for minimizing new risks in the current and post-quantum worlds to solve the issue.

The author of [30] focused on creating digital signature systems that utilized user mistake codes, which prompted an examination of the viability of putting such systems into practice. It enables cryptographers to create strategies resistant to both classical and quantum programming cryptanalysis. The suggested method offers additional defence against specific assaults as well as a comparison of resistance to quantum and classical cryptanalysis, the difficulty of necessary conversions, and the length of generated signatures.

The KeyShield ensures the highest level of security and an exact solution to an underdetermined linear system of equations by taking into account several proposed factors, including forwarding/backward secrecy, minimal trust, guessing resistance, quantum resistance, scalability, computational cost, storage overhead, messages overhead, and entity management [48]. Using a linear system of equations as a key management method is computationally intensive, whereas KeyShiled provides two primary solutions: grouping members and employing a banded matrix.

The research [49] examined the present state of quantum adversarial machine learning and offered a unique approach by focusing on the challenges and proposed solutions. Quantum machine learning methods can handle contemporary quantum probabilistic data-driven challenges, yet, replicating quantum computers on conventional computers still presents unsolved questions. Later in the study, the constraints of datasets, applications, and adversarial instances, as well as the issues for quantum-assisted machine learning, are outlined. This work guarantees that readers will comprehend quantum adversarial machine learning and contributes to future research in this field. This research [6] discussed the current state of quantum computing technology and the accompanying quantum hazard. They provided recommendations on reducing cyberattacks by ensuring security by designing quantum software and hardware components.

Due to the high sensitivity of quantum communication, interference is easily recognized, and safe encryption-key distribution is possible. The report [50] proposed choices for handling this problem: (1) to accept where quantum technology goes, (2) to speed the technology regardless of its use, or (3) to push the technology to include mass usage. The authors suggested that the United States and its allies adopt a public-private strategy to influence high-end and mainstream use. On the other hand, the study [51] presented a QKD-based microgrid (MG) distributed control architecture for enhancing cyber-security. Measurement-device-independent QKD (MDI-QKD) was added to fight against side-channel attacks and make the framework suitable for industrial applications. They presented a method for real-time parameter adjustment in QKD systems based on a deep neural network (DNN) for rapid parameter optimization.

In this study [52], the authors analyzed the properties of quantum cryptography and explored its potential benefits for the future Internet. Notably, they analyzed the QKD protocol in a noise-free channel. In addition, they search for the QKD protocol in a noisy channel to mimic future Internet conditions. Theoretically, the outcomes indicated the total quantum cryptography security, which is acceptable for the Internet, given the inevitability of future difficulties.
While the study [28] introduced a special quantum-classical mixed deep learning approach for applications in cyber-security To investigate the effectiveness of the quantum circuit as a layer in a deep learning model for domain generation algorithms (DGA)-based botnet diagnosis, they compared the results of our hybrid model to that of its classical counterpart. We utilized MinREBotnets, CharLength, TreeNewFeature, and nGramReputation Alexa from the Botnet DGA dataset. They found that Angle Embedding and Strongly Entangled combination yield good precision. However, the remaining instances' overall performance is lower than that of the traditional deep learning model counterpart.

Meanwhile, in the study [53], the researchers introduced a new authentication and encryption system inspired by quantum walks (QIQW). Utilizing the suggested protocol, a blockchain architecture for secure data exchange among IoT devices is constructed. For joining chain blocks, quantum hash algorithms based on QIQW are utilized rather than traditional cryptographic hash methods. The primary benefits of the given architecture consist of enabling IoT nodes to successfully communicate their data with other nodes and granting them complete control over their records.

