STM JOURNALS

Trends in
Electrical Engineering

https://journals.stmjournals.com/tee

ISSN: 2249-4774 (Online)
ISSN: 2321-4260 (Print)
Volume 15, Issue 1, 2025
January–April
DOI (Journal): 10.37591/TEE

Review TEE

Advancing IoT Security Through Blockchain-Based Approaches

Ahmed Abubakar Aliyu*

Abstract

The emergence of blockchain technology has revolutionized various industries, including the Internet of Things (IoT), by providing a decentralized and secure platform for data management and transaction processing. However, securing IoT devices and networks remains a significant challenge due to inherent vulnerabilities and the increasing sophistication of cyberattacks. Blockchain-based security approaches have shown promise in addressing these challenges, yet their adoption is hindered by a lack of comprehensive taxonomy and systematic studies on their architectural design and effectiveness. A standardized taxonomy for blockchain-based security is essential for effectively comparing and evaluating different solutions, facilitating the identification of the most suitable approaches for specific IoT scenarios. Additionally, systematic studies on the architectural design of these security approaches are crucial for understanding the trade-offs between security, performance, and scalability. Empirical evaluations are needed to rigorously assess the effectiveness of blockchain-based security solutions against various attack vectors and performance benchmarks, guiding their optimization for IoT applications. Addressing these gaps in the current literature is critical for advancing the adoption and effectiveness of blockchain-based security approaches in the IoT domain. This paper proposes a comprehensive taxonomy, systematic architectural studies, and empirical evaluations to provide a solid foundation for selecting, designing, and implementing secure and efficient blockchain-based solutions tailored to the specific needs of IoT applications. These efforts will enhance the security, performance, and scalability of IoT systems, fostering greater confidence in blockchain technology's role in securing the IoT ecosystem.

Keywords: Cybersecurity, internet of things, blockchain technology, intrusion detection systems

INTRODUCTION

By offering a decentralized and secure platform for data storage and transaction processing, blockchain technology has transformed several industries, including the Internet of Things. However, securing IoT devices and networks remains a significant challenge, owing to their inherent vulnerabilities and the increasing sophistication of cyberattacks. Blockchain-based security approaches have emerged as promising solutions to address these challenges; however, the lack of a comprehensive taxonomy and systematic studies on their architectural design and effectiveness hinders their widespread adoption and optimization for specific IoT applications. First, the lack of a standardized taxonomy for blockchain-based security approaches makes it difficult to compare and evaluate different solutions effectively. This lack of clarity makes it difficult for researchers, practitioners, and policymakers to identify the most appropriate approach for specific IoT scenarios. Second, the lack of systematic studies on the architectural design of blockchain-based security approaches limits our understanding of the trade-offs among security, performance, and scalability. A

***Author for Correspondence**
Ahmed Abubakar Aliyu
E-mail: ahmed.aliyu@kasu.edu.ng

Head, Department of Secure Computing, Faculty of Computing, Kaduna State University, Nigeria

Received Date: January 10, 2025
Accepted Date: January 14, 2025
Published Date: January 15, 2025

Citation: Ahmed Abubakar Aliyu. Advancing IoT Security Through Blockchain-Based Approaches. Trends in Electrical Engineering. 2025; 15(1): 1–34p.

comprehensive understanding of the design choices and their implications is crucial for the development of efficient and secure IoT systems. Finally, there is an urgent need for empirical studies of the effectiveness of blockchain-based security approaches in the IoT context. Rigorous evaluation of these approaches against various attack vectors, performance benchmarks, and scalability requirements is essential to determine their practical utility and guide their optimization for IoT applications. Addressing these gaps in the literature is critical for advancing the adoption and effectiveness of blockchain-based security approaches in the IoT domain. A comprehensive taxonomy, systematic architectural studies, and empirical evaluations will provide a solid foundation for selecting, designing, and implementing secure and efficient blockchain-based security solutions tailored to the specific needs of IoT applications.

Literature Search

Extensive search was conducted across multiple academic databases including IEEE Xplore, ScienceDirect, PubMed, and Google Scholar. The search used keywords such as *"IoT Security," "Agriculture," "Blockchain-based Security Solutions,"* and *"IDS,"* along with related terms. The search was restricted to publications for the past five years to ensure the inclusion of the most recent developments in the field.

Inclusion Criteria

The initial screening process focused on identifying literature directly related to the application of blockchain technology in IoT security. Only credible research reports, conference papers, and peer-reviewed journal publications were taken into consideration for inclusion. The selected publications specifically addressed the use of blockchain technology in areas such as intrusion detection system (IDS).

Exclusion Criteria

Studies unrelated to the application of blockchain technology in IoT security, duplicate publications, and non-English articles were excluded from the review.

Data Extraction

Key information was systematically extracted from the selected studies, including authors, publication year, research objectives, methodologies, findings, and limitations. The data were organized to facilitate a comprehensive review.

Synthesis and Analysis

To identify recurrent themes, trends, and patterns pertaining to the application of blockchain technology to IoT security, the retrieved data were examined. A comparative analysis was employed to examine the findings across studies, enabling insights into current trends and future research directions.

Critical Assessment

To assess the reliability and validity of the selected studies, the research methodologies, data sources, and sample sizes of each article were critically reviewed. This evaluation ensures the quality and robustness of the evidence presented in the reviewed literature.

Identification of Gaps

A literature analysis revealed several gaps and areas that require further investigation, particularly in the application of blockchain technology within the IoT security domain. These gaps highlight the potential opportunities for future research.

BLOCKCHAIN TECHNOLOGY AND ITS EVOLUTION

The history of blockchain technology can be traced back to the early 1990s when cryptographer David Chamu [1] first proposed a blockchain-like protocol in his 1982 thesis. In 1991, Haber and

Stornetta described more work on a chain of blocks that were cryptographically secured [2]. Their goal was to put in place a system that would prevent tampering with the document timestamps. Merkle trees were added to the concept in 1992 by Haber, Stornetta, and Dave Bayer, which increased its effectiveness by enabling the collection of several document certifications in a single block [3]. Since 1995, the New York Times has published the hashes of its document certificates every week under the name Surety. Satoshi Nakamoto, or a group of people, proposed the idea of the first decentralized blockchain in 2008 [4]. By adding a difficulty parameter to stabilize the rate at which blocks are added to the chain and employing a hash cash-like technique to timestamp blocks without requiring their signature by a trusted party, Nakamoto significantly enhanced the system.

Nakamoto's design was implemented in the Bitcoin cryptocurrency, which was launched in 2009. Bitcoin was the first successful application of blockchain technology, with a capital market of over USD 10 billion, and remains the most popular cryptocurrency today [5]. Since the launch of Bitcoin, blockchain technology has evolved rapidly, with new blockchain platforms developed to support a wide range of applications, including smart contracts, decentralized finance, nonfungible tokens (NFTs), and academic research [6].

Blockchain is a distributed ledger technology that allows for safe, transparent, and impenetrable recording of transactions. It functions as a decentralized database shared among computers in a network [7]. Each block in the chain comprises a series of transactions, and each block is cryptographically linked to the preceding block, making tampering with the data extremely difficult, as shown in Figure 1 [8]. To record transactions, blockchain employs a distributed network of computers, as each computer in the network has a copy of the blockchain, and any new transactions are broadcast to all the computers in the network. The transaction was subsequently verified by computers and added to their copies of the blockchain. The fact that it is very difficult to alter the information pertaining to blockchain is the foundation of one of the key features of blockchain security [9]. This is because each block is cryptographically connected to the preceding block, and any modification to one block would require changes to all subsequent blocks. Because it is possible to construct many blocks simultaneously, Bitcoin implements a consensus process known as Proof-of-Work (PoW) [10]. PoW is the process of finding the correct random number (nonce) in the block header that corresponds to the predicted number of leading zeros in the Secure Hash Algorithm-256 (SHA-256) hash value associated with each block [11].

