The Journal of Supercomputing (2024) 80:3738–3816
https://doi.org/10.1007/s11227-023-05616-2

Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing

Sarra Cherbal[1] · Abdelhak Zier[1] · Sara Hebal[1] · Lemia Louail[2] · Boubakeur Annane[1]

Accepted: 19 August 2023 / Published online: 6 September 2023

Abstract
The Internet of Things (IoT) is an important virtual network that allows remote users to access linked multimedia devices. The development of IoT and its ubiquitous application across various domains of everyday life has led to continuous research efforts. Security is a perceptual concern for researchers involved in IoT as it is a key factor in the acceptance of any innovative technology. Numerous research studies have been conducted concentrating on the level of IoT security on a particular mechanism, on specific applications, or on categorizing vulnerabilities, in order to address a defined situation of securing an IoT network. This present paper aims to comprehensively review potential solutions for securing IoT, between emerging and traditional mechanisms, such as blockchain, machine learning, cryptography, and quantum computing. This study provides a comparative analysis of related papers with their characteristics, pros and cons. Accordingly, it taxonomizes relevant solutions based on their achieved security requirements. Furthermore, the potential benefits and challenges of each of the four mechanisms are discussed.

Keywords Internet of Things (IoT) · Security · Blockchain · Machine learning · Cryptography · Quantum computing

1 Introduction

The Internet of Things (IoT) represents a significant industrial revolution that involves a network of various “things” or embedded devices connected via sensors and communication protocols [1, 2]. These devices are designed to collect, exchange, examine, and monitor data. This interconnectivity enables seamless communication between things and people, things and environment, and between things themselves [3]. IoT collects information for the physical world utilization through smart systems with computational and communication ability [4]. Due to

Extended author information available on the last page of the article its widespread recognition, it is predicted that the number of IoT devices in use will reach 75 billion by 2025 [5] and is expected to grow to 125 billion by 2030 [6].

The potential of IoT lies in its significant impact on different areas of daily life. Users can benefit from the smartness that IoT provides in both their professional and personal lives [3]. Some popular IoT applications are smart homes, smart cities, healthcare, smart industry, agriculture, smart grid, and autonomous vehicles.

1.1 Motivation and paper contributions

IoT applications have the potential to reduce human intervention, improve data collection, and streamline analysis. However, the increasing number of devices and connections in use poses a significant challenge to the security of these systems [7]. Many academics are working to meet IoT security requirements and prevent specific threats. Therefore, existing security solutions are being adapted for IoT, such as classical and quantum cryptography [5, 8], besides the employment of emerging technologies like blockchain [9] and artificial intelligence [10]. The aim of these initiatives is to address further security challenges and establish a more secure environment for IoT.

We have conducted a thorough analysis of review papers and numerous research papers related to IoT applications and the corresponding security solutions. The aim of this paper is to expose security perspectives in IoT and to perform a comprehensive study of potential solutions to enhance IoT security measures. There are many reviews in the literature about IoT security, but the main motivation of this paper is to consolidate the study of IoT security solutions based on blockchain, machine learning, cryptography, and quantum computing in one article to simplify the access of pertinent information. This guideline will be a useful and a timesaving resource for both new and established researchers in the field, as it will enable them to have the necessary concepts, to understand the effectiveness of each mechanism and its challenges.

We summarize the contributions of this review as follows:

- We overview recent related review papers, and discuss and compare them in terms of defined criteria.
- We organize the IoT security solutions into four categories according to the used mechanism.
- We review, analyze, discuss, and compare the research approaches for each category.
- We apply a specific taxonomy for solutions within each category.
- We answer the research question we formulated regarding the global taxonomy that covers solutions from the four categories.
- We answer the research questions we formulated about the benefits and challenges of each category of IoT security mechanisms.

The paper addresses the following research question:

- *RQ*1: What global taxonomy can we apply to the IoT solutions of the four categories?

Additionally, the paper investigates the following two research questions for each “Mechanism *i*” out of the four defined categories:

- RQA_i: What are the potential benefits of using “Mechanism *i*” in securing IoT ?
- RQB_i: What are the challenges of applying “Mechanism *i*” in securing IoT?

1.2 Research methodology

This work overviews recent review papers on “Security in IoT” and thoroughly studies research papers on “IoT security solutions.” The reviewed literature was obtained from reputable academic publishers such as Springer, Elsevier, ACM, Mdpi, Wiley, and IEEE. That contains a wealth of scientific research as journal articles, conference papers, reviews, etc.

The following keys were used in our research, limited to English papers. Key1: “Security AND Internet of Things,” Key2: “Security AND IoT AND Blockchain,” Key3: “Security AND IoT AND Machine Learning,” Key4: “Security AND IoT AND Cryptography,” Key5: “Security AND IoT AND Quantum.”

Figure 1a shows the research results from “Scopus” database using Key1, about the different types of papers. We notice that in this field, research papers had the highest publication rate, such as in 2022, there is 51% for articles and 45% for conference papers compared to 4% for review papers. Figure 1b shows the research results also from “Scopus” Database, using Key2, Key3, Key4, and Key5 for the three types of papers. We can notice that the attention of using emerging technologies such as blockchain and machine learning in securing IoT is in increase from 2019 to 2023. Besides, researchers in this field are consistently interested in applying cryptographic methods through time and they start to consider the use of quantum computing.

The general inclusion criteria for papers analyzed in this study are as follows:

- Papers should include the terms mentioned in the search keys.

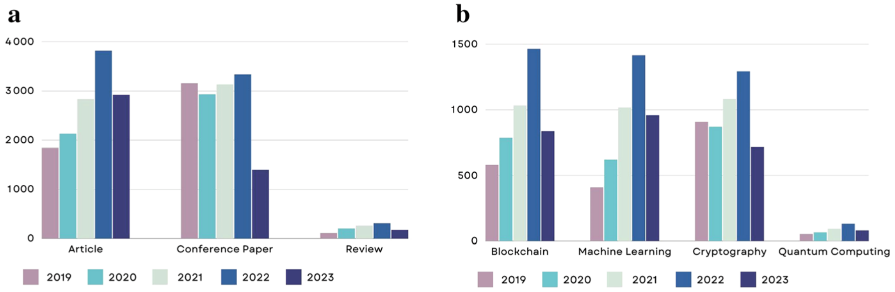

Fig. 1 Published papers on IoT security (2019–August 2023)

- Papers should be from the years 2021 to 2023.
- Papers should be in the English language.

The specific inclusion criteria for papers analyzed in this study are as follows:

- Related surveys: Key1 + Type “Review”
- BC-based approaches: Key2 + Type “Research paper”
- ML-based approaches: Key3 + Type “Research paper”
- Crypto-based approaches: Key4 + Type “Research paper”
- QC-based approaches: Key5 + Type “Research paper”

As a result, among the papers that satisfied the inclusion requirements, 77 papers, including both related surveys and related solutions, were thoroughly analyzed and discussed in this study.

1.3 Paper organization

The rest of the paper is structured in the following manner (Fig. 2). Section 2 presents the security perspectives of IoT. The definitions of the four security mechanisms are provided in Sect. 3. Section 4 overviews and compares the related surveys. Section 5 reviews, analyses, and compares IoT security solutions organized in four categories. The answer to the first research question is presented in Sect. 6. The answers to the following research questions are presented in Sect. 7. Finally, the work is concluded in Sect. 8.

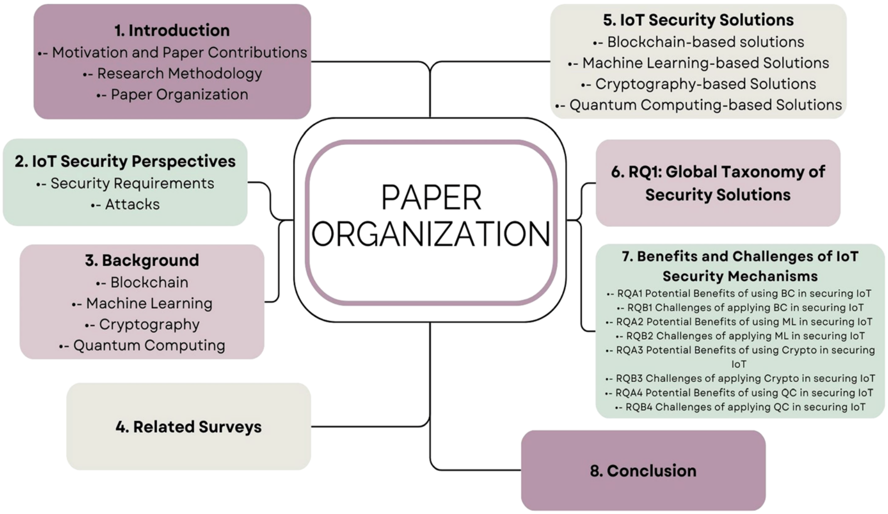
1. Introduction
•- Motivation and Paper Contributions
•- Research Methodology
•- Paper Organization
5. IoT Security Solutions
•- Blockchain-based solutions
•- Machine Learning-based Solutions
•- Cryptography-based Solutions
•- Quantum Computing-based Solutions
2. IoT Security Perspectives
•- Security Requirements
•- Attacks
PAPER ORGANIZATION
6. RQ1: Global Taxonomy of Security Solutions
3. Background
•- Blockchain
•- Machine Learning
•- Cryptography
•- Quantum Computing
7. Benefits and Challenges of IoT Security Mechanisms
•- RQA1 Potential Benefits of using BC in securing IoT
•- RQB1 Challenges of applying BC in securing IoT
•- RQA2 Potential Benefits of using ML in securing IoT
•- RQB2 Challenges of applying ML in securing IoT
•- RQA3 Potential Benefits of using Crypto in securing IoT
•- RQB3 Challenges of applying Crypto in securing IoT
•- RQA4 Potential Benefits of using QC in securing IoT
•- RQB4 Challenges of applying QC in securing IoT
4. Related Surveys
8. Conclusion

Fig. 2 Paper Organization

2 IoT security perspectives

IoT security perspectives refer to requirements and risks associated with the security of connected devices and their data. It is essential to address these security issues to protect the privacy and security of IoT users and prevent malicious activities. In this section, we define some of the most well-known IoT security requirements and attacks (Fig. 3).

2.1 Security requirements

Security approaches in IoT must consider specific requirements to ensure the secure deployment of IoT systems. The literature presents numerous security requirements related to IoT. In this subsection, we highlight the most well-known ones that will be utilized in our study within this paper.

- *Authentication:* Authentication is a fundamental security requirement in IoT systems. It involves verifying the identity of devices, users, or entities. It refers to the method by which one participant in communication gains confidence in the identity of another participant involved in the interaction [11]. By implementing authentication, IoT systems ensure that only legitimate entities can interact with the network, reducing the risk of malicious activities.
- *Access control/Authorization*: define authorizations to the network entities, in order to limit their access to specific actions, resources, or data within the network. Thus, it involves specifying the access privileges of entities, allowing them to engage exclusively with what is relevant to them [12]. It is important as it shields against unauthorized access to sensitive data. Failing to implement proper access control can lead to significant consequences, including serious outcomes such as data breaches, manipulation of devices, and compromised privacy [13].
- *Securely Transmitted Data*:

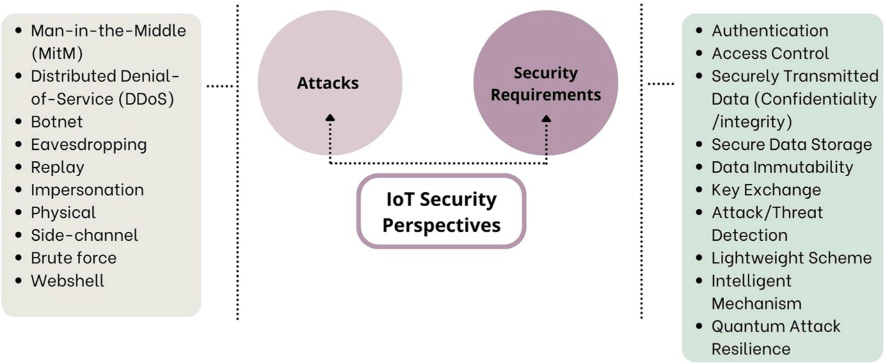

Fig. 3 IoT Security Perspectives

-Confidentiality: Given that IoT data traverses various points within a network, a robust encryption mechanism becomes essential to safeguard data confidentiality [14]. This ensures that only corresponding entities possess the ability to decipher the data [15].

-Integrity: It refers to the assurance that the data generated and transmitted remains accurate, unaltered, and consistent. It ensures that data is not tampered with or modified by unauthorized parties [13].

Failing to prioritize these two aspects can lead to severe consequences. Breaches in confidentiality may lead to privacy violations and data leaks, while compromised data integrity could result in incorrect decisions, device malfunctions, and a loss of user trust [16].

- *Secure Data Storage*: Regarding the sensitive and valuable nature of the information generated and processed by IoT devices, securing data storage is an important requirement [17]. Implementing strong encryption can secure the stored data. IoT systems produce vast amounts of data, often containing personal, financial, and operational details. Without robust data storage security, unauthorized access, tampering, or breaches could lead to privacy violations, financial fraud, and operational disruptions [17, 18].
- *Data Immutability*: Data immutability refers to the state in which information is unable to be altered or modified after it has been recorded [19]. It ensures that once data is documented, it remains tamper-resistant, ensuring its accuracy and credibility over time. This property is significant in contexts where maintaining the fidelity of information is crucial for trust and reliability. Failure to ensure data immutability can result in tampered records and compromised trust, potentially leading to decisions made based on inaccurate or manipulated information [20, 21].
- *Key Exchange*: A secret key is defined and agreed upon between two network entities that want to initiate communication with each other. This key is used to secure this communication and the exchanged data [22, 23].
- *Attack/Threat Detection*: Attack or threat detection in IoT security involves the monitoring and identification of malicious activities, unauthorized access, or abnormal behavior within an IoT ecosystem. It is crucial as it enables the timely detection and response to potential cyber-attacks/threats [24].
- *Lightweight Scheme*: A security lightweight scheme refers to a set of security measures designed to provide effective protection for networks, while minimizing their impact on computational resources and performance. These schemes are important for resource-constrained environments like IoT devices, where limited processing power, memory, and energy availability prevent the use of more resource-intensive security approaches [23, 25].
- *Intelligent Mechanism*: Intelligent mechanisms, driven by artificial intelligence, are essential in IoT security approaches, due to the dynamic and intricate nature of IoT ecosystems [26, 27]. Their usage and significance will be further elaborated in the subsequent sections.
- *Quantum Attack Resilience*: Quantum attack resilience is essential due to the potential threat posed by quantum computers to classical cryptographic meth-

ods [28]. Its usage and significance will be further elaborated in the subsequent sections.

2.2 Attacks

Various types of attacks are usually associated with IoT. In the following, some of the most well-known attacks, including those mentioned later in this paper, will be outlined.

- *Man-in-the-middle (MitM) attack*: an attacker listens to a communication between two IoT devices and can manipulate the information exchanged [29]. This can lead to data theft or to false data injection [30].
- *Denial-of-service (DoS) attack*: floods a target machine with traffic in order to overwhelm it and make it inaccessible to legitimate users [31, 32].
- *Distributed denial-of-service (DDoS) attack*: is a category of DoS attacks. It involves multiple connected devices that are used to overwhelm a target server with fake traffic [31].
- *Botnet attack*: An IoT Botnet is essentially a group of infected IoT devices like routers, wearables, and embedded technologies. This malicious software enables attackers to control these devices and, subsequently, the entire network [29].
- *Eavesdropping attack*: involves intercepting and recording communication between IoT devices to steal sensitive information [29].
- *Replay attack*: entails intercepting and recording data from an IoT device's communication and replaying it to gain unauthorized access [29].
- *Impersonation attack*: The attacker utilizes the identity of an authenticated end user or end node to gain access to the network and exploit any security vulnerabilities [32].
- *Physical attack*: implies physically accessing the IoT device and manipulating it to gain control. This can be done by hacking into a device's firmware or using physical tools to tamper with the device [33].
- *Side-channel attack*: exploits vulnerabilities in a device's hardware to gain unauthorized access or steal data. The attacker exploits side channel data emitted by encryption devices, containing details like power usage, operation time, and fault frequency. This data helps the attacker uncover the encryption key [33]. It exploits information leaked by the device during its operation without the need to physically access the device like in a physical attack.
- *Brute force attack*: refers to a technique used to acquire unauthorized access, in which the attacker systematically guesses various possible combinations of a specific password. This process continues until the correct password is successfully identified. The time it takes and the number of combinations attempted depend on factors such as the length and complexity of the password [29].
- *Webshell attack*: A webshell attack involves inserting a malicious script into a web server, allowing an illicit bypass of sensitive data and unauthorized remote access to the server [34].

3 Background

3.1 Blockchain

Blockchain is a decentralized, distributed digital ledger that safely and openly records transactions. Instead of being administered by a single entity, it is managed by a network of computers. Every entity of the network keeps a copy of the database, and all updates are logged in real-time and are available to everyone on the network [35].

The security of the blockchain derives from the way it is constructed. Each block in the chronological chain contains a distinct encrypted hash that links it to the previous one [36]. By using this method, an unbroken chain of records is created, making it very impossible to alter or delete any previously recorded transaction.

Consensus protocols are an essential component of blockchain technology. They enable a distributed network of nodes to agree on the state of the blockchain without the need for a central authority or intermediary. Consensus protocols ensure that all nodes in the network have a consistent copy of the blockchain and prevent malicious actors from tampering with the data. There are several consensus protocols used in blockchain, including Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) [37].

When combined together, IoT and blockchain technologies become able to ensure secure and transparent data sharing and can help overcome some of the challenges of IoT systems. IoT data can be stored, using the blockchain technology, in a decentralized, tamper-proof manner that is accessible to authorized parties. This can improve data transparency and trust by reducing data alteration or unwanted access [38].

Blockchain can additionally offer a way for IoT devices to securely exchange data and payments without the need for other intermediaries. Blockchain and IoT are being explored for usage in a number of applications, including smart contracts, supply chain management, and energy management. Blockchain can be used, for instance, in supply chain management to track the flow of goods from the producer to the consumer, ensuring that they are authentic and unaltered [39]. Blockchain in energy management can enable peer-to-peer energy trading, allowing people and companies to buy and sell extra renewable energy [40].

3.2 Machine learning

Artificial intelligence (AI) is a broad field that encompasses a range of technologies that enable machines to perform tasks that typically require human intelligence, such as perception, reasoning, and learning. Machine learning is a subset of AI that involves training algorithms to learn from data and make predictions or decisions based on that data [41]. Machine learning algorithms can be used for a variety of tasks, including the detection and prevention of security threats in real-time.

There are a variety of machine learning techniques that can be applied to IoT security, including supervised learning, unsupervised learning, and reinforcement learning [42].

Supervised learning algorithms can be trained to identify known security threats based on labeled data, while unsupervised learning algorithms can be used to identify unknown threats based on patterns in the data. Reinforcement learning algorithms can be used to optimize security protocols and response strategies based on real-world feedback [43].

Deep learning is a type of machine learning that involves using artificial neural networks to model and solve complex problems. These networks are composed of layers of interconnected nodes that can learn to recognize patterns in data and make predictions based on those patterns [44].

AI, machine learning, and deep learning are being used to automate and optimize a variety of tasks, improving efficiency and accuracy in areas such as security in IoT.

3.3 Cryptography

Cryptography is the practice of securing communications and data through the use of mathematical algorithms and protocols. It has been used for thousands of years to protect sensitive information. The basic principles of cryptography involve using complex mathematical algorithms to encode messages or data in a way that makes them unreadable to anyone without the proper key or password. There are two main types of cryptography: symmetric key cryptography and public key cryptography [45].

Symmetric key cryptography, also known as secret key cryptography, uses the same secret key for both encryption and decryption. The advanced encryption standard (AES) is a widely used symmetric key encryption algorithm.

Public key cryptography, also known as asymmetric key cryptography, uses a pair of keys, a public key for encryption and a private key for decryption. The most widely used public key encryption algorithm is the RSA algorithm, which is based on the mathematical properties of prime numbers. Public key cryptography is often used in secure online transactions and digital signatures.

