Internet of Things 25 (2024) 101132

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.sciencedirect.com/journal/internet-of-things

Review article

Securing IoT systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions

Ahmad Alomari, Sathish A.P. Kumar *

Department of Computer Science, Cleveland State University, Cleveland, OH, 44115, USA

ARTICLE INFO

Keywords:
IoT
Quantum computing
Qubit
Cybersecurity
Vulnerabilities
Post-quantum attacks
DREAD
QKD
Layers

ABSTRACT

The Internet of Things (IoT) refers to the distributed systems environment connecting billions of devices to the Internet, and quantum computing is an emerging technology that has a positive impact on IoT security by speeding up data processing while also having a negative impact due to post-quantum security attacks. In this survey, we provide detailed information on the possible post-quantum security attacks that threaten the security of the layers of IoT systems in terms of their vulnerabilities. Also, we provide detailed information on the existing solutions against post-quantum security attacks and show how limitations in these solutions decrease the security performance. Furthermore, we develop classification models to allow the readers to choose the best security approach against post-quantum security attacks in terms of IoT layers. Finally, we show the open challenges of the surveyed quantum security solutions and propose a framework based on quantum machine learning that takes advantage of optical pulses of secure communication as a future solution for detecting post-quantum security attacks.

1. Introduction

The IoT is an emerging networking environment that connects billions of systems securely to the Internet. This significant technology has several advantages, including lower implementation and maintenance costs, simplicity of use, and easy accessibility, since it can be reached anywhere through an internet connection [1,2]. Another emerging technology is called quantum computing, which speeds up the performance of systems, making them perform the execution process of tasks faster. This emerging technology explores the computational power of a system and enhances its performance in terms of data processing [3].

IoT attempts to grantee three main security goals named confidentiality, integrity, and availability. Confidentiality ensures that sensitive data is not shared with unauthorized parties, while integrity prevents data from being altered and availability assures that the systems are available to authorized users [4,5]. To ensure these security goals, IoT utilizes several security protocols, including the IEEE 802.15.4 standard, Constrained Application Protocol (CoAP), and IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN). These protocols are based on different cryptographic techniques. For example, to achieve confidentiality and integrity, these protocols use the Advanced Encryption Standard (AES), and Elliptic Curve Cryptosystems (ECCs), which ensure the integrity and authenticity of a connection for secure keys exchanging among the communicating parties [6].

The recent studies in quantum computing pose a significant threat to the security of IoT systems, as elucidated by the aforementioned protocols. Quantum algorithms, including notable examples like Shor's and Grover's algorithms, the quantum Fourier

* Corresponding author.
E-mail address: s.kumar13@csuohio.edu (S.A.P. Kumar).

https://doi.org/10.1016/j.iot.2024.101132

Available online 20 February 2024
2542-6605/© 2024 Published by Elsevier B.V.

transform, quantum walk algorithms for solving searching problems, and adiabatic quantum algorithms for optimization problems, have demonstrated the ability to efficiently factorize large integer numbers and solve discrete logarithmic problems, accelerating these processes substantially [7]. The emergence of such powerful quantum algorithms raises concerns about the security of current IoT infrastructures. While the timeline for the availability of large-scale quantum computers remains uncertain, some experts argue that recent breakthroughs suggest their arrival within a few years, rendering our existing IoT systems vulnerable [8]. This impending shift could have severe repercussions on the confidentiality, integrity, and overall security of the data utilized in IoT systems. Consequently, fortifying IoT systems against potential quantum attacks becomes imperative to mitigate the security risks.

In this work, we provide a survey of the security issues for the IoT systems in a post-quantum environment in terms of vulnerabilities, post-quantum security attacks, and possible solutions for securing these systems. Thus, the main contributions of this work are as follows:

1. Summarized and identified the most important research works to provide researchers with a comprehensive understanding of the current vulnerabilities of IoT systems in a post-quantum scenario.
2. Illustrated the possible existing post-quantum attacks and demonstrate how they affect the security of the layers of the IoT systems.
3. Utilized the DREAD cybersecurity model to identify the severity of the surveyed post-quantum security attacks, ensuring a systematic and structured evaluation.
4. Provided various solutions and future directions for the current vulnerabilities and quantum attacks that threaten the security of IoT systems.
5. Developed a classification approach to enable the readers to select the best security solution against post-quantum security attacks.
6. Detailed the open challenges and limitations of the surveyed security solutions against post-quantum security attacks.
7. Proposed a Quantum Neural Network (QNN) for detecting post-quantum security attacks.

The remainder of this paper is organized as follows. In Section 2, we provide background information about IoT and quantum computing, describing how the security of IoT can be threatened by quantum technology. Also, we identify the layers of IoT systems in terms of confidentiality, integrity, and availability. Moreover, we detail the quantum computing algorithms that threaten the security of all secure communication technologies, including the IoT. In Section 3, we describe the existing related work in the field of post-quantum security attacks, demonstrating how our proposed survey is unique in terms of describing and clarifying the current existing post-quantum security attacks. In section 4, we illustrate the IoT vulnerabilities that quantum computing can benefit from to launch malicious attacks on IoT systems. In Section 5, we detail all the possible existing post-quantum security attacks on the IoT in terms of its layers. Moreover, we illustrate the attack's limitations and the possible existing solutions to counter these attacks. Furthermore, we identify the limitations of these solutions to enable possible research and enhancements can be conducted to improve the security of IoT systems. In Section 6, we propose classification approach to allow readers to select the optimal security solution against the surveyed post-quantum security attacks according to their research aims. In Section 7, we illustrate the open changes of the surveyed quantum security solutions against post-quantum security attacks on the IoT layers and propose a framework that may enhance the security of the IoT and provide future security defense strategies that will make the IoT more secure. Finally, Section 8 concludes the paper.

2. Background information

This section provides insights about the fields of IoT security and quantum computing, illustrating the intricate interplay between these domains. It delves into the multifaceted landscape of IoT security, addressing its fundamental components and challenges. Simultaneously, it unfolds the transformative potential of quantum computing and the inherent threats posed by quantum algorithms to the security fabric of IoT systems. By navigating the convergence of these fields, this background information sets the stage for a nuanced exploration of post-quantum security attacks, offering a comprehensive understanding of the complex dynamics at the intersection of IoT and quantum computing security.

2.1. IoT security

The IoT describes a future Internet in which people, computing systems, and everyday objects with sensing and actuating capabilities collaborate remarkably and easily. The emergence of IoT allowed novel applications to exist, such as smart cities, intelligent systems, smart homes, smart agriculture, healthcare, and many more. The security of the IoT depends on securing its main layers, which are the application layer, the perception layer, the network layer, and the physical layer [9]. This is because the hardware, software, and connectivity of these layers should all be secured to ensure that the IoT operates efficiently. Without securing these layers, the possibility of cybercrime on IoT systems will increase. Moreover, securing IoT layers ensures the confidentiality, integrity, and authenticity of the data being shared between IoT devices [1].

In a parallel development, quantum computing is emerging and threatening the security of IoT. Here, security means the level of resistance to, or protection of, IoT infrastructure and applications. Many of the machines that are connected to the Internet are insecure and unreliable. Therefore, quantum techniques and properties make it easy for hackers to attack the network layer of these machines or even maliciously utilize them to assault additional devices nearby. Recent studies showed that these quantum algorithms and properties can be integrated with popular security attacks, such as Distributed Denial of Service Attacks (DDoS) to make them more severe [7]. Furthermore, quantum-based security attacks such as quantum insert attacks represent a very harmful threat to the security of communications among IoT systems, such as the systems that use cryptography algorithms [10,11]. However, we should act now to secure IoT layers in a post-quantum world regardless of whether we can predict the arrival time of large-scale quantum computers or not [8]. Therefore, exploring the currently available security solutions will provide the potential for strengthening them or even developing new solutions that are robust against available and future post-quantum attacks.

2.2. Quantum computing

Quantum computing works by performing extensive mathematical calculations according to the object state probability before it is measured, and they are not just 1s or 0s [12]. Therefore, a quantum computer can exponentially process large amounts of data better than classical computers. The process of quantum computing can be illustrated as follows:

1. The operations in quantum computing employ an object quantum state to generate what is known as a qubit (The fundamental unit of information and a quantum particle in a superposition of all conceivable states). These states represent the undefined characteristics of an object before they are observed, such as electrino spin [13].
2. Unmeasured quantum states exist in mixed superpositions. This can be described as the quantum particle's ability to have more than one state at the same time [14].
3. The final result of the superpositions is mathematically related even if we don't understand what they are now. This is because of the superposition and entanglement, meaning that particles can correlate their quantum states with each other [15–17]. If the entangled complex mathematics are placed in an algorithm, a quantum computer will be able to perform tasks in a short time. Unlike classical computers which may take a long time or may not be able to perform them [18].

2.3. Quantum computing algorithms and IoT security threats

There are many works in the quantum computing area to produce high-performance quantum algorithms that can solve complex tasks such as search problems. In this subsection, we describe efficient quantum algorithms that have a great harmful impact on the area of IoT systems security. Shor's algorithm is a quantum computing algorithm that is used to factor a number N to its primes, and this can be done in $O((logN)3)$ time and $O(logN)$ space [19,20]. This algorithm has solved complex factoring problems because it uses public-key cryptography. Shor's algorithm is probabilistic, meaning that it generates the right answer with nearly no failures. This is because the algorithm can repeat itself to minimize the failure rate.

Grover's algorithm, which is a search technique that is used to handle unstructured search problems [21]. Unstructured search means that you are searching among different items to locate an item that has a unique characteristic. The main idea of Grover's algorithm is to utilize quantum superposition and interference to efficiently search an unsorted database. In classical computing, searching an unstructured database of N elements would require $O(N)$, which is a linear time complexity. However, Grover's algorithm may potentially achieve a quadratic run time of approximately $O(\sqrt{N})$. As a recent implementation of Grover's algorithm, [22] applied this algorithm to constrained polynomial binary problems. First, they minimized the number of gates for the portfolio optimization problem, then applied Grover's algorithm to speed up the search process. Eventually, they were able to find the integer coefficients as optimal solutions. Simon's algorithm, which is used to determine the type of an encryption function as a one-to-one or a two-to-one function [23,24]. A one-to-one function $(1:1)$ is used to allocate one unique output to each input (e.g., $f(1)\rightarrow 1$). A two-to-one function $(2:1)$ is used to allocate two unique inputs to each output (e.g., $f(1)\rightarrow 1$ and $f(2)\rightarrow 1$).

In IoT systems, symmetric and asymmetric cryptographic algorithms are used to encrypt and decode data to ensure its confidentiality, integrity, and secrecy. In comparison to asymmetric algorithms, symmetric cryptographic algorithms are more popular and commonly employed because of their minimal overhead properties. Symmetric algorithms have restrictions when it comes to distributing shared keys, making them less safe and trustworthy since malicious attackers can intercept the shared keys. Shor's algorithm, for instance, can efficiently factorize large numbers and solve discrete logarithm problems, making these encryption schemes inefficient. As a result, sensitive data transmitted or stored within IoT systems using these encryption methods can be decrypted and exposed by a quantum computer in a fraction of the time it would take a classical computer [19,20,25,26].

Quantum computing may have the potential to solve this problem by using the Quantum Key Distribution (QKD) technique and the Quantum Key Recycling (QKR). QKD techniques use quantum properties (e.g., entanglement) to encrypt and distribute random and secure keys between the communicating parties. Furthermore, random measurements of the qubits ensure the security of the QKD process as well as the fact that quantum properties prevent a cryptanalyst from collecting any information about the key or qubits [27]. The QKR is an encryption and decryption approach that allows one to reuse encryption keys securely and unconditionally without the need to generate new keys. For example, the QKR technique in [28] is based on an 8-state encoding approach, which means it does not need a quantum computer to perform the encryption and decryption of the message; it only requires a single qubit operation. Researchers are actively working on quantum-resistant cryptographic algorithms and transitioning to quantum cryptographic algorithms is crucial to maintaining the security and privacy of IoT devices and the sensitive data they handle.

The lessons learned in this section provide crucial insights about the IoT security and quantum computing dynamics. Firstly, it stresses the urgency of securing IoT layers to prevent cyber threats, irrespective of large-scale quantum computer arrival predictions. Secondly, it outlines the transformative potential of quantum computing, emphasizing its exponential data processing capabilities through unique qubit properties. Thirdly, it unveils the harmful impact of quantum algorithms on IoT security, particularly encryption schemes. The lessons underscore the vulnerability of current encryption methods to quantum attacks and advocate for the development of quantum-resistant cryptographic algorithms. Lastly, the section highlights the potential of QKD and QKR techniques to bolster IoT security, offering secure communication between devices. This section forms a vital foundation for understanding the challenges and opportunities in securing IoT systems amid quantum advancements.