The computation required to obtain an appropriate nonce is proportional to the expected number of zeros. This means that it is very difficult to generate a new block; however, once a block is generated, it is very easy to verify. This is because nonce is a one-way function, meaning that it is easy to calculate the output of the function given the input, but it is very difficult to calculate the input given the output [12]. Furthermore, after a new block is created, it is sent to and validated by the other network nodes. The miner who generates the block is rewarded with Bitcoin (BTC) as an incentive to continue supporting the network [13] [14]. Moreover, if two miners create blocks simultaneously, the nodes in the network will accept the block with the highest workload. This is because a higher workload implies that the block is more likely to be valid. It is also more difficult for an attacker to declare a false transaction because they would have to recalculate all subsequent blocks [15]. It would be difficult to complete this computationally demanding task.

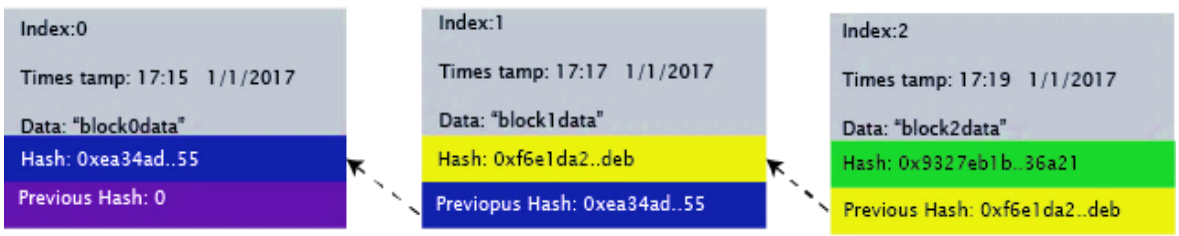

Figure 1. Blockchain illustration.

Blockchain enables Byzantine fault tolerance (BFT) [16] by facilitating consensus in an unreliable environment as well as decentralization, permanence, anonymity, and audibility. Because of the decentralized structure, that is, resilience to denial of service (DoS), the system ensures confidentiality, integrity, and availability [17]. The system is also theoretically resistant to impersonation attacks, provided that legitimate participants control at least 51% of the mining rights [18].

Blockchain's Original Limitations and Technical Response

The original blockchain faces technical challenges and limitations that hinder its adoption. One of these challenges is scalability [19]. Currently, Bitcoin's transaction rate is only seven transactions per second [20], which may become insufficient as the number of users increases. Another challenge is the transaction time. Complete Bitcoin transactions take approximately 10 min [21], which is too long for many applications. Similarly, Bitcoin blocks are almost megabytes in size, which can restrict the flow of information if it reaches the level of financial competition [22]. This can lead to bandwidth shortage. Furthermore, the security of Bitcoin is based on the assumption that most nodes in the network function correctly; however, there are known attacks that can exploit this weakness. In particular, Bitcoin mining consumes considerable energy because of the trial-and-error involved in finding the correct nonce [23]. This is a major concern because it raises environmental and sustainability issues. These restrictions have prompted the creation of substitutes and modifications to blockchain technology. To facilitate the creation of smart contracts and other decentralized applications, Ethereum, for instance, presented blockchains with an integrated Turing-complete programming language [24].

Although Bitcoin and the underlying blockchain have the potential to transform many industries, they face technical challenges and limitations. With the development of blockchain technology, it is critical to address these problems to guarantee its broad acceptance.

The Ethereum Virtual Machine (EVM), a distributed virtual machine, is used to perform smart contracts in the second iteration of the Ethereum blockchain [25]. Ethereum smart contracts (Figure 2) can be considered lightweight, decentralized applications, or dAPPs, which opens the door to application research in various fields [26]. Similarly, Blockchain 3.0 [27] includes applications outside finance and markets in government, science, health, technology, and education. Blockchain 3.0 can run fully integrated dAPPs and intelligent contracts, including automated agents (AAs) and software that operate without human intervention, creating autonomous decentralized organizations (DAOs) [28], where artificial intelligence systems make decisions and humans play a secondary role. The latest versions of cryptocurrencies, along with their respective blockchain changes, address the original flaws and limitations of Bitcoin. New alternative coins or alternative coins (Altcoin) [29] improve block timing, number of transactions per block, and consensus algorithms for security and efficiency. For example, the low-power Proof-of-Stake (PoS) consensus method requires fewer CPU cycles to mine, and its reward system is based on a node's coin balance rather than its computing power [30].

However, the technical hurdles and limitations of Bitcoin and its original blockchain hinder its adaptation as it evolves [31]. First, Bitcoin's current maximum throughput is only seven transactions per second, which may limit its scalability over time, as the number of users increases. Second, the time required to complete a transaction is approximately 10 min [32], and the time required to mine a block is often tied to the number of zeros required for the PoW, with a latency that makes the original blockchain unsuitable for applications that rely on immediacy. Third, because the size of a Bitcoin block is approximately 1 megabyte (MB), the number of transactions is limited to 500, and Bitcoin can suffer from bandwidth shortages if its throughput exceeds that of its financial competitors. Finally, current Bitcoin security relies on the assumption that the majority of nodes in the network behave correctly to maintain the validity of the system [33].

Similarly, a study [34] described three realistic attacks on Bitcoin security involving block manipulation and transaction delivery. Moreover, Sybil attacks rely on IP address control and rapid financial intervention.

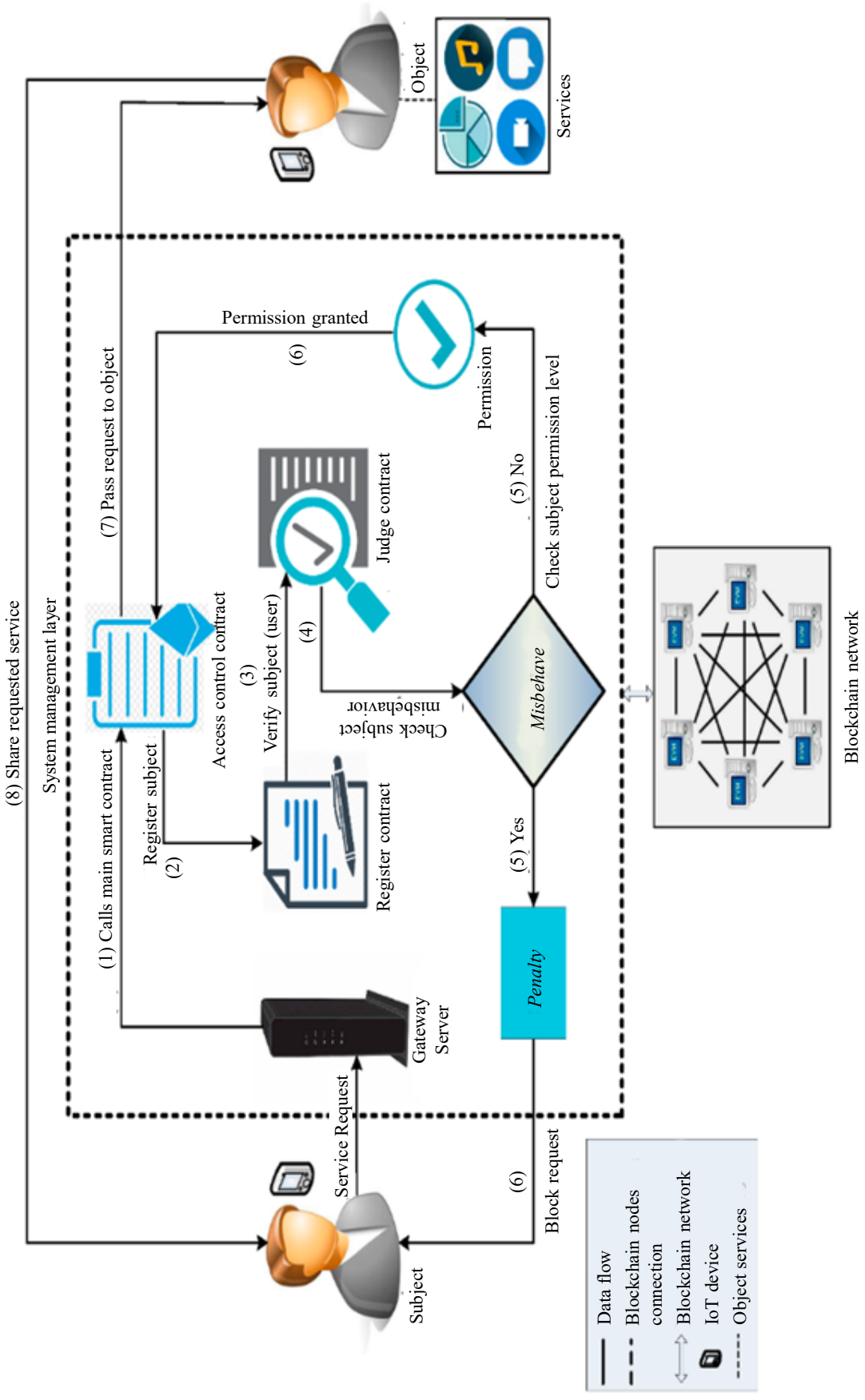

Figure 2. The smart contract.

