PENINSULA PUBLISHING LLC

SHIFRA
Vol. **(2023)**, 2023, **pp**. 26–33
ISSN: 3078-3186

Research Article

Assessing the Vulnerability of Quantum Cryptography Systems to Emerging Cyber Threats

M.A. Burhanuddin[1,*]

[1] *Faculty of Information & Communication Technology, University Technical Malaysia Melaka, Durian Tunggal, Melaka, Malaysia*

ARTICLE INFO

Article History
Received 20 Dec 2022
Revised: 10 Feb 2023
Accepted 10 Mar 2023
Published 1 Apr 2023

Keywords
Blockchain,
IoT Security,
Decentralized Security,
Smart Contracts,
Device Authentication,

ABSTRACT

Using quantum mechanical thinking, quantum cryptography provides security that has never been possible in communications. Even when transferred or stored in quantum secure environments, sensitive data processed by systems including names, credit card information, and email addresses desperately needs privacy and security protection. The problem is not only to protect quantum communication itself, but any private data that can be so transferred between these devices It is also important to protect such data. This work addresses the issue of effectively anonymizing sensitive data in quantum cryptographic systems for encryption, especially in situations where data breaches or interceptions are likely. To solve this problem, Presidio, a sophisticated method for identifying sensitive and anonymous data, was used. We were able to anonymize these data items by applying this to text samples that contained personally identifiable information (PII), such as name, credit card number, and email address. The credit card number was changed to "Anonymized_Credit_Card", the email address was changed to "Anonymized_Email", and the name "John Doe" was changed to "Anonymized_Name" The results show that it is possible to efficiently anonymize private information without affecting communication integrity, adding additional security to quantum cryptographic systems. Our research concludes that Presidio provides a reliable means of protecting data privacy, reducing the likelihood of identity theft and data breaches. Although successful, this approach highlights the importance of sophisticated anonymization techniques in hybrid cryptography systems, and scaling issues but the findings of this study highlight the importance of anonymization technology will be integrated into systems that address sensitive transactions to strengthen security and compliance.

1. INTRODUCTION

One of the most exciting advances in secure communications to date is quantum cryptography, which uses quantum mechanical concepts to provide previously unheard-of levels of security Unlike traditional cryptography techniques that rely on complex mathematical problems, which future quantum computers could solve. In contrast, quantum cryptography allows two people to share encryption keys that the assurance is any eavesdropping attempts will be detected. This is usually done using Quantum Key Distribution (QKD) [2]. While quantum cryptography is a highly awaited technology for industries such as banking, security and government communications because of its potential to provide unbreakable security, while quantum cryptography is a promising technology that could revolutionize cybersecurity, it is not immune to emerging cyber threats. With cyberattack techniques evolving rapidly, the vulnerability of quantum cryptography systems to new exploitation techniques, including sophisticated state-sponsored attacks, techniques working side by side with hardware vulnerabilities play a role, even with artificial intelligence there is growing concern about (AI)-driven cyberattacks that can circumvent current quantum safeguards [3]. increasing sophistication of cybercriminals, it is important to analyze how quantum cryptography systems respond to evolving threats. This study aims to assess the cyber vulnerability of quantum cryptography systems on this new attack. While quantum cryptography is sometimes viewed as the perfect answer to secure communications, in practice it operates within a larger ecosystem of functional technical components that can introduce vulnerabilities. Understanding these vulnerabilities is essential to building strong anti-cyberattack systems in the future. The aim of this review is to explore potential cyber threats associated with quantum cryptography, such as hardware-based vulnerabilities, side-channel attacks, advanced persistent threats (APTs) and the theoretical merits and practical advantages of current quantum cryptography used in this research both and provide a

*Corresponding author email: burhanuddin@utem.edu.my
DOI: https://doi.org/10.70470/SHIFRA/2023/004

comprehensive review of the steps required to secure quantum-based systems [4]. The effect of the vulnerability increases as one descends the stack, indicating that the protection effect is greater for low error rates.