Elliptic curve cryptography (ECC) is also a public key cryptographic method. It is based on the mathematical properties of elliptic curves. ECC is considered to be more efficient than traditional public key cryptography methods, such as RSA, as it uses shorter key lengths and requires fewer computational resources [46]. ECC is used in a wide range of applications, including secure online communication and digital signatures.

Hash functions are another cryptographic method used to ensure the integrity of data. A hash function takes a message or data input and produces a fixed-length output, or hash, that is unique to that input. Even a small change to the input data will produce a completely different hash output, making it virtually impossible to modify the data without being detected [47]. The secure hash algorithm (SHA) is a commonly used hash function that is used to verify the authenticity of digital signatures and other forms of data.

3.4 Quantum computing

Quantum computing is a type of computing that uses the ideas of quantum physics in order to process information. Traditionally, data is represented by bits, which are either 0 or 1 [48]. Contrarily, quantum computers use quantum bits, or qubits, which can be both 0 and 1 at the same time. This phenomenon is called superposition. Entanglement, another technique used in quantum computing, enables the connection of qubits in such a way that the state of one affects the state of another even when they are separated by a great distance [49].

Due to the special characteristics of quantum computing, some types of calculations can be completed more quickly than using traditional computers. In particular, quantum computers excel at simulating quantum systems, cryptography, and optimization issues [50].

In the context of IoT, quantum computing has important implications for security. It provides a new paradigm for cryptography which enhances the security of IoT devices and networks.

Traditional cryptography techniques encrypt data by relying on the complexity of certain mathematical problems. Nevertheless, these techniques are easily broken by quantum computers since the latter can solve such mathematical problems exponentially more quickly than classical computers [51].

For instance, quantum key distribution (QKD) is an alternative approach offered by quantum cryptography, which takes advantage of the characteristics of quantum physics to allow two parties to share a secret key [52].

4 Related surveys

The rising impact of IoT security has motivated researchers to conduct surveys aimed at improving this technology's usefulness to humanity. Therefore, in this section, we review recent survey papers on IoT security.

Williams et al. [53] examined security threats in IoT from three angles: hardware, software, and data in transit. They illustrated how existing security solutions deal with the hardware limitations of IoT devices. Furthermore, the authors presented how cryptography, blockchain, and machine learning can be applied to IoT security. Then, they analyzed the security risks of blockchain and machine learning technologies. In [54], Corallo et al. presented a systematic literature review (SLR) in order to examine how the current state of the art presents the issue of cybersecurity awareness in the industrial IoT. Shirvani et al. [55] conducted a subjective survey study on trust management in IoT security. To design the survey, they considered the commonalities and differences of the state-of-the-art literature. They classified the studied state-of-the-art schemes and compared the published papers on these trust-based schemes.

Swessi and Idoudi [56] offered a comprehensive categorization of the primary security concerns that stem from the IoT architecture, attack implications, and application fields. Then, the authors organized and illustrated various countermeasures adopted to mitigate these risks while taking into consideration the latest advancements in security methodologies. Sadhu et al. [29] are primarily interested in IoT attacks and vulnerabilities by classifying them based on distinct properties. Then, specific countermeasures for each type of attack are provided. Security solutions are presented based on secret key-based cryptography (KBC), physical unclonable functions (PUF), and blockchain.

Alzoubi et al. [57] conducted a thorough examination of the challenges associated with integrating blockchain and IoT. Through a comprehensive analysis of relevant literature reviews and survey papers, this study aims to offer a comprehensive survey of these challenges and suggest strategies for mitigating their impact without discussing related research approaches. Additionally, this paper discusses forthcoming developments in the field of blockchain-IoT integration. In [58], privacy and security concerns in the current deployment of IoT in the industrial environment are defined and explored. Additionally, the critical implementation challenges of blockchain-enabled industrial IoT are analyzed through a review of relevant literature. Shah et al. [6] carried out a survey on blockchain-based solutions to mitigate DDoS attacks in IoT. The article discusses the vulnerability of IoT networks to DDoS attacks, the potential use of blockchain technology to address DDoS attacks in IoT, and their brought challenges. Various existing blockchain-based solutions to mitigate DDoS attacks in IoT are categorized and discussed. Savithri et al. [59] presented a brief overview of IoT security. The paper categorizes the solutions based on blockchain technology into eight distinct issues.

In [60], the objective was to conduct a comprehensive analysis of various intrusion detection systems (IDS) especially those based on deep learning techniques. The study thoroughly examines publicly available network-based datasets of IDS. Besides, it evaluates the effectiveness of deep learning techniques using different performance metrics such as accuracy, precision, recall, false alarm rate, F1 score, and detection rate. Additionally, the research discusses the current challenges and potential solutions for enhancing network security and privacy. In [10], a comprehensive survey is conducted to examine the latest machine learning algorithms employed for the identification of malware in business information systems that operate using IoT technology. The review encompasses existing research that has been conducted in the field of malware detection, comprising static, dynamic, promoted, and hybrid methods of malware detection. Sarker et al. [61] provided a comprehensive review of IoT security intelligence. They presented various machine learning techniques, deep learning architectures, and techniques for creating intelligent security models to address security challenges in the IoT environment. They also identified and discussed the research issues and potential future directions related to the scope of their study.

Raimundo et al. [62] presented a review of type Systematic Review of Bibliometric Literature (LRSB) about cybersecurity in the IoT in Industrial Management (IIoT). The main focus of this review article was to analyze the literature trends related to the opportunities and threats in cybersecurity for IIoT. To achieve this, the authors provided a presentation of the current debate surrounding the topic of IIoT based on existing related literature reviews without analyzing related research papers. Khan et al. [63] aimed to comprehensively review current security issues, requirements, and standards in IoT, by presenting attacks in each IoT layer. Besides studying techniques for securing IoT as blockchain, machine learning, fog, and edge computing without giving the details of proposed approaches based on these techniques. In [64], Heidari and Jamali provided an SLR overview of the state-of-the-art techniques for IDS in IoT. The paper categorizes several important techniques of IDS into: signature-based, anomaly-based, specification-based, and hybrid. Then, it identifies key areas for future improvement in the discussed methods. Issa et al. [65] explored the integration of federated learning, blockchain, and IoT systems to enhance decision making and data analytics security. The survey emphasizes the importance of combining these technologies and provides an extensive review of blockchain-based federated learning solutions for IoT applications. Furthermore, the article also discusses the possible challenges of this integration.

Kumari et al. [5] assessed different post-quantum cryptographic methods that are designed to withstand quantum attacks in resource-limited IoT environments. They explored the significance of these methods and the challenges that they pose. Omolara et al. [4] shed light on possible solutions to address the diverse security challenges faced by IoT. Their review covers topics such as the challenges of blockchain technology, as well as the increase in distributed denial-of-service (DDoS) attacks linked to the COVID-19 pandemic. Kumar et al. [66] reviewed multiple facets of quantum computing that may offer advantages to the current healthcare industry. Besides, they mentioned the possibility of combining this technology with blockchain without discussing existing related solutions.

Jahangeer et al. [67] presented a comprehensive analysis of IoT network security from the standpoint of the network layer, while giving special attention to RPL (Routing Protocol for Low Power and Lossy Networks). The study delves into internal attacks at the network layer, with a specific focus on tackling sinkhole attacks through both detection and prevention measures. The review encompasses recent research developments and it delves into the realm of machine learning-driven algorithms and strategies, exploring their potential to fortify the security of the RPL protocol against internal attacks. Taherdoost's study [68] examines IoT security research, addressing topics such as authentication, wireless networks, use cases, challenges, and prospects. Additionally, it categorizes the examined research according to the context of data security. In the systematic literature research of [69], the authors looked at how AI-driven cyber-attacks are changing threats in Industry 4.0. They explored different cyber-attacks, defenses, and how AI can help. They also discussed the gap between research and real strategies. The purpose of the review is to plan for the future and make security better for Industry 4.0.

In the article of [70], Mangla et al. conducted a comprehensive review of prevalent challenges within emerging technologies and 5G networks. The goal was to address these issues in preparation for secure 6G networks. Then, the authors outlined current quantum-based solutions for security concerns, aiming to establish a robust and secure 6G network environment. Mathur et al. [9] explored the capabilities of blockchain technology and studied its potential to address challenges in emerging IoT applications. The authors covered the role of blockchain in diverse IoT areas such as healthcare, smart homes, supply chain, smart city, and more. They explored important technical aspects related to blockchain-enabled IoT applications and examined challenges while discussing proposed solutions. Thabit et al. [8]

presented an analysis of various cryptographic algorithms and their practical implementations for IoT security. They provided a comparison of security algorithms based on their performance and robustness, taking into account the computational complexity of cryptographic techniques. Additionally, the authors discussed the challenges of IoT security, providing insights into techniques for mitigation.

In Table 1, we summarize the findings of these recent review papers and highlight the different perspectives of our review paper in comparison with others.

5 IoT security solutions

In this section, we review and summarize the key findings of relevant approaches in IoT security, organized into four categories based on the used mechanism. We provide a comparative analysis of these approaches in terms of defined criteria such as used techniques, IoT application, network architecture, main purpose, verification tools, evaluation metrics, pros and cons. Then, a specific taxonomy for each category is provided.

5.1 Blockchain-based solutions

Blockchain technology has emerged as a potential solution to the security challenges faced by IoT devices, with its secure, decentralized, and tamper-proof platform. Thus, in this subsection, we will provide an overview of the blockchain-based solutions proposed for enhancing IoT security.

In [71], the authors proposed a blockchain-based architecture for securing and ensuring trustworthy operations in the industrial Internet of Things (IIoT). The idea is that IIoT poses significant security challenges due to its distributed nature, diverse technologies, and large-scale operations. The authors suggested using blockchain technology to establish a decentralized, tamper-proof, and transparent architecture for IIoT security because conventional security mechanisms are insufficient to meet these issues.

The proposed architecture consists of three layers: the data layer, the blockchain layer, and the application layer. The data layer includes the devices and sensors that generate IIoT data. The blockchain layer uses a permissioned blockchain to manage and store IIoT data securely. The application layer includes the applications and services that use the IIoT data for various purposes.

The proposed architecture was implemented using X-CUBE-CRYPTOLIB library, which has been certified for industrial use by the NIST Cryptographic Algorithm Validation Program. The implementation results show that the proposed architecture can provide secure and trustworthy operations in the IIoT by ensuring data integrity, authentication, and confidentiality while improving resource utilization, energy efficiency, and execution time. Nevertheless, the execution time of the proposed architecture increases rapidly with the increase in the number of devices in the network.

Table 1 Comparative analysis of related surveys (BC: Blockchain, ML: Machine learning, Crypto: Cryptographic techniques, QC: Quantum computing, Comp: detailed comparison of related research approaches)

References	Year	BC	ML	Crypto	QC	Comp.	Main objective
[53]	2022	✓	✓	✓	×	×	Deal with hardware limitations of IoT devices Analyze security risks of BC and ML technologies
[54]	2022	×	×	×	×	✓	SLR on cybersecurity awareness in IIoT
[55]	2022	✓	×	✓	×	✓	A subjective survey study on trust management in IoT
[56]	2022	✓	×	✓	×	✓	Categorize of the primary security concerns from IoT architecture Illustrate various countermeasures to mitigate these concerns
[29]	2022	✓	×	✓	×	✓	Classify IoT attacks and vulnerabilities Present solutions based on secret KBC, PUF and blockchain
[57]	2022	✓	×	×	×	×	Examine challenges of integrating blockchain and IoT Discusses developments in blockchain-IoT integration
[58]	2022	✓	×	×	×	✓	Analyze implementation challenges of blockchain in industrial IoT
[6]	2022	✓	×	×	×	✓	Overview blockchain-based solutions to mitigate DDoS attacks in IoT
[59]	2022	✓	×	×	×	×	Categorize blockchain-based solutions into eight distinct issues
[60]	2022	×	✓	×	×	✓	Analyze various IDS that are based on deep learning techniques
[10]	2022	×	✓	×	×	✓	Examine ML algorithms employed for the identification of malware in business information systems of IoT
[61]	2022	×	✓	×	×	✓	Review IoT security intelligence based on ML and deep learning
[62]	2022	✓	✓	×	×	×	LRSB of cybersecurity in industrial IoT
[63]	2022	✓	✓	×	×	×	Explain how BC, ML, fog, and edge computing can be used in securing IoT
[64]	2022	✓	✓	×	×	✓	Review and categorize various techniques of IDS for IoT
[5]	2022	×	×	×	✓	✓	Assess post-quantum cryptographic methods that withstand quantum attacks in resource-limited IoT
[4]	2022	✓	×	×	✓	✓	Review the challenges of blockchain and the increased DDoS attacks linked to COVID-19
[66]	2022	×	×	×	✓	×	Review multiple facets of QC in healthcare and the possibility of combining QC with blockchain
[65]	2023	✓	✓	×	×	×	Review blockchain-based federated learning solutions for IoT

Table 1 (continued)

References	Year	BC	ML	Crypto	QC	Comp.	Main objective
[67]	2023	×	✓	×	×	×	Analyze IoT network security from the standpoint of RPL Review ML algorithms designed to the security of RPL
[68]	2023	✓	✓	×	×	×	Categorize the examined research according to the context of data security
[69]	2023	×	✓	×	×	×	Explore different cyber-attacks and defenses in Industry 40, and how AI can help
[70]	2023	×	×	×	✓	×	Address the issues of security in 5G networks Outline current quantum-based solutions for 5G security
[9]	2023	✓	×	×	×	✓	Cover the role of BC in diverse IoT applications Explore BC challenges while discussing proposed solutions
[8]	2023	×	×	✓	×	✓	Analyze cryptographic algorithms for IoT security Provide comparison of security algorithms based on their performance and robustness
Ours	-	✓	✓	✓	✓	✓	Organize IoT security solutions into four categories according to: BC, ML, Crypto and QC. Review and compare research approaches for each category Provide specific and global taxonomies of solutions Discuss the benefits and limitations of IoT security mechanisms

Wadhwa et al. [72] proposed a blockchain-based approach for securing the Cognitive Internet of Things (CIoT) using federated learning (FL) and homomorphic encryption. Due to its distributed and heterogeneous nature, the CIoT poses significant security challenges. The authors suggested applying blockchain technology to address these challenges. To enable remote, distributed, and collaborative machine learning while maintaining data privacy, the proposed approach uses a federated learning framework. Homomorphic encryption is used to enable secure computation on encrypted data, without the need for data decryption. The proposed approach was implemented using the Amazon AWS platform with 1000 nodes of different types. The nodes were configured using Linux Virtual Machine. The obtained results showed that the proposed approach can provide secure and trustworthy machine learning in the CIoT by ensuring data privacy and security.

The idea in [73] is to propose a blockchain-based data security storage system for IIoT; more specifically in the context of Industry 5.0. The IIoT poses significant security challenges due to its large-scale and heterogeneous nature that can be solved by using blockchain technology. The proposed mechanism uses a permissioned blockchain to manage the IIoT data securely and transparently. The blockchain is used to verify the authenticity of data and prevent unauthorized access or tampering. The mechanism also uses a distributed file system to store and manage the large-scale data generated by the IIoT. The efficiency of the proposed mechanism was proved formally and the results have shown that it reduces the proof size and the communication consumption. The approach also reduced the storage pressure of nodes by storing a single commitment instead of the entire qualification list. However, by lowering the storage pressure on nodes, the proof size has been decreased from its original data scheme to 15%.

Agyekum et al. [74] proposed a blockchain-based data-sharing mechanism using proxy re-encryption (PRE) to enhance the security of data sharing in edge/cloud architectures. Traditional data-sharing mechanisms in the IoT lack security and privacy protections, making them vulnerable to data breaches and unauthorized access. To address this, the paper proposed a mechanism that uses PRE, a cryptographic technique that enables data owners to delegate access to their data to others while maintaining data confidentiality and integrity. The mechanism also uses blockchain smart contracts to manage access control policies and permissions for data sharing. The proposed approach was first verified formally and then implemented using Windows operating system desktop computer and the jPBC library [75], which is a pairing-based cryptography library for Java. The results prove the efficiency of the approach in terms of data confidentiality, computation cost, and execution time. Nevertheless, once the data is stored in the blockchain, it is immutable and consumes more processing power which is not practical.

In [76], the authors proposed a framework that leverages blockchain technology to provide secure and efficient access control in IoT systems. The framework, called BHE-AC, employs a hierarchical access control mechanism that enables different levels of access privileges for different entities in the IoT network. BHE-AC uses smart contracts to manage access control policies and enforce them in a decentralized manner. The authors also introduced a consensus algorithm called Proof of Access (PoA), which was designed to be more efficient than traditional consensus algorithms used in blockchain systems. PoA uses the access history of nodes in the network as a measure of their trustworthiness and determines the order of block validation based on this metric. The performance of the BHE-AC framework was evaluated using simulations and demonstrated that it can provide high efficiency and scalability while maintaining strong security guarantees. They suggest that BHE-AC can be a promising solution for access control in large-scale IoT systems. However, generating and distributing tokens in such networks can be time-consuming.

Rizzardi et al. [77] proposed a permissioned blockchain-based approach for securing access control policies in IoT environments. The authors identified the challenges faced by traditional access control mechanisms in IoT, such as lack of scalability, flexibility, and reliability. They proposed the use of permissioned blockchain as a solution to these challenges, since it allows for decentralized, secure, and tamper-proof storage of access control policies. The proposed approach involves the deployment of a permissioned blockchain network that stores the access control policies, which can be accessed by authorized IoT devices. The blockchain network is managed by a set of trusted nodes, and each policy update is validated through a consensus mechanism. The proposed approach was evaluated through a case study using 4 Raspberry Pi, a variable number of PCs representing data sources, and an MQTT broker. The approach was evaluated in terms of latency, the time required for storage depletion, and CPU load. The results showed that the proposed approach enables to manage the data provided by heterogeneous sources in a distributed manner. However, the results also showed large packet sizes and much information exchange between the nodes.

The authors in [78] proposed a blockchain-based security mechanism to enhance the security and privacy of medical data in IoT environments. The authors spotted the challenges of securing medical data in IoT environments, which include the need for confidentiality, integrity, availability of data, and the need for access control and accountability. They proposed the use of blockchain technology as a solution to these challenges.

The proposed approach involves a fog computing architecture, which enables data processing and storage at the edge of the network, closer to the source of the data. The medical data is stored in a distributed ledger, and access to the data is controlled by smart contracts. Smart contracts enforce access control policies and enable the auditability of data access.

The proposed approach was evaluated through a real experiment on a medical edge/fog/cloud system, and the results showed that the blockchain-based security mechanism can effectively enhance the security and privacy of medical data in IoT environments. However, the authors noted that the proposed approach is computationally intensive and may require further optimization.

Chaganti et al. [79] discussed the integration of blockchain, cloud computing, and IoT to monitor security in smart agriculture. It highlighted the importance of ensuring security in agricultural processes and suggested that the proposed system can help address challenges such as data privacy and transparency. The work provided a detailed description of the proposed system architecture, which involves the use of blockchain technology to secure the IoT devices, cloud computing to process and store the data, and smart contracts to automate the process of monitoring security.

The proposed architecture was implemented and tested using Arduino Sensor Kit, ESP32, and AWS cloud and the processing time was considered as an evaluation metric.

The advantage of the proposed approach is that it stores malicious information to prevent future attacks for a smart-farm security monitoring framework. However, this framework is implemented to work with only one consensus algorithm which is the Ethereum Proof of Work (POW).

The paper [80] discussed the security challenges associated with IoT and proposed a multilayer blockchain-based security architecture to address these challenges. The proposed architecture involves the use of multiple layers of security, including a blockchain-based secure communication layer, a blockchain-based secure storage layer, and a blockchain-based secure processing layer.

This architecture was implemented and tested using MATLAB 2018a and evaluated through the transaction latency. The provided results showed that the architecture facilitates the lightweight authentication and authorization of IoT networked devices. However, limitations related to IoT devices were not taken into consideration such as energy consumption, small memory size, and low processing capabilities.

In [81], the authors proposed an advanced security model for multimedia data sharing in IoT systems. They highlighted the challenges associated with securing multimedia data in the IoT, including the need to ensure data confidentiality, integrity, and availability. The proposed security model involves the use of multiple security mechanisms, including cryptography, watermarking, and access control, to secure multimedia data in the IoT.