3. Related work

Many surveys have been introduced in the area of post-quantum security attacks. Almost all of the work that has been introduced so far explores how quantum attacks affect the security of IoT systems. Balogh & Gallo, Chawla & Mehra; Dahhak et al.; Schöffel et al., [29–32] proposed surveys that discuss the challenges and security concerns associated with IoT and blockchain systems, emphasizing the vulnerabilities arising from Open Web Security and Mutual Authentication. The surveys highlight the risks posed by post-quantum security attacks to current IoT security protocols while discussing some quantum-resistant solutions.

Althobaiti & Member; Kumar & Garhwal; Lohachab et al., [4,5,33] presented surveys that explore the intersection of IoT and quantum computing, investigating security measures for a post-quantum IoT environment. Focusing on the security solutions of IoT systems and the security features of networks. The authors identify vulnerabilities in the current IoT architecture. Highlighting the inadequacy of existing security algorithms in the face of quantum advancements. Also, the studies advocate for advanced lattice-driven cryptographic techniques to address the emerging risks and demonstrate their quantum resistance. Moreover, [5,34] explore post-quantum cryptography, addressing non-deterministic QKD protocols, quantum secure direct communication, semi-quantum key distribution, secure multiparty communication, and device-independent cryptography.

Njorbuenwu et al., [35] proposed a survey to explore the dual effects of quantum computers on information security, scrutinizing both positive and negative impacts. The paper addresses concerns about potential negative influences on information security posed by quantum computers. Additionally, the paper briefly highlights recent advancements in developing quantum-resistant standards, contributing valuable insights into the ongoing efforts to mitigate the security implications of quantum computing.

Our proposed post-quantum security attacks on IoT systems survey stands out significantly from the studies conducted by [4,29–31,5,33–35,32]. While these studies fall short in revealing the vulnerabilities and offering detailed insights into post-quantum security attacks on IoT systems, our survey makes substantial contributions in several key areas. Firstly, it provides a comprehensive summary and identification of crucial research works, offering researchers a deep understanding of the existing vulnerabilities in IoT systems within a post-quantum context. Secondly, our survey illustrates various post-quantum attacks and elucidates their impact on different layers of IoT systems, thus enhancing the comprehension of potential threats. Moreover, we utilized the DREAD cybersecurity model to identify the severity of the surveyed post-quantum security attacks, ensuring a systematic and structured evaluation. The proposed survey work goes beyond mere observation by offering solutions and future directions to address current vulnerabilities and quantum attacks that pose security risks to IoT systems. It introduces a classification approach that empowers readers to choose the most effective security solutions against post-quantum security attacks. Additionally, the survey delves into the open challenges and limitations of the surveyed security solutions, providing a nuanced understanding of the field's intricacies. Notably, our survey takes a groundbreaking step by proposing QNN for detecting post-quantum security attacks, showcasing an innovative approach to bolstering IoT system security in the face of quantum threats.

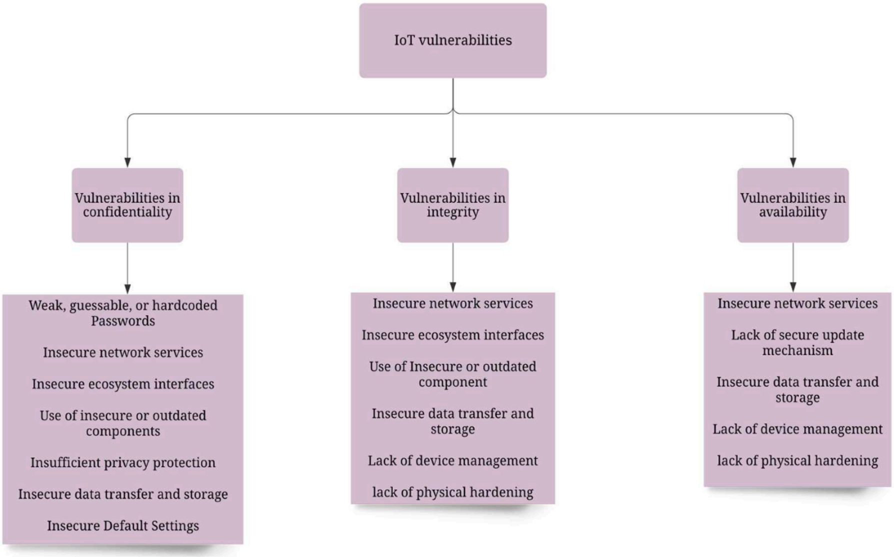
IoT vulnerabilities
Vulnerabilities in confidentiality
Vulnerabilities in integrity
Vulnerabilities in availability
Weak, guessable, or hardcoded Passwords
Insecure network services
Insecure ecosystem interfaces
Use of insecure or outdated components
Insufficient privacy protection
Insecure data transfer and storage
Insecure Default Settings
Insecure network services
Insecure ecosystem interfaces
Use of Insecure or outdated component
Insecure data transfer and storage
Lack of device management
lack of physical hardening
Insecure network services
Lack of secure update mechanism
Insecure data transfer and storage
Lack of device management
lack of physical hardening

Fig. 1. The most common vulnerabilities in IoT services from a post-quantum scenario.

4. Vulnerabilities in IoT systems from a post-quantum perspective

In this section, we discuss the security vulnerabilities of IoT systems from a post-quantum perspective. This severity can be illustrated in two points. First, developing post-quantum secure cryptographic solutions, achieving great efficiency, and generating trust in the security of IoT systems will take years of study by numerous researchers. Thus, it is important to find optimal solutions as soon as possible. Second, changing the cryptographic infrastructure of classical IoT systems to quantum may take a long time [5]. Therefore, finding possible security solutions from the currently available resources will be more effective, while researching to move from a classical cryptographic environment to a quantum environment [35].

As shown in Fig. 1, IoT is one of the most important areas that need to be secured from malicious security threats, especially quantum computing-related threats. However, the current IoT infrastructure suffers from several vulnerabilities in terms of confidentiality, integrity, and availability (Schuld et al., 2017).

One of the major vulnerabilities of classical IoT systems is weak encryption. IoT systems use cryptography algorithms to secure the data that is shared in a communication channel. However, these algorithms have two primary security issues. First, the size of the security key (the number of bits in an encryption key) that is used to encrypt data is small. Second, these algorithms face difficulty in factorizing large prime numbers and handling discrete logarithmic equations. an attacker can employ Shor's factoring technique to interrupt the connection between two communicated parties, and defector the encrypted data to maintain sensitive security information [25,34].

Another common vulnerability is weak or hardcoded passwords. This is due to the use of readily and publicly available credentials as well as backdoors in firmware or client software that allow unauthorized access to the deployed systems. The easiest approach for attackers to access IoT devices and establish large-scale botnets and other malware is to use weak, default, or hardcoded passwords [1]. Password management in a distributed IoT environment is time-consuming and challenging and the attackers can make use of this vulnerability. Unnecessary network services operating on the device itself, particularly those connected to the Internet can threaten the confidentiality, integrity, or availability of information or allow unwanted remote control. Malicious Intruders are attempting to hack and breach sensitive or secret information transmitted between the device and a server by finding bugs in the communication protocol and services operating on IoT devices [10]. Man-in-the-Middle (MITM) attacks try to take advantage of these bugs to steal the credentials used to authenticate these endpoints and use them to conduct larger-scale security attacks.

Insecure ecosystem interfaces are insecure websites, backend API, cloud, or mobile interfaces in the ecosystem that facilitate the compromising of the device or its linked components. Lack of authentication or authorization, poor encryption, and poor input and output are all common problems [1]. Lack of secure update mechanisms includes weak firmware validation on the device, insecure delivery (data is sent unencrypted), lack of anti-rollback procedures, and poor alerts of security changes due to upgrades. Unauthorized software and firmware updates are a common way for hackers to capture IoT devices [1,4]. A hacked update can cause important IoT devices to stop working and have tangible effects in the industries, such as healthcare and energy.

The use of insecure or outdated components associated with the use of out-of-date or insecure software components or libraries may allow the device to be hacked. This includes unsafe operating system platform customizations, as well as the usage of software or hardware components from a corrupted supply chain [35]. Designers who build IoT devices using outdated or risky software, including open-source components, create complex security problems that are hard to trace. These components may have vulnerabilities that are known to attackers, resulting in a larger danger landscape that is ready to be exploited [4]. Due to insecure data transfer and storage, sensitive data (during processing or in transit) suffer from weak encryption and lack of access control. Thus, making it an easy target for different kinds of security attacks.

Lack of device management is another weakness in securing IoT devices, as these supports include asset management, update management, secure decommissioning, systems controlling, and response features [35]. Managing all devices throughout their lifespan is one of the most crucial activities to address the security concerns in the IoT platform. Unauthorized devices will be able to obtain access to business networks and intercept sensitive information [1]. Another common vulnerability is the lack of physical hardening. IoT devices are used in distributed and remote locations, where they are exposed to the field to carry out their tasks [1]. Attackers can interrupt the services provided by IoT devices by obtaining access to their physical layers. However, the lack of essential security built-in mechanisms in IoT devices makes them vulnerable to different kind of security attacks that treats the physical layer.

As discussed, vulnerabilities such as weak or hardcoded passwords, insecure data transfer and storage, insecure ecosystem interfaces, and lack of physical hardening are being used by quantum computing to launch security attacks on IoT services in a post-quantum environment. Moreover, these vulnerabilities are found in the asymmetric and symmetric cryptography techniques (e.g.,

Table 1
Common vulnerabilities in the security of IoT systems.

Vulnerabilities	Security issues	Malicious quantum techniques
Weak or hardcoded passwords. Insecure data transfer and storage. Insecure ecosystem interfaces. lack of physical hardening	The use of readily and publicly available credentials. Weak encryption and lack of access control. Lack of authentication, and poor input and output. Unsecure physical layers.	Quantum brute force attack and quantum key recovery attack.
Unnecessary network services. The lack of a secure update mechanism. The use of insecure or outdated components. The lack of device management	Weak credentials and inefficient input-data validation. Using unsafe libraries that allow the system to be hacked	Quantum key recovery attack
Weak Encryption	Insufficient key size and difficulty in factorizing large numbers	Shor's algorithm

AES) that secure different IoT services [36,35,37]. Attackers using quantum computing can also benefit from vulnerabilities such as unnecessary network services, the lack of a secure update mechanism, the use of insecure or outdated components, and the lack of device management vulnerabilities to capture sensitive information and harm classical systems. Furthermore, attackers can launch quantum key recovery attacks on IoT systems that suffer from the above vulnerabilities to harm them [38]. Table 1 shows the Common Vulnerabilities in the Security of IoT Systems.

The lessons learned in this section provide crucial insights about the vulnerabilities of IoT systems in a post-quantum context. Firstly, it stresses the time-intensive nature of developing post-quantum secure cryptographic solutions and the prolonged transition to quantum cryptographic infrastructure. Urgency is emphasized, urging the need for effective security solutions using existing resources. Fig. 1 outlines the prevalent vulnerabilities in IoT services from a post-quantum perspective, highlighting major issues like weak encryption, passwords, insecure interfaces, and more. These vulnerabilities are exploited by quantum computing, posing threats to both asymmetric and symmetric cryptography techniques. quantum key recovery attacks are identified as potential exploits for the identified vulnerabilities in IoT systems. In essence, this section underscores the critical need for proactive measures to address vulnerabilities in the post-quantum landscape.

5. Post-quantum security attacks on IoT layers

In this section, we will investigate the possible post-quantum attacks on IoT systems in terms of IoT layers. The IoT has four main layers, namely the application layer, perception layer, network layer, and physical layer [9]. The application layer contains the services and applications aspects of the IoT platform. Smart cities, smart homes, smart transportation, and smart healthcare IoT systems are good examples of popular IoT applications. The perception layer is the layer that contains sensor technologies, such as pressure sensors, temperature sensors, etc. The network layer describes the communication protocols and networking topologies that are used by the IoT systems. The main role of the network layer is to transmit data between communicating parties. The physical layer encompasses the fundamental hardware physical systems for supporting the networking of smart objects [9].

In the proposed survey, we employed the DREAD cybersecurity model as a comprehensive framework to assess and prioritize the various post-quantum security attacks that were investigated. The DREAD cybersecurity model is a framework designed to assess and prioritize potential security risks in software development [39–41]. It consists of five key elements, each representing a different aspect of the security threat landscape. These elements are Damage, Reproducibility, Exploitability, Affected Users, and Discoverability. Damage refers to the potential harm that could result from a security breach, while Reproducibility assesses how easily an attacker can replicate the exploit. Exploitability gauges the level of difficulty involved in carrying out the attack, while Affected Users consider the scope and impact on end-users. Discoverability focuses on how likely it is that the vulnerability will be found. By systematically evaluating these factors, the DREAD model helps organizations prioritize and address security vulnerabilities based on their potential severity and impact. By incorporating DREAD model, we contribute to a more robust understanding of the severity levels associated with post-quantum security threats aligning with the reviewer's valuable suggestion.