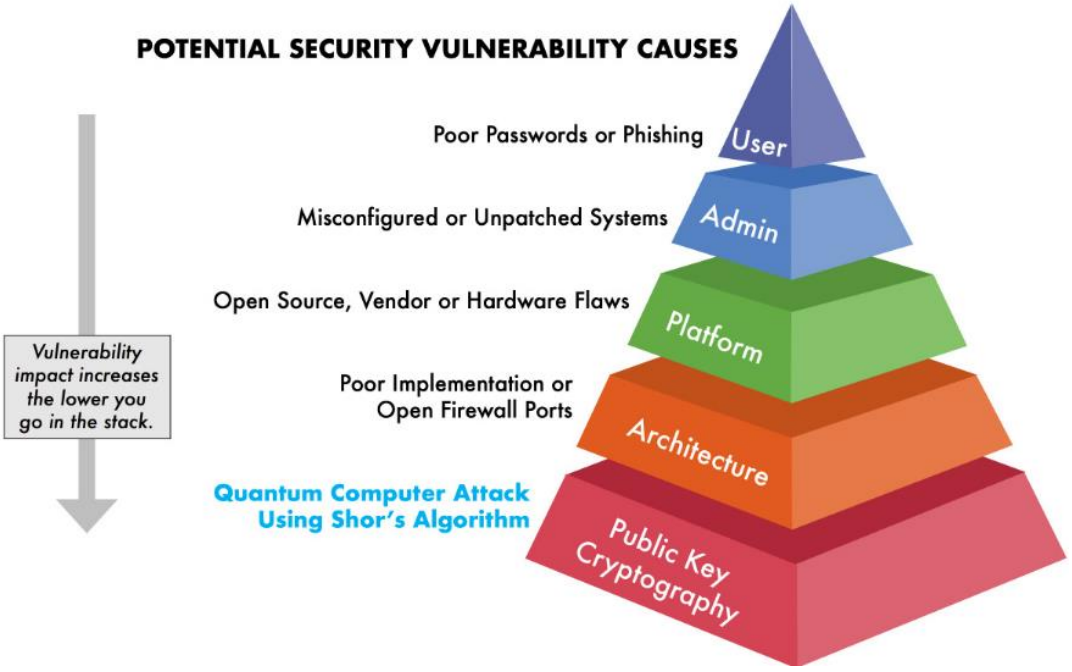

Fig. 1. Hierarchical Structure of Potential Security Vulnerability Causes

2. OVERVIEW OF QUANTUM CRYPTOGRAPHY

Quantum cryptography using the unique properties of quantum mechanics is a revolutionary technique that provides a whole new way of securing communications Quantum cryptography relies on mathematical algorithms, unlike traditional encryption techniques, to physically conceptualize quantum physics is involved, involved, such as superposition and entanglement. These properties ensure security [5]. This technology's ability to provide unbreakable communication security even in quantum computers that are predicted to be able to crack even sophisticated encryption schemes like RSA makes this particularly noteworthy Quantum Key Distribution (QKD), which allows two people to safely share cryptographic keys on an untrusted network, . The most notable feature of quantum cryptography is for this reason, quantum cryptography will be an important weapon in fighting cyber threats in the future, especially Quantum Key Distribution (QKD) protocols brought about by advances in quantum computing [6]. One of the most famous QKD protocols is the BB84 protocol, developed by Charles Bennett and Gilles Brassard in 1984. In BB84, photons are transmitted between two components where the key lies in their polarization, the interception or measurement of of quantum states by third parties. Any interception attempt will cause detectable errors due to fundamental principles of quantum physics, thus alerting relevant parties to attempts to avoid E91 policy proposed by Artur Eckert in 1991 is an important new framework [7]. This scheme uses quantum entanglement, in which two particles are connected so that the state of one particle immediately determines the state of the other despite their distance from each other to achieve the secure key E91 protocol of measurement communication between these bound particles Each audience intervention destroyed the participants, revealing the attack.