The implementation and testing of the proposed security model were provided using IPFS [82]. IPFS is a decentralized system used for storing and sharing multimedia files. Through the results, the authors demonstrated that their approach can provide high levels of security and can be applied in a variety of IoT applications. However, some interoperability problems are still unsolved in this context.

The authors in [83] addressed the inherent challenges associated with traditional electronic voting (e-voting) methods, such as vulnerability to hacking, lack of transparency, and potential privacy breaches. They discussed the application of blockchain technology to enhance the security and privacy of e-voting systems by developing secure, trusted and democratized smart city services.

The proposed e-voting system is implemented on the Ethereum platform and is made up of three core parts. The first part is an Ethereum wallet which handles users' authentication by creating encryption keys (public and private keys). The second part is the smart contracts which implement the core logic of the user voting process and counting the votes of users. The third part is the Ethereum blockchain which is the engine of the proposed e-voting system.

The proposed system ensures that voters are legitimate, and the contract transactions are distributed and decentralized.

The authors in [84] proposed an architecture for E-healthcare data security using a blockchain-distributed ledger technology named BHIIoT. In this work, a consortium hyperledger network is designed and deployed with two communication channels for node-to-node interconnectivity and data sharing. The proposed BHIIoT uses the NuCypher threshold re-encryption mechanism for data encryption and protects shared resources in the form of blocks preserved in a blockchain immutable storage.

The BHIIoT distributed application is able to tackle data security issues, such as ransomware attacks, insider attacks, and data-sharing vulnerabilities in mobile medical applications and telemedical services.

The proposed architecture achieves a reduction in the consumption of resources, such as computational energy, network bandwidth, and cost of data preservation, and increases productivity in terms of handling the generation of day-to-day data.

Table 2 illustrates the comparative analysis of solutions based on the blockchain mechanism.

According to this study, we classify BC-based approaches into three categories: permissionless blockchain, permissioned blockchain, and hybrid, as illustrated in Fig. 4.

5.2 Machine learning-based solutions

The aim of analyzing and exchanging data among the various sensors is to enable an efficient decision making of how the systems should operate. Decisions are made based on artificial intelligence algorithms, machine learning (ML) and deep learning (DL) algorithms specifically. To clarify, ML and DL algorithms are playing a key role in the field of cybersecurity as an alternative security solution for IoT-based applications, and by designing and implementing secure systems for IoT environment to protect the IoT devices from any authorized access and threats.

Mihoub et al. [85] designed and implemented new architecture based on machine learning techniques that allow both detecting and mitigating the denial-of-service “DOS” as well as distributed denial-of-service “DDOS” attacks in IoT. The proposed architecture consists of two main components: DOS/DDOS detection component and DOS/DDOS mitigation component. The first component serves to identify the type of attack “DOS or DDOS” and the type of packets: UDP, TCP, and HTTP. This component uses conventional ML methods such as decision trees and K-nearest neighbors (KNN) to more advanced DL methods including the multilayer perceptron (MLP) and long short-term memory (LSTM) to predict the type of the attack. The second component mitigates the attack based on the result of the first component, and more precisely, the packets are denied from one IP address.

The proposed architecture was evaluated based on two popular metrics such as accuracy and F1 measure using the Bot-IoT dataset. In addition, the work was compared with basic classifiers (machine learning algorithms). The classifiers are used to detect threats, which could include security breaches, malware, or other types of cyber-attacks. To this end, the evaluation shows highly promising accuracy results for the detection and mitigation of attacks that achieve an accuracy of 99.81%. However, IoT devices have limited resources such as memory and computing capabilities, which make it difficult to implement complex machine learning algorithms on the device itself. Thus, using cloud services to offload the computation may introduce other security concerns. Furthermore, the machine learning algorithms may provide false attack detection “false positive behavior”

Table 2 Comparative analysis of blockchain-based solutions

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools	Evaluation metrics	Pros & Cons
[71]	2021	asymmetric cryptography + ECDSA + consensus mechanism proof of authentication	IIoT (fruit processing plant)	Decentralized IoT network	Ensure secure and trustworthy operations in IIoT	X-CUBE-CRYPTOLIB library	Resource utilization + energy efficiency + service execution time	(+) ensures data integrity, authentication, and confidentiality Improves resource utilization and energy efficiency (−) rapid increase of the execution time
[72]	2022	Proof of Work (PoW) consensus mechanism	Cognitive learning	Client/server	Ensure data security on cognitive IoT	Amazon AWS platform	Effect of the number of blocks on memory utilization and impact of data sample size on accuracy	(+) provide secure and trustworthy machine learning in the CIoT (−) machine learning models can inherit biases present in the training data, potentially leading to unfair decisions
[73]	2022	Incremental aggregator subvector commitment (IASVC) + bilinear mapping	IIoT (Industry 5.0)	Not specified	Reduces the size of proof and communication consumption reduces the storage pressure of nodes	Formal proof (mathematical)	Proof size communication consumption	(+) reduces the storage pressure of nodes (−) decreases the proof size from its original data scheme to 15%

Table 2 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools	Evaluation metrics	Pros & Cons
[74]	2021	A proxy re-encryption approach	Cloud environment	Edge/cloud architecture	Data confidentiality	Formal proof (mathematical) + Experiments by jPBC library	Computation cost Execution time Data confidentiality	(+) ensures data confidentiality, lower computation cost, and lower execution time (−) storing the data in the blockchain consumes more processing power
[76]	2021	a blockchain-based token-requesting mechanism	IoT in general	Not specified	Secure and trusted access control	Solidity language + Ethereum	Gas cost + requesting time	(+) provides high efficiency and scalability while maintaining strong security guarantees (−) generating and distributing tokens can be time-consuming
[77]	2022	The integration of a permissioned blockchain within a not trusted IoT-distributed middleware layer	Fog-based IoT network	Distributed fog network	Guarantee the correct management of access to resources by the interested parties + manage the data produced by IoT devices	Test bed in networked smart object middleware platform (NOS) + 4 raspberry Pi + a variable number of data sources (running from PCs) + MQTT broker	Storage occupancy Time required for storage depletion CPU load Latency	(+) enables to manage data provided by heterogeneous sources in a distributed manner (−) large packet sizes and many information exchanges

Table 2 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools	Evaluation metrics	Pros & Cons
[78]	2021	Elliptic curve crypto (ECC) digital signature	Healthcare	Edge/fog/cloud	Provide security countermeasures against medical data mining threats	Real experiment on a medical edge/fog/cloud system	Transaction latency Certification time Data retrieval time Certificate size	(+) guarantees security and privacy of medical data (−) the approach is computationally intensive
[79]	2022	Defined a lambda function to parse the data from the AWS IoT core component and extract the required data	Smart agriculture	Cloud architecture	Implement security monitoring for smart farming monitor device status monitor sensors anomalies mitigate security attacks	Arduino Sensor Kit, ESP32, AWS cloud	Processing time	(+) stores malicious information to prevent future attacks (−) works with only one consensus algorithm: the Ethereum Proof of Work (POW)
[80]	2021	Hybrid Evolutionary Computation Algorithm	IoT in general	Distributed random networks	Facilitate the lightweight authentication and authorization of IoT networked devices	MATLAB 2018a	Transaction latency	(+) facilitates the lightweight authentication and authorization of IoT networked devices (−) limitations related to the IoT devices were not taken into consideration

Table 2 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools	Evaluation metrics	Pros & Cons
[81]	2022	Distribution of InterPlanetary file system	Multimedia data sharing	Distributed networks	Ensure security against eavesdropping	Formal proof	Average delay	(+) provide high levels of security (−) some interoperability problems
[83]	2023	Public and private encryption keys + Ethereum platform	Electronic voting for smart cities	Distributed IoT network	Enhance the security and privacy of e-voting systems	Ethereum platform	Privacy of voters, transparency of the e-voting system	(+) allows users to verify the legitimacy of the voting process, promoting trust and reducing suspicions of fraud or manipulation (−) needs voter education and accessibility (−) must adhere to legal and regulatory requirements
[84]	2023	Consortium blockchain and data re-encryption	Healthcare IIoT	Distributed IIoT	Ensure data security in healthcare IIoT	Simulations on a healthcare system	Computational energy, network bandwidth, cost of data preservation	(+) efficient performance of the proposed approach (−) changes in the consortium's composition or objectives can impact the blockchain's future

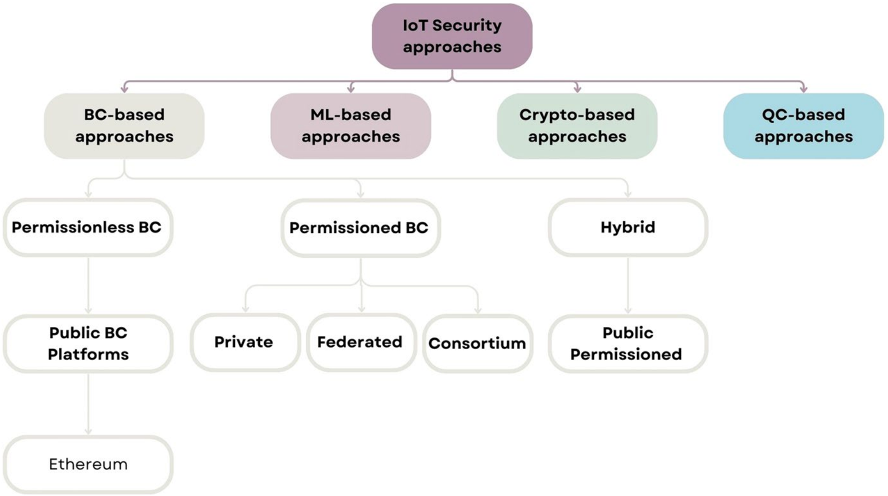

Fig. 4 Blockchain-based approaches

and lead to unnecessary disruption of normal device functioning. In contrast, the researchers need to test their proposed architecture on other IoT datasets.

Yazdinejad et al. [86] proposed multiple deep learning models to identify cyber threats and improve the accuracy of attack detection in the industrial IoT environment. The idea behind the proposed work is to combine various machine and deep learning models like long short-term memory (LSTM) and auto-encoder (AE) to detect abnormal attacks in the IoT environment. The combination of these models aims to create a powerful deep learning model and improve threat detection, additionally offering more detailed network traffic analysis, resulting in more precise and efficient cyber threat detection and mitigation. The proposed model was evaluated using two real datasets named secure water treatment (SWaT) and gas pipeline (GP). The evaluation results show a higher accuracy rate of 99.7% when compared with other machine learning classifiers even when with advanced existing models. However, the proposed model does not provide the exact location of anomalies in the system and its accuracy needs to be optimized and compared with other proposed advanced solutions

Alkahtani et al. [87] proposed a robust framework based on deep learning for intrusion detection in IoT environment. The proposed work used three deep learning algorithms to classify the malicious activities: a long short-term memory (LSTM), a convolution neural network (CNN), and a hybrid convolution neural network with the long short-term memory (CNN-LSTM) model. Moreover, to improve the classification algorithms, the particle swarm optimization method (PSO) was applied in the preprocessing stage. An attack dataset named IoTID20 was used to test the proposed framework. The experimental results have shown that the proposed framework can reduce attacks and enhance security in IoT environments, whereas the accuracy achieved was 96.60% and 99.82%, for CNN and

LSTM, respectively, and 98.80% for CNN-LSTM combined. Thus, the framework proves that it can effectively detect real-world attacks.

An intrusion detection system (IDS) based on deep reinforcement learning (DRL) algorithm was proposed by Tharewal et al. [88] to detect malicious activities and authorized access to industrial systems. In recent years, DRL has gained popularity among researchers due to its ability to learn how to deal with complicated issues via experimentation and failure and then improve its performance over time using a reward-based system. The system proposed is trained to detect patterns in data that are related to different kinds of malicious behavior, which help recognize possible risks on the industrial IoT. To clarify more, the combination IDS-based DRL provides various advantages compared to traditional IDS systems where it can both detect new and unknown intrusion, and it takes actions on incomplete or noisy data: typically in an industrial environment where devices "sensor and other" might not constantly provide accurate or complete data. The proposed system was evaluated using the real dataset of the industrial IoT publicly released by the US Department of Energy's Oak Ridge National Laboratory. The experiments have shown that IDS-based DRL is a powerful tool for protecting against several types of network threats on the industrial IoT. Thus, it gave better results compared with existing IDS based on deep learning in terms of accuracy, precision, recall rate, and F1 score. However, the proposed system does not provide intrusion detection in a distributed architecture which makes it vulnerable to adversarial attacks. Moreover, it needs high computational resources, which affects real-time performance.

A framework based forensics analysis was presented by Mazhar et al. [89] to detect attacks in IoT devices. Forensic analysis involves the identification, extraction, and assessment to what degree have the devices been damaged by the various attacks. The forensic analysis is carried out on the "logs" of the IoT devices, where logs refer to activities that have occurred on the device, like user actions, network activity or system events. The logs contribute significantly to investigating and identifying cyber-attacks on the device. The method used to detect cyber-attacks on IoT devices entails analyzing the device's logs to identify signs of a cyber attack, such as unusual network activity or suspicious user behavior. This research uses various machine learning model for the test, whereas forensic logging server named security onion generate the dataset from the logs. The models' performance is assessed based on accuracy, precision, recall, and F1 score. Based on the results obtained, the decision tree algorithm outperforms the other algorithms and demonstrates the best performance.

The goal of Javeed et al. [90] research paper is to provide a hybrid deep learning mechanism to protect the communication between various devices in IoT. The mechanism is a combination of deep learning and software defined network (SDN) for securing communication in IoT. The attackers can compromise the exchange of the large amount of data among the IoT devices. In this research, the deep learning enhance the security and determine the potential anomalies and threats in IoT data, while SDN prevents and mitigate these anomalies by implementing secure policies. The classifiers used in this research for threat detection are Cuda-deep neural network, gated recurrent unit (Cu-DNNGRU), and Cuda-bidirectional long short-term memory (Cu-BLSTM). These are considered a type of deep neural network that is often used for natural language processing and speech recognition tasks. The mechanism's evaluation achieves high performance in terms of accuracy, F1 score, precision, speed efficiency, and other evaluation metrics. The accuracy of the proposed mechanism achieved 99.87%. However, it is costly in terms of hardware and infrastructure implementation.

Liu et al. [91] addressed how DRL is potentially utilized to protect industrial IoT systems. They started by developing a DRL-based controller to manage a specific process in an industrial setting (for example, manufacturing assembly). The DRL-based controller is installed on an edge computing server to enable automated control in an IIoT context. Secondly, the authors examined two types of attacks: function-based attacks and performance-based attacks. Function-based attacks are attacks that occurred before the training phase, which can be performed when the controller is learning how to carry out an assigned work or controlling an industrial process or system. On the other hand, performance-based attacks are attacks that happened after the training phase which provide either poor decision making or failure to adapt to changing conditions. They investigated these attacks to understand the potential sorts of threats that exist and develop strategies to mitigate them. Thus, in the evaluation of the impacts of the two investigated attacks, the researchers discovered that the success of the attacks increased as the accuracy of the control model increased. This emphasizes the importance of developing strong defenses against DRL-based controller attacks, especially as these controllers become more precise and complicated. However, the proposed work focused only on two types of attacks—many other attacks can occur against DRL-based controllers. Furthermore, it provided a simplified simulation environment—not accurate in real-world IIoT systems.

Saba et al. [92] presented an intrusion detection framework based on advanced machine learning algorithms for IoT environment. In this solution, two fundamental methods were proposed. The first method is the genetic algorithm (GA) which was applied to choose the suitable features to enhance the accuracy of threat detection. The second method was dedicated to employing various advanced ML such as support vector machine (SVM), ensemble classifier, and decision tree. The evaluation results have shown that the accuracy achieved 99.8% using a multi-class NSL-KDD dataset (dataset commonly used in the field of intrusion detection to evaluate the performance of ML and DL algorithms) and 10-fold cross-validation. The model is capable of correctly classifying the various classes in the dataset. However, it is essential to point out that accuracy solely could not be the most effective metric to assess a classification model's performance.

Sahu et al. [93] proposed a new attack detection framework based on deep learning model to protect the IoT from malicious devices. Convolution neural network (CNN) is a type of neural network that is used to extract and analyze accurate data features. Furthermore, long short-term memory (LSTM) was combined with CNN to detect a wide range of attacks. Compared to other existing works, this research was evaluated using an up-to-date dataset that contains a bigger number of attack samples named IoT-23. The evaluation has shown that the hybrid proposed model can be an effective approach to detect a wide range of attacks and protect sensitive data in IoT environment. Additionally, the proposed model achieved an accuracy of 96%, which is a high percentage of malicious devices detection. However, the framework's computational overhead was extremely high.

Hasan et al. [94] examined the security challenges of the IIoT, especially the Botnet attacks. They proposed a hybrid DL approach to secure the IIoT from this kind of attack. Botnet attacks are a type of attack that compromises the network via computers to steal sensitive data, spamming, DDOS attacks or malware. To overcome this threat, a novel combination of long short-term memory-Deep Neural Network (LSTM-DNN) was proposed to identify attacks. To classify the various attacks, the N BaIoT dataset (the latest available dataset) was applied. The model proposed was compared with the existing hybrid detection model and it showed that can achieve a 99.94% of detection rate. However, their solution needs to be tested against other IoT attacks.

Yong et al. [34] presented a solution based on an ensemble of machine learning models to detect the webshell's threat in IoT environment. The webshell attack is a kind of malicious script that is injected inside a web server to perform an illegal bypass to the sensitive data and gain unauthorized remote access to the server. The solution used various traditional machine learning algorithms such as random forest (RF), extremely randomized trees (ET), and voting. The experiments were conducted on these models to measure the validity of webshell intrusion. The experiments found that RF and ET were effective in detecting webshell intrusion in lightweight IoT devices, which means they are suitable for devices with limited resources. On the other hand, voting is effective for devices that have unlimited resources in IoT environment. However, The proposed model only tested for webshell threats on PHP scripts whereas IoT servers could be implemented with other programming languages.

Jothi et al. [95] proposed a novel intrusion detection system (IDS) designed for IoT networks. The techniques used involve DL-based LSTM and a modified version called "whale integrated LSTM" (WILS) networks. The proposed system consists of three fundamental components: 1) The data collection component which collects the performance data of connected IoT devices, and 2) Device Recognition: when an attack is taking place, it recognizes devices that are performing maliciously, 3) The attack type prediction: The system forecasts the kinds of attacks that have been launched in the IoT network. Real-time simulations of IoT networks under various attack scenarios are created using an API called OMENT-python to assess the proposed IDS. Furthermore, the performance of the suggested model is also compared to other well-known datasets including CIDDS-001, UNSWNB15, and KDD. WILS models have proven to perform better than other intelligent models that are already in use. They demonstrate greater accuracy, precision, and recall, proving they are suitable for protecting IoT networks.

Musleh et al. [96] investigated the use of machine learning-based intrusion detection systems in IoT. The study primarily examined how feature extraction methods can boost intrusion detection's accuracy. The study compared several feature extraction methods and machine learning models. The relevant data is extracted by feature extraction algorithms from the raw data gathered by IoT devices. These algorithms significantly affect the IDS's overall performance and detection accuracy. Moreover, the study investigated methods for feature extraction, including image filters and transfer learning models (such VGG-16 and DenseNet). Several machine learning techniques are also evaluated, including SVM, K-nearest neighbors, and random forest. The study also investigated how well-stacked models combinations of several ML models perform. The integrated models' performance is assessed using the IEEE Dataport dataset. According to the study's findings, the VGG-16 (a particular neural network architecture) and stacking technique produced the best accuracy of 98.3%. This shows that the suggested methodology was successful in precisely identifying intrusions in the Internet of Things environment.

Xu et al. [97] presented a novel approach for addressing cyber-attacks and network intrusion in (IoT) applications. The proposed work investigated machine learning-based intrusion detection techniques. But these algorithms frequently have issues with classification accuracy and their capacity to deal with multi-class classification problems. The research introduces a combination of a data-driven approach and automated machine learning (AutoML) for intrusion and anomaly detection. AutoML is employed to select the most appropriate algorithm with optimized hyperparameters for classifying the data. Thus, an algorithm that solves a multi-class classification problem possibly referring to categorizing various forms of attacks or anomalies is the result of this research. The algorithm's outstanding 99.7% accuracy is achieved. This degree of accuracy far exceeds that of existing algorithms, demonstrating the accuracy of the suggested approach.