Assessment [54] is based on three quantities: the security shelf life of the information assets, the migration time to systems built to withstand quantum assaults, and the remaining time until quantum computers compromise security. Existing encryption and key exchange systems are becoming less effective due to the availability of quantum algorithms. Using a novel post-quantum encryption key management method that eliminates the need for PKI, this study [55] has developed technology that simplifies data protection in transit. In this work, the researchers suggested a modified advanced encryption standard (AES) method and employed quantum computing encrypt/decrypt AES picture files [56]. Since the shift is regular during the AES Shift Row operation, the change approach caused the shift to become irregular when a quantum random walk was employed. IBM Qiskit quantum simulators were used to mimic computing resources and speeds for performance evaluation, while encryption performance was evaluated using the number of pixels change rate (NPCR) and unified average changing intensity (UACI).

The D-Wave 2000Q is a quantum computer used for machine learning by its quantum effect. RBMs were trained using the Bars-and-Stripes (BAS) and Cyber-security (ISCX) datasets [57]. Using the weights and biases of trained RBMs, the D-Wave was mapped. Classification and image reconstruction was carried out. This article [58] examined QC's speed-up performance on Quantum Machine Learning algorithms (QML). They used QML approaches like QSVM and QNN to detect SSC assaults. The authors compared QML's speed and accuracy to its traditional predecessors. QC promises to speed up SSC assaults. However, testing findings show increased computational time and lesser precision. The extracted information from the literature is presented in Table 2.

Table 2: information extraction from the systematic literature review description

Ref	Published Year	Technology used	Study significant
[7]	2018	RNG	Random number generators based on quantum mechanics for use in cyber-security
[52]	2018	QKD	Quantum cryptography is important for the future safety of the Internet
[20]	2020	Blockchains, DLTs	Blockchain cryptography that is not vulnerable to assaults from quantum computers is introduced
[59]	2020	Post-quantum IoT security	Post-quantum IoT cyber-security challenges
[30]	2020	Cryptography, digital signature	Digital signature technologies based on post-quantum error-correcting codes
[49]	2020	Public-key cryptography, hash functions	Resistance to quantum computing assaults in post-quantum blockchain cryptography
[48]	2021	QSC	A Key Management Protocol That Is Scalable and Quantum-Safe
[6]	2021	Quantum threats	Quantum risks are the main focus of cyber security for quantum computers.
[50]	2021	Communication Cyber-security	Quantum communication for post-pandemic cyber-security
[60]	2021	MDI-QKD	Architecture for microgrid control based on quantum keys
[53]	2021	QIQW	Identification and cryptography protocol using quantum walks as inspiration
[57]	2021	BAS	implementing a constrained Boltzmann machine for quantum computing (RBM)
[55]	2021	CoreVUE	Using CoreVUE, a post-quantum security protocol, they can bypass public-key infrastructure encryption and key exchange.
[56]	2021	AES, NPCR, UACI	IBM Qiskit quantum simulators were used to model computational assets and speeds for performance analysis.
[61]	2022	Quantum annealing	Quantum annealing-based cyber-security using restricted Boltzmann machine
[28]	2022	DGA	Using a Quantum-Classical Deep Learning Model for Cyber-security
[58]	2022	QSVM, QNN	Measured how well QML performed in terms of speed and accuracy of processing

5. Conclusions and Recommendations for Future Work

Quantum computing has the potential to transform modern computers and cryptography. However, integrating quantum technology into ordinary life would need decades of progress and attention. Multiple algorithms have been created to tackle certain problems more efficiently than traditional computers, accelerating the theory's development. These algorithms have laid the groundwork for expanding research to meet future demands. However, hardware improvements did not match the speed of theoretical work. The existence of a universal quantum computer remains an extremely distant goal. In this paper, we examined the current state of the art in quantum computing and cyber-security and outlined the recommended techniques to date. Quantum computing for cyber security denotes the use of quantum computing to reduce cyber-security vulnerabilities. In addition, utilizing quantum

computing technology to combat cybercrime carries risks. Our findings imply a substantial need for more study in this burgeoning field. This current systematic review will give practitioners and scholars in quantum and cyber-security a deeper knowledge and shed light on future research possibilities.