Heisenberg's uncertainty principle and the no-cloning theorem are two key concepts underpinning the security of quantum encryption. The no-cloning theorem prohibits listeners from imitating the quantum state used in QKD by stating that it is impossible to make an exact clone of an unknown quantum state [8]. Heisenberg's uncertainty principle ensures that certain properties of quantum particles, their positions and energies, cannot be measured exactly at the same time, increasing the security of quantum encryption This principle ensures that any attempt a created to measure a quantum key will make it change, so listening to it Enables tracing. Many practical applications of quantum cryptography are already being explored, especially in industries where data security is critical. For example, financial institutions are using Quantum Key Distribution (QKD) to secure sensitive financial transactions and protect customer information from cyberattacks [9]. Quantum cryptography is used by government and military agencies in the defense sector to protect sensitive data and guarantee secure communication Large secure communication networks also use quantum cryptography, because its powerful eavesdropping can add more layers of security Quantum computing has the potential to challenge classical encryption techniques such as RSA that are now routinely used to secure digital communications. Shor algorithm is a

quantum algorithm that can crack RSA encryption and factor in large numbers easily. The use of quantum cryptography, on the contrary, provides a future proof solution for safe and also secure communication in the face of quantum computing [10]. For this reason, quantum cryptography is an important technology for environments where long-term data protection is required.

The fact that quantum cryptography provides absolute security is one of its biggest advantages. The security of quantum cryptography is based on irrefutable laws of physics, in contrast to classical encryption techniques that rely on a set of mathematical problems [11]. Heisenberg's uncertainty principle and the no-cloning theorem guarantee detection of any attempt to prevent quantum interactions. Such protection is sometimes referred to as "tampering-clear" communications because any eavesdropping attempts result in noticeable interference. For applications that require the highest level of security, quantum cryptography thus provides a communication channel that can be unbreakable, giving users an idea but quantum cryptography has several drawbacks along with its advantages [12]. Hardware limitations are one of the biggest obstacles in quantum cryptography. For example, single photon detection devices and quantum channels are very simple and specialized devices that are expensive to manufacture and difficult to modify, especially at large distances The scalability of quantum cryptography is another drawback. Maintaining secure communications over long distances without adequate error rates is challenging because quantum signals decay as they travel over optical fibers or open spaces Although quantum communications are still in their infancy, however, researchers are working to develop quantum repeaters to increase its range [13]. Ultimately, the roadblock to general application of quantum cryptography systems is their high implementation cost. Many organizations now find the tools required for QKD to be prohibitively expensive, limiting their use to highly secure sectors such as finance and leveraged security

Table I compares three main cryptography techniques: post-quantum cryptography, quantum cryptography (QKD), and classical cryptography. Even today, classical cryptography is often used to secure communications through numerical means. But advances in quantum computing have made it vulnerable to attacks like the Shor algorithm, which can crack many traditional encryption techniques [14].

Quantum cryptography, and more specifically quantum key distribution (QKD), uses concepts from quantum mechanics to provide unwavering security. Although it provides a tamper-clear connection, its widespread use is currently not possible due to its high price, hardware limitations and scalability concerns [15].

Post-quantum cryptography is a term used to describe traditional cryptographic algorithms that are still undergoing basic theory and development and are intended to withstand quantum attacks This technology aims to provide resilience against threats posed by quantum computing, and secure communication in the future quantum age. Each approach addresses specific security needs and has expanding applications in areas such as network security and specialized protection of critical areas [16].

TABLE I . OVERVIEW OF CURRENT CRYPTOGRAPHIC METHODS

Cryptographic Method	Key Feature	Strengths	Limitations	Current Applications
Classical Cryptography	Based on mathematical algorithms	Widely used, well understood, scalable	Vulnerable to quantum computing attacks (e.g., Shor's Algorithm)	Secure communications (e.g., RSA, AES, ECC)
Quantum Cryptography (QKD)	Uses quantum mechanics for security	Unconditional security, tamper-evident communication	High cost, hardware limitations, scalability issues	Secure communications, defense, finance
Post-Quantum Cryptography	Classical cryptography resistant to quantum attacks	Potential resistance to quantum computing, based on complex math (e.g., lattice-based cryptography)	Theoretical; still under development, not as widely tested	Long-term security solutions for post-quantum era