Table 2 illustrates the five criteria of the DREAD cybersecurity model for assessing post-quantum security attacks. The attack rating column indicates the severity based on the sum of scores from damage, reproducibility, exploitability, affected users, and discoverability. The categories include Critical (40–50), high (25–39), medium (11–24), and low (1–10), guiding the urgency for addressing vulnerabilities. High suggests a need for prompt review and resolution, medium indicates a moderate risk after addressing severe and critical risks, while low denotes a low risk to infrastructure and data. This provides a concise yet structured approach for prioritizing and addressing post-quantum security threats.

5.1. Physical layer attacks and solutions

As shown in Fig. 2 and Table 3, there are five quantum physical attacks on IoT devices, namely node tampering attacks, code injection, code injection, brute force attacks, and quantum attacks based on the HHL and QKD techniques. Node tampering is a security

Table 2
DREAD cybersecurity model.

Damage	Reproducibility	Exploitability	Affected users	Discoverability	Attack rating
0: No damage	0: Difficult or impossible	2.5: Advanced programming and networking skills	0: No users	0: Hard to discover the vulnerability	Critical (40–50): Critical vulnerability; address immediately
5: Information disclosure	5: Complex	5: Available attack tools	2.5: Individual user	5: HTTP requests can uncover the vulnerability	High (25–39): Severe vulnerability; consider for review and resolution soon.
8: Non-sensitive data compromised related to individuals or employer	7.5: Easy	9: Web application proxies	6: Few users	8: Vulnerability found in the public domain	Medium (11–24): Moderate risk; review after addressing severe and critical risks.
9: Non-sensitive administrative data compromised	10: Very easy	10: Web browser	8:Administrative users 10: All users	10: Vulnerability found in web address bar or form	Low (1–10): Low risk to infrastructure and data.
10: Destruction of an information system					

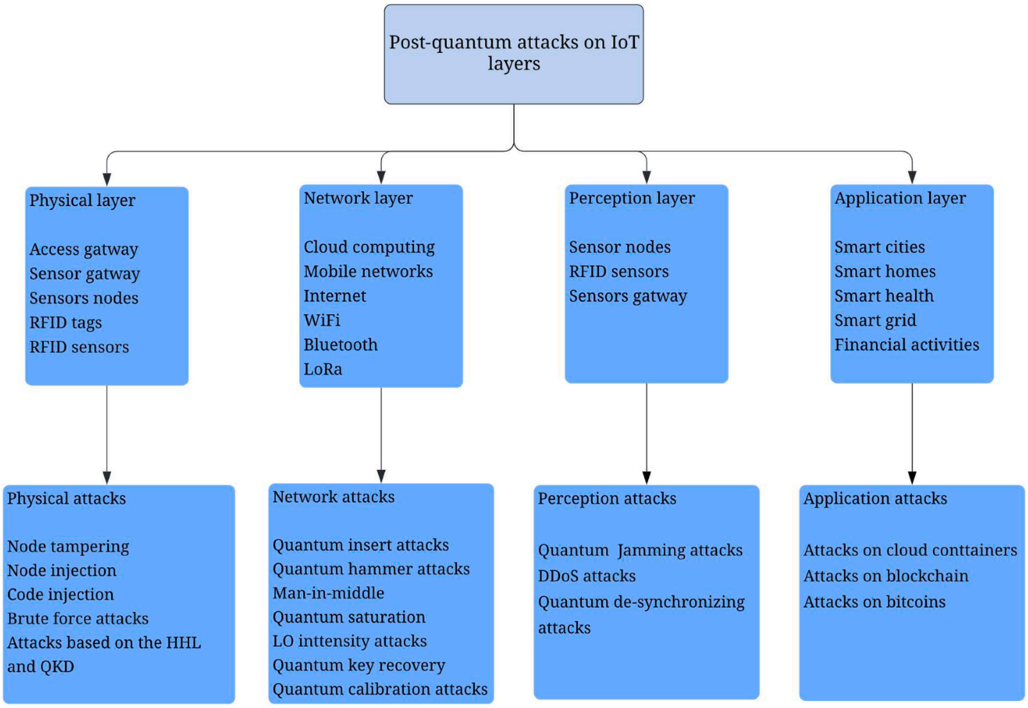

Fig. 2. Post-quantum security attacks.

attack that requires physical access to IoT devices. The attacker's goal is to capture sensitive information such as the encryption key that communicates nodes with each other. The quantum version of this attack uses Shor's algorithm to break up the physical security defenses and capture the encryption key by solving the factorization and generating physical access to the source code of the communication [19,42]. This problem can be solved using the Trusted Platform Modules (TPM), which are security chips installed on an IoT device near the CPU. This chip is mainly used for cryptographic operations, such as creating and storing security keys. Thus, TPM provides security defenses against all kinds of security attacks including post-quantum attacks [43].

Node injection is an attack that causes collisions in a network. In this attack, the cybercriminal has to gather specific data about the node to be attacked, such as the encryption key. The attack works by creating a copy of the attacked node [44]. This malicious node has the features of an authorized node, but it has malicious properties. The malicious node creates another copy and when an authorized node is requested, this node perform collision on the network to block the network packets. There is no quantum enhancement on this attack, but attackers can benefit from quantum brute force attacks based on Grover's algorithm to easily obtain encryption keys and generate node injection attacks [35].

Brute force is a security attack that is used to find sensitive information such as passwords and encryption keys. A quantum brute force attack is based on Grover's search algorithm, which allows attackers to factorize complex encryption keys in terms of quadratic factors [45]. Here, Grover's algorithm allows attackers to search for the right key encryption pattern in $O(\sqrt{N})$.

Asymmetric and symmetric cryptographic techniques that secure different IoT services [34,46] are vulnerable to these kinds of attacks. For example, as shown in Fig. 3, a cryptographic technique such as Advanced Encryption Standard (AES) utilizes a secret key of length 128 named AES-128 to encrypt data in a communication channel. However, a cipher criminal uses the quantum Grover's algorithm to generate a brute force search attack to capture the secret key. Thus, the communication can be altered and harmed. Here, Grover's algorithm is used to speed up the search process [36]. However, this attack can be countered using QKD and QKR encryption methods.

Code injection is a security attack that controls a large number of IoT systems to harm the IT infrastructure by launching generating DDoS attacks [29]. The quantum version of this attack is called quantum SQL injection. (Schuld et al., 2017) developed a quantum SQL injection attack called Malware Photon Injection Attack (MPIA). This attack is based on the quantum entanglement property and the classical SQL injection attack. The attacker injects the quantum communication channel (the database) with a malware photon (malicious code). As a result, the attacker can perform entanglement measurement on this code to harm and disclose the communication channel of the receivers and take complete control of the network. Furthermore, this attack can be seen as a sleep deprivation attack that targets the battery life of IoT devices. As a result, the devices rapidly run out of battery and turn off permanently. This attack can be countered using the Address Space Layout Randomization (ASLR) technique. However, this approach cannot be implemented by IoT devices with low-power batteries since it is an energy-intensive option [10].

Liu & Gao, [47] developed a quantum algorithm based on the HHL algorithm to attack the Grain-128 and Grain-128a stream ciphers. The attack is based on solving a nonlinear system of equations, which makes it very efficient in finding the location and length

Table 3
Post-quantum security attacks on the physical layer of IoT devices.

Authors	Attacks	Descriptions	IoT vulnerabilities	Tools to perform the attacks	Solutions	Limitations of the solutions
[42]	Quantum tampering	Break up the physical security defenses and capture the encryption key	Lack the essential security built-in to protect against attacks	Qiskit	TPM	Qubit decoherence due to the surrounding environment
[45]	Quantum brute force	Sometimes this attack fails to factorize large-sized security keys	Weak or hardcoded passwords. Insecure data transfer and storage. Insecure ecosystem interfaces	Matlab	QKD and QKR	Sometimes the distribution results in small-sized unsecured symmetric keys.
(Schuld et al., 2017)	MPIA	Based on the quantum entanglement property and the classical SQL injection attack	Default or weak encryption of the security of databases	Python	ASLR	Unusual forms of the photon may not be exposed by the solution
[47]	Quantum attacks based on the HHL algorithm	A quantum attack based on the HHL algorithm to attack the Grain-128 and Grain-128a stream ciphers	Default or weak encryption of the security of physical devices	N/A	Grain-128 and Grain-128a encryption algorithms	Sometimes the Grain-128 and Grain-128a algorithms generate small-sized security keys, which makes them easy to attack.
[48]	Quantum attacks based on the QKD	Injects malicious signals into the optical fiber of an optical network	Insecure data transfer and techniques. Insecure ecosystem interfaces	Real-world emulation of quantum parameters through a three dB coupler	Quantum seals	The transistors and receivers are limited to measuring a single photon at a time

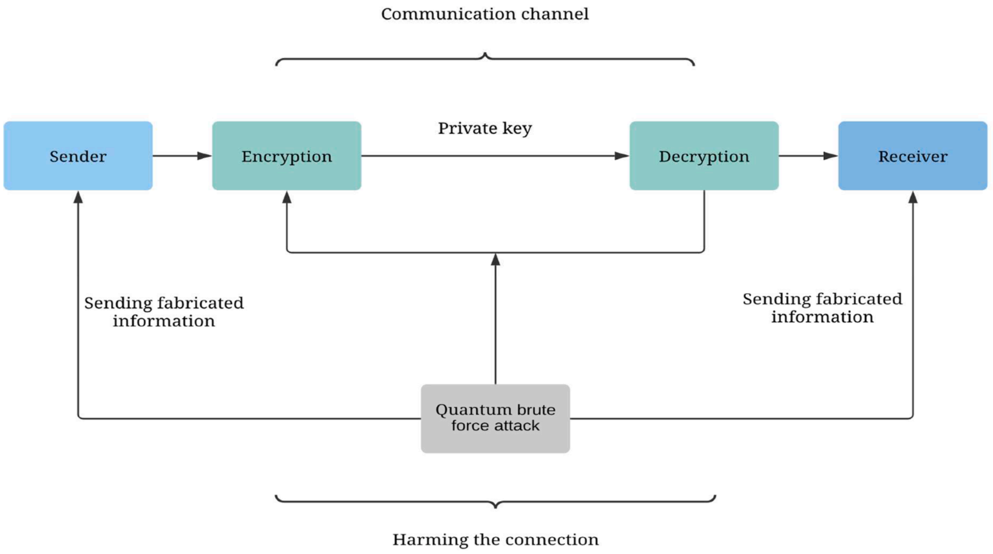

Fig. 3. Quantum Brute Force Attack.

of plaintext and ciphertext pairs. However, the complexity of the proposed algorithm is correlated with the length of plaintext and ciphertext pairs, and even if there is not enough length, the algorithm works efficiently. This attack is limited to finding the keystream segment that makes up the security key, which means that one cannot employ a quantum state to restore that key.

Hugues-Salas et al., [48] proposed a quantum attack based on the QKD technique for attacking the physical layer of optical networks. The attack directly targets the optical links of the physical layer by injecting harmful signals directly into the optical fiber, therefore harming the distribution of symmetric keys between communicating parties. Humble [49] utilized the quantum seals as a unique security solution against the proposed attack. The goal of the quantum seals approach is to verify the integrity and authenticity of a communication medium and secure the physical layer. Moreover, the approach provides a quantum optical encoding technique used at the sender and tests for nonlocality at the receiver to make sure that there is no injection of malicious signals into the optical fiber. However, the solution is insufficient for long-term monitoring of the data transmitted over the physical layer because the transistors and receivers measure only a single quantum state at a time or require weak light pulses.

Table 3 shows the existing solutions to the quantum-related attacks on the IoT physical layer. However, these solutions have drawbacks that limit their performance against quantum threats. For example, the solution in [43] does not successfully capture the quantum attacks in [42], which results in qubit decoherence [50]. In addition, the solutions in [27,47] may generate small-sized encryption keys, which makes them vulnerable to attacks in [45,47]. Moreover, the solution in [10] cannot expose all the forms of a photon (qubit states) that attempt to break up the security of a physical layer (Schuld et al., 2017). Furthermore, the solution in [49] suffers from weak transistors and receivers that handle only a single photon at a time and cannot handle multiple photons launched by the attack in [48]. Table 4 shows the severity of the attacks discussed in Table 3 based on the DREAD model. The quantum brute force attack has a rating of 42.5, making it the most critical attack in Table 4.

5.2. Network layer attacks and solutions

Fig. 2 and Table 5 show quantum-based network attacks on IoT devices, namely quantum insert attacks, quantum key recovery attacks, quantum man-in-middle attacks, quantum saturation attacks, the Local Oscillator (LO) intensity attack, and the quantum calibration attack. A quantum insert attack (HTML redirection attack) is designed to harm communication protocols such as the TCP protocol. Here, the attacker injects malicious content into a certain TCP session, that is selected based on a specific selector (e.g., tracking cookies that identify the appearance of users for a long time) to maintain control over the entire network [11].

Fig. 4 shows how the quantum insert attack captures the control of a TCP communication session. To perform the attack, the attacker must have three pieces of information, the IP addresses of the source and the destination, the port number of the source and

Table 4
DREAD model for the physical layer attacks.