Another study [35] showed that a small number of mining pools can use a technique known as "Selfish mining" to collect more than their fair share of mining rewards, eventually leading other pools to adopt the same strategy and effectively launch double-spending attacks. In addition, software problems have been discovered in Bitcoin, resulting in vulnerabilities such as CVE-2010-5139 (integer overflow) [36]. Finally, because Bitcoin mining uses a trial-and-error technique to find the nonce that provides PoW, it requires a significant amount of computational power.

The limitations of Bitcoin have forced the search for alternatives or modifications to the original method to improve the application and scope of the blockchain. The first and subsequent versions of blockchain are classified according to their possible activities. The blockchain community has defined three categories of blockchain technology: 1.0, 2.0, and 3.0 [37]. Blockchain 1.0 is the original blockchain technology implemented using Bitcoin. It primarily focuses on cryptocurrencies and digital payments. Blockchain 2.0 is an extension of Blockchain 1.0, which introduces smart contracts and apps. While dAPPs are blockchain-based applications that are not governed by a single entity, smart contracts are self-executing contracts kept on the blockchain.

Blockchain 3.0 is a future vision of blockchain technology, which aims to expand its capabilities beyond cryptocurrency and smart contracts. Blockchain 3.0 is expected to be more scalable, secure, and efficient than the previous versions of blockchain technology. Finally, Blockchain 4.0 [38], which is based on neural networks, introduces new consensus algorithms that improve the fault tolerance of the system. In addition, Blockchain 4.0 platforms include a new network design, artificial intelligence for decision-making, and a low-latency internet connection protocol for integration with internet resources and the development of blockchain-based services [39]. Table 1 summarizes the key differences between Blockchain 1.0, 2.0, 3.0, 4.0, and 5.0, whereas Table 2 compares Blockchain's key performance from literature.

Essentially, we can divide consensus algorithms into three categories:

1. *Traditional consensus algorithms:* The traditional consensus algorithm is discussed in this section. BFT and PoW on the Paxos and its variations are discussed.
    a. *Paxos and its variations:* These algorithms, including Raft, are frequently employed in distributed networks to provide fault tolerance and consistency. They work by a designated leader, proposing values, and other nodes vote on them.

Table 1. Comparative summary of Blockchain 1.0, 2.0, 3.0, 4.0, and 5.0.

	Primary focus	**Key features**
Blockchain 1.0	Cryptocurrency and digital payments	Bitcoin and Proof-of-Work
Blockchain 2.0	Smart contracts and dAPPs	Ethereum, Hyperledger Fabric and Proof-of-Stake
Blockchain 3.0	Enterprise applications, and supply chain management	Scalability, security, efficiency, distributed ledger technology (DLT)
Blockchain 4.0	Network Architecture, Industry, and IoT	Flexibility, scalability, usability, and Blockchain-as-a-Service
Blockchain 5.0	AI	User-centric design, privacy-preserving techniques, integration with emerging technologies

Table 2. Comparing blockchain's performance from the literature.

System type	**Size of block**	**Interval**	**Consensus mechanism**	**Energy saving**	**Practical tolerated adversary power**
Bitcoin	96 Gigabytes	10 min	Proof-of-Work	No	Less than 25%
Litecoin	16.55 Gigabytes	2.5 min	Proof-of-Work	No	Less than 49%
Dogecoin	13.93 Gigabytes	1 min	Proof-of-Work	No	Less than 47%
Ethereum	17-60 Gigabytes	12 sec	Proof-of-Work	No	Less than 25%
Tendermint	10 Gigabytes	5 sec	Byzantine Fault Tolerance, Proof-of-Stake	Yes	Less than 33%

   b. *Byzantine fault tolerance:* This family of algorithms is designed to tolerate malicious Byzantine failures, where nodes can fail arbitrarily. BFT algorithms are typically more complex than Paxos but can provide stronger guarantees.
   c. *Proof-of-work:* The consensus technique employed by Bitcoin and other digital currencies is called PoW. The first minor to solve a cryptographic puzzle wins the right to add the next block to the network, which is secure but can be energy-intensive and slow.
2. *Blockchain-based consensus algorithms*
   a. *Proof-of-stake:* To participate in the consensus process, validators stake their coins in place of miners. Validators vote on new blocks and are chosen according to the cryptocurrency they stake. Although the PoS requires less energy than the PoW, it may be more susceptible to attacks.
   b. *Delegated proof-of-stake:* In the Delegated Proof-of-Stake (DPoS) form of PoS, users assign a limited number of representatives to their voting authority. DPoS can be faster and more efficient than PoS but can also be more centralized.
   c. *Proof-of-authority:* The algorithm uses a predefined set of validators that are trusted to act honestly. Proof-of-Authority (PoA) is fast and efficient but can be less secure than other consensus algorithms.
3. *Emerging consensus algorithms*
   a. *Proof-of-elapsed time:* This algorithm uses elapsed time to measure consensus. The first node that provides a random number has the right to add a subsequent block to the network. Proof-of-Elapsed Time (PoET) is less energy-intensive than PoW, but it may be more vulnerable to attacks [40].
   b. *Proof of activity:* This algorithm rewards nodes to perform useful activities such as storing data or processing transactions. Proof of activity (PoA) can be more efficient than PoW and PoS; however, it can be more complex to implement.
   c. *Proof-of-reputation:* Security, speed, and centralization issues with the current permissionless blockchain consensus algorithms are addressed by a new reputation-based consensus method known as proof-of-reputation (PoR). PoR achieves a balance between scalability, security, and decentralization by combining the BFT, reputation, reward, and punishment mechanisms [41].
   d. *Sharding:* Sharding is a scalability-enhancing approach that can be used in various consensus techniques. The blockchain is split into smaller units, known as shards, by sharding, which allows for separate processing. Consequently, more transactions may be handled every second.

In summary, the original limitations of the blockchain include scalability, security, energy consumption, and usability. Scalability is the capacity of a blockchain network to swiftly and effectively handle large volumes of transactions. Current blockchain networks are often slow and expensive to use, particularly for high-volume applications [42]. Security is another concern with blockchain networks, as they can be vulnerable to attacks, such as 51% attacks and double-spending attacks. Because mining and validating transactions require considerable processing power, blockchain networks can also be very energy intensive. Some people are concerned about this because it brings about sustainability and environmental issues. Another drawback is that non-technical users may find blockchain technology complicated and challenging to utilize [43]. This may have prevented some industries from adopting it.

Current Challenges for the Blockchain

Given that blockchain is a public ledger, all transactions are visible to everyone, and in many circumstances, user activity can be tracked even after the latest version of the protocol is released. To enhance privacy protection and prevent data breaches, one-time accounts [44], individual private keys for each transaction [45], and transaction chaff [46] can all be used. A recent study has published a framework for creating smart contracts that respect user privacy [47]. The framework includes a compiler that converts scripts into cryptography-based protocols. As smart contracts are computer programs, they can potentially be abused by bad actors, which can exacerbate the loss of data, including

private keys and other information. Furthermore, flaws exist in the technical and functional principles of smart contracts. One study highlighted undetectable flaws in the automated execution of contracts during forks, which can change their operational state [48]. This study also revealed a malicious miner attack on time-dependent contracts that was used to manipulate the results of transactions executed by the contract. This study also simulated a DAO attack [49] in which an attacker steals money by exploiting a flaw in the payout function after a fallback. Another challenge identified in a recently published paper is the four significant security flaws in blockchain systems. These are transaction order dependency, timestamp dependency, anomaly mishandling, and reinternalization [50]. Attackers can also exploit these flaws to steal funds, disrupt the network, or even bring down the system.