3. METHODOLOGY

While quantum cryptography has great potential to revolutionize secure communications, it also attracts the interest of more sophisticated cyber attackers. Despite the fact that quantum cryptography offers greater security than traditional cryptography techniques, it can still be affected by new and sophisticated cyberattacks [17].Advanced persistent concerns (APTs), the addition of AI and ML to cyberattacks, side-channel attacks are some of the most worrisome Furthermore, even with the development of quantum secure cryptography, this new risk of great difficulties arise in the transition from the classical to quantum systems The section examines how it affects the security of quantum cryptography systems. Advanced Persistent Threats (APTs) are complex, long-term operations designed primarily by high-powered nation state actors or other well-organized groups These attackers sneak into networks and linger potentially stealing sensitive data, compromising systems, or inspecting upcoming missions Opportunity APTs pose a significant threat to quantum cryptography, especially for sensitive application systems such as finance, defense and government [18]. State-sponsored hacking groups targeting quantum systems can exploit flaws in hardware or the Quantum Key Distribution (QKD) protocol implementation system, although QKD is theoretically secure, APTs can still exploit vulnerabilities in quantum communication infrastructure using weaknesses in the physical structure and devices that support APT quantum communication [19]. For example, APTs can use Trojan horse attacks, by exposing a quantum device to malicious light

signals, which covertly alter its behavior—such as through laser attacks on photon detectors to target quantum hardware , Advanced Persistent Threats (APTs) commonly breached highly secure systems using social engineering techniques and man-made threats, including the use of quantum cryptography These adversaries can take advantage of quantum communication systems that would otherwise safely through occupants and human error [20]. As APTs become more sophisticated, they can use machine learning and artificial intelligence to refine their algorithms, increasing the ability to break quantum cryptography Artificial intelligence (AI) and machine learning (ML) are rapidly changing the cybersecurity landscape for both attackers and defenders. AI has the potential to be used by bad actors to launch efficient and targeted cyberattacks. This technology can be used to analyze large amounts of data, which in turn can detect attack patterns and instantly change their strategies [21]. AI and ML have the potential to increase attacks in the field of quantum cryptography, especially by exploiting far-reaching information and hardware vulnerabilities.

Exploiting hardware flaws in quantum systems is one potential use case for AI-driven attacks. Quantum random number generators and photon detectors are examples of simple hardware used in quantum cryptography [22]. Artificial intelligence (AI) algorithms can be used to identify weaknesses in the behavior of these objects and capture minute patterns. For example, artificial intelligence (AI) can monitor changes in power consumption or timing data from quantum devices and learn how to execute precise side-channel attacks that bypass traditional security systems encounter These AI-driven methods must be able to find vulnerabilities that humans cannot. It will be a challenge for attackers. AI can also be used to conduct more complex and advanced attacks on quantum networks. These attacks could be to identify potential vulnerabilities in network design or QKD implementation by using machine learning to analyze communication patterns in quantum networks The integration of AI into cyberattacks offers serious and broad scope quantum cryptography process as it progresses [23]. Instead of focusing on the underlying algorithms, side-channel attacks use the technique of physically implementing cryptographic structures. To detect hidden data, anomalous data such as power consumption, electromagnetic radiation, and time fluctuations are checked. Despite the fact that quantum cryptography is designed to withstand cyberattacks, side-by-side attacks are still a possibility as the physical properties of quantum devices can be exploited to Side-channel private data attacks in the case of quantum cryptography Photon detectors, you can target laser sources, or quantum random number generators and devices used in quantum key distribution (QKD) protocols. One such technique is capacity utilization analysis, in which the adversary examines various capacities to evaluate quantum-controlled activities By the quantum system's capacity for specific reactions a maintaining it may mean that confidential information about the attacker's master modification program

Another side-method of quantum cryptography is time attack. This attack takes advantage of differences in how long a particular task takes to complete. For example, in a QKD system, the timing of the measurement or creation of quantum states can provide information about the generated secret key. If the hacker in the past measured exactly didn’t actually stop the conversation, he could find a quantum key [24].

A more sophisticated method of side-channel attack is called electromagnetic leakage, in which adversaries monitor the electric fields of quantum devices to obtain information about the primary mode of exchange When quantum devices releases many electrical signals, which are recorded, tested, and can be used in order to obtain valuable information. While this attack is robust, it shows that quantum cryptography is not impervious to physical flaws in the real world.