Attack	Damage	Reproducibility	Exploitability	Affected users	Discoverability	Attack rating
Quantum tampering	5	5	2.5	8	8	High (28.5)
Quantum brute force	10	7.5	5	10	10	Critical (42.5)
MPIA	5	5	2.5	6	0	Medium (18.5)
Quantum attacks based on the HHL algorithm	8	5	5	8	5	High (31)
Quantum attacks based on the QKD	10	5	2.5	10	8	High (35.5)

Table 5
Quantum security attacks on the network layer of IoT devices.

Authors	Attacks	Descriptions	IoT vulnerabilities	Tools to perform the attacks	Solutions	Limitations of the solutions
[11]	Quantum Insert	The real and inflected packets have the same sequence number. The TTL value for the infected packet is sooner than the TTL value of the real one	Insufficient session keys in the communication area that has a high traffic flow	Matlab	Packet analysis based on the sequence number and TTL value.	Sometimes the solution fails to capture the sequence number of the malicious packet
[46]	Quantum key recovery	Combine two quantum algorithms called Shor's and Simon's algorithms to harm a secure communication channel	Weak credentials and inefficient input-data validation. Using unsafe encryption libraries	N/A	QKD	Sometimes the solution generates insecure symmetric keys
[53]	Quantum man-in-the-middle	The attacker tries to utilize quantum entanglement to capture the gateway packet to know the nodes associated with it	Weak authentication techniques	Solidity	Post-quantum end-to-end encryption	Cannot counter quantum attacks that are performed using more than two qubits
[54]	Quantum saturation	An active side-channel attack that affects the Gaussian-modulated coherent state of the CVQKD protocol	Insufficient mathematical encryption equations	Numerical simulation	The radical post-selection and the Gaussian post-selection techniques	Allows Eve to know which data is post-selected and which one is not. High complexity
[11]	Quantum LO intensity	Enables Eve to attack the signal beam of the data transmitted over a network	Insufficient session keys in the communication area that has a high traffic flow	Matlab	Machine learning approach based on the neural network	High complexity. The performance is sensitive to the number of neurons in the hidden layer.
[55]	Quantum calibration attack	This attack allows Eve to intercept a part of the quantum measurements by utilizing a PIR attack and modifies the structure of the LO pulses	Weak authentication techniques	Matlab	Machine learning approach based on the neural network	High complexity. The performance is sensitive to the number of neurons in the hidden layer.

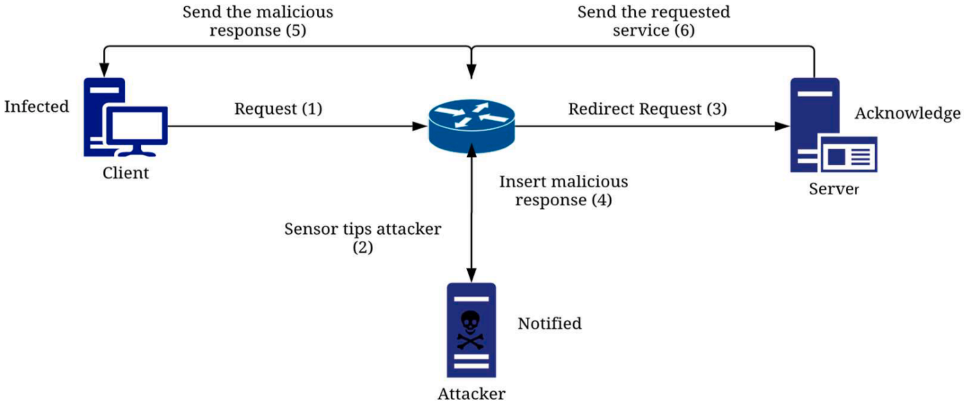

Fig. 4. Quantum insert attack.

destination, and the sequences and acknowledgments numbers [11]. The injection is carried out by listening to the network traffic and watching HTTP requests. Another device, the attacker, is tipped to send a faked TCP packet when an intriguing destination is detected. For the attack to succeed, the attacker's injected packet has to arrive at the destination before the acknowledgment of the server. This is only possible by using the entanglement property to find the speed difference or race condition, which allows the malicious packet to arrive faster [10]. This attack can be countered by analyzing the packets in response to a request for a specific service from the destination. One packet will have the real response, and the other one will have the malicious data, but both of them will have the same sequence number, which helps to expose the quantum insert attack. Also, this attack can be countered using the Time To Live of the packets (TTL). The TTL of the infected packet will always be sooner than the TTL of the real packet [11,23].

Quantum Key Recovery attacks combine two quantum algorithms called Shor's and Simon's algorithms to harm a secure communication channel. In terms of information security, a cryptography algorithm secures a connection between two communicating parties by using an encryption function that encrypts the shared data using a hidden string (security key). Here, a quantum key recovery attack uses Simon's algorithm to determine the type of the encryption function, and then Shor's algorithm is used to factor the hidden string of the encryption key to capture the connection and harm IoT systems [46,51].

Fig. 5 shows the quantum circuit of the quantum key recovery attack [16,52]. For example, suppose we have a connection that is encrypted using a security key with a string $b = 11$. A quantum key recovery attack can capture this string as follows:

1. Two qubit registers are initialized to the zero state ($|0\rangle$).

$$|\psi_1\rangle = |00\rangle_1 .$$

$$|\psi_2\rangle = |00\rangle_2 .$$

2. Apply Hadamard gates to the qubit for the first register.

$$\Big|\psi_2\rangle = \frac{1}{2}\left(|00\rangle_1 + |01\rangle_1 + |10\rangle_1 + |11\rangle_1\right) |00\rangle_2.$$

3. The Query function (Qf) for $b = 11$ can be initialized as follows:

$$Qf = \frac{1}{2}(|00\rangle_1|0 \oplus 0 \oplus 0,\ 0 \oplus 0 \oplus 0\rangle_2 + |01\rangle_1|0 \oplus 0 \oplus 0,\ 0 \oplus 0 \oplus 1\rangle_2$$
$$+|10\rangle_1|0 \oplus 1 \oplus 0,\ 0 \oplus 1 \oplus 0\rangle_2 + |11\rangle_1|0 \oplus 1 \oplus 0 = 1,\ 0 \oplus 1 \oplus 1\rangle_2$$

Therefore, $= \frac{1}{2}(|00\rangle_1|00\rangle_2 + |01\rangle_1|11\rangle_2 + |10\rangle_1|11\rangle_2 + |11\rangle_1|00\rangle_2$. However, this indicates that Qf is a two-to-one function, then we will factor the register states that are measured in the connection to find b.

1. Now we will estimate register two with a 50 % probability. We can begin randomly with any state, so for this example, we will begin with $|11\rangle_1$. The system state will be as follows.

$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle_1 + |10\rangle_1)$. We will remove register two since is estimated and does not include $|11\rangle_2$.

1. Apply Hadamard gate to the first register.

$$|\psi_4\rangle = \frac{1}{2\sqrt{2}}[(|0\rangle + |0\rangle) \otimes (|0\rangle - |1\rangle) + (|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle)]$$

$$|\psi_4\rangle = \frac{1}{2\sqrt{2}}[|00\rangle - |01\rangle + |10\rangle - |11\rangle + |00\rangle + |01\rangle - |10\rangle - |11\rangle]$$

$$|\psi_4\rangle = \frac{1}{2\sqrt{2}}(|00\rangle - |11\rangle)$$

2. After we measured the first register, we can conclude that $b = 11$ or $b = 00$. To ensure that $b = 11$ we take a random value measured by the second register value and plug it in Qf. $01 \oplus b = 10,\ Qf(01) = Qf(10) = 11,$ then we will see that $b = 11$.

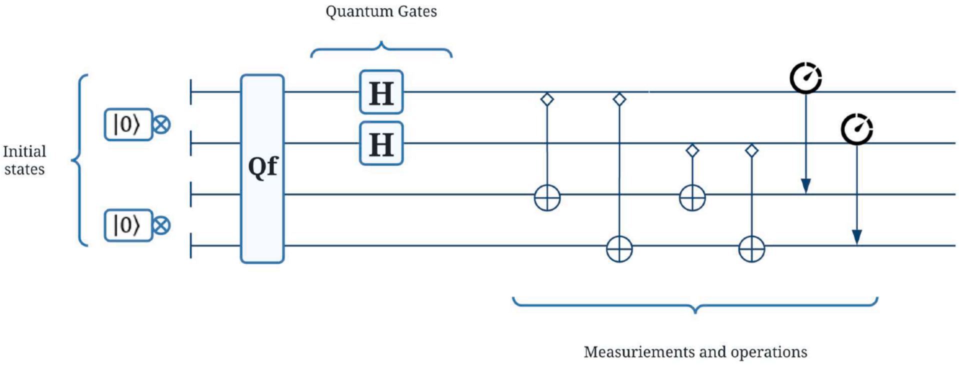

Fig. 5. Quantum key recovery attack circuit.

Karbasi & Shahpasand, [53] proposed the quantum man-in-middle attack against secure network sessions such as secure sessions in cryptocurrency networks. The quantum version of this attack is based on the IP/ARP poisoning attack. Here, the attacker tries to utilize quantum entanglement to capture the gateway packet to know the nodes associated with it. Finding the victim and the gateway IP addresses, allows the attacker to send an ARP reply to the victim notifying that the gateway MAC address is now the attacker's MAC address. This results in hacking the secure session and arming the communication. This attack can be countered using a post-quantum end-to-end encryption solution provided by [53]. The solution uses the Inter-Planetary File System (IPFS) and Ethereum contracts to provide secure session keys for end-to-end encryption.

Qin et al., [54] proposed a quantum saturation attack on the Continuous-Variable Quantum Key Distribution (CVQKD) technique. This attack is an active side-channel attack that affects the Gaussian-modulated coherent state of the CVQKD protocol. On the receiver side, the attack combines an intercept-resend attack with an induced saturation of the homodyne detection to harm a secure communication channel. This attack, on the other hand, can be mitigated by using the radical post-selection and Gaussian post-selection solutions [54]. The radical post-selection technique post-selects the quadrature measurement results that lie within a confidence interval, where the homodyne detection is known to be linear. The problem with this solution is that it gives Eve (the attacker) the ability to control the displacement value, which allows it to know which data is post-selected and which one is not. This means that no security is provided across the communication channel. However, as an improvement to the radical post-selection solution, Gaussian post-selection was developed to solve this problem. The idea is to perform a Gaussian post-selection of the measurement results rather than control the displacement value, which will ensure security in the communication channel [54]. The problem of the Gaussian post-selection solution is that it has a high complexity, which makes it difficult to perform.

Mao, et al., [11] proposed the LO intensity attack on the CVQKD and a machine learning approach for detecting this attack. This attack enables Eve to attack the signal beam of the data transmitted over a network using a general Gaussian collective attack and the LO beam using a non-changing phase intensity attenuator with an attenuation coefficient r $(0 < r < 1)$. Therefore, Eve can capture the quantum measurements (the session security keys) estimated by Alice and Bob to harm the communication channel. To counter the LO intensity attack, [11] developed a machine learning solution based on the neural network that classifies and detects the malicious signal and LO pulses of a network to expose this attack. The solution has an efficient performance, it achieved 99 % recall and precision values.

Ma et al., [55] presented the quantum calibration attack on the CVQKD. This attack allows Eve to intercept a part of the quantum measurements by utilizing a Partial Intercept-Resend (PIR) attack and modifies the structure of the LO pulses. This results in controlling the network communication medium among the communicated parties and harms the sensitive shared data.

Table 5 describes the solutions to the existing post-quantum security attacks on the IoT network layer. However, these solutions have gaps that limit their performance against quantum threats. For example, the solution in [11,23] is not accurate in capturing the sequence number of the malicious packet to counter the attack in [11]. Also, the solutions in [27] may generate small-sized symmetric security keys that are easily breakable by the attacks in [46]. In addition, the solution in [53] is not able to counter quantum security threats that use more than two qubits to launch an attack. Moreover, the solution in [54] can expose the security quantum measurements between Alice and Bob to Eve, and it is hard to implement due to its complex computations. Furthermore, the solutions in [11] are sensitive to the number of neurons that are used to detect the attacks in [11,55], such that if the number of neurons is insufficient, the solution is not accurate. Table 6 shows the severity of the attacks discussed in Table 5 based on the DREAD model. The quantum man-in-the-middle attack has a rating of 46.5, making it the most critical attack in Table 6.

5.3. Perception layer attacks and solutions

As seen in Fig. 2 and Table 7 the quantum attacks on the perception layer include jamming attacks, DDoS attacks, and quantum desynchronizing attacks. desynchronizing attacks such as quantum faked state attack and quantum trojan hours attacks. Makarov & Hjelme, [56] proposed the quantum faked state attack that enables Eve to generate false states or pulses of light, which are incorporated into the communication between Alice and Bob. What makes this attack particularly insidious is that, despite the introduction of these faked states by Eve, there is a subtlety in the method employed the error rate, a potential indicator of compromise, remains unaltered. This strategic manipulation by Eve conceals the presence of the attack, making it challenging for Alice and Bob to detect any anomaly during the quantum key distribution process, thereby heightening the sophistication and evasiveness of the adversarial maneuver.