However, the potential of blockchain enables the development of applications that aim to address these security challenges. One of the most powerful features of blockchain is its ability to rely on proven cryptographic qualities to ensure data integrity and its natural time perception [51], which allows for the extension of services to other areas, particularly security. Beyond financial applications, there are some out-of-the-box benefits of blockchain, according to one study [52], such as distributed P2P network fault tolerance, practical consensus, and predictable, trustless participation.

Data invariance and authentication were added to the list [53], bringing data security to the table. Based on the same argument, one study goes so far as to claim that blockchain technology can ensure the tracking of virtually any value [54]. However, not all security solutions are suitable for replacement or supplementation with blockchain applications. A recent study [55] proposed a scenario in which distributed ledger applications can be utilized for security purposes, which includes (1) various counterparties transacting through a third party; (2) the third party is not entirely trusted; (3) the priority is to validate the transaction, with a system that offers authenticity and integrity of data being the top priority; (4) integrity is tolerated over trade-offs between secrecy and performance; and (5) the third party is not fully trusted. Furthermore, other studies call for a comprehensive technological strategy before incorporating blockchain into diverse solutions [56–58]. Despite its drawbacks, blockchain innovation can completely transform the security landscape, despite its drawbacks [59]. Decentralization, immutability, and transparency are distinctive features that make it ideal for a variety of security applications [60]. One area where blockchain has already had a significant impact is data storage, as blockchain-based data storage solutions offer several advantages over traditional centralized systems, including enhanced security, improved transparency, and increased efficiency [61]. Blockchain is also being used to improve the security of protected health information (PHI) [62]. Blockchain-based PHI management solutions can help provide patients with more control over their PHI, improve the efficiency of PHI exchange, and reduce the risk of PHI breaches. In addition to data storage and PHI management, blockchain is being used to improve the security of a variety of other applications, including data control, DDoS defense, breeding file protection, and general IoT security [63]. In summary, blockchain technology can address security issues and its practical use; however, the security issues that need to be addressed should be thoroughly researched, understood, and tested prior to deployment.

INTRUSION DETECTION SYSTEMS

Traditional Intrusion Detection Systems

A security solution that focuses on network traffic for malicious activity is called an IDS [64]. Malware infections, DOS attacks, and unauthorized access attempts are just a few of the attacks that IDSs can identify. Additionally, IDSs function by looking for patterns in network data that indicate malicious behavior. These patterns can be based on the specific characteristics of malicious traffic, such as unusual packet sizes or unusual traffic patterns. IDSs can be used in various ways, such as monitoring network traffic at the perimeter of a network, or they can be deployed on individual hosts to monitor traffic for that host [65]. Moreover, an IDS is a critical reactive security measure that detects potential attacks on a host system [66]. In addition, an IDS has long been regarded as a powerful security solution that monitors network traffic and then detects and prevents suspicious requests [67]. In other words, the task of observing and evaluating occurrences in a computer network system for any signs of potential

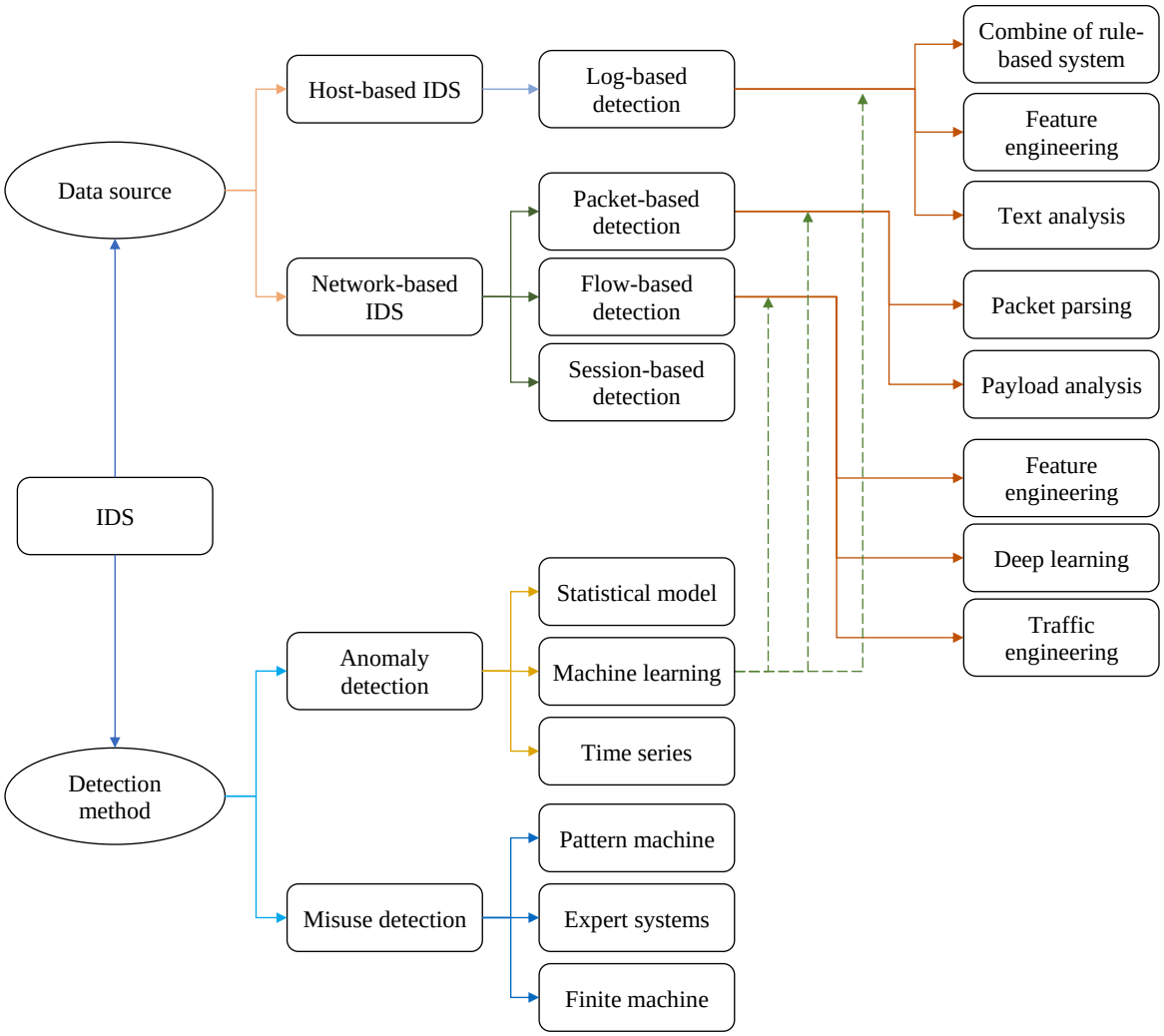

Figure 3. The traditional IDS structure.

attacks that could be harmful or looming threats of violations of computers and network security policies is known as an IDS, as shown in Figure 3 [65].

An IDS is typically supported in its decision-making by two-component technologies: a neural network that detects security anomalies and an attack graph that informs the IDS of system states of interest [68]. With the widespread adoption of networking technology, IDSs have strived to detect and make them aware of normal or abnormal networking activities. Intruders try to damage, compromise, or devastate systems with the help of wirelessly communicating packets. Recently, several IDS have been used in cybersecurity systems to detect and mitigate malicious traffic from normal traffic. IDS are traditionally classified into five types, as seen below [69].