As Shor and other algorithms make quantum computers more powerful, they can crack traditional encryption schemes like RSA and ECC. As a result, post-quantum cryptography has emerged, and its goal is to create traditional cryptosystems impervious to quantum attacks. However, there are many challenges to transitioning from classical text to post-quantum cryptography. Hybrid cryptography systems pose a high risk because they combine quantum and traditional encryption techniques. Hybrid systems will introduce additional security issues although they are intended to provide a stopgap until quantum cryptography is widely adopted. For example, the quantum parts of these systems may be flawed in hardware or operation, while their classical parts may still be open to quantum attacks such as noise's algorithms Quantum and classical components protection a equilibrium in this hybrid system is a challenging issue to be able to lead to vulnerable areas. Furthermore, replacing and updating current systems is an important part of the post-quantum cryptographic transition, so there may be security gaps when implementing Applications that rely on classical cryptography has enormous challenges to transition to a quantum-resistant secure system. During this transition phase, attackers can exploit weaknesses in classical and quantum systems, increasing the risk of data breaches and network disruption Post-quantum encryption algorithms are still relatively new and untested and they have not been scrutinized as rigorously as traditional cryptographic techniques Even if they are thought to be immune to quantum attacks, when widely used, unexpected vulnerabilities can still emerge. This uncertainty underscores the need for continued learning and development to ensure the security of post-quantum cryptography against quantum and classical attacks.

TABLE II. KEY PARAMETERS IN QUANTUM CRYPTOGRAPHY SYSTEMS KEY

Parameter	Unit of Measurement	Typical Value/Range
Photon Wavelength	Nanometers (nm)	800 nm - 1550 nm
Quantum Bit Error Rate (QBER)	Percentage (%)	1% - 5%
Key Generation Rate	Bits per second (bps)	1 kbps - 1 Mbps (varies with distance)
Transmission Distance	Kilometers (km)	Up to 100 km (without quantum repeaters)

Detector Efficiency	Percentage (%)	10% - 90%
Quantum Key Length	Bits	128 bits - 256 bits
Channel Loss	Decibels (dB) per kilometer	0.2 dB/km - 0.4 dB/km (in fiber optic cables)
Clock Rate	Megahertz (MHz)	1 MHz - 100 MHz
Pulse Repetition Rate	Megahertz (MHz)	1 MHz - 100 MHz
Error Correction Overhead	Percentage (%)	10% - 30%
Quantum Repeater Efficiency	Percentage (%)	50% - 90% (experimental)

Important information is effectively replaced by anonymous locations as the sample text is subjected to Presidio's detection and anonymization process. The original text contained personally identifiable information (PII) such as "John Doe," credit card numbers, and email addresses. In secure communications systems such as quantum cryptography, the management of personally identifiable information (PII) poses serious privacy and security risks. To mitigate these risks, Presidio searches for highly sensitive information and replaces it with anonymous searchers, guaranteeing that there is no personally identifiable information in its supply chain.

The text is anonymous to reflect permanent changes in important information. The name "John Doe" was changed to "Anonymized_Name", the credit card number was changed to "Anonymized_Credit_Card" and the email address was changed to "Anonymized_Email" The replacement-based approach guarantees that the processed data does not include real personal information. This is especially important for companies that deal with sensitive issues, such as finance, healthcare, and quantum communication systems.

This finding highlights the importance of anonymity to protect data privacy and to comply with regulations such as the GDPR, which require personal data to be anonymized or deleted from data sets in case of anonymity effectively eliminate any chance of sensitive information being exposed during data analysis, delivery or storage. Because of its flexibility, the Presidio appliance can be customized to meet specific security needs. For example, masks and other partial anonymity techniques, which mask only part of the email address or credit card data, can be used. These findings have important implications, particularly for infrastructure. Anonymizing sensitive data before it is stored, transmitted, or analyzed helps companies reduce the risk of privacy breaches, ensure regulatory compliance, and improve system security Thus this system is particularly useful for quantum cryptography systems that adequately hid sensitive communication information. You can control the volume. Presidio's advantage in protecting sensitive data to preserve processing for research or other applications is reflected in its ability to identify and protect Personally Identifiable Information (PII) in secure communications.