Investigating non-discrete logarithmic cryptosystems is important to thwart quantum computers. Quantum data processing and communication outperform traditional communication due to their unique properties. A particle's location in the micro world is difficult to determine because of its numerous locations. Additionally, quantum cloning enables the restoration of any data that an opponent took from the quantum. Extensive research is continuing to broaden the breadth and availability of QKD data. Quantum cryptography protocols and their applications are adequately defined.

References

[1] H. Vella, "Quantum cyber security; The race for quantum-resistant cryptography; process; overview of a chip-based quantum cryptography communication system," Eng. Technol., vol. 17, no. 1, pp. 56–59, 2022, doi: 10.1049/et.2022.0109.

[2] A. Ali, "A Pragmatic Analysis of Pre- and Post-Quantum Cyber Security Scenarios," in 2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST), 2021, pp. 686–692, DOI: 10.1109/IBCAST51254.2021.9393278.

[3] F. Farahmand, "Introducing Hilbert Space and Quantum Cognition to Cyber Security Risk Management," IEEE Lett. Comput. Soc., vol. 3, no. 1, pp. 1–4, 2020, doi: 10.1109/LOCS.2019.2963875.

[4] H. T. Larasati, M. Firdaus, and H. Kim, "Quantum Federated Learning: Remarks and Challenges," in 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2022, pp. 1–5, DOI: 10.1109/CSCloud-EdgeCom54986.2022.00010.

[5] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," Veh. Commun., vol. 23, p. 100249, 2020, doi: https://doi.org/10.1016/j.vehcom.2020.100249.

[6] N. Kilber, D. Kaestle, and S. Wagner, "Cybersecurity for quantum computing," CEUR Workshop Proc., vol. 3008, pp. 20–28, 2021.

[7] C. Abellan and V. Pruneri, "The future of cybersecurity is quantum," IEEE Spectr., vol. 55, no. 7, pp. 31–35, 2018, DOI: 10.1109/MSPEC.2018.8389185.

[8] D. Rosch-Grace and J. Straub, "Analysis of the Necessity of Quantum Computing Capacity Development for National Defense and Homeland Security," in 2021 IEEE International Symposium on Technologies for Homeland Security (HST), 2021, pp. 1–8, DOI: 10.1109/HST53381.2021.9619831.

[9] T. H. Szymanski, "The 'Cyber Security via Determinism' Paradigm for a Quantum-Safe Zero Trust Deterministic Internet of Things (IoT)," IEEE Access, vol. 10, pp. 45893–45930, 2022, DOI: 10.1109/ACCESS.2022.3169137.

[10] W.-K. Lee, K. Jang, G. Song, H. Kim, S. O. Hwang, and H. Seo, "Efficient Implementation of Lightweight Hash Functions on GPU and Quantum Computers for IoT Applications," IEEE Access, vol. 10, pp. 59661–59674, 2022, DOI: 10.1109/ACCESS.2022.3179970.

[11] F. Borges, P. R. Reis, and D. Pereira, "A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography," IEEE Access, vol. 8, pp. 142413–142422, 2020, DOI: 10.1109/ACCESS.2020.3013250.

[12] P. C. S., K. Jain, and P. Krishnan, "Analysis of Post-Quantum Cryptography for Internet of Things," in 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022, pp. 387–394, DOI: 10.1109/ICICCS53718.2022.9787987.

[13] A. Vaishnavi and S. Pillai, “Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods,” J. Phys. Conf. Ser., vol. 1964, no. 4, 2021, doi: 10.1088/1742-6596/1964/4/042002.

[14] D. Hoornweg and P. Bhada-Tata, “A Global Review of Solid Waste Management - Review, Global Management, Solid Waste,” World Bank Urban Dev. Ser. Knowl. Pap., vol. 1, no. 11, pp. 1–116, 2012.

[15] A. Aji, K. Jain, and P. Krishnan, “A Survey of Quantum Key Distribution (QKD) Network Simulation Platforms,” in 2021 2nd Global Conference for Advancement in Technology (GCAT), 2021, pp. 1–8, DOI: 10.1109/GCAT52182.2021.9587708.