Lucamarini et al., [57] proposed quantum trojan horse attack scenario, Eve attacks the communication between Alice and Bob by injecting a high-intensity light pulse containing trojan photons into the optical fiber. This pulse is targeted at the user initiating the

Table 6
DREAD model for the network layer attacks.

Attack	Damage	Reproducibility	Exploitability	Affected users	Discoverability	Attack rating
Quantum Insert	9	5	2.5	10	5	High (31.5)
Quantum key recovery	8	5	2.5	6	8	High (29.5)
Quantum man-in-the-middle	10	7.5	9	10	10	Critical (46.5)
Quantum saturation	5	5	2.5	6	0	Medium (18.5)
Quantum LO intensity	5	0	2.5	8	8	Medium (23.5)
Quantum calibration attack	5	0	2.5	8	8	Medium (23.5)

Table 7
Quantum security attacks on the perception layer of IoT devices.

Authors	Attacks	Descriptions	IoT vulnerability	Tools to perform the attacks	Solutions	Limitations of the solutions
[56]	Quantum faked state attack	Enables Eve to generate false states or pulses of light, which are incorporated into the communication channel	Heterogeneous integration technology	Python	QKD	Sometimes the solution generates insecure symmetric keys
[57]	Quantum trojan horse	Infiltrates the communication by injecting a high-intensity light pulse containing trojan photons into the optical fiber	Weak authentication techniques	Python	QKD	Sometimes the solution generates insecure symmetric keys
[59]	Quantum jamming	Attacks aim to crash the communication medium by sending many requests to the server or alternating in the communication to block responses to reach the destination	Insufficient session keys in the communication area that has a high traffic flow	Optisystem software	Channel hopping and Frequency hopping.	In WSN, more than 10 unsuccessful attempts to capture a jammer attack results in qubit decoherence
[33]	Quantum desynchronizing	The idea of this attack is to block the communication medium between the communicating parties	Heterogeneous integration technology	N/A	spread-spectrum variants, lower duty cycle, and message prioritizing	N/A
[60]	Quantum DDoS attack	Sends malicious qubits that can be in a superposition state to harm the perception layers	Insufficient session keys in the communication area that has a high traffic flow	Mininet	Security quantum-inspired ensemble model	No real implementation of the solution in a quantum environment.

photon transmission for encryption key distribution, i.e., Alice. While Alice is encoding her photons to transfer information to Bob, she unwittingly encodes Eve's photons simultaneously, as she remains unaware of the ongoing attack. The quantum trojan photons, reflected from elements on Alice's side, travel through the optical fiber toward Bob. Eve intercepts the Trojan photons upon their arrival from Alic side. Despite Alice knowledge of her photon initial state, Eve can determine the information encoded by Alice in this covert attack.

Jamming attacks usually happen in the perception layer, such as Wireless Sensor Networks (WSN). These attacks crash the communication medium by sending many requests to the server or alternating in the communication to block responses to reach the destination [58,59]. The quantum version of this attack uses the entanglement property between the qubits that are sent to alter the communication and listen to the traffic. The entanglement property allows each entangled pair of qubits to correlate their output states. These outputs are the measurements for finding the encryption key among the communication channels. This results in, speeding up the process of capturing the encryption key, which allows attackers to send an extensive number of requests to the server to harm the communication channel [15].

Lohachab et al., [33] proposed a survey about the major threats and challenges of the IoT in a post-quantum world. In this survey, the author proposed a jamming attack against the perception layers of IoT devices called the quantum desynchronizing attack. This attack sends malicious entangled qubits to block the communication medium between the communicating parties, which results in harming the WSNs and making them unable to send or receive data.

Saritha et al., [60] developed a security quantum-inspired ensemble model to detect the quantum DDoS attack at the perception layers of IoT devices. The quantum DDoS attack works as the classical DDoS attack, but the difference is that the quantum version of this attack sends malicious qubits that can be in a superposition state. This results in sending an autonomous number of malicious data that cannot be handled by the perceptions, which makes them unable to send or receive data and blocks their secure connection. The proposed security solution countermeasures the quantum DDoS attack at two levels. First, it utilizes a quantum protocol to address the secured communication at the data plane, then a machine learning-inspired ensemble classifier is devised to detect DDoS attack traffic at the control plane.

As shown in Table 7, there are critical drawbacks that limit the performance of current solutions against quantum security attacks

Table 8
DREAD model for the perception layer attacks.

Attack	Damage	Reproducibility	Exploitability	Affected users	Discoverability	Attack rating
Quantum faked state attack	5	0	2.5	6	0	Medium (13.5)
Quantum jamming	10	5	2.5	10	5	High (32.5)
Quantum trojan horse	10	7	5	10	5	High (37)
Quantum desynchronizing	5	0	2.5	6	5	Medium (18.5)
Quantum DDoS	9	7.5	5	8	5	High (29.5)

on the perception. In [60], the solutions are not implemented in a real quantum environment and have complicated computations. Moreover, the solutions in [59] suffer from an insufficient correlation between the entangled qubits due to bad correcting techniques, which results in qubit decoherence [50]. Table 8 shows the severity of the attacks discussed in Table 7 based on the DREAD model. The quantum trojan horse attack has a rating of 37, making it the most critical attack in Table 8.

5.4. Application layer attacks and solutions

As seen in Fig. 2 and Table 9 the quantum attacks on the application layer include security attacks on bitcoins, security attacks on cloud containers, and security attacks on blockchain (Quantum state attacks). Aggarwal et al., [61] presented the quantum attacks on bitcoins. These attacks target the Elliptic Curve Digital Signature (ECDS) algorithm that is used to secure the transactions of bitcoins. The attack works by implementing Shor's algorithm to capture the private key of a public key, which is broadcast to a specific network address by the ECDS algorithm. Therefore, a cybercriminal can employ the private key to broadcast a new transaction from the same address to his address. This results in stealing all the bitcoins of the original address. However, this attack can be countered using post-quantum end-to-end encryption [53].

Jain et al., [62] proposed a quantum laser damage attack that enables an attacker to manipulate optical pulses directed toward the communication channel. By causing damage to the avalanche photodiode of the detector, the attacker exploits a loophole that can harm the ECDS algorithm. The eavesdropper executes an attack that harms the error rate, but the total error rate remains unchanged after detector damage. The attack can exploit not only detector loopholes but also vulnerabilities in other elements on the legitimate user's side. However, this attack can be countered using post-quantum end-to-end encryption [53].

Mus et al., [63] proposed the quantum hammer attack, which is an encryption attack that combines a bit-tracing attack enabled through rowhammer fault injection and a divide and conquer attack. The attack uses the rowhammer bit-tracing to gather the bits of the secret keys and integrates the divide and conquer technique to speed up this process. The quantum version of the divide and conquer technique discovers the structure in the key generation and solves the equations systems of the secret keys more efficiently, making it suitable for harming the ECDS algorithm. This attack can be solved using the QKR technique that utilizes the 8-state encoding, which will generate secure encryption keys and allow them to be reused during the connection [28].

Kelley et al., [64] presented quantum attacks on the cloud container platforms, and a quantum solution framework to counter these attacks. The idea of these quantum threats (e.g., DDoS) is to attack the host among independent containers to capture the root of the container Daemon. This may enable attackers to have root access into the host kernel thereby disclosing the entire system. Therefore, one may launch a DDoS attack on other user applications, or harm services of other applications. To counter these quantum attacks on the containers, [64] developed a quantum network security protocol that utilizes a secure quantum channel that works on a use-once-only policy (only when an application requires root privileges), so the key quantum information cannot be regenerated without detection.

Gao et al., [65] developed a quantum blockchain scheme to optimize the security of blockchain in the IoT world. The proposed security approach works by using the entanglement property and the Delegated Proof of Stake (DPoS) to provide secure keys and quantum coins for securing different blockchain operations in the IoT platforms. However, the author tested the performance of the

Table 9
Quantum security attacks on the application layer of IoT devices.

Authors	Attacks	Descriptions	IoT vulnerability	Tools to perform the attacks	Solutions	Limitations of the solutions
[61]	Quantum bitcoins	Targets the ECDS algorithm that is used to secure the transactions of bitcoins	Insecure public key broadcasting by IoT devices.	N/A	Post-quantum end-to-end encryption	The correction schema of this attack is insufficient in terms of qubits decoherence
[62]	Quantum laser damage attack	Enables an attacker to manipulate optical pulses directed towards the communication channel	Weak authentication techniques	Python	Post-quantum end-to-end encryption	The correction schema of this attack is insufficient in terms of qubits decoherence
[63]	Quantum hammer	Fails to solve large-sized complex encryption keys	Insufficient mathematical encryption equations	Haswell system	QKR	Sometimes the solution generates insecure encryption keys
[64]	Quantum DDoS	Attacks the host OS among independent containers to capture the root of the container Daemon	Unsecure host OS	Docker environment	Quantum secure protocol	The algorithms used to update the quantum network topology and routing tables, among nodes duplicate the information, which makes it difficult to detect the security attacks. Suffer from qubit decoherence
[65]	Quantum state	Changes the state of the secret keys	Insecure cryptography algorithms	N/A	Secure blockchain approach based on entanglement and DPoS	No real implementation of the solution and it is not clear how the solution counters quantum state attacks

proposed security approach against quantum state attacks (e.g., man-in-the-medial attacks). These attacks decrypt the traditional quantum cryptography algorithms by computing mathematical encryption problems to change the state of the secret keys to be breakable. The security analysis in shows that the proposed solution can counter all types of quantum state attacks.

As shown in Table 9, there are critical drawbacks that limit the performance of current solutions against post-quantum security attacks on the perception layer. In [64,65], the solutions are not implemented in a real quantum environment and have complicated computations. In addition, the solutions in [61] suffer from an insufficient correlation between the entangled qubits due to limitations in correcting techniques, which results in qubit decoherence [50]. Furthermore, the solution in [64] has bad routing algorithms that make it difficult to detect quantum security attacks. However, these major limitations need to be addressed to provide efficient and robust solutions against post-quantum attacks on IoT devices. Table 10 shows the severity of the attacks discussed in Table 9 based on the DREAD model. The quantum bitcoins attack has a rating of 32.5, making it the most critical attack in Table 10.

The lessons learned from the analysis of post-quantum security attacks on IoT layers reveal the intricate vulnerabilities inherent in various domains. The exploration of attacks on the application layer, perception layer, network layer, and physical layer of IoT systems demonstrates the diverse range of threats posed by quantum computing. Leveraging the DREAD cybersecurity model for assessment provides a structured framework, aiding in prioritizing these threats based on factors such as damage, reproducibility, exploitability, affected users, and discoverability. The severity ratings, categorized as critical, high, medium, and low, offer a nuanced perspective on the urgency of addressing vulnerabilities. The findings underscore the critical importance of developing robust post-quantum security solutions, considering the unique challenges posed by attacks on IoT layers. Addressing these challenges requires innovative approaches to counter quantum-based threats effectively and ensure the continued security and reliability of IoT systems in a post-quantum era.

6. The classification approach for selecting post-quantum IoT security solutions

To guide readers in selecting the best cybersecurity solution against post-quantum security attacks that meets their intended tasks, we developed a classification approach based on the performance and complexity of the surveyed security solutions. This will allow a security solution approach to be selected based on the aims of the research that the readers want to perform and the features of the post-quantum security attacks that they wish to counter. More details about these solution techniques are described in Section 4.

Fig. 6 shows the proposed classification model that allows readers to select the best security defense approach against post-quantum security attacks on the physical layer of IoT systems. We developed this model based on the surveyed security solutions in section 4 to enable readers to choose the best solution that suits their intended tasks. For example, if the reader is interested in countering a quantum tampering attack in terms of the IoT physical layer and is concerned about whether the solution has an error mechanism that solves the qubits decoherence problem, then the best solutions are the QKR techniques. Otherwise, the reader can select the TMP solution.

Fig. 7 shows the proposed classification model that allows readers to select the best security solution against post-quantum security attacks on the network layer of IoT systems. If the reader is interested in countering a quantum insert attack and is concerned about the sequence number of the transmitted packets during a connection, then the best solutions are the packet analysis solutions based on the sequence number. Otherwise, the reader can select the packet analysis solutions based on the TTL value. If one is interested in detecting and preventing quantum hammer attacks and is concerned about reusing the same encryption keys during a connection and not generating new secret keys, then the best option is the QKR solution. Otherwise, the best option is the QKD solutions.

Fig. 8 presents the classification model that enables the readers to select the best security countermeasure technique against post-quantum security attacks on the IoT perception layer. For example, if one wants to counter quantum desynchronizing attacks and is concerned about prioritizing the messages sent during a connection, then message prioritizing solutions are the best security defense mechanisms. Otherwise, the reader can select the QKD solutions.