The comparative analysis of solutions based on machine learning is presented in Table 3.

According to this study, various approaches have been proposed for IoT security using ML. We can classify them into three main categories: 1) traditional ML-based approaches [34, 89, 92, 96, 97], 2) DL-based approaches [88, 90, 91], and 3) hybrid approaches [85–87, 93–95], a solution that combines the first two ones. For ML-based approaches, the approches used were: supervised and unsupervised approaches. For DL-based approaches, the approaches used were: deep reinforcement learning (DRL) and Software Defined Network (SDN). For hybrid approaches, the exisiting works combine LSTM with ML methods. Figure 5 shows the taxonomy proposed for ML-based relevant solutions.

5.3 Cryptography-based solutions

Cryptography includes all the processes aimed to encrypt information to ensure its security between the connected objects. Technically, the capacities of IoT are so limited that we cannot implement classic cryptography. In order to guarantee the authentication, integrity, and confidentiality of the data, it is necessary to design appropriate cryptographic mechanisms. Those cryptography mechanisms aim to respond to this, by building optimized solutions for these resource-constrained devices without compromising their level of protection.

In [98], M. Khalifa et al. discussed a lightweight cryptography framework to secure memory heap in IoT. This solution deals with the problem of security loophole generated by the garbage collection used by object programming languages. This security vulnerability can be seen in the Next Memory Address Occupation

Table 3 Comparative analysis of machine learning-based solutions

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools and datasets	Evaluation metrics	Pros & Cons
[85]	2022	Looking-Back concept based on conventional and advanced machines and deep learning methods: decision trees, random forest, K-nearest neighbors (KNN), the multilayer perceptron (MLP), and long short-term memory (LSTM)	IoT	Not mentioned	Detect and mitigate the denial of service "DOS" as well as distributed denial-of-service "DDOS" attacks in IoT	Data science libraries: Keras, Scikit-learn, and Pandas Bot-IoT dataset	Accuracy, precision, recall, and F1 score	(+) Real-time prediction of the cyber-attacks and ensure the continued functionality and security of IoT devices (−) The proposed work needs to be tested against adversarial learning attacks (−) The proposed work need to be applied with other datasets
[86]	2023	Hybrid machine and deep learning models: long short-term memory (LSTM) an auto-encoder (AE)	Industrial Internet of Things (IIoT)	Edge computing architecture	Identify the cyber threats and improve the accuracy of attacks detection in the industrial IOT environment	Real two datasets: secure water treatment (SWaT) and gas pipeline (GP)	Accuracy, precision, F1 score, recall, and training time(s)	(+) Higher accuracy rate of 99.7% while compared with other machine learning classifier (−) the proposed model does not provide the exact location of anomalies in the system (−) Needs accuracy optimization by comparing with other proposed advanced solutions

Table 3 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools and datasets	Evaluation metrics	Pros & Cons
[87]	2021	Deep learning algorithms: convolution neural network (CNN), long short-term memory (LSTM and hybrid convolution neural network with the long short-term memory (CNN-LSTM), Particle swarm optimization method (PSO)	IoT	Cloud-based architecture	Enhance intrusion detection in IoT environment	Jupyter Python 3.6, IoTID20 dataset	F1 score, accuracy, precision, sensitivity, recall, and specificity	(+) Evaluated with various evaluation metrics (−) High computational resources
[88]	2022	Deep reinforcement learning (DRL), Feature selection algorithm based on LightGBM	Industrial Internet of Things (IIoT)	Not mentioned	Detect malicious activities and authorized access to industrial IoT systems	Stable (2.10.0), TensorFlow (1.14.0), OpenAI Gym library (0.17.2), Real dataset: natural gas pipeline and transportation network	F1 score, recall, precision, and accuracy	(+) It can detect new and unknown intrusions (+) It can take actions on incomplete or noisy data (−) does not provide intrusion detection in distributed architecture (−) Vulnerable to adversarial attacks. (−) High computational resources, which affect the real-time performance

Table 3 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools and datasets	Evaluation metrics	Pros & Cons
[89]	2022	Forensic techniques analysis Third-party logging server Machine learning: Decision tree	IoT	Not mentioned	Protecting IoT devices from cybersecurity attacks such as launch brute force (BF) and denial of service	Metasploit framework that launch BF attack Raspberry Pi(IoT device), Kali Linux (attacking device), HPING3 (framework that launch DoS attack), Wireshark and squert Own generated dataset	Accuracy, precision, recall, and F1 score	(+) The ability to analyze a huge amount of data without affecting IoT devices' performance (+) Own generated and updated scalable dataset for IoT device attack detection (−) limited dataset of attacks
[90]	2021	Combination of deep learning and software defined network (SDN): Cuda-deep neural network and Gated recurrent unit (Cu-DNNGRU) Cuda-bidirectional long short-term memory (Cu-BLSTM)	IoT	Distributed fog/edge architecture	Protect the communication between various devices in IoT	Pandas, TensorFlow, Numpy, Scikit-learn, and Keras libraries (3.8 version of Python) CICIDS2018 dataset	Accuracy, F1 score, precision, and speed efficiency	(+) Dataset includes IoT network flow features with 14 up-to-date attacks: bot, botnet, DDoS, brute force (−) Higher cost in terms of hardware and infrastructure

Table 3 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools and datasets	Evaluation metrics	Pros & Cons
[91]	2021	Deep reinforcement learning (DRL): The deep deterministic policy gradient (DDPG) and The deep Q network (DQN)	IIoT (gravity water tank control)	Edge computing architecture	Protect and Increase the control performance of the physical plant to avoid the complete disruption of the IIoT system	TensorFlow, Keras (Python), OpenAI gym	Accuracy (control loss), Convergence threshold	(+) Ensure security against relevant attacks (−) The proposed work focused only on two types of attacks- Many other attacks can be occured against DRL-based controllers (−) Simplified simulation environment—not accurate in real-world IIoT systems
[92]	2021	Advanced machine learning algorithms: Support vector machine (SVM), ensemble classifier, Decision tree Genetic algorithm (GA)	IoT	Not mentioned	Protect the IoT environment against intrusion and enhance the detection rate	NSL-KDD dataset	Accuracy, confusion matrix	(+) Enhance the accuracy of intrusion detection (−) The proposed work need to be evaluated with other performance metrics such as precision, recall, and F1 score

Table 3 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools and datasets	Evaluation metrics	Pros & Cons
[93]	2021	A hybrid deep learning model: convolution neural network (CNN) and short-term memory (LSTM)	IoT	Not mentioned	New attack detection framework based on deep learning model to protect the IoT from malicious devices	TensorFlow, IoT devices: a Somfy smart door lock, an Amazon Echo home-based intelligent personal assistant, anda Philips HUE smart LED lamp, Raspberry Pi IoT-23 dataset	Accuracy, precision, recall, specificity, and F- measure	(+) Up-to-date dataset with bigger number of attack samples (325 million traffic flows) (+) Identifying malicious devices with higher accuracy rate (−) Computational overhead
[94]	2022	Hybrid deep learning approach: long short-term memory-deep and neural network (LSTM-DNN)	IIoT	Edge computing architecture	Secure the IIoT sensitive data from the Botnet attacks	TensorFlow, Keras (Python library), Pandas, Scikit-learn, Numpy, sklearn library, Spyder Tool, Anaconda Platform, NBaIoT dataset	Accuracy, precision, recall, and F1 score	(+) Achieve a high-security rate (−) Needs to be tested against other IoT attacks

Table 3 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools and datasets	Evaluation metrics	Pros & Cons
[34]	2022	Ensemble of machine learning models: traditional machine learning algorithms such as random forest (RF), extremely randomized trees (ET), and voting	IoT	Not mentioned	Detect the webshell's threat in IoT environment	Malicious PHP scripts dataset	Accuracy, precision, recall, and F1 score	(+) Detecting webshell intrusion in lightweight IoT devices—suitable for devices with limited resources (−) The proposed model only tested for webshell threat on PHP scripts—IoT server could be implemented with other programming languages
[95]	2023	DL-based LSTM and a modified version called "whale integrated LSTM" (WILS) networks	IoT	Client-server	Intrusion detection system (IDS) designed for IoT networks	OMENT-python CIDDS-001, UNSWNB15, and KDD datasets	Accuracy, precision, recall	(+) Perform better than other intelligent models that are already existed: greater accuracy, precision, and recall (−) The proposed work is less effective as IoT networks get more complicated and large

Table 3 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools and datasets	Evaluation metrics	Pros & Cons
[96]	2023	Feature extraction with ML-based algorithms: K-Nearest Neighbor (KNN), Random forest (RF), and Sequential Minimal Optimization (SMO)	IoT	Not mentioned	Examine how feature extraction methods can boost intrusion detection's accuracy	VGG-16 Transfer Model, DenseNet IEEE Dataport dataset	Accuracy, precision, recall, and F-measure	(+) The combined VGG-16 (a particular neural network architecture) and stacking technique produced the best accuracy of 98.3% (−) Collecting and labeling large and diverse datasets for intrusion detection consume time and resources
[97]	2023	Combination of a data-driven approach and automated machine learning (AutoML) for intrusion and anomaly detection	IoT	Not mentioned	Intrusion and anomaly detection in IoT	MATLAB KDDcup99 dataset	Accuracy, Normalized Mutual Index (NMI), F1 score, and Kappa	(+) Higher accuracy compared to existing intrusion detection system: 99.7% (−) Needs to be tested with new types of attacks and using reinforcement learning

(NMAO) attack, the memory replay attack, and the Learning Tasks Behaviors (LTB) attack. The aim of this study is to protect the system operation of the IoT environment from memory heap penetration and address modification attack, caused by the NMAO attack, which is capable of using the garbage in the heap attack through the LTB process.

The authors used two steps to solve this problem: the first step is to execute a protection process from the user address using a trusted platform module, and to prevent the malicious operations which consist of usurping the identity of a third party, this step is called hardware authentication step. The second step consists of using a cryptographic hash function in order to make access violation more difficult for garbage collection in the object being executed.

To secure the memory heap, authors used the garbage collection encryption based on cryptographic hash function, one-time key, and L-function-based elliptic curve cryptography. The hash function is used because it provides a large key space, that is why it has higher security.

The IoT prototyping, the proposed frameworks, AES with SHA-1 and RSA with SHA-1 algorithms, have been simulated and implemented using Java NetBeans. The analysis of encryption and decryption computational times for the three algorithms shows that the proposed ECC-based hash and OTK has the lowest encryption and decryption times compared to AES and RSA with SHA-1.

In [99], Liu et al. proposed a Multiple Application Secure Data Aggregation (MASDA) mechanism to ensure data confidentiality without losing the integrity of data transmission. The idea of this mechanism is based on cluster network topology. Each cluster member encrypts the data to send using the privacy homomorphic encryption algorithm based on the elliptic curve encryption algorithm, after encrypting the data, the same cluster member creates a shared key with the cluster head; this key will be used to generate a message authentication code that will be sent with the ciphertext to the cluster head. When the latter receives the message, it checks if the message authentication code of the ciphertext is valid. If so, the cluster head aggregates and transmits the ciphertext to the base station. Then, this aggregated ciphertext will be decrypted.

The use of the homomorphic encryption algorithm is essential because even if someone knows the data, he could not calculate the message authentication code. The authors used a mechanism that includes the signature, the aggregation, and the verification algorithms; this mechanism is called iHMAC, which is an improved homomorphic message authentication code. The iHMAC can verify the integrity of the data and prevent the injection of false data by an attacker.

The elliptic curve encryption scheme can reduce the communication overhead and the computation complexity by encrypting different application data that will be aggregated later at the cluster head in the ciphertext. Using this algorithm, the proposed mechanism provides confidentiality in the presence of a probabilistic polynomial time adversary; therefore, MASDA can defend against both active and passive attacks.

OMNET++ is used as the simulation platform. The authors compared the simulation results of MASDA with those of EC-OU and EC-EG mechanisms. In terms of computation overhead, EC-EG is better than EC-OU and MASDA, but it has weaker

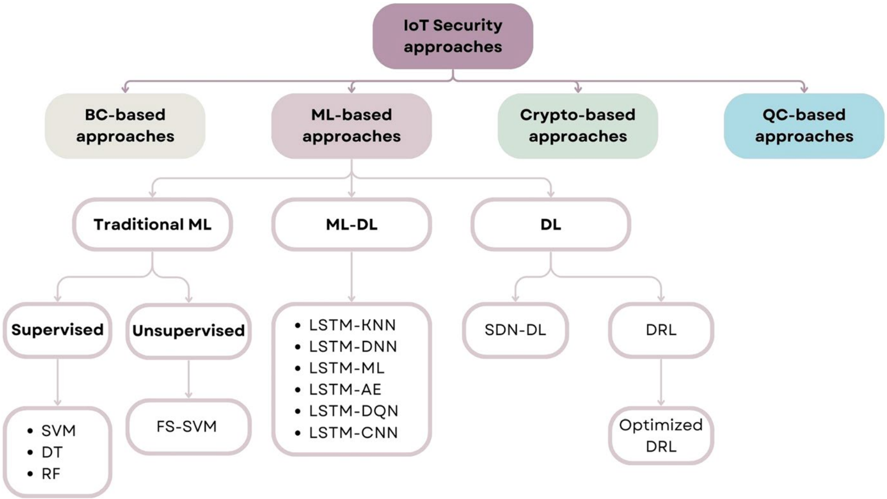

Fig. 5 ML-based approaches

encryption strength. As the base station has unlimited resources, the big computation overhead of MASDA in decryption does not affect the lifetime of WSNs. The second evaluation metric is communication cost; this metric is related to the length of the ciphertext. Results show that the length of ciphertext in EC-EG is smaller than the length of ciphertext in MASDA, and the ciphertext length of MASDA is also gradually smaller than EC-OU. Therefore, the decrease in communication cost is a challenge for future studies. The authors also compared the aggregation accuracy of the three mechanisms, and from the results, we can see that MASDA is the best one. Despite that, the impact of packet loss rates on aggregation accuracy should be verified.

A Certificate-Based Signature Scheme for IIoT based on hyperelliptic curve cryptography (HECC) was presented by Ullah et al. in [100], in order to improve the security while using a small key size. This proposed system network is composed of five parts: the certificate authority that act as trusted third party, the cloud server that could be used to store the generated data from the IIoT devices, the IIoT objects and devices responsible for generating data and send it to the edge using the Bluetooth Low Energy technology, the fourth entity is the edge node, after receiving the certificate from the certificate authority, it creates the key pair and produce the certificate-based signature. This certificate-based signature is validated by the fifth entity, data users, after receiving it from IIoT devices. Both IIoT devices and data users transmit the data to a cloud server using a 5G wireless link.

The authors used hyperelliptic curve cryptography that is similar to ECC but with a smaller key size, which is suitable for this type of network. A formal security analysis was performed using the Random Oracle Model and the hyperelliptic curve discrete logarithm problem (HECDLP), to ensure the security of the proposed scheme against two types of adversaries. After performing a comparison study about computational cost of the proposed scheme compared to other approaches, using exponential operation EPL, hyperelliptic curve divisor multiplications, and bilinear pairing. Results show an improvement in the computational cost of the proposed scheme, which means it consumes less time. Same as computational cost, results of communication cost show an improvement in computational communication overhead compared to the same other approaches.

Khan et al. [101] developed a methodology with cosine function hybrid chaotic map encryption to deal with the huge data theft and privacy leak of patients' data security and confidentiality in smart healthcare systems and industrial IIoT.

Authors proposed an architectural adjustment to control the healthcare and IIoT system in a smart way. First, they presented the concept of extracting keyframes from images and visual information by installing visual sensors, they employed a keyframe extraction methodology with energy and bandwidth constraints in order to diminish data redundancy, and this lightweight extraction methodology used the improved YOLOv3 algorithm. The main focus of this methodology is to extract the proper keyframe from the summarized visual information (video), which comes from installed wireless multimedia objects in the smart healthcare system. Secondly, they used a lightweight cosine encryption function based on chaotic hybrid map, the idea is to generate a pseudorandom number sequence from the cosine function of chaotic sequence with the incorporation of a secret key into the keyframe images, and then, it performed confusion and diffusion operation into the keyframe image. This approach has a strong security against any type of adversary. This methodology could be applied to, not only, YOLOv3 algorithm, but to many other hybrid technologies such as Python and TensorFlow.

Simulation of this approach has been done by MATLAB, and the security analysis has been made with the help of test images from the USC-SIPI database of digital images. This analysis shows an efficient security in terms of encryption speed compared to eight other methods with different keyframe sizes. The second metric is the histogram analysis, which is an illustration of the graphical representation of the pixel rate distribution in the keyframe images. This analysis shows that the proposed approach has avoided statistical and numerical attacks, and also has ensured integrity and consistency during transmission. Numerous other security analysis results show the efficiency of the proposed methodology. This approach has also minimized the storage cost, the bandwidth and the communication and transmission cost. The weak aspect in this work is the use of public keys for encryption.

Jerbi et al. [102] investigated the security issues that threatened IoT networks. They developed a lightweight cryptographic technique based on ECC. The proposed scheme is called CoopECC that requires distributed and cooperative tasks between the network nodes to alleviate the ECC computations, specifically, the scalar multiplication point. The authors considered a cluster-based architecture where the cluster head (CH) is responsible for collecting, encrypting, and forwarding the data to the IoT gateway. The CH memory is shared between its cluster members and contains all exchanged data. To accelerate the ECC point multiplication, the scalar bits are divided into several parts equal to the number of cluster members. Each member performs the multiplication and returns the output to the CH that combines all received results. The CoopECC provides better time consumption compared to the baseline ECC. However, it is not secure against malicious cluster members.

Chanal et al. [103] proposed a hybrid encryption scheme that leverages the advantages of message digest algorithm (MD5), advanced encryption standard (AES), and ECC to secure IoT communications. It involves three phases: generation of plaintext's hash value at the source node using MD5, key generation using ECC, and encryption of the digest using AES. The ciphertext is added with the public key and a geotag (i.e., the receiver location information shared with the sender) and then sent to the destination node. The proposed scheme achieves an improved encryption time, low end-to-end delay, and high throughput compared to AES algorithm. Nevertheless, it is vulnerable to collision attacks since it is based on MD5 algorithm.

Unal et al. [104] proposed the SCSS, a secure cloud storage system for cloud-based storage environment without the need for complex certificate management, with secure and efficient Type-3 pairings, supporting Encryption-as-a-Service (EaaS) and multiple Public Key Generators (PKGs), based on SAKKE-IBE scheme. The first fundamental concept of the SCSS-SAKKE-IBE scheme is EaaS, the role of EaaS is to avoid implementing an encryption application on the user's device, encryption can therefore be provided by this service; therefore, it makes it possible to reduce the difficulty of encryption and key management tasks without losing data confidentiality. The second fundamental concept is identity-based cryptography (IBC) and its most important application: identity-based encryption (IBE). In IBE, the unique information about the identity of a user is his public key, as it is a type of asymmetric encryption, the encryption is performed using the public key and the decryption using the private key, if the user keeps its private key safe, EaaS will never be able to decrypt the data. The problem of EaaS service provider is the lack of trust, and the key generation method in the identity-based cryptography is based on escrow mechanism that requires trust, the solution of this problem is the distribution of trust by using the PKG method. To improve system security and distribute trust to the encryption service, the authors used an additional Trusted Third Party (TTP).

The main components of the proposed scheme are the user client or end users, service controller where the services are listed, key management service responsible for generating the public keys, encryption service ensures all encryption processes, and storage service that performs file storage on local or cloud storage.

Analytical and experimental results show that the proposed SCSS-SAKKE-IBE scheme gave better results compared to other IBE-based cloud security solutions such as HIBE and ABE, first it managed to reduce the encryption and decryption time. Scalability also has been improved, especially for the decryption process, which increases the level of security and performs well in IoT-based environments where the number of users is large. The improvement of decryption operation is necessary since it is needed for forensic analysis.