(1) A network intrusion detection system (NIDS) monitors an entire network through one or more points of contact. To deploy a NIDS, it is typically necessary to install it on a hardware device within a network facility [44]. Upon installation, the NIDS samples each data packet that flows through it. Standard NIDS can scan all the traffic that passes through it. (2) A network node-based IDS (NNIDS) is a subset of a NIDS; however, because it works differently, we classify it as a separate type of IDS [70]. Packets that pass through an NNIDS were also analyzed. The system keeps an eye on every node linked to the network, rather than depending on a single device to keep an eye on all network activities. This distinction has some advantages, such as a faster speed and the use of fewer resources. (3) A Host IDS (HIDS) extends the device independence of an NNIDS. All devices connected to the network can

have IDS software installed using HIDS. HIDSs operate by capturing "snapshots" of the device they are tasked with protecting. By comparing the latest snapshot with previous records, HIDS can detect differences that could indicate intrusion. (4) An IDS that monitors the protocol used is known as a protocol-based IDS (PIDS). Typically, this type of IDS examines the HTTP or HTTPS protocol stream that connects the devices to the server, as it is usually routed to the front end of the server. The system can monitor incoming and outgoing traffic to safeguard the web server. (5) Another type of IDS that focuses on the security of software applications is an application protocol-based IDS (APIDS). APIDSs, also known as host-based intrusion detection systems (HIDSs), focus on how apps and servers communicate. Typically, an APIDS is set up on clusters of servers. Moreover, an APIDS is unlikely to meet all network monitoring needs; however, it can be used in conjunction with other types of IDS. There are also three (3) IDS: implementation and detection methods. These are:

1. Signature-based IDS
2. Anomaly-based IDS
3. Hybrid IDS

Unauthorized program execution, unauthorized network access, unauthorized directory access, and irregularities in the usage of network rights are examples of typical footprints or patterns that can be considered signatures [71]. Network traffic linked to a malevolent attack on a computer network or system can also be a series of bytes in a file. Signature-based IDS is one of the most widely used techniques for dealing with software threats such as malware viruses, worms, and trojans on a computer system or network. A well-designed, advanced signature-based detection system is critical for achieving this level of protection [72]. Antivirus software uses signature-based detection to identify unusual threats. It is also known as an essential component of security systems, such as IDSs, Address Verification Services (AVSs), Intrusion Prevention Systems (IPSs), and firewalls. Signature-based IDS can be categorized into pattern-matching and Rule-based Models [73]. Although the pattern-matching approach remains the most widely used model in the signature-based IDS approach, there has been little research on it in relation to blockchain. Pattern recognition models employ one or more pattern-matching algorithms to identify malware. By contrast, rule-based approaches have a set of rules that are compared to network traffic or audit data. They can identify an attack if the rules are in agreement. The two models were combined into a hybrid model.

Anomaly-based IDSs identify malicious activities by detecting deviations from normal behavior. On the other hand, IDSs that are based on signatures identify malicious behavior by comparing them to established attack patterns. They are often more effective at detecting new and emerging threats than signature-based IDSs because they do not rely on a database of known attack patterns [74]. However, anomaly-based IDSs can also be more prone to false positives, as they may flag legitimate activities as malicious if they deviate from normal behavior. There are several approaches for anomaly-based intrusion detection. One common approach is to use machine learning algorithms to learn what constitutes normal behavior for a system or network. Once the machine learning algorithms have learned what is normal, they can flag any activity that deviates from normal behavior as malicious [75]. Utilizing statistical techniques to detect departures from typical behavior is an additional strategy [76]. For example, an anomaly-based IDS may track the number of packets sent between two hosts over a period of time. If the number of packets sent between two hosts suddenly increases, the anomaly-based IDS may flag this activity as malicious. Anomaly-based IDSs are often used in conjunction with other types of IDS, such as signature-based IDSs, known as hybrid IDSs, which can help reduce the number of false positives generated by anomaly-based IDSs. Some of these advantages include the detection of new and emerging threats and flexibility. Its disadvantages include being more prone to false positives and being more difficult to configure and maintain.

Blockchain-Based Intrusion Detection Systems

Blockchain-based Intrusion Detection Systems are a new type of IDSs that use blockchain technology to improve the security and effectiveness of intrusion detection by developing new and innovative

techniques for malware detection and then preventing it by using protective mechanisms such as firewalls, quarantine, and blacklists [77]. For example, blockchains can be used to create distributed reputation systems that can track the behavior of malware and other suspicious activities across multiple networks [78]. Malware attacks can then be detected more successfully and stopped using this information. Adopting blockchain technology in an IDPS necessitates a high degree of technical know-how and comprehension of the underlying technology, which presents a big obstacle for companies without the resources and know-how to set up and manage blockchain-based systems. Furthermore, the use of blockchain technology can introduce new vulnerabilities and attack vectors, such as 51%, smart contracts, and consensus attacks. To reduce such dangers, blockchain-based intrusion detection systems must be carefully designed and placed.

A recent study [79] proposed a novel distributed multi-agent IDPS (DMAIDPS) for intrusion detection and prevention in cloud IoT. The learning agents in DMAIDPS categorize network behavior as either normal or under attack using a six-step detection process with the KDD Cup 99 and NSL-KDD datasets. Based on the recall, accuracy, and F-score metrics, the experimental results were compared with those of other techniques in the field. The Multi-Zone-Wise Blockchain (MZWB) model was proposed in another study [80], where the Enhanced Blowfish Algorithm (EBA), which considers a number of metrics, is first used by all authenticated IoT nodes in the network to confirm their legitimacy. Then, the nodes that are deemed legitimate for network construction are used in the Bayesian Direct Acyclic Graph (B-DAG) for network management, taking into account multiple metrics. Two layers were used in the intrusion detection process. A Deep Convolution Neural Network (DCNN) analyzes the packet flow properties obtained from the data packets in the top tier to categorize them as malicious, suspicious, and normal. In the second stage, the Generative Adversarial Network (GAN) is used to classify suspicious packets as malicious or normal. Finally, the intrusion scenario was reconstructed to reduce the intensity of the attacks using the (IMO). Furthermore, a study [81] proposed a permission-based blockchain system that uses lightweight technology and an arbiter PUF model to secure key pairs of IoT devices. The authors proposed a collaborative detection system that detects DDoS attacks on IoT devices using an ensemble technique based on machine learning. This system has a lower false-positive rate and a higher detection rate than the previous classification methods. The blockchain system was then used by the authors to securely distribute alerts to all IoT network nodes that have undergone sufficient authentication. Table 3 compares traditional and blockchain-based IDSs.

INTERNET OF THINGS

The network of physically connected objects that are equipped with sensors, software, and other technologies to allow them to gather and share data is known as the Internet of Things [82]. These gadgets are challenging to secure because they are frequently scarce and have few resources. Therefore, IoT is a great target for cyberattacks [83]. The sheer volume of devices involved is one of the main obstacles to IoT security. According to a study [84], by 2025, there will be over 75 billion IoT devices, as shown in Figure 4. This massive scale makes it difficult to track and manage all devices and increases

Table 3. Comparison of traditional and blockchain-based IDSs.

Feature	Traditional IDS	Blockchain-based IDS
Technology	Centralized	Decentralized
Deployment	Complex	Relatively simple
Scalability	Limited	High
Security	Vulnerable to attacks	Highly secure
Transparency	Opaque	Transparent
Cost	Relatively low	Relatively high
Benefits	Can detect and prevent a wide range of attacks	More secure, scalable, and transparent
Limitations	Can be complex to configure and manage, prone to false positives, and expensive	Still under development and can be expensive

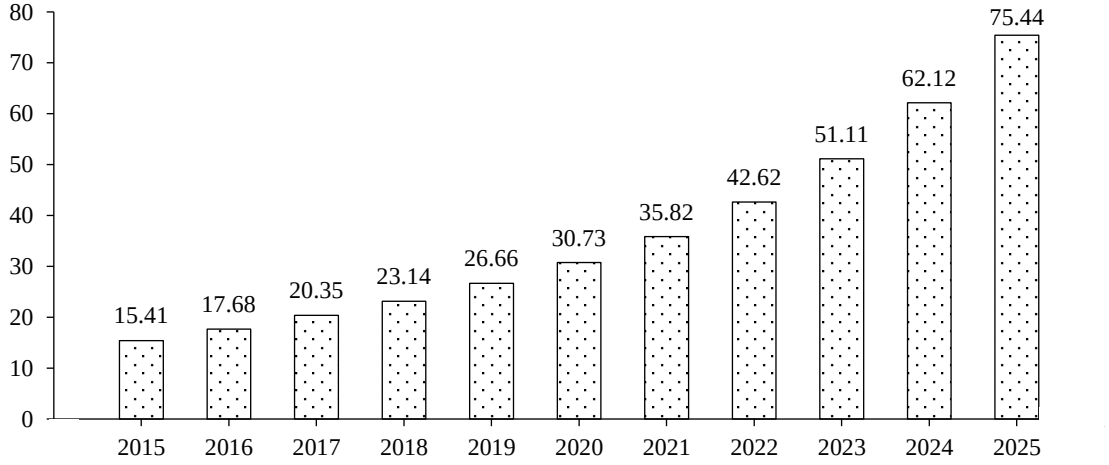

Figure 4. Prediction of the global number of IoT devices from 2015 to 2025 [84].

the likelihood that vulnerabilities will go unnoticed. The variety of IoT devices presents another challenge [85]. IoT devices are used in many different applications and have a wide range of sizes and designs. Because of this variability, it is challenging to create security solutions that work with all types of IoT devices. Furthermore, sensitive data, including financial and personal information, is frequently gathered and processed by IoT devices. Attackers may steal or compromise these data if they are not adequately safeguarded [86]. Despite these obstacles, numerous actions can be taken to enhance IoT security. Implementing security measures at the device level is a crucial first step [87]. This includes using strong passwords, enabling encryption, and keeping software up-to-date. Another important step is to segment the IoT network from other networks [88]. This lessens the likelihood that hackers will obtain private information on other networks. Finally, it is important to monitor the IoT network for suspicious activity [89]. Numerous tools and methods, including detection systems for intrusions, security data, and event management infrastructure, can be used for this [90].