[16] H. Zhang, Z. Ji, H. Wang, and W. Wu, “Survey on quantum information security,” China Commun., vol. 16, no. 10, pp. 1–36, 2019, DOI: 10.23919/JCC.2019.10.001.

[17] Y. Yao, Z. Zhai, J. Liu, and Z. Li, “Lattice-Based Key-Aggregate (Searchable) Encryption in Cloud Storage,” IEEE Access, vol. 7, pp. 164544–164555, 2019, DOI: 10.1109/ACCESS.2019.2952163.

[18] S. K. H. Islam, N. Mishra, S. Biswas, B. Keswani, and S. Zeadally, “An efficient and forward-secure lattice-based searchable encryption scheme for the Big-data era,” Comput. Electr. Eng., vol. 96, p. 107533, 2021, DOI: https://doi.org/10.1016/j.compeleceng.2021.107533.

[19] L. Li, K. Thakur, and M. L. Ali, “Potential Development on Cyberattack and Prospect Analysis for Cybersecurity,” in 2020 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS), 2020, pp. 1–6, DOI: 10.1109/IEMTRONICS51293.2020.9216374.

[20] T. M. Fernández-Caramès and P. Fraga-Lamas, “Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks,” IEEE Access, vol. 8, pp. 21091–21116, 2020, DOI: 10.1109/ACCESS.2020.2968985.

[21] T. Dhieb, H. Boubaker, S. Njah, M. Ben Ayed, and A. M. Alimi, “A novel biometric system for signature verification based on score level fusion approach,” Multimed. Tools Appl., vol. 81, no. 6, pp. 7817–7845, 2022, DOI: 10.1007/s11042-022-12140-7.

[22] S. Shafeeq, S. Zeadally, M. Alam, and A. Khan, “Curbing Address Reuse in the IOTA Distributed Ledger: A Cuckoo-Filter-Based Approach,” IEEE Trans. Eng. Manag., vol. 67, no. 4, pp. 1244–1255, 2020, doi: 10.1109/TEM.2019.2922710.

[23] S. Ha, H. Lee, D. Won, and Y. Lee, “Quantum-resistant Lattice-based Authentication for V2X Communication in C-ITS,” in 2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM), 2020, pp. 1–8, DOI: 10.1109/IMCOM48794.2020.9001682.

[24] B. Arslan, M. Ulker, S. Akleylek, and S. Sagiroglu, “A study on the use of quantum computers, risk assessment and security problems,” 6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding, vol. 2018-January, no. March, pp. 1–6, 2018, DOI: 10.1109/ISDFS.2018.8355318.

[25] H. Boche and V. Pohl, “On Non-Detectability of Non-Computability and the Degree of Non-Computability of Solutions of Circuit and Wave Equations on Digital Computers,” IEEE Trans. Inf. Theory, vol. 68, no. 8, pp. 5561–5578, 2022, DOI: 10.1109/TIT.2022.3172837.

[26] A. Herman, “The Executive ’ s Guide to Quantum Computing and Quantum-secure Cybersecurity,” 2019,. Available: https://s3.amazonaws.com/media.hudson.org/Executive%27s Guide to Quantum WEB FINAL.pdf.

[27] K.-F. Cheung, M. G. H. Bell, and J. Bhattacharjya, “Cybersecurity in logistics and supply chain management: An overview and future research directions,” Transp. Res. Part E Logist. Transp. Rev., vol. 146, p. 102217, 2021, DOI: https://doi.org/10.1016/j.tre.2020.102217.

[28] H. Suryotrisongko and Y. Musashi, “Evaluating hybrid quantum-classical deep learning for cybersecurity botnet DGA detection,” Procedia Comput. Sci., vol. 197, pp. 223–229, 2022, DOI: https://doi.org/10.1016/j.procs.2021.12.135.

[29] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, "A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain," IEEE Access, vol. 6, pp. 27205–27213, 2018, DOI: 10.1109/ACCESS.2018.2827203.