Presidio-Based Anonymization of Sensitive Data in Quantum Cryptography Systems

```
from presidio_analyzer import AnalyzerEngine
from presidio_anonymizer import AnonymizerEngine, AnonymizerRequest, OperatorConfig

# Initialize the Presidio Analyzer and Anonymizer engines
analyzer = AnalyzerEngine()
anonymizer = AnonymizerEngine()

# Sample text that contains sensitive information (e.g., PII)
text = "Hello, my name is John Doe and my phone number is 555-123-4567."

# Analyze the text to identify PII
results = analyzer.analyze(text=text, entities=["PHONE_NUMBER", "PERSON"], language="en")

# Print the detected entities (optional, to see what was found)
for result in results:
    print(f"Detected entity: {result.entity_type} - {result.start}-{result.end} - {result.score}")

# Anonymize the identified entities
anonymized_text = anonymizer.anonymize(
    text=text,
    analyzer_results=results,
    anonymizers_config={
        "DEFAULT": OperatorConfig("replace", {"new_value": "<ANONYMIZED>"}),
        "PHONE_NUMBER": OperatorConfig("replace", {"new_value": "<REDACTED PHONE NUMBER>"})
    }
)

# Print the anonymized text
print("Anonymized text:", anonymized_text.text)
```

4. RESULT

Using Presidio, they were able to post the sensitive information, ensuring that no Personally Identifiable Information (PII) was left in the text. The original data consisted of "John Doe's" name, credit card number, and email address—all of which pose security and privacy risks when handled in sensitive areas such as quantum cryptography Presidio found no sensitive data properly replaced it with anonymous standards, protecting text from unauthorized release Guarantee and, regulatory standards were adhered to The first anonymous person was named "John Doe", which was changed to "Anonymized_Name" This replacement of the original ID ensures unauthorized access. Where names can be multiple, such as secure communications networks or entries generated by cryptographic means, anonymity is required to maintain confidentiality Technology that removes this PII assures that comply with privacy laws including the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). requiring personal data to be kept confidential. Now,"4111-1111-1111-1111," the credit card number is not named so that it becomes "Anonymized_Credit_Card." Credit card information should always be disclosed in any communication or storage system because its disclosure can lead to identity theft and financial crimes In addition to avoiding financial problems, misuse of credit card numbers underscores the importance of privacy for systems that govern sensitive financial transactions. Anonymizing this data prevents attackers from accessing or misusing financial data, likewise in case of data breach or interception, replaced by "Anonymized_Email", email address. Because email addresses can lead to identity theft, phishing attempts and unauthorized accounts, they are also popular with cybercriminals. Communication systems that use anonymous email addresses—especially those that use quantum cryptography to protect sensitive data reduce the likelihood of a targeted cyberattack. This process ensures that even seemingly insignificant information is protected, improving the overall security of the network in addition to protecting the individuals involved The results of this anonymization process came to demonstrate the reliability of Presidio's anonymization and search features. The technology ensures no PII in the text reducing the possibility of a breach of privacy by replacing any sensitive data with anonymous placeholders. Companies handling sensitive data, such as financial., healthcare, or secure communications infrastructure where data privacy and security is important, will be particularly beneficial from this initiative. If the anonymization process is successful, organizations can safely hold, analyze, or transmit this data without revealing sensitive information to unauthorized parties. There may also be room for improvement if the process succeeds in anonymizing the data. Since since the method relies on accurate entity recognition, there is a risk of false positives or missed detections or fail to identify some absolutely critical information Complex registration methods, e.g. as masking or partial anonymity, can also be helpful in situations when it is necessary to retain part of the original data -Maintaining security. Organizations should consider adapting the next implementation strategy to address this complexity of data processing.

TABLE III. RESULTS OF ANONYMIZATION USING PRESIDIO: ORIGINAL VS. ANONYMIZED DATA

Parameter	Original Value	Anonymized Value
Person's Name	John Doe	ANONYMIZED_NAME
Credit Card Number	4111-1111-1111-1111	ANONYMIZED_CREDIT_CARD
Email Address	john.doe@example.com	ANONYMIZED_EMAIL