The IoT Reference Model (IoT-RM) shown in Figure 3 is a conceptual framework that provides a consistent understanding of the diverse components and interactions that constitute the IoT. It is designed with modularity, flexibility, and extensibility to accommodate the evolving and dynamic nature of the IoT ecosystem [91]. IoT-RM offers several benefits, including improved communication and collaboration, reduced complexity, and increased interoperability [92]. The IoT-RM consists of four main components: the IoT Domain Model, which provides a conceptual overview of the different entities and relationships that exist in the IoT; the IoT Information Model, which defines the data models used to represent and exchange information in the IoT; the IoT Functional Model, which describes the different functions performed by IoT devices, IoT services, and virtual entities; and the IoT Architecture Model, which describes the different architectural components of an IoT system, such as the device, communication, edge, and cloud layer [93].

Although the complex and rapidly evolving nature of the IoT ecosystem makes it difficult to develop a single taxonomy that encompasses all its aspects, several taxonomies have been proposed, each with its focus and strengths [94]. A common approach to IoT taxonomy is to divide IoT into layers based on the architectural components of IoT system computing. These layers include the device, communication, edge, and cloud layers [95]. Another approach to IoT taxonomy, as shown in Figure 5, is to divide the IoT into different domains based on the specific applications and use cases for which it is being used as in Figure 5. These domains include smart homes, smart cities, industrial IoT, healthcare IoT, agricultural IoT, transportation IoT, energy IoT, and environmental IoT [96]. Finally, IoT can be taxonomized based on the underlying technologies used to implement it. These technologies include radio-frequency identification (RFID), Wireless Sensor Networks (WSNs), cloud computing, AI, blockchain, edge computing, and fog [97].

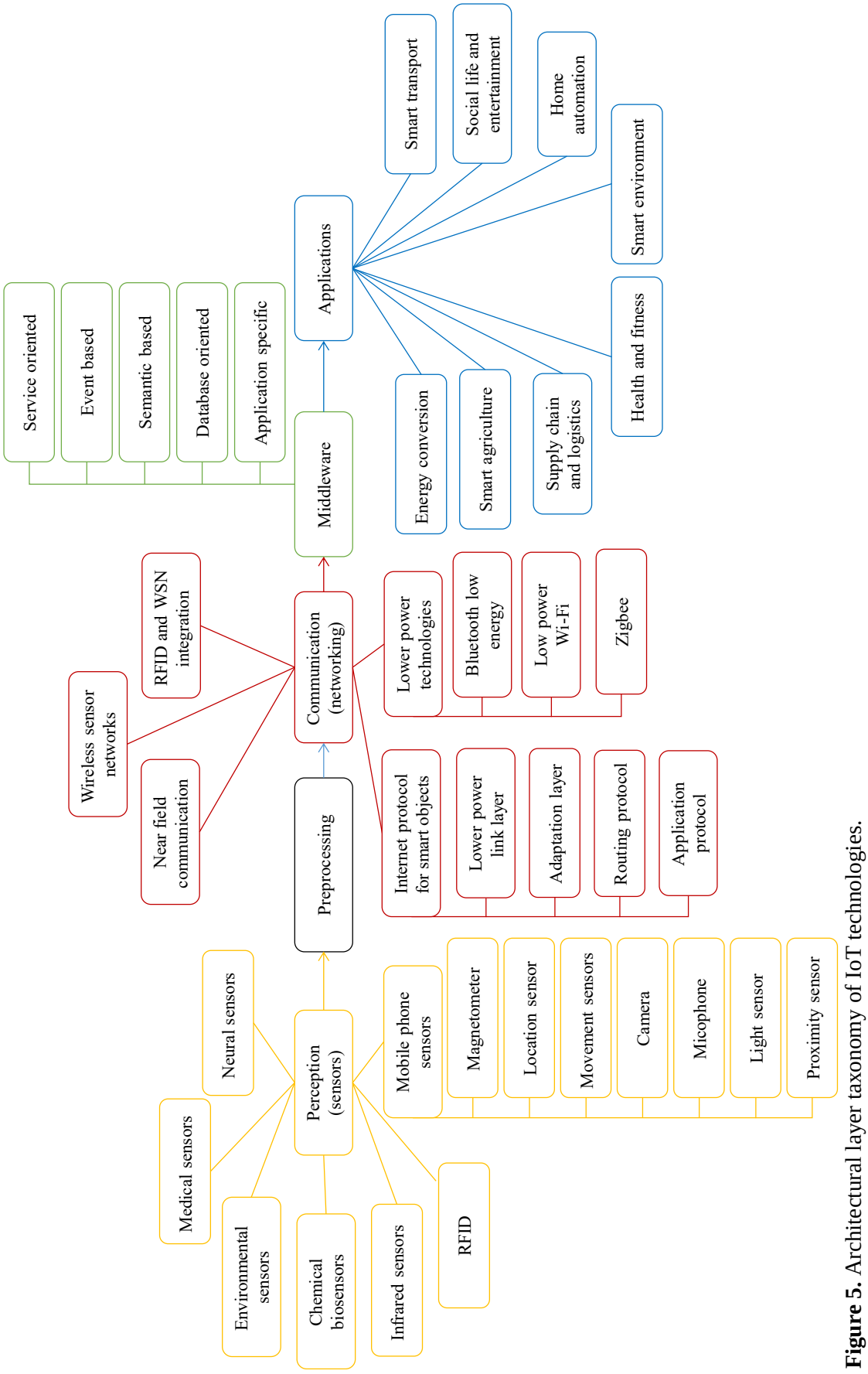

Figure 5. Architectural layer taxonomy of IoT technologies.

IoT Security Challenges

The rapid expansion of the IoT has exposed various security challenges that need to be addressed. A key concern is the large number of IoT devices and their diverse nature, which makes it difficult to adopt uniform security measures [98]. Furthermore, the limited computational power and resources of IoT devices often restrict the implementation of robust security mechanisms. Security researchers have analyzed different perspectives to understand the current state of IoT and identify existing challenges. Insecure network interfaces, insufficient authentication, insecure web services, inadequate privacy controls, insufficient security configurability, insecure software, and inadequate physical security are among the most prevalent problems associated with IoT devices [99].

In the perception layer, wireless communication jamming, interception or modification, and physical security must be considered [100]. Similarly, the network layer is vulnerable to DoS, eavesdropping, and weak authentication, which are major concerns [101]. Additionally, the application layer can be complicated by the heterogeneity of IoT, as the lack of policies and standards can complicate interactions, such as the use of different authentication mechanisms [102]. Other challenges include weak passwords [103], different storage and data processing methods [104], poor security controls, insufficient privacy, and trust filtering capabilities [105], poor identification integrity, lack of global authentication procedures, inadequate privacy policies, insufficient lightweight encryption solutions [106], poor software development practices and software analysis limitations, and malware [107]. Additional challenges include various entry points, domain diversity (ownership, policy, and connectivity), and extensions of internet networks from mobile non-IP sensors to cloud and fog computing [108]. Furthermore, Inadequate perimeter protection, host-based detection mechanisms, and patching procedures adapted to the IoT world are also important issues that must be addressed [109]. Figure 6 shows the cyberattacks to which IoT devices are vulnerable.