[30] A. Kuznetsov, A. Kiian, V. Babenko, I. Perevozova, I. Chepurko, and O. Smirnov, "New Approach to the Implementation of Post-Quantum Digital Signature Scheme," in 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020, pp. 166–171, DOI: 10.1109/DESSERT50317.2020.9125053.

[31] M. D. Noel, O. V Waziri, M. S. Abdulhamid, and A. J. Ojeniyi, "Stateful Hash-based Digital Signature Schemes for Bitcoin Cryptocurrency," in 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), 2019, pp. 1–6, DOI: 10.1109/ICECCO48375.2019.9043192.

[32] F. Of and C. Security, "An Introduction to Quantum Cyber Security QUANTUM WILL COMPLETELY CHANGE THE," no. December 2021, pp. 1–11, 2022.

[33] G. R. Mounica, G. Manimaran, L. B. Jerome, and P. Bhattacharjee, "Implementation of 5-Qubit approach-based Shor's Algorithm in IBM Qiskit," in 2021 IEEE Pune Section International Conference (PuneCon), 2021, pp. 1–6, DOI: 10.1109/PuneCon52575.2021.9686492.

[34] O. Pal, M. Jain, B. K. Murthy, and V. Thakur, "Quantum and Post-Quantum Cryptography," in Cyber Security and Digital Forensics: Challenges and Future Trends, Wiley, 2022, pp. 45–58.

[35] D. Tulli, C. Abellan, and W. Amaya, "Engineering High-Speed Quantum Random Number Generators," in 2019 21st International Conference on Transparent Optical Networks (ICTON), 2019, p. 1, DOI: 10.1109/ICTON.2019.8840502.

[36] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," IEEE Access, vol. 8, pp. 21091–21116, 2020, DOI: 10.1109/ACCESS.2020.2968985.

[37] S. Wu, J. Li, F. Duan, Y. Lu, X. Zhang, and J. Gan, "The Survey on the development of Secure Multi-Party Computing in the blockchain," in 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC), 2021, pp. 1–7, DOI: 10.1109/DSC53577.2021.00008.

[38] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," J. Netw. Comput. Appl., vol. 182, p. 103035, 2021, DOI: https://doi.org/10.1016/j.jnca.2021.103035.

[39] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-Secure Networked Microgrids," in 2020 IEEE Power & Energy Society General Meeting (PESGM), 2020, pp. 1–5, DOI: 10.1109/PESGM41954.2020.9281884.

[40] K. K. Rangan et al., "Quantum Computing and Resilient Design Perspectives for Cybersecurity of Feedback Systems," IFAC-PapersOnLine, vol. 55, no. 7, pp. 703–708, 2022, DOI: https://doi.org/10.1016/j.ifacol.2022.07.526.

[41] T. R. Vance and A. Vance, "Cybersecurity in the Blockchain Era," 2019 IEEE Int. Sci. Conf. Probl. Infocommunications Sci. Technol. PIC S T 2019 - Proc., pp. 107–112, 2019.

[42] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," J. Netw. Comput. Appl., vol. 149, p. 102481, 2020, DOI: https://doi.org/10.1016/j.jnca.2019.102481.

[43] A. Prakasan, K. Jain, and P. Krishnan, "Authenticated-Encryption in the Quantum Key Distribution Classical Channel Using Post-Quantum Cryptography," in 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022, pp. 804–811, DOI: 10.1109/ICICCS53718.2022.9788239.

[44] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-Secure Microgrid," IEEE Trans. Power Syst., vol. 36, no. 2, pp. 1250–1263, 2021, DOI: 10.1109/TPWRS.2020.3011071.

[45] D. AL-Mubayedh, M. AL-Khalis, G. AL-Azman, M. AL-Abdali, M. Al Fosail, and N. Nagy, "Quantum Cryptography on IBM QX," in 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1–6, DOI: 10.1109/CAIS.2019.8769567.

[46] I. B. Djordjevic, "Cluster States-based Quantum Networks," in 2020 IEEE Photonics Conference (IPC), 2020, pp. 1–2, DOI: 10.1109/IPC47351.2020.9252479.