Liu et al. [105] a multi-keyword encryption and searchable scheme based on attributes supporting privacy and integrity concepts of health data to ensure the application functions of the medical IoT (mIoT). The proposed scheme relies on two main properties, anonymous key generation, and access validity. First property was used because the private key must be generated anonymously based on blind signature, the main idea here is that the Trusted Center Authority generates private keys but cannot decrypt the ciphertext. To ensure the access validity of the shared data, authors presented a time division mechanism with a hash function.

The main framework is composed of seven phases: System Setup, User Registration where the anonymous key generation algorithm is called between the Center Authority and the system user, Ciphertext Uploading to encrypt data, Trapdoor Generation, Authorization, Ciphertext Retrieval, and Ciphertext Decryption.

A theoretical performance evaluation and comparison was made between the proposed work and several related works in terms of functions and computational complexities of the proposed schemes, and a series of experimental performance evaluation shows the efficiency and feasibility of this scheme. Results show that this scheme has better functionality compared to ABKS schemes in terms of access validity, integrity verifiability, and key escrow. The proposed work provides an anonymous key generation mechanism which is suitable for cloud storage and practical applications in mIoT. Results of computation overhead show also that this scheme has less amount of computation in encryption, index generation, trapdoor generation, search and decryption compared to other schemes. Simulation results show that the computation costs of the proposed scheme are efficient in application compared to the other ABKS schemes. Therefore, it can be used to resource-constrained devices.

Sahmi et al. [106] discussed a new approach that secures the MQTT IoT application protocol, this approach consists of using AugPAKE Algorithm and PRESENT lightweight encryption on the PUBLISH messages. The main idea is based on Aug-MQTT solution by bringing more lightness and security to the MQTT communication between publisher and subscriber. The difference between Aug-MQTT and the proposed approach is that authors in Aug-MQTT used AES as a secure symmetric key encryption, which is too heavy for IoT environment also they only used encryption in client to broker way. In the proposed scheme, authors used an end-to-end encryption using PRESENT algorithm, and AugPAKE algorithm to establish a secure key session. The solution supported some security properties: authentication between the broker and their clients, confidentiality because the message is protected using the secure session generated by AugPAKE and encrypted using the PRESENT encryption. Also, the solution ensures Integrity and non-repudiation properties by maintaining end-to-end security in the communication.

The proposed contribution has some advantages compared with other works like mutual authentication, confidentiality, privacy, and integrity. It also shows robustness against Man-in-the-middle attack, the offline password guessing attack, and replay attack. But the comparison of the estimated cost time between the proposed solution and Aug-MQTT and Auth-MQTT approaches does not show advantages of the proposed scheme. This approach needs to be simulated on an appropriate architecture in order to see its robustness against attacks.

Gong et al. [107] addressed the lack of security caused by resource-limited in IoT environments, they presented an efficient certificateless hybrid signcryption scheme. The purpose behind this scheme is to ensure security and efficiency of data transmission in IoT. The advantage of the certificateless cryptography system is that it solves the problem of public key authentication and key escrow in IoT by forming a public key using the public information of the connected object; moreover, it uses the Key Generation Center to generate the private 2key. But it still has some problems in securing the transmission, because it is not easy to simultaneously ensure the different IoT security concepts such as semi-public verifiability, forward security, and known session-specific temporary information security with the existing systems, and also, the problem of resource-constrained devices created by the big amount of resources consumed by bilinear operation. The proposed solution to this last problem is to put the bilinear calculation process in the initialization phase to guarantee security in the communication process, and to replace the communication process with an exponential computation.

Authors used Random Oracle Model, Computational Diffie-Hellman, and Decisional Bilinear Diffie-Hellman (DBDH) problem assumptions to prove the security of the proposed scheme. The efficiency of the proposed scheme has been compared to existing certificateless hybrid signcryption schemes using computing overhead and communication cost. Results show that the proposed scheme improves computational efficiency and has higher security.

Mousavi et al. [108] addressed the security of data transmission in IoT-based smart irrigation systems. They proposed an encryption scheme based on ECC, secure hash algorithm (SHA-256), and artificial bee colony algorithm (ABC). This latter is employed to optimally generate the private key in ECC that is used for the decryption process. The SHA-256 guarantees data integrity in all types of communications. Furthermore, bit-wise and left-shift operations were applied after ECC encryption to strengthen data confidentiality. The proposed scheme is assessed in terms of encryption/decryption times and throughput. It outperforms three cryptographic models including RSA-AES, 3DES-ECC-SHA-256, and RC4-ECC-SHA-256. In addition, it tackles relevant security attacks orchestrated by malicious adversaries, such as man-in-the-middle and brute force attacks.

Bettoumi et al. [109] proposed LC-DEX: a secure and efficient energy solution to deal with the challenges of IoT environments such as requirements of high-level security and limited capabilities of its connected devices. Authors used a suitable protocol for constrained devices: the Host Identity Protocol Diet EXchange (HIP DEX) because it is resistant to some types of attacks like denial-of-service and man-in-the-middle attacks. The solution is based on the compression of 6LoWPAN header, using CoAP and RPL protocols.

To reduce the energy costs, authors used four essential HIP signaling packets (UPDATE, NOTIFY, CLOSE, and CLOSE_ACK), but proposed to remove the NOTIFY packet for security consideration, and as another possible optimization is to remove the CLOSE_ACK packet and terminate immediately the connection after sending the CLOSE packet. To optimize the communication overhead of HIP DEX packets, HIT_I and HIT_R header fields have been omitted and DNS has been introduced in the HIP DEX opportunistic mode to minimize the computation cost.

The evaluation of the proposed scheme was conducted on a real experimental platform called FIT IoT-LAB using CoAP as an application protocol, TCP protocol in transport layer, and 6LowPAN-RPL as a network protocol. HIP DEX code has been modified to enable handshakes in 6LoWPAN. The performance of HIP DEX packet header compression shows an excellent minimization in HIP DEX handshake packets' sizes, end-to-end transmission and propagation delay, and processing overhead. The evaluation of the energy consumption during the HIP DEX handshake execution shows improvement in multi-hop energy communication cost in comparison of some existing solutions. The proposed distribution model contributes to secure communication over the IoT-based-WSN architectures with minimal energy.

In [110], Kumari et al. proposed a secure data transmission model for e-health applications, using the two principal encryption algorithms RSA and AES, and two steganography techniques. The suggested scheme is made up of four processes, in the first step, data is encrypted using AES's secret key and RSA's secret public key. The RSA's private key will also be encrypted using the AES key. In step two embedding procedure, the steganographic approach Haar-DWT is implemented. The 2D-DWT-2L method is used in the third step to extract the secret message. And in the last step RSA's private key is used to decrypt the encrypted data.

The numerical simulation tests show that the proposed model results better peak signal-to-noise ratio (PNSR), Structural Similarity Index Measure (SSIM), and mean squared error (MSE) compared to DWT and DWT-DCT works. It also shows better resilience to attacks on the filter, and noise.

Al-Zubaidie [111] presented a new key exchange model based on lightweight and high-security techniques for e-health applications. Two algorithms were used in this scheme; Elliptic curve Diffie-Hellman (ECDH) protocol which is a lightweight version of Standard Diffie-Hellman (DH) used to reduce the large keys size of DH. The second algorithm used in this protocol is the lightweight QUARK hash function (QH). The proposed model contains five steps; first, in the pre-deploiment phase, the network devices are loaded to the Base Station with default settings.

In the second step, the sensors complete the registration process, the Quark algorithm is used in this step. Keys update phase is the third phase which ensures that keys are new and safe using ECDH protocol. The next phase is session key distribution. And final step is the session protection phase where the keys are stored on a protected device. The proposed protocol has been simulated using the Scyther tool and results showed that it was safe against attacks and threats, and also it balanced security and performance results.

Table 4 presents the comparative analysis of solutions based on cryptography.

According to this study, we classify Crypto-based approaches into three categories: Traditional cryptography, Modern cryptography and Lightweight cryptography, as illustrated in Fig. 6.

5.4 Quantum Computing-based Solutions

The emergence of quantum computing has the potential to revolutionize various fields, including the security of IoT. Researchers have proposed quantum computing-based solutions to enhance the security and privacy of IoT devices.

In [112], the authors proposed a quantum computing-based optimization technique for the IoT platform using a modified deep residual approach. The IoT platform generates a vast amount of data, which requires efficient processing and optimization techniques. The proposed approach combines quantum computing with deep learning techniques to optimize the performance of the IoT platform.

The idea of the proposed approach is to first convert the classical deep residual network into a quantum circuit using a quantum circuit library. Then, the quantum circuit is trained on a quantum simulator or quantum computer using a quantum neural network. Finally, the trained quantum circuit is converted back into a classical deep residual network.

This method leverages a quantum hash function to enhance the security of information transmission. It also uncovers potential threats within an RNN and CNN architecture and facilitates the analysis of threats and the exploration of intricate network patterns in noisy data, in order to establish robust security measures for IoT data.

It is also designed to reduce the training time and to improve the accuracy of the IoT platform. The experimental results showed that the proposed approach outperforms traditional techniques in terms of accuracy and training time.

Shahid et al. [113] proposed a new approach to secure the IoT using a distributed ledger that is resistant to attacks from quantum computers since the current security measures used in IoT are vulnerable to quantum computing attacks. The idea is to use a post-quantum distributed ledger that is based on a lattice-based cryptosystem. The latter is known to be resistant to attacks from quantum computers due to the difficulty of solving certain mathematical problems in this system. Each IoT device participating in the ledger keeps a copy of the ledger and contributes to the consensus process by validating transactions and verifying the integrity of the ledger. Blocks containing transactions are added to the ledger in a decentralized and secure way. The ledger also makes use of a consensus method to guarantee that everyone agrees on the ledger's current status.

To ensure that the proposed approach is lightweight, energy-efficient, and suitable for resource-constrained IoT devices, the authors proposed the use of a proof of storage mechanism, which eliminates the need for participants to perform computationally demanding proof of work (PoW) or proof of stake (PoS) calculations in favor of storing a small amount of data.

The proposed approach also included a security analysis which proves that the system is resistant to attacks from both classical and quantum computers. Moreover, the performance results showed that the system is efficient and suitable for use in resource-constrained IoT devices. However, the use of a lattice-based cryptosystem, which is the backbone of the proposed approach, may require additional computational resources, especially for devices with limited processing power. This may limit the adoption of the proposed method in some IoT applications.

In [114], the authors proposed a new approach to improve the security of the internet of vehicles (IoV). The approach uses a post-quantum signature and is based on a new technique to perform division operations in the lattice-based cryptosystem, called systolic divisions, which improves the system's efficiency. The main idea is to use digital signatures to ensure the authenticity and integrity of messages exchanged between IoV devices. This provides enhanced security compared to traditional cryptographic algorithms.

Table 4 Comparative analysis of Cryptography-based Solutions

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification Tools	Evaluation metrics	Pros & Cons
[98]	2020	Cryptographic Hash Function (CHF), One-time key (OTK), Elliptic curve cryptography (ECC)	IoT	IoT embedded systems and sensor networks	Protect the IoT system operation from memory heap penetration and address modification attack by encrypting the object garbage collection at run time	Java NetBeans platform for the IoT prototyping and the implementation	Encryption and decryption time	(+) The proposed work has minimum encryption and decryption time comparing to AES-SHA-1 and RSA-SHA-1 methods (−) The proposed work needs to be compared with other hash functions
[99]	2022	Elliptic curve cryptography (ECC), Homomorphic message authentication	Multiple applications of WSN	WSN Cluster network topology	Implementation of a multiple applications secure data aggregation mechanism to ensure the data confidentiality without losing the integrity of data transmission	OMNET++	Computation overhead, Communication cost, Aggregation accuracy	(+) The proposed mechanism can maintain the higher security, the longer lifetime, and better accuracy (−) The impact of packet loss ratio on the aggregation accuracy is not discussed (−) Not the lowest costs in comparison results

Table 4 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification Tools	Evaluation metrics	Pros & Cons
[100]	2022	Certificate-based signature, Hyperelliptic curve cryptography (HECC),	IIoT	Edge computing architecture for IIoT that uses BLE and 5G	Reduce computational and communication costs in the IIoT environment	Random Oracle Model (ROM), a formal security analysis	Computational Cost, Communication Cost	(+) The proposed scheme is better in terms of computation and communication costs (+) It improves security against known and unknown attacks (−) Computational and communication costs of the proposed scheme were compared with some schemes from 2016, while the proposed work was published in 2022 (−) The small key size used by the HECC can lead to password attack vulnerabilities

Table 4 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification Tools	Evaluation metrics	Pros & Cons
[101]	2022	Cosine function, Hybrid chaotic map encryption	Healthcare, Industrial Internet of Things (IIoT)	Integral sensor-based IoT architecture	Preserve the personal patients' data and stop the data theft and the privacy leakage	MATLAB	Encryption speed, Information entropy, Differential attack, Correlation analysis, Produced key, Surveillance systems analysis	(+) The work endorses the commanding characteristics of patient-based privacy in terms of an encrypted matrix to avoid any adversary outbreak (+) The work also approved that the numerous rigorous security threads can withstand (−) The use of a public key
[102]	2021	Elliptic curve cryptography (ECC)	WSN-based IoT	Cluster-based WSNs for IoT	Using parallel and cooperative technique to distribute ECC complex operations between the cluster nodes	TOSSIM simulator	Computation time, Consumed energy, Network's lifespan	(+) Distributed and collaborative computations among cluster members to speed up cryptographic operations (−) CH selection and CM authentication are not discussed

Table 4 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification Tools	Evaluation metrics	Pros & Cons
[103]	2021	Elliptic curve cryptography (ECC), MD5 AES	IoT	Three-layered IoT	Combination of MD5, ECC, and AES to provide data confidentiality for IoT devices	Not mentioned	Encryption time Decryption time Memory cost End-to-end delay Key size Throughput	(+) Improved encryption time, Data confidentiality and integrity (−) Vulnerability against collision attacks (MD5) (−) Secret key distribution is not considered
[104]	2021	Identity-based cryptography (IBC), Encryption-as-a-Service (EaaS) Public Key Generators (PKG)	IoT	Cloud systems	Development of a secure cloud storage system with secure and efficient Type-3 pairings, supporting Encryption-as-a-Service (EaaS) and multiple Public Key Generators (PKGs).	MIRACL cryptographic library	Setup time Private key generation time, Encryption time Decryption time	(+) The proposed scheme has very low private key generation, encryption, and decryption times (+) It demonstrates higher scalability then other pairing-based IBE schemes (−) Applying the proposed scheme in other scenarios that require higher level of security and where the key management becomes highly complex

Table 4 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification Tools	Evaluation metrics	Pros & Cons
[105]	2021	Attribute-based encryption, Anonymous Key Generation	Medical Internet of Things	mIoT electronic medical sensors	A multi-keyword searchable encryption scheme based on attributes supporting the data privacy preservation and integrity verification of the electronic health files to ensure the application business functions of the mIoT	Java pairing-based cryptography library (jPBC)	Computation overhead, Encryption time, Decryption time, Search time, Index generation time, Trapdoor generation time	(+) Data security, keyword security, integrity verification, collusion resistance, fast multi-keyword search (+) Reduce the computational costs of encryption, decryption and search (−) Completeness of the files including the keyword returned by the cloud has not been verified

Table 4 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification Tools	Evaluation metrics	Pros & Cons
[106]	2021	Augmented Password-Authenticated Key Exchange (AugPAKE) PRESENT encryption	IoT	Not mentioned	Secure the MQTT protocol using AugPAKE Algorithm and PRESENT encryption	No simulation	Estimated cost time	(+) Proposed solution support: user anonymity, mutual authentication, confidentiality, privacy, integrity, robustness against some attacks like man in the middle, offline password guessing attack, the replay attack (+) Better estimated cost time. (−) The work does not support the authorization property (−) No simulation

Table 4 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification Tools	Evaluation metrics	Pros & Cons
[107]	2021	Certificateless hybrid signcryption	IoT	Not mentioned	The purpose behind this work is to ensure the security and efficiency of data transmission in IoT using a lightweight certificateless hybrid signcryption scheme	Random Oracle Model (ROM)	Computing overhead Communication cost	(+) The scheme satisfies confidentiality, unforgeability, semi-public verifiability, forward security and known session-specific temporary information security (−) It would be better to perform a simulation to compare the proposed work with other schemes, especially the signcryption and unsigncryption time
[108]	2021	Elliptic curve cryptography (ECC), SHA-256 Artificial Bee Colony	IoT smart irrigation system	IoT smart sensor nodes	Leveraging ECC, SHA-256, and ABC to improve IoT data confidentiality and integrity	Not mentioned	Encryption time Decryption time Throughput	(+) Security against relevant attacks (−) Comparison to optimization methods for generating private keys

Table 4 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification Tools	Evaluation metrics	Pros & Cons
[109]	2021	Elliptic curve cryptography (ECC)	IoT	WSN-based-IPv4-IoT, WSN-based-6LoWPAN-IoT	Secure and energy-efficient end-to-end communications based on the compression of 6LoWPAN header for HIP DEX packets	FIT IoT-LAB	Energetic communication and computational costs, Communication and processing overhead End-to-end transmission and queuing delay Handshake packets' sizes	(+) Optimization of cryptographic computation overhead, delay, and energy costs (+) Secure the communication over the IoT architectures (−) No formal security analysis has been provided in the results

Table 4 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification Tools	Evaluation metrics	Pros & Cons
[110]	2023	Advanced encryption standard (AES) algorithm. Rivest, Shamir, and Adleman (RSA) algorithm 2D-DWT-1L and 2D-DWT-2L steganography techniques	E-health applications	Medical sensors networks	Hybrid security model to secure the diagnostic text data in medical images, by encrypting data using a hybrid encryption method, then the encrypted data is hidden in a cover picture using steganography techniques	Not mentioned	Peak Signal to noise atio (PNSR), Structural Similarity Index Measure (SSIM) Mean squared error (MSE)	(+) The proposed work has better MSE, PSNR, and SSIM (+) Resilience to attacks on the filter, and noise (−) RSA and AES use long keys; thus, encryption and decryption process will take longer time, which is not suitable for IoT applications (−) No Computational and Communication Cost

Table 4 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification Tools	Evaluation metrics	Pros & Cons
[111]	2023	Elliptic curve Diffie-Hellman (ECDH) QUARK hash function (QH)	E-health applications	Health sensor networks	A key exchange protocol which balances security and performance using lightweight and high-security techniques	Scyther tool	Computational Cost Communication Cost Execution time for key exchange. Data size Number of handshakes	(+) The proposed protocol is safe against attacks and threats (+) Ensuring authentication, authorization, access control, and data availability (+) Balanced performance of computational and communication costs (−) The protocol is dependent on the Base Station (−) The proposed scheme has not been verified if it is scalable

On the one hand, the lattice-based cryptosystem is based on the mathematical concept of lattices, which are complex mathematical structures that can be used to encode information in a way that is difficult to decipher. On the other hand, the use of systolic divisions improves the efficiency of the signature generation and verification process, making it suitable for use in resource-constrained IoV devices. Systolic divisions are based on a hardware-efficient approach that allows the efficient implementation of division operations in hardware.

A security analysis of the proposed approach was used to prove its efficiency. It showed that it is resistant to attacks from both classical and quantum computers.

Qu et al. [115] proposed a new secure quantum fog computing model based on blind quantum computation (BQC). The proposed model combines quantum computing and fog computing in order to provide a more secure and efficient approach to data processing in a distributed computing environment.

The proposed architecture consists of three layers: the cloud layer, the fog layer, and the device layer. The cloud layer provides high-level services. The fog layer provides local services to devices in proximity. The device layer consists of the edge devices that collect and process data.

The authors also proposed a new quantum fog computing protocol based on BQC, which enables secure data processing in a distributed environment. The protocol uses homomorphic encryption to encrypt the input data, and BQC to perform the computation on the encrypted data. The computation result is then decrypted using a private key, ensuring that the data is processed in a secure and private manner.

The authors proved the efficiency of the proposed architecture and the proposed approach by analyzing different attacks on one fog node. However, the use of homomorphic encryption can add computational overhead, which may impact the performance of the system.