The aforementioned IoT security issues can be summarized under two main themes: data protection and privacy. The scope of security has broadened, but the available resources are still insufficient for the current environment. The difficulties are not only difficult to identify, but they may also be considerably difficult to solve. The literature suggests that consensus and prioritization are still needed before society can commit to action. In general, IoT security challenges are complex and multifaceted, but there are several things that can be done to mitigate these risks. By implementing robust security measures, educating users and stakeholders, and investing in security solutions, we can help make IoT a safer environment for everyone.

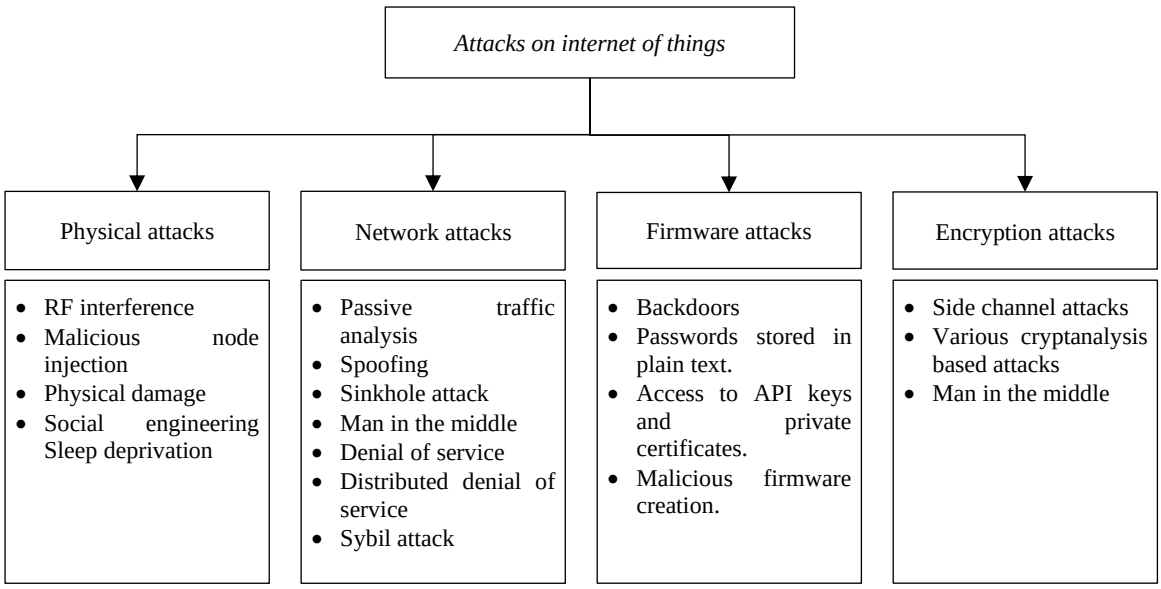

Figure 6. IoT devices are vulnerable to cyberattacks.

Figure 7. Author's IoT security requirements.

Table 4. IoT security issues and architectural collaboration requirements.

IoT layer	IoT security challenge	Collaborators	Security/safety requirement
Sensing	Lightweight encryption and collision avoidance, Inadequate Physical Security, Lack of Integrity and Confidentiality	Researchers, device manufacturers, and standards organizations	Lightweight encryption and collision avoidance algorithms, tamper Resistance
Networking	Scarce lightweight cryptography, insufficient authentication, insecure network services, DoS, eavesdropping, insufficient filtration capacity, Insufficient perimeter defenses, multiple entry points, and network heterogeneity extension	Researchers, network operators, and security vendors	Secure routing, network encryption, intrusion detection/prevention systems, availability
Application	Malware, insecure cloud environments, weak passwords, Inadequate Security and Privacy Measures, antivirus software and unsafe Software, Inaccessible Host-based classification and detection, security education	Researchers, cloud providers, and security vendors	Secure storage, privacy, secure cloud environments, secure execution environments, security education programs

Researchers have proposed various security requirements for IoT devices [110–114]. For example, a recent study [115] proposed requirements for lightweight encryption and collision avoidance algorithms, secure routing, network encryption mechanisms, attack detection/avoidance, secure cloud environments, antivirus software, and security education. A study [116] proposed a more detailed and structured set of security requirements based on the IoT architecture. However, it is more acceptable to list the requirements than to develop solutions, and some of the above authors have ignored the existing limitations of restricted equipment. Other authors have proposed broad requirements that include holistic solutions outside the security realm. Figure 7 explains the author's IoT security requirements, and Table 4 shows the IoT security issues and architectural collaboration requirements.

Existing IoT Security Solutions

Based on the requirements presented previously, security solutions for IoT problems can be developed and analyzed. For example, researchers have developed solutions to the problem of interference in wireless networks in the sensing layer [117]. These solutions rely on signal strength, packet transmission efficiency, correction codes, and frequency variations to avoid interference. Other researchers have developed similar solutions to detect and prevent forgery and spoofing attacks at the sensing layer [118]. In addition, solutions have also been proposed to secure physical interfaces and unauthenticated network modules [119]. At the network layer, authentication and access control solutions have received considerable attention from security researchers in recent years. For instance, researchers have suggested condensed versions of Encapsulating Security Payload (ESP) and Authentication Header (AH) techniques for WSNs [120]. Similar IPSec techniques have also been suggested for IPv6 low-power wireless personal area networks (6LoWPAN). However, these approaches may incur energy overhead and increase response times. Researchers have proposed new authentication and access control methods such as authentication and ability-based access control (IACAC) [121]. The IACAC considers the capabilities of IoT devices when making access control decisions. This can help improve the security of IoT systems by preventing unauthorized devices from accessing sensitive data or resources.

Similarly, Ali et al. [122] proposed a secure, lightweight end-to-end authentication scheme that uses public and private keys to authenticate both IoT devices and users. In addition, Rao and Deebak [123] proposed a password-based authentication scheme using smart cards and biometrics with a standby solution in the case of server failure. Furthermore, Meng et al. [124] proposed a secure low-cost authentication scheme for distributed cloud environments. Moreover, Chen et al. [125] proposed a distributed data access scheme using a Kerberos authentication application to secure IoT devices in the cloud.

Furthermore, a cross-device authentication and key distribution system that eliminates the need for a central server was proposed [126]. More and Sakhare [127] also proposed a context-based authentication and access control scheme that considers the fact that IoT devices are often managed by different users in the same location. In a recent study [128], a mutual trust approach that creates a centralized, token-based, object-level access control system was proposed. Another study [129] proposed a trust model that could calculate the trustworthiness of IoT devices based on various factors. Finally, a recent study [130] developed a security framework for low-power wireless personal area networks (LoWPANs) that includes elliptic curve cryptography (ECC)-based modules for secure neighbor discovery, authentication, and data encryption.

Several other security solutions have been proposed for IoT, including the proposed end-to-end security solution for CoAP using TLS-PSK for transport layer security [131], an approach to provide data encryption, integrity, and authentication using PKI at the IoT gateway level [132], and a proposed lightweight cryptographic algorithm that uses a symmetric five-round key algorithm to encrypt a 64-bit key with a 64-bit key [133]. Others include a proposed hybrid approach that combines cryptography and steganography techniques to achieve confidentiality and data integrity between home and cloud servers [134] and a two-step approach for verifying the integrity of IoT data, which involves a random-time hope sequence using a shared secret between a data server and an IoT device, followed by the generation of a verification message using a lightweight randomized permutation algorithm [135].

For IoT availability, a study [136] proposed a service-oriented architecture that aims to prevent DDoS attacks on IoT by using LA approaches to optimize the packet inspection problem to identify malicious packets. Jenkins proposed an approach that attempts to catalog IoT devices vulnerable to Mirai to incentivize administrators to solve this problem. Several network-level security solutions have also been proposed, including a dynamic defense architecture that uses AIS adaptation to detect attacks through IoT gateways and additional monitoring servers [137], a network-based security architecture that relies on security gateways to monitor the context of IoT devices [138], and a proposed IoT framework that includes an ABA IDS to detect anomalies at the sensor and network layers [139].