Fig. 9 illustrates the classification model that enables the readers to select the best security approach against post-quantum security attacks on the IoT application layer. For example, if a reader wants to counter quantum security attacks on bitcoins, then post-quantum end-to-end encryption solutions are the best security countermeasures techniques.

This section offers a vital classification approach for readers to choose effective cybersecurity solutions against post-quantum security attacks on IoT layers. The lessons stress aligning security measures with specific research goals and attack characteristics. Figs. 6–9 provide practical models for informed decision-making. For example, in countering quantum tampering attacks on the physical layer, readers choose between QKR techniques and TMP solutions based on factors like error mechanisms. Similar decision-making applies to other layers, such as network and perception, with a focus on specific concerns like sequence numbers or message prioritizing. The section provides concise insights for strategically selecting tailored security countermeasures across diverse post-

Table 10
DREAD model for the application layer attacks.

Attack	Damage	Reproducibility	Exploitability	Affected users	Discoverability	Attack rating
Quantum bitcoins	10	5	2.5	10	8	High (35.5)
Quantum laser damage attack	8	5	2.5	6	0	Medium (21.5)
Quantum hammer	9	5	2.5	8	5	High (29.5)
Quantum DDoS	9	7.5	5	8	5	High (29.5)
Quantum state	5	5	2.5	2.5	0	Medium (15)

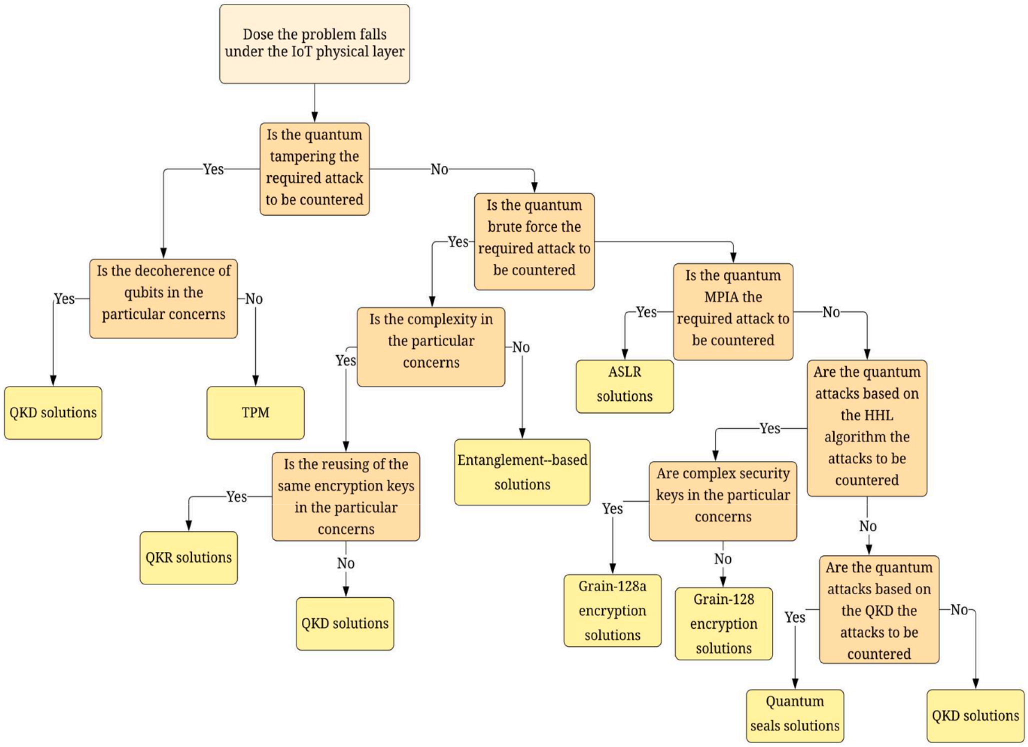
Dose the problem falls under the IoT physical layer
Is the quantum tampering the required attack to be countered
Yes
No
Is the decoherence of qubits in the particular concerns
Yes
No
QKD solutions
TPM
Is the quantum brute force the required attack to be countered
Yes
Is the complexity in the particular concerns
Yes
No
Is the reusing of the same encryption keys in the particular concerns
Yes
No
QKR solutions
QKD solutions
Entanglement--based solutions
Is the quantum MPIA the required attack to be countered
Yes
No
ASLR solutions
Are the quantum attacks based on the HHL algorithm the attacks to be countered
Yes
No
Are complex security keys in the particular concerns
Yes
No
Grain-128a encryption solutions
Grain-128 encryption solutions
Are the quantum attacks based on the QKD the attacks to be countered
Yes
No
Quantum seals solutions
QKD solutions

Fig. 6. The classification approach for selecting the best security solution against post-quantum security attacks on the IoT physical layer.

quantum threats on IoT layers.

7. Future work recommendations

In this section, we propose open challenges and limitations of the surveyed quantum security solutions against post-quantum security attacks and a quantum machine learning approach for detecting and preventing post-quantum security attacks presented in earlier sections.

7.1. *Quantum computing open security challenges*

Quantum computing has sparked a lot of interest in terms of securing the layers of IoT systems against post-quantum security attacks. However, despite the security benefits provided by quantum computing in a post-quantum era, it has several limits and issues that need to be solved, as detailed below.

1. Qubit decoherence. Some security solutions, including the QKD, QKR, and the solutions in [43,50,59,61], suffer from the qubit decoherence problem that makes the qubits inaccurately process the data, which results in decreased performance when countering post-quantum security attacks. This problem arises due to the insufficient correlation relationship between the entangled qubits. Therefore, attackers can easily harm the communication security protocol, if the number of entangled qubits is exponentially related to the original message size.
2. Insecure small-sized security keys. The security solutions approach in [27,47] as well as the QKR and QKD solutions, may generate insufficient small-sized encryption keys, allowing attackers to capture the superposition bit of the generated encryption key, which will result in fully controlling the communication channel and harming the transmitted sensitive data.
3. Insecure two-parties quantum communication protocols. Even though the quantum communication channels are secure against post-quantum security attacks, a leak of quantum information might cause catastrophic harm to the entire connection. For example, the quantum security protocol in [64] utilizes inefficient algorithms to update the quantum network topology and routing tables among the communicating nodes. The algorithms duplicate the routing information, which makes it difficult to detect post-quantum security attacks.
4. Since quantum computers are still in their early stages, researchers are constantly confronted with new challenges as they work to construct quantum-based algorithms. There is still some ambiguity concerning the types of cryptosystems that can be broken by quantum algorithms, as well as how to choose the security parameters and complexity of a problem [33]. Quantum cryptography

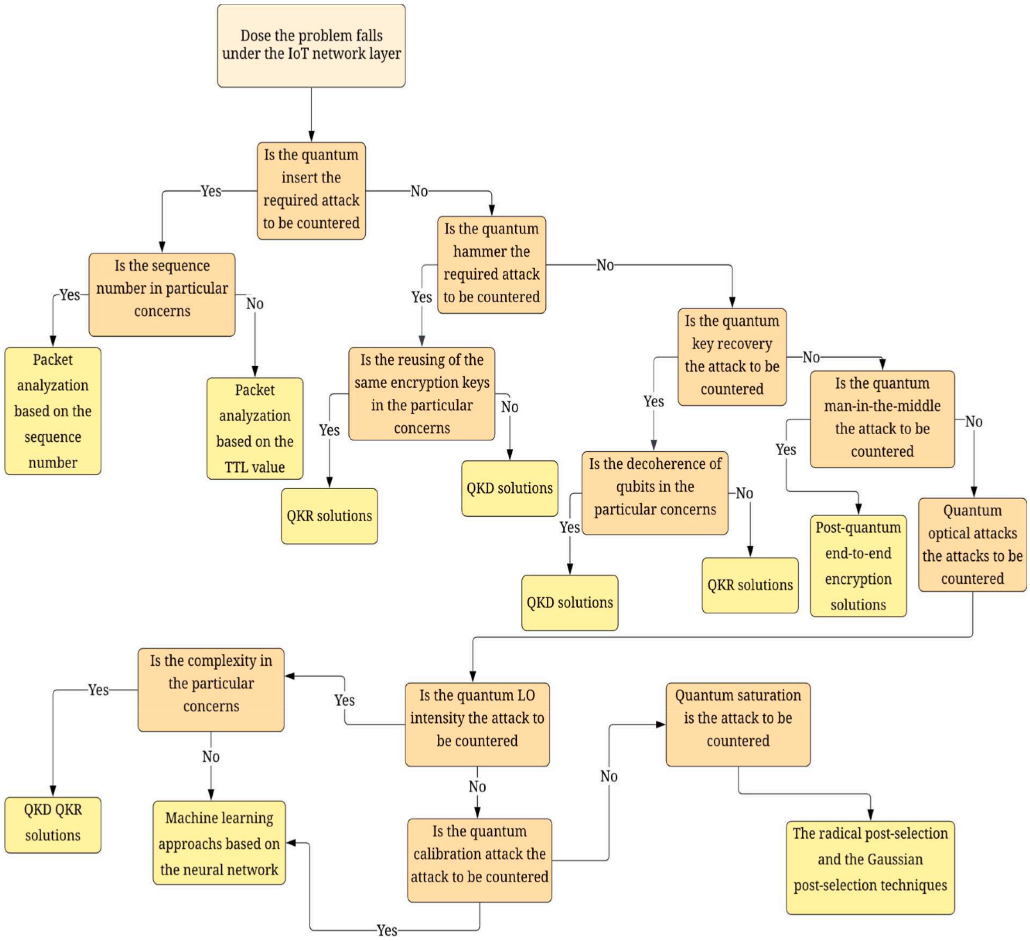
Dose the problem falls under the IoT network layer
Is the quantum insert the required attack to be countered
Yes
No
Is the sequence number in particular concerns
Yes
No
Packet analyzation based on the sequence number
Packet analyzation based on the TTL value
Is the quantum hammer the required attack to be countered
Yes
No
Is the reusing of the same encryption keys in the particular concerns
Yes
No
QKR solutions
QKD solutions
Is the quantum key recovery the attack to be countered
Yes
No
Is the decoherence of qubits in the particular concerns
Yes
No
QKD solutions
QKR solutions
Is the quantum man-in-the-middle the attack to be countered
Yes
No
Post-quantum end-to-end encryption solutions
Quantum optical attacks the attacks to be countered
Is the quantum LO intensity the attack to be countered
Yes
No
Is the complexity in the particular concerns
Yes
No
QKD QKR solutions
Machine learning approachs based on the neural network
Is the quantum calibration attack the attack to be countered
Yes
No
Quantum saturation is the attack to be countered
The radical post-selection and the Gaussian post-selection techniques

Fig. 7. The classification approach for selecting the best security solution against post-quantum security attacks on the IoT network layer.

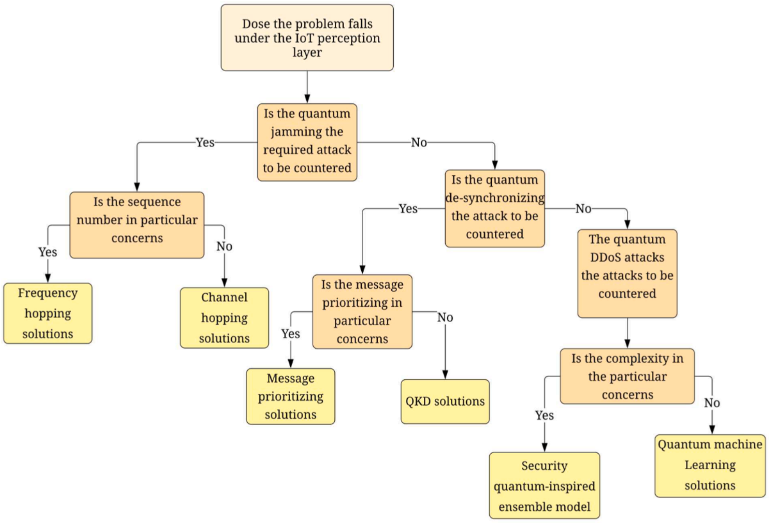
Dose the problem falls under the IoT perception layer
Is the quantum jamming the required attack to be countered
Yes
No
Is the sequence number in particular concerns
Yes
No
Frequency hopping solutions
Channel hopping solutions
Is the quantum de-synchronizing the attack to be countered
Yes
No
Is the message prioritizing in particular concerns
Yes
No
Message prioritizing solutions
QKD solutions
The quantum DDoS attacks the attacks to be countered
Is the complexity in the particular concerns
Yes
No
Security quantum-inspired ensemble model
Quantum machine Learning solutions

Fig. 8. The classification approach for selecting the best security solution against post-quantum security attacks on the IoT perception layer.