In [116], a new scheme based on continuous-wave (CW) technology was proposed. The idea is that CW is more compatible with existing fiber-optic communication networks than previous pulse-based quantum cryptography schemes. The approach was designed to be adaptable, allowing for various security levels and network condition changes. Additionally, it has zero-trust security, which means that it does not rely on a central authority or key distribution.

In the proposed scheme, the sender (IoT device) creates a stream of single-photon pulses using a continuous-wave laser, which are subsequently sent via the fiber-optic network. The single-photon detectors used by the IoT devices that are receiving the pulses measure the photons' states to identify the communication's encryption key.

The scheme incorporates various security measures to prevent attacks, such as eavesdropping and man-in-the-middle attacks. It also includes mechanisms for error correction and privacy amplification to ensure that the transmitted data is accurate and private.

The performance of the proposed idea was demonstrated formally and the results showed its ability to provide secure communication for IoT devices.

Even though the proposed scheme is flexible, allowing for different levels of security and adaptability to changing network conditions, its transmission distance may be limited by factors such as photon loss and noise in the fiber-optic network. It also may not be scalable to large-scale IoT networks.

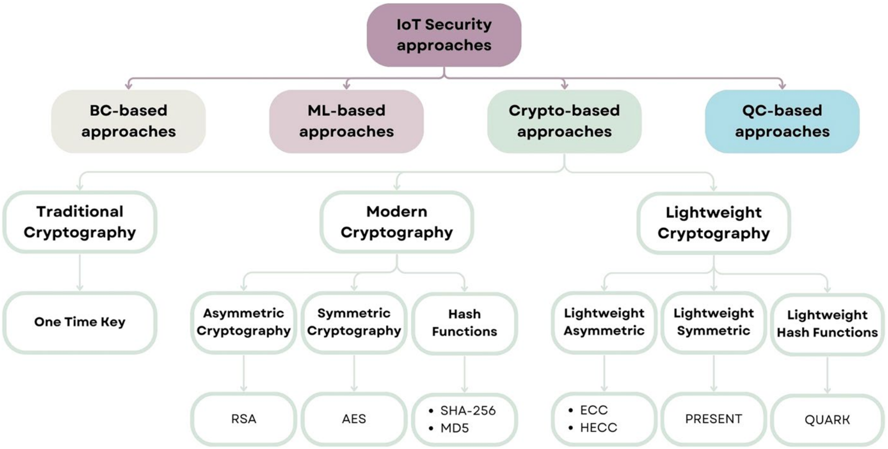

Fig. 6 Crypto-based approaches

A post-quantum signature strategy based on the MQ (Matsumoto-Imai) cryptosystem was proposed in [117]. The MQ cryptosystem is a family of public key cryptosystems based on multivariate polynomials over finite fields. It is suitable for securing IoT devices against attacks by quantum computers.

As the suggested scheme was designed to be efficient and scalable, large-scale IoT networks can use it effectively.

The idea is to use a one-way function a trapdoor function in order to generate a secret key and a public key. The one-way function is a mathematical function that is easy to compute in one direction but difficult to compute in the opposite direction, making it suitable for generating a secret key that cannot be easily reversed. The trapdoor function is a variant of the one-way function that includes a secret parameter, known as the trapdoor, which allows the function to be easily reversed when the secret parameter is known. The secret key is used to sign messages, while the public key is used to verify the signature.

The authors also proposed a parallel implementation of the signature scheme, which utilizes the multi-core architecture of modern processors to improve efficiency and reduce computation time. The parallel implementation is adaptable to different hardware configurations, making it practical for use in a wide range of IoT devices.

The proposed scheme was implemented on a GPU device and proved its efficiency and scalability. However, the idea requires significant computational resources.

Chikouche et al. [118] proposed a privacy-preserving code-based authentication protocol for IoT devices that assures secure communication between devices and prevents unauthorized access. The idea of the proposed approach is to use the McEliece cryptosystem which is a code-based encryption algorithm that is resistant to attacks by quantum computers. The protocol consists of three phases: key generation, authentication, and session key establishment. Using the McEliece cryptosystem, a private key and a public key are formed during the key generation stage. While the device owner keeps the private key a secret, other devices can access the public key. During the authentication phase, the device sends a request to the server including its public key and a random challenge. The server responds with an encrypted challenge, which the device decrypts using its private key. The device then sends the server the decrypted challenge in order to validate its authenticity. In the session key establishment phase, The Diffie-Hellman key exchange protocol is used by the server and the device to create a shared session key. All subsequent messages sent between the device and the server are then encrypted and decrypted using this key.

Even though the efficiency of the proposed idea was proved formally, it requires significant computational resources to be implemented.

In [119], a secure data encryption scheme for the 5G IoT scenario based on quantum walks was proposed. It uses the properties of quantum walks to encrypt data and ensure its security during transmission. The idea is to encode the data into quantum states that are then put through quantum walks. A quantum walk operator modifies the quantum states based on the encryption key after generating the encryption key by a quantum random number generator. The receiver receives the encrypted data and uses the same encryption key to decrypt it.

The authors proved the effectiveness of the proposed approach and showed that their idea is resistant to common attacks such as brute force. They also showed that the approach has low computational overhead and can be efficiently implemented in resource-constrained IoT devices. Yet, the proposed approach has limited scalability.

L. Chen et al. [120] proposed a dynamic on-demand key allocation scheme for securing the communication between IoT devices in a quantum network. The proposed approach is based on quantum key distribution (QKD) technology in order to establish secure keys between IoT devices, and dynamically allocates keys based on the communication requirements of the devices. The approach is designed to be scalable and efficient and can be adapted to different network topologies.

The approach is mainly composed of two phases: initialization and key allocation. During the first phase, a central authority generates a unique identifier for each QIoT device. The private keys are safely kept on the devices while the public keys are made accessible on a public key server. In the second phase, a device can request a new key from the central authority anytime it needs to establish a secure communication with another device. The central authority assigns a new key to the requesting device via the Dynamic Distributed Key Allocation (DDKA) technique.

The proposed approach was evaluated through simulation using MATLAB R2020b and the obtained results showed its efficiency. However, the approach suffers from the key distribution overhead.

In [121], the authors proposed a location-based lattice cryptography scheme for IoT systems. The proposed scheme uses a combination of lattice-based cryptography and location information to establish secure communication channels between IoT devices. It has two main components: a key distribution protocol and a data encryption/decryption protocol.

The key distribution protocol implicates generating a shared secret key between two devices based on their location information and a pre-shared secret key. The shared secret key is created using the location-based lattice cryptography method and is resistant to quantum attacks. The shared secret key is used in the data encryption/decryption protocol to encrypt and decode data sent between the two devices.

The proposed approach was evaluated using the open-source NB-IoT D2D simulation. The obtained results showed that the approach is resistant to many attacks but its dependency on the location information is one of its main limits.

Shamshad et al. [122] proposed an enhanced architecture to resolve public key cryptographic issues in IoT by employing quantum computing supremacy. This proposed architecture seeks to address the security flaws of widely utilized classical public key cryptography algorithms in IoT by using more secure quantum-based alternatives.

The proposed architecture consists of three main components: a quantum key distribution (QKD) system, a quantum random number generator (QRNG), and a quantum digital signature scheme. The QKD system is used to establish a secure communication channel between IoT devices by transmitting quantum states between a sender and a receiver which guarantees that any attempt to eavesdrop on or intercept the transmission will be quickly discovered. The QRNG is used to generate random numbers that are used in the encryption process which makes the latter much more secure. The quantum digital signature scheme is used to sign and verify messages exchanged between IoT devices. It is based on using one-way functions that are easy to compute in one direction but hard to reverse.

The proposed approach was simulated using SimuloQron for quantum key distribution (QKD) and the obtained results showed its efficiency and flexibility. Nevertheless, the proposed approach is limited to certain types of IoT systems.

Authors in [123] proposed a nested hash access system with post-quantum encryption to solve the issue of secure ultrareliable low-latency communication in mission-critical Internet of Things (IoT).

The proposed system performs random repetition coding and nested hash coding on multidomain physical-layer resources to encode and decode preambles precisely and resiliently. The idea is to use an encryption mechanism based on quasi-cyclic (QC)-moderate-density parity-check (MDPC) code between repetition and hashing operations to avoid passive eavesdropping during the preamble encoding process.

The authors have presented the security analysis by developing several optimization problems and the proposed approach was proved to be secure against active attacks with a tolerable loss of decoding errors. However, the proposed approach showed some computational requirements.

Table 5 illustrates the comparative analysis of solutions based on quantum computing.

According to this study, we classify QC-based approaches into two categories: Quantum/post-quantum and QC requirements, as illustrated in Fig. 7.

6 RQ1: global taxonomy of security solutions

Based on the study provided in Sect. 5, we construct a taxonomy that encompasses solutions from the four categories. We classify IoT solutions according to their main purposes, specifically addressing the achieved security requirements (defined in

Sect.2.1). Thus, the pertinent purposes we have selected are: authentication, access control, securely transmitted data (Confidentiality/integrity), secure data storage, data immutability, key exchange, attack/threat detection, lightweight scheme, intelligent mechanism and quantum attack resilience. Table 6 illustrates this taxonomy applied to related solutions for each mechanism.

6.1 Discussion

According to Table 6, we observe that blockchain-based approaches share the primary purpose of achieving immutability of data, ensuring that data cannot be altered once recorded. These approaches can also enhance other security factors when combined with cryptographic functions, such as authentication [71, 73, 76, 80, 83, 84] and the secure transmission of data [71, 74, 81, 84]. Moreover, blockchain smart contracts can serve into multiple functions, including threat detection and mitigation of attacks, as seen in [79]. Furthermore, they can be employed to control access by defining authorizations for users [73, 74, 76–78, 80, 81, 83]. Additionally, blockchain can be integrated with intelligent mechanisms like federated learning in [72].

Machine learning-based approaches are part of intelligent mechanisms. The majority of these methods in IoT security share the primary purpose of intelligent threat and attack detection. Moreover, they can achieve additional functionalities in the security field, such as access control by detecting malicious behavior [88], identifying function and performance-based attacks [91], or detecting web shell threats [34]. Furthermore, they contribute to securing transmitted data by implementing secure policies [90] or by focusing on detecting botnet attacks that steal sensitive data [94].

When considering cryptographic-based approaches and quantum computing-based approaches in IoT security, it becomes evident that many of them prioritize and fulfill specific requirements. These requirements encompass ensuring the secure transmission of data and the exchange of keys. Users initiate key exchange processes to establish secure communication channels between them. It is important to note that achieving the criteria for secure key exchange often implies achieving the criteria for secure data transmission, in classical [99, 104–107] and in quantum [116, 118–122]. However, the reverse is not always applicable, which is due to the availability of alternative cryptographic techniques, such as asymmetric cryptography, or other operations, which can also serve this purpose, in classical [101–103, 108, 109] and in quantum [112, 115].

However, the major distinguishing requirement between these two approaches is that quantum computing-based approaches in IoT security are designed to prevent quantum attacks.

A significant portion of cryptographic-based approaches is designed to be lightweight and adaptable for IoT devices with constrained resources [98, 100–107, 109]. Another significant aspect of these approaches is their ability to fulfill the authentication security factor [98–100, 104–106]. They can also be employed to achieve controlled access [98, 105] or secure stored data [98]. Furthermore, they can be combined with intelligent mechanisms, such as the artificial bee colony algorithm, for generating private keys, as demonstrated in [108].

A good portion of quantum computing-based approaches in IoT security focuses on achieving the authentication requirement [114, 117, 118, 122]. Furthermore, these approaches can be integrated with emerging technologies such as blockchain to ensure data immutability [113], as well as with intelligent mechanisms like deep residual learning for analyzing data [112]. Additionally, they can be designed to be lightweight [119].

7 Benefits and challenges of IoT security mechanisms

7.1 RQA_1 Potential benefits of using blockchain in securing IoT

The distribution nature and the decentralized architecture are the most valuable features of blockchain, which allow blockchain-based solutions to be more resistant against some attacks as DDoS. Besides, they offer efficient data immutability and elimination of the single point of failure [6]. Devices can perform direct communications without necessarily having to go through intermediaries. The tamper-proof nature of blockchain is also a primary feature, which increases its security [124].

Blockchain uses cryptographic functions as ECC and hash functions to offer integrity and authenticity. These functions are also used to sign transactions, which prove the legitimacy of the senders [71]. Moreover, blockchain offers validated and transparent record, which increase trust in IoT network and reduce the risk of malicious activities [6], such as adding malicious blocks with faulty data. Furthermore, smart contracts offer automated execution of defined rules, which increase trust, minimize delays and reduce the need for human intervention [125].

- Permission-less: offer a high level of decentralization, and their openness enables transparency, which can improve trust in certain scenarios [126]. Some of these approaches involve utilizing Ethereum, which allows them to create smart contracts [79, 83].
- Permissioned: allow authorized entities to work as consensus nodes and access data in the blockchain. This access control makes it easier to ensure privacy in permissioned blockchain compared to permissionless blockchain [126]. On the other side, federated learning blockchain is able to train a global model from local data available on heterogeneous IoT devices [72]. Some approaches used consortium blockchain [84], to control the limited set of pre-selected nodes involving in consensus process, while involving multiple entities in its governance [127].
- Hybrid: combining features of both permissioned and permissionless systems allows organizations to customize security, transparency, and decentralization according to their requirements [78]. It allows, for example, to regulate access to particular data stored within the blockchain and determine which data will be made accessible to the public [128].

Table 5 Comparative analysis of quantum computing-based solutions

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools	Evaluation metrics	Pros & Cons
[112]	2022	Convert the classical deep residual network into a quantum circuit, then train it using a quantum neural network and convert it back into a classical deep residual network	IoT in general	Not specified	Optimize the cost function routine for deeper networks	Formal	Cost Throughput value Intensity Security	(+) Protect information transfer and discover the deeper network noisy data (+) Improved Performance in terms of energy efficiency, accuracy, and speed (−) Scalability
[113]	2020	Distributed ledger (DL) technology + One-time signature (OTS) scheme	IoT in general with an example of a smart home	Distributed	Ensuring the security of IoT devices	Security analysis	Signature size Signature verification time	(+) Reduce signature size (+) Reduce signature creation time (+) Energy-efficient scheme compared to the popular Winternitz OTS (−) Require additional computational resources for lattice-based cryptosystem

Table 5 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools	Evaluation metrics	Pros & Cons
[114]	2022	Post-quantum signature + Systolic divisions	IoV (Internet of Vehicules)	Distributed	Resist quantum computer attacks	Security analysis	Multivariate signatures	(+) efficient implementation of division operations in IoV hardware (−) interoperability issues with systems and devices that use different cryptographic algorithms.
[115]	2021	Blind quantum computation with identity authentication	Fog computing	1 fog node	Ensuring the security of fog nodes	Analysis of different attacks		(+) The use of blind quantum computation and homomorphic encryption ensures data security (+) The use of fog computing provides efficient local processing of data, reducing the latency and bandwidth requirements (−) Homomorphic encryption overhead

Table 5 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools	Evaluation metrics	Pros & Cons
[116]	2022	Continuous-wave quantum cryptography	IoT in general	Not specified	Efficiently generate quantum random numbers for quantum key distribution	Formal	Analysis	(+) Compatible with existing fiber-optic communication networks (+) Do not rely on a trusted authority or centralized key distribution (+) Include mechanisms for error correction and privacy amplification (−) Transmission distance limited by factors such as photon loss and noise in the fiber-optic network (−) May not be scalable to large-scale IoT networks

Table 5 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools	Evaluation metrics	Pros & Cons
[117]	2020	Multivariate polynomials with efficient key and signature sizes	IoT in general	Not specified	Ensuring the authentication of edge nodes	Implemented on a GPU device	Number of generated signatures	(+) Fast, efficient, and scalable (+) Parallel implementation (−) Require significant computational resources (−) Do not address the issue of key distribution
[118]	2019	Mutual authentication using coding theory	IoT in general	Not specified	Secure communication between IoT components	Formally + implementation	Storage requirement Computation cost Communication cost	(+) Privacy preservation (+) Scalability (−) Require significant computational resources (−) Assume that the device owner has a trusted key distribution center

Table 5 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools	Evaluation metrics	Pros & Cons
[119]	2020	Quantum walks (QWs)	5G IoT	Example of 1 base station with many clients	Store and share the sensitive data over 5G networks in a secure way and prevent unauthorized entities from obtaining any useful information	Formal	Key sensitivity Correlation, coefficients, NPCR, and information entropy	(+) Consider 5G networks (+) Low computational overhead (+) Resistant to common attacks such as brute force and interception (−) Sensitivity to environmental noise (−) Limited scalability
[120]	2022	Quantum key pool (QKP) key allocation + Quantum key distribution (QKD)	QIoT	Architecture based on SDN	Quantum key distribution in IoT systems	MATLAB R2020b	Average delay of the key service Success rate of the no-waiting requests Traffic load	(+) Scalability (+) Flexible and can dynamically allocate keys based on the communication requirements of the devices (−) Dependence on QKD technology (−) Key Distribution Overhead

Table 5 (continued)

References	Year	Used techniques	IoT application	Network architecture	Main purpose	Verification tools	Evaluation metrics	Pros & Cons
[121]	2021	Location-Based Lattices	IoT/IoMT	Not specified	Ensure communication security in IoT	Open-source NB-IoT D2D simulation	Threat modeling Delay Energy disipated Throughput	(+) The first secure and unrestricted position-based protocol that guards against any number of collusion attackers and against quantum attacks (−) Dependency on Location Information
[122]	2022	Quantum cryptography and the BB84 protocol	IoT	Three layers: perception layer, network layer, and application layer.	Ensure security on all levels Resolve public key cryptographic issues Prevents eavesdroppers from performing destructive operations in the communication channel	SimuloQron to implement the BB84 protocol for quantum key distribution (QKD) and one-time pad (OTP)	Key length Estimated error Eavesdropping rate	(+) Flexible and can be customized to meet the specific security requirements of different IoT applications (−) Limited to certain types of IoT applications
[123]	2023	Post-quantum encryption	Mission-critical IoT	Not specified	Ensure secure ultrareliable low-latency communications	Formal	Reliability-latency Failure probability	(+) Ensures quantum-resistant security (−) Computational requirements

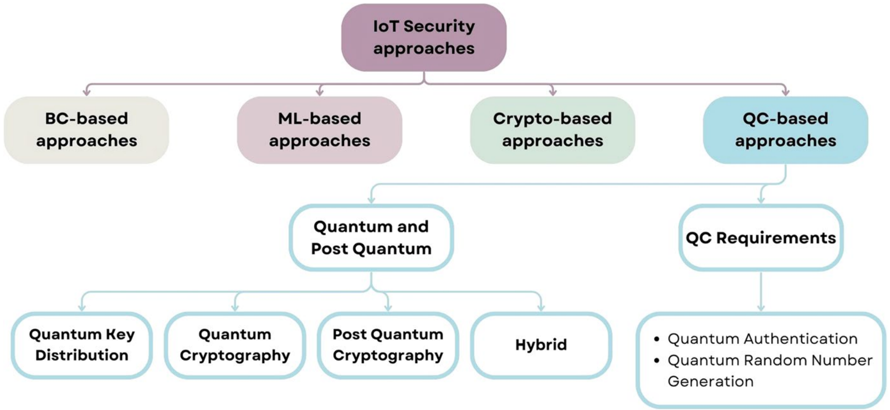

Fig. 7 Quantum Computing-based approaches

7.2 RQB_1 Challenges of applying blockchain in securing IoT

The high processing time required to validate and add blocks to the blockchain is not adequate to IoT devices with limited processing power [129]. Thus, it is a challenge task for researchers to envision and contribute to lightweight blockchain-based solutions [80]. Besides, the excessive generation of data transactions in a blockchain IoT system results in high bandwidth consumption, which leads to time latency issues for real-time applications [6, 80]. Additionally, some of the consensus algorithms, such as Proof of Work, requires a significant amount of computational power and energy consumption [130].

On the other hand, a smart contract that has vulnerabilities in its source code will put in risk all the parties using it as it can be used for malicious purposes [131]. Besides, once a smart contract is created with bugs in its code, it becomes complicated to fix. Furthermore, IoT security mechanisms based on blockchain faces the attacks of blockchain, such as 51% attack [6], where a single entity or a group control 51% of the network which allow them to manipulate data transactions to be validated. Besides, malware attacks that can be used to gain access to a user's private key and then use it for malicious activities [14].