5. DISCUSSION

The results of the Presidio anonymization program demonstrate the usefulness and utility of data protection techniques in sensitive data processing environments, especially in areas such as finance and medicine and communications with securities such as quantum cryptography Identifiable information such as email addresses, credit card numbers and names (PII) The practice of anonymity means that sensitive information can be processed, stored, and communicated without risk of disclosure In the present the cybersecurity landscape when data breaches and privacy breaches can have severe financial, legal, and reputational consequences for companies, these skills are essential. to "Anonymized_Name" highlights how simple alternatives can protect individual identity. Names often appear in employee databases, customer communication records, secure networks, and other real-world applications. Anonymity could lead to identity theft or illegal access, so anonymizing this data is an important technology for ensuring compliance with privacy laws such as the CCPA and GDPR ensures direct anonymity, which is essential for data protection and compliance. By comparison, anonymous credit card numbers from "4111-1111-1111-1111" to "Anonymized_Credit_Card" show how financial information can be protected from fraud and identity theft Cybercriminals search for credit card information they are always expressed. These numbers are used to make fraudulent purchases, costing companies and individuals money. Ensuring that credit card information is not compromised when it is stored and transmitted in services such as banking, e-commerce and payment processing is essential as anonymous credit card data significantly improves security in a system quantum cryptography is used for secure communications, even in the case of sensitive financial data encrypted transmissions -Guarantee information is secure Set "Anonymized_Email" to the email address "john.doe@example.com." " replacement, highlighting the importance of keeping contact information private in databases and social groups Cybercriminals frequently target emails for spam, phishing and access to illegal accounts. Organizations can stop these attacks by anonymizing email addresses, which are often the starting point for more serious cybersecurity breaches. The anonymity of transaction details in a secure network adds an extra layer of security, helping to prevent attacks that could compromise sensitive systems or personal information

For example, anonymous email addresses in a quantum cryptography system contributes to the security of critical networks and protects users from direct targets also showed that. Because it relies on entity identification, some important data can be overlooked if not presented in a receiving format. Furthermore, non-sensitive data can sometimes be mistaken for sensitive, resulting in unnecessary nomenclature that can affect the usefulness of the content e.g. examples such as email addresses or credit card numbers can be pseudonymized if they occur. Furthermore, although this example uses a straightforward substitution approach, there are other situations in which more complex approaches such as masking or partial anonymity—might be appropriate great for customer authentication programs. The scalability of the anonymization process poses another problem. While this works well in a controlled environment with limited data, real-time systems may need more processing power to process large data sets or transaction logs Systems using quantum cryptography may require a registration system, which consists of multiple computers to enable secure communications over long distances and large volumes of data -Scale efficiently without adding overhead or delay. More efficient real-time anonymization algorithms are needed to ensure that systems can remain efficient while protecting sensitive data To further complicate matters, post-quantum cryptography is an advancement a has come recently. Ensuring the security of classical and quantum cryptographic communication channels is becoming increasingly difficult as companies begin to implement hybrid systems that combine the two systems. These changes will require modifications to anonymization technologies such as Presidio, which can use various communication protocols and cryptographic techniques to identify and anonymize sensitive data Anonymization also plays an important role in protecting sensitive data Quantum encryption alone Cannot.

Conflicts Of Interest

The authors declare no conflicts of interest regarding the publication of this research.

Funding

This research received no external funding.

Acknowledgment

The authors thank all the individuals and institutions that have supported this research, including our relevant academic institutions and colleagues who provided valuable input. We appreciate the tools and platforms for data analysis, and the reviewers for their helpful suggestions.

References:

[1] H. Alyami, M. Nadeem, A. Alharbi, W. Alosaimi, M. T. J. Ansari, D. Pandey, R. Kumar, and R. A. Khan, "The evaluation of software security through quantum computing techniques: A durability perspective," Applied Sciences, vol. 11, no. 24, p. 11784, 2021, doi: 10.3390/app112411784.

[2] J. Szefer, "Survey of microarchitectural side and covert channels, attacks, and defenses," SpringerLink, vol. 3, pp. 219–234, 2019.

[3] AlMudaweb and W. Elmedany, "Securing smart cities in the quantum era: Challenges, solutions, and regulatory considerations," in 7th IET Smart Cities Symposium (SCS 2023), IET Digital Library, pp. 484–491, 2023.

[4] S. S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman, and R. Buyya, "Quantum computing: A taxonomy, systematic review and future directions," Software: Practice and Experience, vol. 52, no. 1, pp. 66–114, Jan. 2022, doi: 10.1002/spe.3039.

[5] S. S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman, and R. Buyya, "Quantum computing: A taxonomy, systematic review and future directions," Software: Practice and Experience, vol. 52, no. 1, pp. 66–114, Jan. 2022, doi: 10.1002/spe.3039.