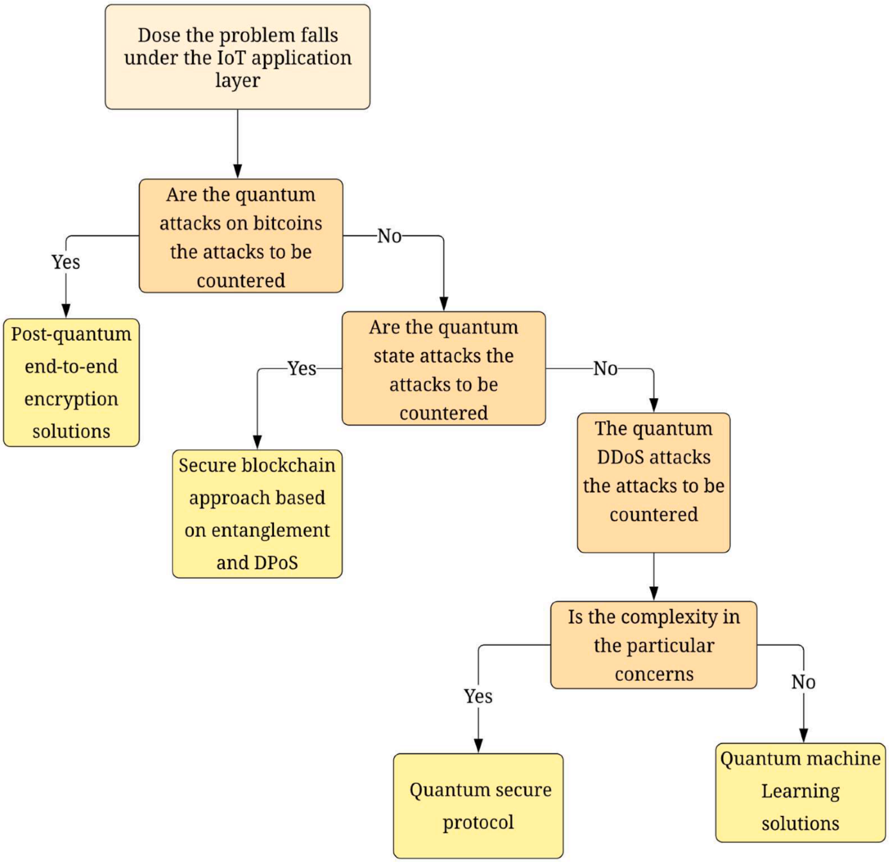
Dose the problem falls under the IoT application layer
Are the quantum attacks on bitcoins the attacks to be countered
Yes
No
Post-quantum end-to-end encryption solutions
Are the quantum state attacks the attacks to be countered
Yes
No
Secure blockchain approach based on entanglement and DPoS
The quantum DDoS attacks the attacks to be countered
Is the complexity in the particular concerns
Yes
No
Quantum secure protocol
Quantum machine Learning solutions

Fig. 9. The classification approach for selecting the best security solution against post-quantum security attacks on the IoT application layer.

that is device-independent is still a difficult challenge. Identifying a genuine verifier in position-based cryptography can use a lot of energy, making it inappropriate for IoT devices [66]. Furthermore, quantum cryptography resource requirements are still not clear. As a result, implementing these protocols to counter post-quantum security attacks necessitates the use of external quantum-enabled servers with sufficient capacity [33].

5. According to the proposed survey, we found that there are few studies about post-quantum security attacks on the application and perception layers of IoT systems. However, despite the lack of a large presence of quantum computers, it is crucial to develop efficient countermeasure solutions for these types of attacks due to their severity. For example, if a quantum computer is the third party in secure communication between two comminating parties, it can compute reversible computations, which will be a major problem [67]. Therefore, we have to be prepared to face this emerging technology.

7.2. *The proposed QNN*

Various post-quantum attacks damage the practical security of a CVQKD system, and the existing defenses in section 4 rely on various real-time monitoring modules to avoid various forms of attacks, which are highly dependent on the accuracy of the estimated qubits noise and lack a uniform defensive technique [11,33,68,69]. In our future solution, we intend to address these limitations by developing a QNN approach that can detect post-quantum security attacks. In a CVQKD protocol, an attacker can capture secure communication between two parties by harming the optical pulses that are used to transmit and receive the qubit's information during the connection [11,54,55,70]. Thus, we intend to use the measurable features of the optical pulses to train our model to predict and detect post-quantum security attacks, and Fig. 10 illustrates the whole detection process.

Fig. 10 presents the workflow of the proposed QNN [71,72]. Here, the input represents the optical pulses (e.g., signals and LO pulses) that will be encoded into quantum states in the encoding layer. The evaluation layer represents the calculation of the unitary matrix multiplications and the estimation of the quantum activation functions. The results of the evaluation layer will be fed forward to the measurement layer to learn the model to predict post-quantum security attacks. The output is a trained QNN circuit (trained model) that is measured to perform data prediction.

This section provides key insights from quantum computing open security challenges. It underscores the challenges of qubit decoherence in solutions like QKD and QKR, emphasizes vulnerabilities in generating insecure small-sized security keys, and highlights the potential risks in two-party quantum communication protocols. The evolving landscape of quantum computers introduces

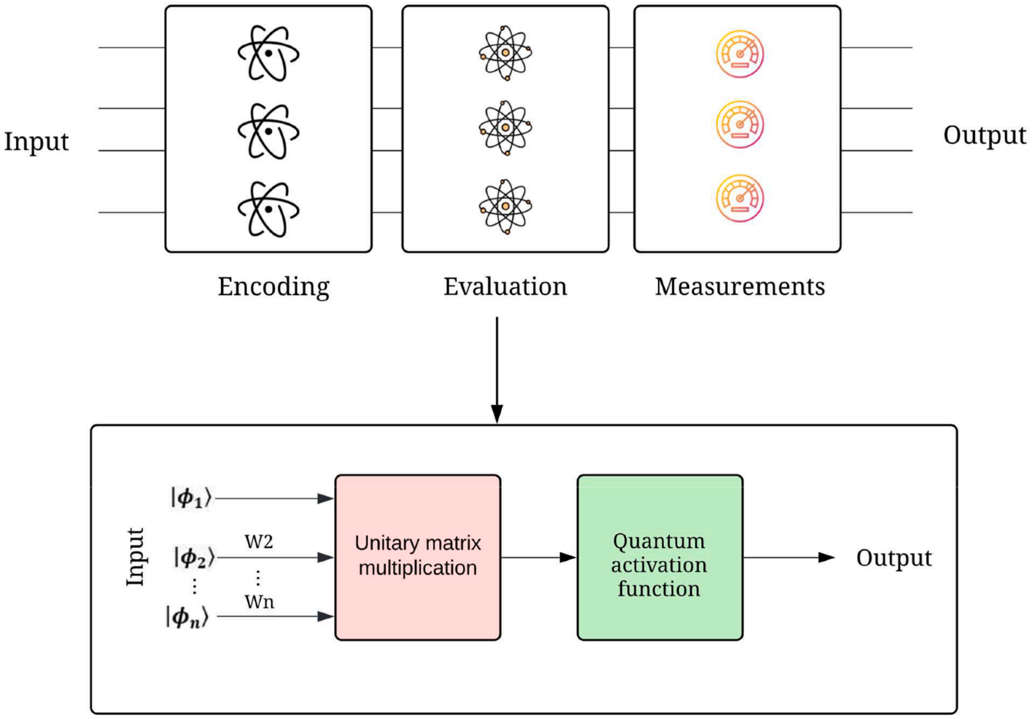

Fig. 10. The proposed QNN.

challenges for researchers, urging clarity on breaking cryptosystems and addressing quantum algorithm complexity. The scarcity of studies on post-quantum security attacks on the application and perception layers emphasizes the need for efficient countermeasure solutions. In Section 7.2, the proposed QNN stands out as a forward-looking solution for enhancing the practical security of CVQKD systems by predicting and detecting post-quantum security attacks.

8. Conclusion

In this comprehensive survey, we have presented a thorough analysis of existing post-quantum security attacks targeting the layers of IoT systems. Our examination covered potential threats to the physical, perception, network, and application layers, offering insights into the advantages and disadvantages of each attack. Emphasizing the critical need for secure communication in IoT systems, we delved into the existing solutions and countermeasures, revealing their limitations, such as susceptibility complexity and implementation challenges in quantum environments. Crucially, we employed the DREAD cybersecurity model to systematically assess and identify the severity of the surveyed post-quantum security attacks, ensuring a structured and comprehensive evaluation. The survey not only highlighted the vulnerabilities in IoT systems that these attacks exploit but also detailed the challenges associated with existing countermeasures, addressing complexities and inefficiencies. Moreover, we developed classification models based on the performance and characteristics of the surveyed attacks and countermeasures to assist readers in selecting the most suitable security solutions.

We illustrated the role of commonly used quantum algorithms in compromising IoT system security, emphasizing the potential of post-quantum security attacks to exploit these algorithms for malicious purposes. In anticipation of future advancements, we proposed a solution framework that leverages quantum machine learning to detect and predict post-quantum security attacks. This proposed framework aims to enhance IoT system security by utilizing measurable features of optical pulses during qubit transitions for training a quantum machine learning model. By providing a nuanced understanding of post-quantum security threats, evaluating existing solutions, and proposing innovative future approaches, our survey contributes to the ongoing discourse in IoT security, bridging current gaps and paving the way for robust defenses against evolving quantum threats.

CRediT authorship contribution statement

Ahmad Alomari: Writing – original draft. **Sathish A.P. Kumar:** .

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing

interests: Ahmad Alomari reports financial support was provided by National Science Foundation. Sathish Kumar reports financial support was provided by National Science Foundation. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

No data was used for the research described in the article.

References

[1] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations, IEEE Commun. Survey Tutor. 21 (3) (2019) 2702–2733, https://doi.org/10.1109/COMST.2019.2910750.

[2] N.MA A. Kofahi, M. Al-Khatib, A. Omari, T. Mansi, A smart real-time IoT-based system for monitoring health of athletes, Int. J. Comput. Digital Syst. (2021) 141–148.

[3] E.G. Rieffel, W.H. Polak, Quantum computing: A Gentle Introduction, MIT Press, 2011.

[4] O.S. Althobaiti, G.S. Member, Cybersecurity challenges associated with the internet of things in a post-quantum world, IEEE Access. 8 (2020) 157356–157381, https://doi.org/10.1109/ACCESS.2020.3019345.

[5] A. Kumar, S. Garhwal, State-of-the-art survey of quantum cryptography, Arch. Comput. Methods Eng. 28 (5) (2021) 3831–3868, https://doi.org/10.1007/s11831-021-09561-2.

[6] J. Granjal, E. Monteiro, J. Sa Silva, Security for the internet of things: a survey of existing protocols and open research issues, IEEE Commun. Surveys Tutor. 17 (3) (2015) 1294–1312, https://doi.org/10.1109/COMST.2015.2388550.

[7] T. Monz, et al., Realization of a scalable Shor algorithm, Science 351 (6277) (2016) 1068–1070, https://doi.org/10.1126/science.aad9480.

[8] P. Dorey, Securing the internet of things in a quantum world, Smart Cards, Tokens, Secur. Appl. Second Ed 55 (2) (2017) 116–120, https://doi.org/10.1007/978-3-319-50500-8_16.

[9] S.A. Kumar, T. Vealey, H. Srivastava, Security in internet of things: challenges, solutions and future directions, in: Proceedings of the Annual Hawaii International Conference on System Sciences, IEEE, 2016, pp. 5772–5781, https://doi.org/10.1109/HICSS.2016.714.

[10] J. Habibi, A. Gupta, S. Carlsony, A. Panicker, E. Bertino, MAVR: code reuse stealthy attacks and mitigation on unmanned aerial vehicles, in: Proceedings of the 2015 IEEE 35th International Conference on Distributed Computing Systems, 2015, pp. 642–652.

[11] Y. Mao, et al., Detecting quantum attacks: a machine learning-based defense strategy for practical continuous-variable quantum key distribution, New J. Phys. 22 (8) (2020), https://doi.org/10.1088/1367-2630/aba8d4.

[12] T.M. Khan, A. Robles-Kelly, Machine learning: quantum vs classical, IEEE Access. 8 (2020) 219275–219294, https://doi.org/10.1109/ACCESS.2020.3041719.

[13] N. Liu, P. Rebentrost, Quantum machine learning for quantum anomaly detection, Phys. Rev. A 97 (4) (2018) 1–10, https://doi.org/10.1103/PhysRevA.97.042315.

[14] S.J. Pauka, K. Das, R. Kalra, A. Moini, Y. Yang, M. Trainer, A. Bousquet, C. Cantaloube, N. Dick, G.C. Gardner, M.J. Manfra, D.J. Reilly, A cryogenic CMOS chip for generating control signals for multiple qubits, Nat. Electron. 4 (1) (2021) 64–70, https://doi.org/10.1038/s41928-020-00528-y.

[15] H. Boche, G. Janßen, S. Kaltenstadler, Entanglement-assisted classical capacities of compound and arbitrarily varying quantum channels, Quant. Inf. Process. 16 (4) (2017) 1–31, https://doi.org/10.1007/s11128-017-1538-6.