- Permission-less: the openness of permissionless blockchains can lead to privacy concerns in scenarios where transactions may contain sensitive information of users, as all transactions are visible to everyone on the network [126, 130].
- Permissioned: they require a higher level of trust between participants, as access to the network is restricted to a select group of users. This can reduce the potential benefits of blockchain technology, such as decentralization. Additionally, permissioned blockchains may require more resources to maintain, as they often require a higher level of governance and oversight [130]. On the other side, many studies in the literature that explore blockchain-based federated learning for IoT applications often do not consider the requirement for a more lightweight implementation. Moreover, heterogeneous resources of IoT devices hinder synchro-

Table 6 Global taxonomy of IoT security solutions

Main purpose				
Security mechanism	BC	ML	Crypto	QC
Authentication	[71, 73, 76, 80, 83, 84]		[98–100, 104–106, 111]	[114, 117, 118, 122]
Access control	[73, 74, 76–78, 80, 81, 83]	[34, 88, 91]	[98, 105, 111]	
Securely transmitted data (Confidentiality/integrity)	[71, 74, 81, 84]	[90, 94]	[99, 101–111]	[112, 115, 116, 118–123]
Secure data storage	[71–73, 76, 78, 81, 84]		[98]	
Data immutability	[71–74, 76–81, 83, 84]			[113]
Key exchange			[99, 104–107, 111]	[116, 118–122]
Attack/Threat detection	[79]	[34, 85–97]		[112]
Lightweight scheme			[98, 100–107, 109, 111]	[119]
Intelligent mechanism	[72]	[34, 85–97]	[108]	[112]
Quantum attack resilience				[112–122] [123]

nous transmission of trained models, potentially causing failures [65]. Regarding consortium blockchain like in [84], the potential inclusion of a new consortium member, who is a competitor of another powerless member, through a majority decision by governing nodes, poses a risk to the system's sustainability [127].
- Hybrid: the implementation and maintenance of a hybrid blockchain in an IoT environment is more complex and thus more costly [37].

7.3 RQA_2 Potential benefits of using machine learning in securing IoT

The evolution of IoT results in the continuous emergence of new threats and attacks. Thus, the traditional security measures used in IoT are insufficient to address the current security issues. The use of machine learning, deep learning or other artificial intelligence techniques is beneficial for developing an advanced and an up-to-date security mechanism for an IoT system that is constantly evolving. The main reason is that AI algorithms can continuously learn from data, allowing them to adapt to new threats and improve their accuracy over time.

Through the collection and analysis of input data across various components of the IoT system, ML techniques can discern typical interaction patterns and detect malicious intent in the initial phases [132]. Thus, ML-based techniques help to identify and detect anomalies and threats in IoT [133]. An ML model analyzes data from different sources and learn how to diagnose abnormal behavior patterns that indicate a possible attack such as a sudden increase in network traffic, which may indicate a DDoS attack. An ML model can also detect anomalies as changes in device behavior or performance, which may indicate device malfunction or tampering [134]. ML can automate tasks that require human intervention [134], which can save time and cost while enhancing security.

- Traditional ML: Some of the ML-based solutions in IoT use traditional ML models [34, 89, 92]. These types of models are often simpler and computationally less intensive compared to DL methods. They require less data for training and can be trained quickly, making them suitable for real-time or near-real-time decision making in IoT security scenarios.
- DL: Other solutions are based on DL [88, 90, 91], which can be more suitable for IoT environments as IoT devices produce a substantial volume of data, and DL can perform well with large datasets [135]. DL excels in automatically learning features from raw data, eliminating the need for precisely designed features or manual feature engineering [135]. This can be particularly useful in IoT security, where the data can be complex and unstructured [136]. DL models can be adapted over time to learn from new security threats and adjust their responses accordingly.
- ML-DL: Combining ML and DL techniques [85–87, 93, 94] can leverage the strengths of both approaches. For example, using DL for feature extraction and ML for decision making, or using ML for simpler scenarios and switching to DL for more intricate challenges.

7.4 *RQB*$_2$ Challenges of applying machine learning in securing IoT

In ML systems for IoT security, there are two main and important factors, which are data and learning methods. Data is collected and preprocessed to be chosen as a dataset for learning algorithms. It has to be of high quality to have an effective training. This can be a challenging task, as when collecting data in IoT environments, sensors may collect unnecessary, incomplete or inaccurate data. IoT devices also generate heterogeneous data with wide range of styles, which complicate the task of preprocessing for ML models. Additionally, ML models can be complex and difficult to interpret, making it challenging to understand how they arrive at their decisions [134]. Besides, the security and privacy of dataset is essential, as some attacks aim to poison data by manipulating or adding malicious data to the dataset [137]. Bad data as unnecessary, irrelevant or malicious lead to garbage processing and incorrect decisions to be made by the ML model. Therefore, mechanisms to deeply analyze the collected data and to secure the dataset are paramount.

In processing, training and making predictions, ML models that consume considerable resources are not adaptable to IoT devices with limited computational power, memory and energy [138]. Thus, it is challenging to implement an ML model that is both sophisticated and lightweight. Besides, in IoT security, many applications need to rapidly detect and respond to security threats. Thus, ML models also need to consider making predictions in real-time.

- Traditional ML: ML models may have reliability and accuracy issues, such as false positives and true negatives, which can affect the precision of predictions. Therefore, ML models may require amendment and proper guidance for making precise predictions [133].
- DL: DL models can be computationally intensive than ML, requiring significant hardware resources for training and deployment [88, 90, 134]. Furthermore, the training duration can significantly extend as the training dataset size expands [138].
- ML-DL: The required computational resources can be also high in Hybrid ML-DL approaches [93].

7.5 *RQA*$_3$ Potential benefits of using cryptography in securing IoT

Cryptographic methods have been in practice for centuries and they still useful and present several benefits in securing IoT. They are used to respond to security requirements as confidentiality, integrity, authentication, etc [99, 104–106]. This safety is thoroughly tested during all these years of using cryptographic methods. For example, hash functions can ensure data integrity through generating unique hash values for input data, among its functions, SHA-256 [108] is considered more secure than MD5 [103]. Moreover, cryptography is known by its interoperability, as it can be standardized and supported by a wide range of devices and systems. Thus, it makes it easier to secure communication between heterogonous IoT devices with different software and hardware specifications [139, 140].

- Lightweight: a big part of cryptography solutions for IoT security are destined to be lightweight [98, 100–107, 109]. Lightweight cryptographic protocols can be more efficient than other emerging solutions in terms of suitability and adaptability to IoT devices with constrained memory, computational power and battery life. Specifically, a lightweight protocol is a protocol that is designed to minimize computational time, memory complexity, transmitted data and energy consumption [25, 141]. Therefore, researchers have been and continue to be interested in developing IoT secure protocols based on cryptography.
- Asymmetric Cryptography: it enables secure exchange of data and key establishment without requiring a prior shared secret. Provides digital signature to verify the authenticity. It is used in a big part of crypto-based solutions for IoT, such as RSA [110] and especially ECC [98, 99, 102, 103, 108, 109].
- Symmetric Cryptography: It is generally faster and more efficient for encrypting and decrypting large amounts of data compared to asymmetric algorithms. When it is combined with asymmetric, they can offer better security [103]. AES is a type of symmetric cryptography that is used for securing IoT [103, 110].

7.6 *RQB_3* Challenges of applying cryptography in securing IoT

Cryptographic protocols employing classical methods that do not consider making these methods lighter cannot be feasibly applied to IoT devices with limited capacities. Additionally, some attacks cannot be prevented by methods based only on classical encryption, such as side channel and physical attacks where the attacker can access the device to steal sensitive parameters used in the cryptographic method. Thus, although researchers continue to evolve cryptographic methods, it still challenging to adapt them to keep pace with ever-evolving attacks [142].

Efficient protocols based on classical cryptography are hard to break using classical computers. However, when quantum computers become a reality, they will be able to solve mathematical problems in a snap; thus, it will become possible to break classical cryptographic solutions within a short time [5, 143]. In other words, they will be vulnerable to QC attacks.

- Lightweight: lightness is an important factor to take into consideration in this field [25, 141]. It is a challenging task for researchers to find a cryptographic protocol that is both lightweight and provides adequate security [23].
- Asymmetric: can be computationally more intensive than symmetric algorithms [25]. Besides, longer key lengths, as for approaches using RSA [110], can lead to performance slowdowns. Thus, they are required for comparable security to symmetric algorithms.
- Symmetric: Securely sharing secret keys among parties is a complex task, particularly in distributed systems like IoT [103, 110]. If a key is exposed, it jeopardizes all past and future communications encrypted with it. Moreover, as the

number of parties involved in communication expands, the need for keys grows exponentially, causing scalability problems. Additionally, symmetric ciphers use reduced key length compared to the asymmetric algorithm. Hence, they are vulnerable to security attacks because of their less complex nature [25].

7.7 RQA_4 Potential benefits of using quantum computing in securing IoT

The main benefit of QC in securing IoT is the quantum cryptography that can create unbreakable encryption keys [120]. This is because quantum computers, which can make calculations faster than classical computers, can break traditional cryptographic keys [143]. Quantum cryptography is based on the rules of quantum mechanics. It provides safe transmission of data, such as the attacker cannot read or tamper with transmitted data without being detected [5].

- Quantum key distribution: eavesdropping attack can be detected in contrast to classical cryptographic algorithms [52].
- Post-quantum cryptography: the benefit of post-quantum cryptography is to develop cryptographic techniques that can be resistant to QC attacks unlike classical techniques [115, 117, 123]. Lattice-based cryptography is one of the most promising techniques of post-quantum cryptography, as it is based on hard mathematical problems that can provide robustness against attacks launched by classical or quantum computers [114]. Moreover, lattice-based techniques offer encryption/decryption algorithms that are suitable for IoT devices with constrained resources [113, 121].
- Quantum cryptography: some of QC techniques that can be used to ensure security in IoT are quantum circuit [112], continious wave technology [116], quantum walks [119], etc.
- Hybrid: refers to approaches that combine different methods of quantum cryptography [114, 121, 122] or combine them with other technologies like blockchain [113] or deep learning [112], thus providing an adaptable way to leverage the strengths of multiple techniques.
- Quantum random number generation: QC can be used to generate random numbers employed to calculate a classical cryptographic key [122]. Traditional generators of random numbers are based on deterministic algorithms and thus the attacker can predict the result. In contrast, QC based on quantum mechanics can generate large and unique random numbers that are unpredictable [144].
- Authentication: QC-based approaches in IoT security can be used in authenticating legitimate entities [114, 117, 118, 122].

7.8 RQB_4 Challenges of applying quantum computing in securing IoT

One of the challenges of applying quantum cryptography in IoT devices is the need for quantum hardware that can ensure generation and transmission of quantum states such as quantum key distribution (QKD) [145]. Thus, researchers are interested by finding lightweight and effective solutions to implement quantum cryptography in IoT [146]. Besides, QKD can establish a secret key between only two entities [147]; hence, it is challenging to apply it between more than two of IoT devices that want to share a secret key.

Some post-quantum cryptographic algorithms are designed to be lightweight, implementing this type may still present challenges as they consume more resources than classical algorithms. Moreover, post-quantum algorithms necessitate significantly larger key sizes, making it essential to thoroughly analyze key size, security levels, network performance, and scalability when integrating IoT networks with these cryptographic methods [146]. Furthermore, the migration to post-quantum cryptography requires considerable changes to existing protocols and systems, which can be expensive in terms of time and cost [148].

8 Conclusion

Despite all the research that has been done so far, security in IoT is still an open issue, especially with the growth of IoT applications, the evolution of technologies combined with IoT and the continuous evolution of attacks and threats. In this paper, we addressed the most used mechanisms in this field, which are blockchain, machine learning, cryptography, and quantum computing. According to these mechanisms, we organized the relevant approaches into four categories. Consequently, we conducted a comprehensive discussion and comparative analysis of these approaches in each specified category, according to some defined criteria. We presented a specific taxonomy for solutions within each category. Thereafter, we provided a global taxonomy of solutions based on their achieved security requirements.

This survey aims to provide a thorough understanding of the current state of research in IoT security by analyzing the strengths and limitations of the four relevant mechanisms in one paper. The provided taxonomy can assist researchers in selecting suitable mechanisms according to the desired security outcomes. Thus, this paper is intended to serve as a useful and a timesaving guideline to interested researchers.

Author contributions All authors contributed to this paper.

Funding Our work has not been funded and has been worked without financial support.

Availability of data and materials No datasets were used in this review article.

Declarations

Conflict of interest We declare that we have no conflict of interest.

Ethical approval Not applicable.

References

1. Ray PP (2018) A survey on internet of things architectures. J King Saud Univ-Comput Inf Sci 30(3):291–319
2. HaddadPajouh H, Dehghantanha A, Parizi RM, Aledhari M, Karimipour H (2021) A survey on internet of things security: requirements, challenges, and solutions. Internet of Things 14:100129
3. Bandyopadhyay D, Sen J (2011) Internet of things: applications and challenges in technology and standardization. Wireless Pers Commun 58:49–69
4. Omolara AE, Alabdulatif A, Abiodun OI, Alawida M, Alabdulatif A, Arshad H et al (2022) The internet of things security: a survey encompassing unexplored areas and new insights. Comput & Secur 112:102494
5. Kumari S, Singh M, Singh R, Tewari H (2022) Post-quantum cryptography techniques for secure communication in resource-constrained internet of things devices: A comprehensive survey. Softw: Pract and Exper 52(10):2047–2076
6. Shah Z, Ullah I, Li H, Levula A, Khurshid K (2022) Blockchain based solutions to mitigate distributed denial of service (ddos) attacks in the internet of things (iot): a survey. Sensors 22(3):1094
7. Kumar A, Saha R, Conti M, Kumar G, Buchanan WJ, Kim TH (2022) A comprehensive survey of authentication methods in internet-of-things and its conjunctions. J Netw and Compt Appl 204:103414
8. Thabit F, Can O, Aljahdali AO, Al-Gaphari GH, Alkhzaimi HA (2023) A comprehensive literature survey of cryptography algorithms for improving the iot security, Internet of Things, 100759
9. Mathur S, Kalla A, Gür G, Bohra MK, Liyanage M (2023) A survey on role of blockchain for iot: applications and technical aspects. Comput Netw 227:109726
10. Gaurav A, Gupta BB, Panigrahi PK (2022) A comprehensive survey on machine learning approaches for malware detection in iot-based enterprise information system. Enterprise Inf Syst 17(3):2023764
11. Papaioannou M, Karageorgou M, Mantas G, Sucasas V, Essop I, Rodriguez J, Lymberopoulos D (2022) A survey on security threats and countermeasures in internet of medical things (iomt). Trans on Emerg Telecommun Technol 33(6):e4049
12. Razzaq MA, Gill SH, Qureshi MA, Ullah S Security issues in the internet of things (iot): A comprehensive study, Int J Adv Comput Sci and Appl 8(6)
13. Alfandi O, Khanji S, Ahmad L, Khattak A (2021) A survey on boosting iot security and privacy through blockchain: exploration, requirements, and open issues. Clust Comput 24:37–55
14. Khan MA, Salah K (2018) Iot security: review, blockchain solutions, and open challenges. Futur Gener Comput Syst 82:395–411
15. Dhillon PK, Kalra S (2017) Secure multi-factor remote user authentication scheme for internet of things environments. Int J Commun Syst 30(16):e3323
16. La Torre M, Dumay J, Rea MA (2018) Breaching intellectual capital: critical reflections on big data security. Meditari Accountancy Res 26(3):463–482
17. Kumar A, Jain V, Yadav A (2020) A new approach for security in cloud data storage for iot applications using hybrid cryptography technique, In: 2020 international conference on power electronics & IoT applications in renewable energy and its control (PARC). IEEE, pp 514–517
18. Yang P, Xiong N, Ren J (2020) Data security and privacy protection for cloud storage: a survey. IEEE Access 8:131723–131740
19. Steichen M, Fiz B, Norvill R, Shbair W, State R (2018) Blockchain-based, decentralized access control for ipfs, In: 2018 Ieee international conference on internet of things (iThings) and ieee green computing and communications (GreenCom) and ieee cyber, physical and social computing (CPSCom) and ieee smart data (SmartData). IEEE, pp 1499–1506
20. Raja Santhi A, Muthuswamy P (2022) Influence of blockchain technology in manufacturing supply chain and logistics. Logistics 6(1):15
21. Benzaïd C, Taleb T, Farooqi MZ (2021) Trust in 5g and beyond networks. IEEE Netw 35(3):212–222
22. Mall P, Amin R, Das AK, Leung MT, Choo K-KR (2022) Puf-based authentication and key agreement protocols for iot, wsns, and smart grids: a comprehensive survey. IEEE Internet Things J 9(11):8205–8228
23. Cherbal S, Benchetioui R (2023) Scpuak: smart card-based secure protocol for remote user authentication and key agreement. Comput Electr Eng 109:108759

24. Khraisat A, Alazab A (2021) A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity 4:1–27
25. Rana M, Mamun Q, Islam R (2022) Lightweight cryptography in iot networks: a survey. Futur Gener Comput Syst 129:77–89
26. Ahanger TA, Aljumah A, Atiquzzaman M (2022) State-of-the-art survey of artificial intelligent techniques for iot security. Comput Netw 206:108771
27. Wu H, Han H, Wang X, Sun S (2020) Research on artificial intelligence enhancing internet of things security: a survey. Ieee Access 8:153826–153848
28. Fernández-Caramés TM (2019) From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things. IEEE Internet Things J 7(7):6457–6480
29. Sadhu PK, Yanambaka VP, Abdelgawad A (2022) Internet of things: security and solutions survey. Sensors 22(19):7433
30. Mothukuri V, Khare P, Parizi RM, Pouriyeh S, Dehghantanha A, Srivastava G (2021) Federated-learning-based anomaly detection for iot security attacks. IEEE Internet Things J 9(4):2545–2554
31. Uprety A, Rawat DB (2020) Reinforcement learning for iot security: a comprehensive survey. IEEE Internet Things J 8(11):8693–8706
32. Mohanta BK, Satapathy U, Panda SS, Jena D (2019) A novel approach to solve security and privacy issues for iot applications using blockchain, In: 2019 International Conference on Information Technology (ICIT), IEEE, pp 394–399
33. Deogirikar J, Vidhate A (2017) Security attacks in iot: A survey, In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), IEEE, pp 32–37
34. Yong B, Wei W, Li K-C, Shen J, Zhou Q, Wozniak M, Połap D, Damaševičius R (2022) Ensemble machine learning approaches for webshell detection in internet of things environments. Trans Emerg Telecommun Technol 33(6):e4085
35. Gamage H, Weerasinghe H, Dias N (2020) A survey on blockchain technology concepts, applications, and issues. SN Comput Sci 1:1–15
36. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: Architecture, consensus, and future trends, In: 2017 IEEE international congress on big data (BigData congress). IEEE, pp 557–564
37. Alkhateeb A, Catal C, Kar G, Mishra A (2022) Hybrid blockchain platforms for the internet of things (iot): a systematic literature review. Sensors 22(4):1304
38. Huo R, Zeng S, Wang Z, Shang J, Chen W, Huang T, Wang S, Yu FR, Liu Y (2022) A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges. IEEE Commun Surveys & Tutorials 24(1):88–122
39. Kumar S, Raut RD, Agrawal N, Cheikhrouhou N, Sharma M, Daim T (2022) Integrated blockchain and internet of things in the food supply chain: adoption barriers. Technovation 118:102589
40. Wu Y, Wu Y, Cimen H, Vasquez JC, Guerrero JM (2022) P2p energy trading: blockchain-enabled p2p energy society with multi-scale flexibility services. Energy Rep 8:3614–3628
41. Sarker IH (2022) Ai-based modeling: techniques, applications and research issues towards automation, intelligent and smart systems. SN Comput Sci 3(2):158
42. Dalal KR (2020) Analysing the role of supervised and unsupervised machine learning in iot, In: 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, pp 75–79
43. Xiao L, Wan X, Lu X, Zhang Y, Wu D (2018) Iot security techniques based on machine learning: how do iot devices use ai to enhance security? IEEE Signal Process Mag 35(5):41–49
44. Nikam SS (2015) A comparative study of classification techniques in data mining algorithms. Oriental J Comput Sci and Technol 8(1):13–19
45. Mousavi SK, Ghaffari A, Besharat S, Afshari H (2021) Security of internet of things based on cryptographic algorithms: a survey. Wireless Netw 27:1515–1555
46. Jose DV, Vijyalakshmi A (2018) An overview of security in internet of things. Procedia Comput Sci 143:744–748
47. Almazrooie M, Samsudin A, Gutub AA-A, Salleh MS, Omar MA, Hassan SA (2020) Integrity verification for digital holy quran verses using cryptographic hash function and compression. J King Saud Univ-Comput and Inf Sci 32(1):24–34
48. Bernhardt C (2019) Quantum computing for everyone. Mit Press
49. Gill SS, Kumar A, Singh H, Singh M, Kaur K, Usman M, Buyya R (2022) Quantum computing: a taxonomy, systematic review and future directions. Software: Practice and Exper 52(1):66–114