[47] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," Int. J. Surg., vol. 8, no. 5, pp. 336–341, 2010, doi: 10.1016/j.ijsu.2010.02.007.

[48] M. Y. Al-darwbi, A. A. Ghorbani, and A. H. Lashkari, "KeyShield: A Scalable and Quantum-Safe Key Management Scheme," IEEE Open J. Commun. Soc., vol. 2, pp. 87–101, 2021, DOI: 10.1109/OJCOMS.2020.3046110.

[49] D. Edwards and D. B. Rawat, "Quantum Adversarial Machine Learning: Status, Challenges and Perspectives," in 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2020, pp. 128–133, DOI: 10.1109/TPS-ISA50397.2020.00026.

[50] M. C. Libicki and D. Gompert, "Quantum Communication for Post-Pandemic Cybersecurity," in 2021 13th International Conference on Cyber Conflict (CyCon), 2021, pp. 371–386, DOI: 10.23919/CyCon51939.2021.9468295.

[51] R. Yan, Y. Wang, J. Dai, Y. Xu, and A. Q. Liu, "Quantum-Key-Distribution-Based Microgrid Control for Cybersecurity Enhancement," IEEE Trans. Ind. Appl., vol. 58, no. 3, pp. 3076–3086, 2022, DOI: 10.1109/TIA.2022.3159314.

[52] T. Zhou, J. Shen, X. Li, C. Wang, and J. Shen, "Quantum Cryptography for the Future Internet and the Security Analysis," Secur. Commun. Networks, vol. 2018, p. 8214619, 2018, DOI: 10.1155/2018/8214619.

[53] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities," Inf. Process. Manag., vol. 58, no. 4, 2021, DOI: 10.1016/j.ipm.2021.102549.

[54] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," IEEE Secur. Priv., vol. 16, no. 5, pp. 38–41, 2018, DOI: 10.1109/MSP.2018.3761723.

[55] N. Edwards, J. B. Haynes, and S. B. Kiser, "Post-Quantum Security: CoreVUE Breaks Through PKI A Look at an Emerging Technology in Cybersecurity ," J. Strateg. Innov. Sustain., vol. 16, no. 1 SE-Articles, Jun. 2021, doi: 10.33423/jsis.v16i1.4187.

[56] K. K. Ko and E. S. Jung, "Development of cybersecurity technology and algorithm based on quantum computing," Appl. Sci., vol. 11, no. 19, 2021, doi: 10.3390/app11199085.

[57] V. Dixit, Y. Koshka, T. Aldwairi, and M. A. Novotny, "Comparison of quantum and classical methods for labels and patterns in Restricted Boltzmann Machines," J. Phys. Conf. Ser., vol. 2122, no. 1, 2021, doi: 10.1088/1742-6596/2122/1/012007.

[58] M. Masum et al., "Quantum Machine Learning for Software Supply Chain Attacks: How Far Can We Go?," pp. 530–538, 2022, DOI: 10.1109/compsac54236.2022.00097.

[59] O. S. Althobaiti and M. Dohler, "Cybersecurity Challenges Associated With the Internet of Things in a Post-Quantum World," IEEE Access, vol. 8, pp. 157356–157381, 2020, DOI: 10.1109/ACCESS.2020.3019345.

[60] R. Yan, J. Dai, Y. Wang, Y. Xu, and A. Q. Liu, "Quantum-Key-Distribution Based Microgrid Control for Cybersecurity Enhancement," in 2021 IEEE Industry Applications Society Annual Meeting (IAS), 2021, pp. 1–7, DOI: 10.1109/IAS48185.2021.9677160.

Technium Vol. 5, pp.1-12 (2023)
ISSN: 2668-778X
www.techniumscience.com

[61] V. Dixit et al., “Training a Quantum Annealing Based Restricted Boltzmann Machine on Cybersecurity Data,” IEEE Trans. Emerg. Top. Comput. Intell., vol. 6, no. 3, pp. 417–428, 2022, doi: 10.1109/TETCI.2021.3074916.