[16] P.I. Hagouel, I.G. Karafyllidis, Quantum computers: registers, gates and algorithms, in: 2012 28th International Conference on Microelectronics - Proceedings, MIEL 2012, 2012, pp. 15–21, https://doi.org/10.1109/MIEL.2012.6222789.

[17] M. Schuld, I. Sinayskiy, F. Petruccione, An introduction to quantum machine learning, Contemp. Phys. 56 (2) (2015) 172–185, https://doi.org/10.1080/00107514.2014.964942.

[18] F. Jazaeri, A. Beckers, A. Tajalli, J.M. Sallese, A review on quantum computing: from qubits to front-end electronics and cryogenic mosfet physics, in: *Proceedings of the 26th International Conference Mixed Design of Integrated Circuits and Systems, MIXDES 2019*, 2019, pp. 15–25, https://doi.org/10.23919/MIXDES.2019.8787164.

[19] M. Amico, Z.H. Saleem, M. Kumph, Experimental study of Shor's factoring algorithm using the IBM Q experience, Phys. Rev. A 100 (1) (2019), https://doi.org/10.1103/PhysRevA.100.012305.

[20] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134, https://doi.org/10.1109/SFCS.1994.365700.

[21] L.K. Grover, A fast quantum mechanical algorithm for database search, in: Proceedings of 28th ACM STOC, 1996, pp. 212–219.

[22] Gilliam, A., Woerner, S., & Gonciulea, C. (2021). Grover adaptive search for constrained polynomial binary optimization. *arXiv:1912.04088*. https://doi.org/10.22331/q-2021-04-08-428.

[23] A.A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S.E. Venegas-Andraca, J Peng, Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities, Inf. Process. Manag. 58 (4) (2021) 102549, https://doi.org/10.1016/j.ipm.2021.102549.

[24] D.R. Simon, On the power of quantum computation, SIAM Journal on Computing 26 (5) (1997) 1474–1483, https://doi.org/10.1137/S0097539796298637.

[25] N.A. Arshinov, N.G. Butakova, Modelling of quantum channel parameters impact on information exchange security, in: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronics Engineering (EIConRus), 2018, pp. 1463–1466.

[26] A. Sharma, V. Ojha, S.K Lenka, Security of entanglement-based version of BB84 protocol for quantum cryptography, in: 2010 3rd International Conference on Computer Science and Information Technology 9, 2010, pp. 615–619.

[27] S. Baili, H. Shangfu, Z. Xiao, W. Zhihui, An improved method of quantum key distribution protocol, in: 2009 International Forum on Computer Science-Technology and Applications 1, 2009, pp. 115–117.

[28] D. Leermakers, B. Škorić, Optimal attacks on qubit-based quantum key recycling, Quantum. Inf. Process. 17 (57) (2018), https://doi.org/10.1007/s11128-018-1819-8.

[29] S. Balogh, O. Gallo, IoT security challenges: cloud and blockchain, postquantum cryptography, and evolutionary techniques, Electronics (Basel) 10 (21) (2021) 2647–2669.

[30] D. Chawla, P.S. Mehra, A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: challenges, opportunities and solutions, Internet Things (2023) 24.

[31] Dahhak, H., Afifi, N., & Hilal, I. (2023). Impact of quantum attacks on IoT and blockchain. COC2023.

[32] M. Schöffel, F. Lauer, C.C. Rheinländer, N. Wehn, Secure IoT in the era of quantum computers—where are the bottlenecks? Sensors 22 (7) (2022) 2484.

[33] A. Lohachab, A. Lohachab, A. Jangra, A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks, Internet Things 9 (2020), https://doi.org/10.1016/j.iot.2020.100174.

[34] L.O. Mailloux, C.D. Lewis II, C. Riggs, M.R Grimaila, PostQuantum cryptography: what advancements in quantum computing mean for IT professionals, IEEE J. Mag. 18 (5) (2019) 42–47.

[35] M. Njorbuenwu, B. Swar, P. Zavarsky, A survey on the impacts of quantum computers on information security, in: Proceedings - 2019 2nd International Conference on Data Intelligence and Security, ICDIS 2019, 2019, pp. 212–218, https://doi.org/10.1109/ICDIS.2019.00039.

[36] P.S. Lakshmi, G. Murali, Comparison of classical and quantum cryptography using QKD simulator, in: Int. Conf. on Energy, Communication, Data Analytics and Soft Computing (ICECDS2017), 2017, pp. 3543–3547.

[37] Y. Subaşl, R.D. Somma, D. Orsucci, Quantum algorithms for systems of linear equations inspired by adiabatic quantum computing, Phys. Rev. Lett. 122 (6) (2019) 1–5, https://doi.org/10.1103/PhysRevLett.122.060504.

[38] X. Dong, Z. Li, X. Wang, Quantum cryptanalysis on some generalized Feistel schemes, Sci. China Inform. Sci. 62 (2) (2019) 1–12, https://doi.org/10.1007/s11432-017-9436-7.

[39] Microsoft. (2020). STRIDE/DREAD, *The DREAD approach to threat assessment*. https://docs.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers.

[40] S. Sicari, A. Rizzardi, D. Miorandi, A. Coen-Porisini, A risk assessment methodology for the Internet of Things, Comp. Commun. 129 (2018) 67–79.

[41] L. Zhang, A. Taal, R. Cushing, et al., A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces, Int. J. Inf. Secur. 21 (5) (2022) 509–525, https://doi.org/10.1007/s10207-021-00566-3.

[42] A.B. Price, J.G. Rarity, C. Erven, A quantum key distribution protocol for rapid denial of service detection, EPJ. Quantum. Technol. 7 (1) (2020), https://doi.org/10.1140/epjqt/s40507-020-00084-6.

[43] S. Paul, F. Schick, J. Seedorf, TPM-based post-quantum cryptography: a case study on quantum-resistant and mutually authenticated TLS for IoT environments, in: ARES 2021: The 16th International Conference on Availability, Reliability and Security, 2021, pp. 1–10, https://doi.org/10.1145/3465481.3465747.

[44] J. Wang, M. Luo, F. Suya, J. Li, Z. Yang, Q. Zheng, Scalable attack on graph data by injecting vicious nodes, Data Min. Knowl. Discov. 34 (5) (2020) 1363–1389, https://doi.org/10.1007/s10618-020-00696-7.

[45] L.H. Gong, X.T. He, S. Cheng, T.X. Hua, N.R. Zhou, Quantum image encryption algorithm based on quantum image XOR operations, Int. J. Theor. Phys. (Dordr) 55 (7) (2016) 3234–3250, https://doi.org/10.1007/s10773-016-2954-6.

[46] H. Liu, L. Yang, Quantum key recovery attack on SIMON32/64, Cybersecur. (Singap) 4 (1) (2021), https://doi.org/10.1186/s42400-021-00089-3.

[47] W. Liu, J. Gao, Quantum security of Grain-128/Grain-128a stream cipher against HHL algorithm, Quantum. Inf. Process. 343 (10) (2021), https://doi.org/10.1007/s11128-021-03275-x.

[48] E. Hugues-Salas, F. Ntavou, D. Gkounis, G.T. Kanellos, R. Nejabati, D. Simeonidou, Monitoring and physical-layer attack mitigation in SDN-controlled quantum key distribution networks, J. Opt. Commun. Netw. 11 (2) (2019) A209–A218, https://doi.org/10.1364/JOCN.11.00A209.

[49] T.S. Humble, Quantum security for the physical layer, IEEE Commun. Mag. 51 (8) (2013) 56–62, https://doi.org/10.1109/MCOM.2013.6576339.

[50] M. Schlosshauer, Decoherence, the measurement problem, and interpretations of quantum mechanics, Rev. Mod. Phys. 76 (4) (2005) 1267–1305.

[51] J. Cui, J. Guo, S Ding, Applications of Simon's algorithm in quantum attacks on Feistel variants, Quantum. Inf. Process. 20 (3) (2021) 1–50, https://doi.org/10.1007/s11128-021-03027-x. \.

[52] H. Zhu, H. Zhang, Efficient verification of quantum gates with local operations, Phys. Rev. A 101 (4) (2020) 1–7, https://doi.org/10.1103/PhysRevA.101.042316, 2020.

[53] A.H. Karbasi, S. Shahpasand, A post-quantum end-to-end encryption over smart contract-based blockchain for defeating man-in-the-middle and interception attacks, Peer-to-Peer 13 (2020) 1423–1441, https://doi.org/10.1007/s12083-020-00901-w.

[54] H. Qin, R. Kumar, R. Alléaume, Quantum hacking: saturation attack on practical continuous-variable quantum key distribution, Phys. Rev. (2015), https://doi.org/10.1103/PhysRevA.94.012325.

[55] X.C. Ma, S.H. Sun, M.S. Jiang, L.M. Liang, Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol, Phys. Rev. A - Atomic Mol. Opt. Phys. 87 (6) (2013), https://doi.org/10.1103/PhysRevA.87.052309.

[56] V. Makarov, D.R. Hjelme, Faked states attack on quantum cryptosystems, J. Mod. Opt. 52 (5) (2005) 691–705.

[57] M. Lucamarini, I. Choi, M.B. Ward, J.F. Dynes, Z.L. Yuan, A.J. Shields, Practical security bounds against the Trojan-horse attack in quantum key distribution, Phys. Rev. X 5 (3) (2015) 031030.

[58] M. Bensalem, S.K. Singh, A. Jukan, On detecting and preventing jamming attacks with machine learning in optical networks, in: 2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1–6, https://doi.org/10.1109/GLOBECOM38437.2019.9013238.

[59] K. Sharma, S. Bhatt, Jamming attack – a survey, Int. J. Recent Res. Aspects 5 (1) (2018) 74–80.

[60] A. Saritha, B.R. Reddy, A.S. Babu, QEMDD: quantum inspired ensemble model to detect and mitigate DDoS attacks at various layers of SDN architecture, Wirel. Pers. Commun. (2021), https://doi.org/10.1007/s11277-021-08805-5.

[61] D. Aggarwal, G. Brennen, T. Lee, M. Santha, M. Tomamichel, Quantum attacks on bitcoin, and how to protect against them, Ledger 3 (2018) 1–21, https://doi.org/10.5195/ledger.2018.127.

[62] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, G. Leuchs, Attacks on practical quantum key distribution systems (and how to prevent them), Contemp. Phys. 57 (3) (2016) 366–387.

[63] K. Mus, S. Islam, B. Sunar, QuantumHammer: a practical hybrid attack on the LUOV a practical hybrid attack on the LUOV signature scheme, in: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20), Association for Computing Machinery, New York, NY, USA, 2020, pp. 1071–1084, https://doi.org/10.1145/3372297.3417272.

[64] B. Kelley, J.J. Prevost, P. Rad, A. Fatima, Securing cloud containers using quantum networking channels, in: 2016 IEEE International Conference on Smart Cloud (SmartCloud), 2016, pp. 103–111, https://doi.org/10.1109/SmartCloud.2016.58.

[65] Y.L. Gao, X.B. Chen, G. Xu, K.G. Yuan, W. Liu, Y.X. Yang, A novel quantum blockchain scheme based on quantum entanglement and DPoS, Quantum. Inf. Process. 19 (420) (2020), https://doi.org/10.1007/s11128-020-02915-y.

[66] L. Malina, L. Popelova, P. Dzurenda, J. Hajny, Z. Martinasek, On feasibility of post-quantum cryptography on small devices, in: 15th IFAC Conference on Programmable Devices and Embedded Systems PDeS 2018 51, 2018, pp. 462–467, https://doi.org/10.1016/j.ifacol.2018.07.104.

[67] M.S. Rahman, M. Hossam-E-Haider, Quantum IoT: a quantum approach in IoT security maintenance, in: 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), 2019, pp. 269–272, https://doi.org/10.1109/ICREST.2019.8644342.

[68] A. Alomari, S.A.P. Kumar, Hybrid classical-quantum neural network for improving space weather detection and early warning alerts, in: 2023 IEEE Cognitive Communications for Aerospace Applications Workshop (CCAAW), Cleveland, OH, USA, 2023, pp. 1–6, https://doi.org/10.1109/CCAAW57883.2023.10219316.

[69] Y. Pan, L. Zhang, D. Huang, Practical security bounds against trojan horse attacks in continuous-variable quantum key distribution, Appl. Sci. 10 (21) (2020) 7788, https://doi.org/10.3390/app10217788.

[70] A. Alomari, S.A.P. Kumar, DEQSVC: dimensionality reduction and encoding technique for quantum support vector classifier approach to detect DDoS attacks, IEEE Access. 11 (2023) 110570–110581, https://doi.org/10.1109/ACCESS.2023.3322723.

[71] J. Allcock, C.-Y. Hsieh, I. Kerenidis, S. Zhang, Quantum algorithms for feedforward neural networks, ACM Trans. Quant. Comput. 1 (1) (2020), https://doi.org/10.1145/3411466. Article 1.

[72] S. Yan, H. Qi, W. Cui, Non-linear quantum neuron: a fundamental building block for quantum neural networks, Phys. Rev. A 102 (5) (2020).