50. Cusumano MA (2018) The business of quantum computing. Commun ACM 61(10):20–22
51. Bhatt AP, Sharma A (2019) Quantum cryptography for internet of things security. J Electr Sci and Technol 17(3):213–220
52. Broadbent A, Schaffner C (2016) Quantum cryptography beyond quantum key distribution. Des Codes Crypt 78:351–382
53. Williams P, Dutta IK, Daoud H, Bayoumi M (2022) A survey on security in internet of things with a focus on the impact of emerging technologies. Internet of Things 19:100564
54. Corallo A, Lazoi M, Lezzi M, Luperto A (2022) Cybersecurity awareness in the context of the industrial internet of things: a systematic literature review. Comput Ind 137:103614
55. Shirvani MH, Masdari M (2022) A survey study on trust-based security in internet of things: Challenges and issues, Internet of Things, 100640
56. Swessi D, Idoudi H (2022) A survey on internet-of-things security: threats and emerging countermeasures. Wireless Pers Commun 124(2):1557–1592
57. Alzoubi YI, Al-Ahmad A, Kahtan H, Jaradat A (2022) Internet of things and blockchain integration: security, privacy, technical, and design challenges. Future Internet 14(7):216
58. Khan AA, Laghari AA, Shaikh ZA, Dacko-Pikiewicz Z, Kot S Internet of things (iot) security with blockchain technology: a state-of-the-art review, IEEE Access
59. Savithri G, Mohanta BK, Dehury MK (2022) A brief overview on security challenges and protocols in internet of things application, In: 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). IEEE, pp 1–7
60. Khan AR, Kashif M, Jhaveri RH, Raut R, Saba T, Bahaj SA (2022) Deep learning for intrusion detection and security of internet of things (iot): current analysis, challenges, and possible solutions, Security and Communication Networks
61. Sarker IH, Khan AI, Abushark YB, Alsolami F (2022) Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions, Mobile Networks and Applications, 1–17
62. Raimundo RJ, Rosário AT (2022) Cybersecurity in the internet of things in industrial management. Appl Sci 12(3):1598
63. Khan NA, Awang A, S. A. Karim BA Security in internet of things: A review, IEEE Access
64. Heidari A, Jabraeil Jamali MA (2022) Internet of things intrusion detection systems: A comprehensive review and future directions, Cluster Computing, 1–28
65. Issa W, Moustafa N, Turnbull B, Sohrabi N, Tari Z (2023) Blockchain-based federated learning for securing internet of things: a comprehensive survey. ACM Comput Surv 55(9):1–43
66. Kumar A, Bhushan B, Shriti S, Nand P (2022) Quantum computing for health care: a review on implementation trends and recent advances, Multimedia Technologies in the Internet of Things. Environment 3:23–40
67. Jahangeer A, Bazai SU, Aslam S, Marjan S, Anas M, Hashemi SH A review on the security of iot networks: From network layer's perspective, IEEE Access
68. Taherdoost H (2023) Security and internet of things: benefits, challenges, and future perspectives. Electronics 12(8):1901
69. de Azambuja AJG, Plesker C, Schützer K, Anderl R, Schleich B, Almeida VR (2023) Artificial intelligence-based cyber security in the context of industry 4.0-a survey. Electronics 12(8):1920
70. Mangla C, Rani S, Qureshi NMF, Singh A (2023) Mitigating 5g security challenges for next-gen industry using quantum computing. J of King Saud Univ-Comput and Inf Sci 35(6):101334
71. Latif S, Idrees Z, Ahmad J, Zheng L, Zou Z (2021) A blockchain-based architecture for secure and trustworthy operations in the industrial internet of things. J Indus Inf Int 21:100190. https://doi.org/10.1016/j.jii.2020.100190
72. Wadhwa S, Rani S, Kaur G, Koundal D, Zaguia A, Enbeyle W (2022) Heterofl blockchain approach-based security for cognitive internet of things, Wireless Communications and Mobile Computing
73. Wang J, Chen J, Ren Y, Sharma PK, Alfarraj O, Tolba A (2022) Data security storage mechanism based on blockchain industrial internet of things. Comput & Industrial Eng 164:107903
74. Agyekum KO-BO, Xia Q, Sifah EB, Cobblah CNA, Xia H, Gao J (2021) A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain. IEEE Syst J 16(1):1685–1696
75. De Caro A, Iovino V (2011) jpbc: Java pairing based cryptography, In: 2011 IEEE Symposium on Computers and Communications (ISCC). IEEE, pp 850–855

76. Chai B, Yan B, Yu J, Wang G (2021) Bhe-ac: a blockchain-based high-efficiency access control framework for internet of things, Personal and Ubiquitous Computing, 1–12
77. Rizzardi A, Sicari S, Miorandi D, Coen-Porisini A (2022) Securing the access control policies to the internet of things resources through permissioned blockchain. Concurrency and Comput: Pract and Exp 34(15):e6934
78. Ngabo D, Wang D, Iwendi C, Anajemba JH, Ajao LA, Biamba C (2021) Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. Electronics 10(17):2110
79. Chaganti R, Varadarajan V, Gorantla VS, Gadekallu TR, Ravi V (2022) Blockchain-based cloud-enabled security monitoring using internet of things in smart agriculture. Future Internet 14(9):250
80. Honar Pajooh H, Rashid M, Alam F, Demidenko S (2021) Multi-layer blockchain-based security architecture for internet of things. Sensors 21(3):772
81. Dhar S, Khare A, Singh R (2022) Advanced security model for multimedia data sharing in internet of things, Trans Emerg Telecommun Technol, e4621
82. Ipfs: a decentralised cloud and file system for the blockchain environment (2020) https://www.opensourceforu.com/2020/08/ipfs-a-decentralised-cloud-and-file-system-for-the-blockchain-environment
83. Chentouf FZ, Bouchkaren S (2023) Security and privacy in smart city: a secure e-voting system based on blockchain. Intl J of Electr and Comput Eng 13(2):1848
84. Khan AA, Bourouis S, Kamruzzaman M, Hadjouni M, Shaikh ZA, Laghari AA, Elmannai H, Dhahbi S Data security in healthcare industrial internet of things with blockchain, IEEE Sensors Journal
85. Mihoub A, Fredj OB, Cheikhrouhou O, Derhab A, Krichen M (2022) Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. Comput & Electrical Eng 98:107716
86. Yazdinejad A, Kazemi M, Parizi RM, Dehghantanha A, Karimipour H (2023) An ensemble deep learning model for cyber threat hunting in industrial internet of things. Digital Commun and Netw 9(1):101–110
87. Alkahtani H, Aldhyani TH (2021) Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms. Complexity 2021:1–18
88. Tharewal S, Ashfaque MW, Banu SS, Uma P, Hassen SM, Shabaz M (2022) Intrusion detection system for industrial internet of things based on deep reinforcement learning. Wirel Commun Mob Comput 2022:1–8
89. Mazhar MS, Saleem Y, Almogren A, Arshad J, Jaffery MH, Rehman AU, Shafiq M, Hamam H (2022) Forensic analysis on internet of things (iot) device using machine-to-machine (m2m) framework. Electronics 11(7):1126
90. Javeed D, Gao T, Khan MT, Ahmad I (2021) A hybrid deep learning-driven sdn enabled mechanism for secure communication in internet of things (iot). Sensors 21(14):4884
91. Liu X, Yu W, Liang F, Griffith D, Golmie N (2021) On deep reinforcement learning security for industrial internet of things. Comput Commun 168:20–32
92. Saba T, Sadad T, Rehman A, Mehmood Z, Javaid Q (2021) Intrusion detection system through advance machine learning for the internet of things networks. IT Professional 23(2):58–64
93. Sahu AK, Sharma S, Tanveer M, Raja R (2021) Internet of things attack detection using hybrid deep learning model. Comput Commun 176:146–154
94. Hasan T, Malik J, Bibi I, Khan WU, Al-Wesabi FN, Dev K, Huang G Securing industrial internet of things against botnet attacks using hybrid deep learning approach, IEEE Trans on Netw Sci and Eng
95. Jothi B, Pushpalatha M (2023) Wils-trs-a novel optimized deep learning based intrusion detection framework for iot networks. Pers Ubiquit Comput 27(3):1285–1301
96. Musleh D, Alotaibi M, Alhaidari F, Rahman A, Mohammad RM (2023) Intrusion detection system using feature extraction with machine learning algorithms in iot. J Sens Actuator Netw 12(2):29
97. Xu H, Sun Z, Cao Y, Bilal H (2023) A data-driven approach for intrusion and anomaly detection using automated machine learning for the internet of things, Soft Computing, 1–13
98. Khalifa M, Algarni F, Khan MA, Ullah A, Aloufi K (2021) A lightweight cryptography (lwc) framework to secure memory heap in internet of things. Alex Eng J 60(1):1489–1497
99. Liu X, Wang X, Yu K, Yang X, Ma W, Li G, Zhao X (2022) Secure data aggregation aided by privacy preserving in internet of things, Wireless Communications and Mobile Computing

100. Ullah I, Alkhalifah A, Althobaiti MM, Al-Wesabi FN, Hilal AM, Khan MA, Ming-Tai Wu J (2022) Certificate-based signature scheme for industrial internet of things using hyperelliptic curve cryptography, Wireless Communications and Mobile Computing
101. Khan J, Khan GA, Li JP, AlAjmi MF, Haq AU, Khan S, Ahmad N, Parveen S, Shahid M, Ahmad S et al (2022) Secure smart healthcare monitoring in industrial internet of things (iiot) ecosystem with cosine function hybrid chaotic map encryption, Scientific Programming
102. Jerbi W, Guermazi A, Cheikhrouhou O, Trabelsi H (2021) Coopecc: a collaborative cryptographic mechanism for the internet of things. J of Sens 2021:1–8
103. Chanal PM, Kakkasageri MS (2021) Preserving data confidentiality in internet of things. SN Comput Sci 2(1):53
104. Unal D, Al-Ali A, Catak FO, Hammoudeh M (2021) A secure and efficient internet of things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption. Futur Gener Comput Syst 125:433–445
105. Liu X, Yang X, Luo Y, Zhang Q (2021) Verifiable multikeyword search encryption scheme with anonymous key generation for medical internet of things. IEEE Internet Things J 9(22):22315–22326
106. Sahmi I, Abdellaoui A, Mazri T, Hmina N Mqtt-present: Approach to secure internet of things applications using mqtt protocol., Int J of Electr & Comput Eng (2088-8708) 11 (5)
107. Gong B, Wu Y, Wang Q, Ren Y-H, Guo C (2022) A secure and lightweight certificateless hybrid signcryption scheme for internet of things. Futur Gener Comput Syst 127:23–30
108. Mousavi SK, Ghaffari A (2021) Data cryptography in the internet of things using the artificial bee colony algorithm in a smart irrigation system. J Inf Security and Appl 61:102945
109. Bettoumi B, Bouallegue R (2021) Lc-dex: Lightweight and efficient compressed authentication based elliptic curve cryptography in multi-hop 6lowpan wireless sensor networks in hip-based internet of things. Sensors 21(21):7348
110. Kumari KS, Priya JL, Pravallika B, Bhargavi KM, Priya G (2023) Two stage secure medical data transmission for iot based e-health application. Turkish J of Comput and Math Educ (TURCOMAT) 14(2):352–364
111. Al-Zubaidie M (2023) Implication of lightweight and robust hash function to support key exchange in health sensor networks. Symmetry 15(1):152
112. Abd El-Aziz RM, Taloba AI, Alghamdi FA (2022) Quantum computing optimization technique for iot platform using modified deep residual approach. Alex Eng J 61(12):12497–12509
113. Shahid F, Khan A, Jeon G (2020) Post-quantum distributed ledger for internet of things. Comput & Electr Eng 83:106581
114. Yi H, Chi R, Huang X, Cai X, Nie Z (2022) Improving security of internet of vehicles based on post-quantum signatures with systolic divisions. ACM Trans Internet Technol 22(4):1–15
115. Qu Z, Wang K, Zheng M (2021) Secure quantum fog computing model based on blind quantum computation, J of Ambient Intell and Humanized Comput, 1–11
116. Shen Y, Tang X, Zhang X, Zhou Y, Zou H (2022) A flexible continuous-wave quantum cryptography scheme with zero-trust security for internet of things. Int J Distrib Sens Netw 18(11):15501329221136978
117. Akleylek S, Soysaldı M, Lee W-K, Hwang SO, Wong DC-K (2020) Novel postquantum mq-based signature scheme for internet of things with parallel implementation. IEEE Internet Things J 8(8):6983–6994
118. Chikouche N, Cayrel P-L, Mboup EHM, Boidje BO (2019) A privacy-preserving code-based authentication protocol for internet of things. J Supercomput 75:8231–8261
119. Abd El-Latif AA, Abd-El-Atty B, Mazurczyk W, Fung C, Venegas-Andraca SE (2020) Secure data encryption based on quantum walks for 5g internet of things scenario. IEEE Trans Netw Serv Manage 17(1):118–131
120. Chen L, Chen Q, Zhao M, Chen J, Liu S, Zhao Y (2022) Ddka-qkdn: dynamic on-demand key allocation scheme for quantum internet of things secured by qkd network. Entropy 24(2):149
121. Althobaiti OS, Dohler M (2021) Quantum-resistant cryptography for the internet of things based on location-based lattices. IEEE Access 9:133185–133203
122. Shamshad S, Riaz F, Riaz R, Rizvi SS, Abdulla S (2022) An enhanced architecture to resolve public-key cryptographic issues in the internet of things (iot), employing quantum computing supremacy. Sensors 22(21):8151
123. Xu D, Liu L, Zhang N, Dong M, Leung VC, Ritcey JA Nested hash access with post quantum encryption for mission-critical iot communications, IEEE Internet of Things J

124. Xi P, Zhang X, Wang L, Liu W, Peng S (2022) A review of blockchain-based secure sharing of healthcare data. Appl Sci 12(15):7912
125. Zheng Z, Xie S, Dai H-N, Chen W, Chen X, Weng J, Imran M (2020) An overview on smart contracts: challenges, advances and platforms. Futur Gener Comput Syst 105:475–491
126. Peng L, Feng W, Yan Z, Li Y, Zhou X, Shimizu S (2021) Privacy preservation in permissionless blockchain: a survey. Digital Commun and Netw 7(3):295–307
127. Dib O, Brousmiche K-L, Durand A, Thea E, Hamida EB (2018) Consortium blockchains: overview, applications and challenges. Int J Adv Telecommun 11(1):51–64
128. Mamun Q (2022) Blockchain technology in the future of healthcare. Smart Health 23:100223
129. Pabitha P, Priya JC, Praveen R, Jagatheswari S (2023) Modchain: a hybridized secure and scaling blockchain framework for iot environment. Int J Inf Technol 15(3):1741–1754
130. Helliar CV, Crawford L, Rocca L, Teodori C, Veneziani M (2020) Permissionless and permissioned blockchain diffusion. Int J Inf Manage 54:102136
131. Kushwaha SS, Joshi S, Singh D, Kaur M, Lee H-N (2022) Ethereum smart contract analysis tools: a systematic review. IEEE Access 10:57037–57062
132. Al-Garadi MA, Mohamed A, Al-Ali AK, Du X, Ali I, Guizani M (2020) A survey of machine and deep learning methods for internet of things (iot) security. IEEE Commun Surv & Tutorials 22(3):1646–1685
133. Farooq U, Tariq N, Asim M, Baker T, Al-Shamma'a A (2022) Machine learning and the internet of things security: solutions and open challenges. J Parallel and Distributed Comput 162:89–104
134. Hussain F, Hussain R, Hassan SA, Hossain E (2020) Machine learning in iot security: current solutions and future challenges. IEEE Commun Surveys & Tutorials 22(3):1686–1721
135. Alzubaidi L, Zhang J, Humaidi AJ, Al-Dujaili A, Duan Y, Al-Shamma O, Santamaría J, Fadhel MA, Al-Amidie M, Farhan L (2021) Review of deep learning: concepts, cnn architectures, challenges, applications, future directions. J big Data 8:1–74
136. Thakkar A, Lohiya R (2021) A review on machine learning and deep learning perspectives of ids for iot: recent updates, security issues, and challenges. Archives of Comput Methods in Eng 28:3211–3243
137. Goldblum M, Tsipras D, Xie C, Chen X, Schwarzschild A, Song D, dry A, Li B, Goldstein T (2022) Dataset security for machine learning: data poisoning, backdoor attacks, and defenses. IEEE Trans Pattern Anal Mach Intell 45(2):1563–1580
138. Ahmad R, Alsmadi I (2021) Machine learning approaches to iot security: a systematic literature review. Internet of Things 14:100365
139. Ammar M, Washha M, Ramabhadran GS, Crispo B (2018) slimiot: Scalable lightweight attestation protocol for the internet of things, In: 2018 IEEE Conference on Dependable and Secure Computing (DSC), IEEE, pp 1–8
140. Fang D, Qian Y, Hu RQ (2020) A flexible and efficient authentication and secure data transmission scheme for iot applications. IEEE Internet Things J 7(4):3474–3484
141. Dhanda SS, Singh B, Jindal P (2020) Lightweight cryptography: a solution to secure iot. Wireless Pers Commun 112:1947–1980
142. Lo'Ai AT, Somani TF (2016) More secure internet of things using robust encryption algorithms against side channel attacks, In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). IEEE, pp 1–6
143. Kumar A, Garhwal S (2021) State-of-the-art survey of quantum cryptography. Arch Comput Methods in Eng 28:3831–3868
144. Chowdhury S, Covic A, Acharya RY, Dupee S, Ganji F, Forte D (2021) Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions, J of Cryptogr Eng, 1–37
145. Wang H-W, Tsai C-W, Lin J, Yang C-W (2022) Authenticated semi-quantum key distribution protocol based on w states. Sensors 22(13):4998
146. Kumar A, Ottaviani C, Gill SS, Buyya R (2022) Securing the future internet of things with post-quantum cryptography. Secur and Privacy 5(2):e200
147. Bassi R, Zhang R, Gatto A, Tornatore M, Verticale G (2023) Quantum key distribution with trusted relay using an etsi-compliant software-defined controller, In: 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN), IEEE, pp 1–7

148. Zeydan E, Turk Y, Aksoy B, Ozturk SB (2022) Recent advances in post-quantum cryptography for networks: A survey, In: 2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ). IEEE, pp 1–8

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Sarra Cherbal[1] · Abdelhak Zier[1] · Sara Hebal[1] · Lemia Louail[2] · Boubakeur Annane[1]

✉ Sarra Cherbal
sarra_cherbal@univ-setif.dz

Abdelhak Zier
abdelhak.zier@univ-setif.dz

Sara Hebal
sara.hebal@univ-setif.dz

Lemia Louail
lemia.louail@univ-lorraine.fr

Boubakeur Annane
boubakeur.annane@univ-setif.dz

[1] LRSD Laboratory, Department of Computer Science, Faculty of Sciences, Univ Ferhat Abbas Setif 1, Setif, Algeria

[2] Université de Lorraine, CNRS, CRAN, F-54000 Nancy, France