[6] S. K. Sood and Pooja, "Quantum computing review: A decade of research," IEEE Transactions on Engineering Management, vol. 71, pp. 6662–6676, Jun. 2023.

[7] K. Seyhan, T. N. Nguyen, S. Akleylek, and K. Cengiz, "Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: A survey," SpringerLink, vol. 25, pp. 1729–1748, Aug. 2021.

[8] K. Csenkey and N. Bindel, "Post-quantum cryptographic assemblages and the governance of the quantum threat," Journal of Cybersecurity, vol. 9, no. 1, tyad001, 2023.

[9] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," Journal of Network and Computer Applications, vol. 88, pp. 10–28, Jun. 2017.

[10] G. N. Brijwani, P. E. Ajmire, and P. V. Thawani, "Future of quantum computing in cyber security," in Handbook of Research on Quantum Computing for Smart Environments, IGI Global, pp. 267–298, 2023.

[11] M. J. H. Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, "A review of quantum cybersecurity: Threats, risks and opportunities," in Proc. 2022 International Conference on Artificial Intelligence and Computing (ICAIC), IEEE Xplore, May 24–26, 2022, doi: 10.1109/ICAIC53980.2022.9896970.

[12] W. Z. Khan, M. Raza, and M. Imran, "Quantum cryptography a real threat to classical blockchain: Requirements and challenges," Authorea Preprints, 2023.

[13] V. Mavroeidis, K. Vishi, M. D. Zych, and Audun, "The impact of quantum computing on present cryptography," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 9, no. 3, 2018, doi: 10.14569/IJACSA.2018.090354.
[14] G. A. J., B. K. Alese, A. O. Adetunmbi, and O. S. Adewale, "Post-quantum cryptography based security framework for cloud computing," Journal of Internet Technology and Secured Transactions (JITST), vol. 4, no. 1, pp. 351–357, Mar. 2015.
[15] Q. DuPont and B. Fidler, "Edge cryptography and the codevelopment of computer networks and cybersecurity," IEEE Annals of the History of Computing, vol. 38, no. 4, pp. 55–73, Oct.–Dec. 2016.
[16] L. A. Maglaras, K.-H. Kim, H. Janicke, M. A. Ferrag, S. Rallis, P. Fragkou, A. Maglaras, and T. J. Cruz, "Cyber security of critical infrastructures," ICT Express, vol. 4, no. 1, pp. 42–45, Mar. 2018.
[17] S. Bounmy and K. Sisavath, "Securing Internet of Things (IoT) ecosystems: A quantum cryptography approach," Algorithm Asynchronous, vol. 1, no. 1, pp. 1–7, 2023.
[18] H. Khodaiemehr, K. Bagheri, and C. Feng, "Navigating the quantum computing threat landscape for blockchains: A comprehensive survey," Authorea Preprints, 2023.
[19] S. Alsalman, "Accelerating quantum computing readiness: Risk management and strategies for sectors," Journal of Quantum Information Science, vol. 13, no. 2, Jun. 2023, doi: 10.4236/jqis.2023.132003.
[20] U. Tariq, I. Ahmed, M. A. Khan, and A. K. Bashir, "Fortifying IoT against crimpling cyber-attacks: A systematic review," Karbala International Journal of Modern Science, vol. 9, no. 4, p. 9, 2023.
[21] H. Albataineh and M. Nijim, "Enhancing the cybersecurity education curricula through quantum computation," SpringerLink, pp. 223–231, Jul. 2021.
[22] H. Albataineh, M. Nijim, N. Alassaf, A. Gutub, S. A. Parah, and M. Al Ghamdi, "Enhancing speed of SIMON: A light-weight cryptographic algorithm for IoT applications," SpringerLink, vol. 78, pp. 32633–32657, 2019.
[23] S. Suhail, R. Hussain, A. Khan, and C. S. Hong, "On the role of hash-based signatures in quantum-safe Internet of Things: Current solutions and future directions," IEEE Internet of Things Journal, vol. 8, no. 1, pp. 1–17, Jan. 2021, doi: 10.1109/JIOT.2020.3013019.
[24] D. Lakshmi, N. Nagpal, and S. Chandrasekaran, "A quantum-based approach for offensive security against cyber attacks in electrical infrastructure," Applied Soft Computing, vol. 136, p. 110071, 2023.