In addition to the attack defense applications described above, several complementary solutions can improve the reliability and scalability of the system. For example, a recent study [140] proposed the use of distributed SDN networks to maintain consistency among controllers and secure interactions between them, enabling secure network control and threat defense for IoT networks. Similarly, a recent study [141] presented a conceptual reference architecture that incorporates network data flow analysis to provide contextual information for real-time risk assessment and traffic control on IoT gateways. This platform uses blockchain and smart contracts to ensure data security and code integrity and can be used for distributing information sharing with other IoT gateways.

In the application layer, some security solutions designed for privacy, enforcement, and cloud environments also interact with two other layers or external or non-technical approaches. This is especially true for privacy and data sharing at the user level because different controls are required from a management perspective. However, policies must be adapted to a dynamic IoT environment, and technology should be able to provide tools to ensure that policies are applied and enforced. For data protection (on the move or at rest), additional solution layers such as encryption technologies, authentication, and access control methods are required to meet this requirement. To ensure a secure execution environment, in addition to the security applications described in the previous layers, the confidentiality, integrity, or availability of an IoT system can be ensured by testing its response to various attacks and resulting failures. Furthermore, some researchers [142] proposed a Markov model to better understand the results of simulated attacks on the vulnerability or availability of various components of an IoT infrastructure without causing harm.

The IoT has found a place in the cloud to offload storage and computing capabilities that limited hardware cannot support. This brings the inherent threats and security issues of IoT into a new realm,

which can be addressed to some extent by the approaches presented above. However, much of the current research has been conducted in isolation and no significant effort has been made to address this challenge as a whole. Additionally, a study [143] proposed a secure packet forwarding and privacy-preserving framework for cloud-based IoT (considered as a single environment) based on a Threshold Credit-Based Incentive (TCBI) and Symmetric Homomorphic Mapping (SHM) encryption for packet forwarding and privacy protection through one-way trapdoor licensing. Additionally, intrusion prevention and detection systems (IDS and IPS) assist in detecting and averting possible security breaches.

In summary, IoT solutions that rely on traditional centralized systems are still vulnerable to single points of failure, costly dedicated infrastructure and support requirements, and scalability issues. However, these systems offer reliability because they have long been under intense scrutiny by the security community, and their limitations and shortcomings have been recognized and can be exploited in the appropriate context.

Blockchain Security Solutions

Blockchain technology is a promising solution for improving authentication and access control in IoT, as it offers several advantages over traditional client/server solutions, such as decentralization, transparency, and auditability. Blockchain-based authentication and access control systems eliminate the need for a centrally trusted authority that can be exploited by attackers. Rather, trust is dispersed among a network of nodes, increasing the system's resistance to intrusion. Blockchain-based systems provide a high level of transparency and auditability given that all transactions are publicly visible and cannot be tampered with without detection [144].

Several examples of blockchain-based authentication and access control systems for the IoT have been proposed in recent years. These systems offer a variety of features such as flexible and granular access control policies [145], auditable access control and secure key distribution [146], single sign-on authentication, fair access, and secure communication within virtual security zones [147]. However, several challenges still need to be addressed before blockchain-based authentication and access control systems can be widely deployed in IoT. These challenges include scalability, privacy, and complexity [148]. Blockchain-based systems can be computationally expensive and slow to process transactions [149], which can be problematic for IoT applications that require real-time access controls. In addition, blockchain-based systems are typically public, meaning that all access control transactions are visible to anyone [150]. Applications that require private control over access decisions may be problematic. Finally, blockchain technology is complex, and it is difficult to implement and manage blockchain-based solutions [151].

Despite these challenges, blockchain-based authentication and access control have the potential to revolutionize the way IoT devices and networks are secured. We can anticipate an increasing number of blockchain-based authentication and access control systems implemented in the real world as the technology develops and becomes more scalable. Blockchain-based security solutions for IoT.

IoT Service Classification

To explore different IoT security applications, it is useful to categorize IoT devices by using operational domains and communication models. This is because the security requirements of IoT applications differ depending on the domain and the model. A recent study [152] proposed three operational domains for IoT devices:

1. Individual and Home
2. Governmental and Utilities
3. Industry and Enterprises

Another study added a fourth domain, which is an intelligent transport system [153]. Each operational domain has a unique security requirement. For example, privacy protection is an important security

Table 5. Detailed IoT security applications categorization.

Category	Description	Example Applications
Device security	Protects individual IoT devices from unauthorized access and attacks.	Device authentication, data encryption, secure firmware updates
Network security	Protects IoT networks from unauthorized access and attacks.	Network segmentation, firewalls, intrusion detection systems
Data security	Protects IoT data from unauthorized access, disclosure, modification, or destruction.	Data encryption, data loss prevention, data masking
Identity and access management (IAM)	Provides a way to manage the identities and access privileges of IoT users and devices.	User authentication, authorization, access control
Threat intelligence and analytics	Collects and analyses data about IoT threats to help organizations identify and respond to threats more quickly and effectively.	Threat intelligence feeds, security information, and event management (SIEM) systems
Compliance	Help organizations comply with applicable IoT security regulations and standards.	Policy management systems, audit, and reporting tools
Smart homes security	Protect smart homes from unauthorized access and attacks.	Smart door locks, security cameras, motion sensors
Industrial control system (ICS) security	Protects industrial control systems from unauthorized access and attacks.	Firewalls, intrusion detection systems, asset management systems
Connected vehicle security	Protects connected vehicles from unauthorized access and attacks.	Vehicle authentication, data encryption, secure firmware updates

requirement for IoT devices in the individual and family domains, whereas scalability and collaboration capabilities are more important for IoT devices in the government and utilities domains. Similarly, one study proposed three communication models for IoT devices: device-to-device (D2D), device-to-cloud (D2C), and device-to-gateway (D2G) [154]. Devices that connect directly with one another employ communication between device models. However, D2C is used when devices communicate with a cloud server, whereas D2G is used when devices communicate with a gateway device, which then relays the communication to another device or network. However, these modes of communication preclude each other. For example, a D2C device can communicate with other devices using a D2D communication model [155]. When designing IoT security applications, it is important to consider the operational domain, and the communication model of the devices involved. This will assist in guaranteeing that the security requirements of the application are fulfilled. Table 5 provides the details of the IoT security application classification.

Blockchain Operational Classification

Blockchain operations can be divided into on- and off-chain operations [156]. Operations documented on the blockchain that are accessible to all network users are referred to as on-chain operations. Usually, they entail the exchange of assets or values, such as tokens or cryptocurrencies. On-chain operations can be further subdivided into state-changing and nonstate-changing operations. State-changing operations change the state of the blockchain, such as by creating a new transaction or updating an existing account balance. Non-state-changing operations, such as reading a transaction or querying the account balance, do not change the state of the blockchain [157]. Off-chain operations are those that are not recorded on the blockchain and are not visible to all the participants in the network. Typically, they are employed to increase the scalability and effectiveness of blockchain networks. Off-chain operations can be further subdivided into payment channels, state channels, and layer-two solutions [158]. While state channels enable players to execute smart contracts without broadcasting every state change to the blockchain, payment channels enable participants to send money to one another, without broadcasting every transaction to the network. Furthermore, protocols developed on top of a blockchain to increase its scalability and efficiency are known as layer-two solutions.

While on-chain operations offer the benefits of transparency, security, and immutability, they can be slow and expensive to process, especially in popular blockchain networks [159]. Furthermore, sensitive data may be exposed, and user activity is tracked via on-chain processes. However, off-chain operations

offer the benefits of scalability, efficiency, and privacy. However, they can be more vulnerable to attack than on-chain operations and can lead to centralization of power in the hands of the parties involved in the operation [160]. Furthermore, sensitive data may be exposed, and user activity is tracked via on-chain processes. If security and transparency are paramount, on-chain operations should be used. If scalability and efficiency are more important, then off-chain operations can be used. Figure 8 shows the on- and off-chain blockchain consensus.

Blockchain technology can also be categorized into three main types based on its accessibility and governance model, as shown in Table 6: public, federated, and private blockchains [161]. Public blockchains enable users to engage with blockchain without authorization and are available to anybody with an internet connection. A dispersed network of nodes that upholds the blockchain ledger and verifies transactions protects it.

Several studies have been conducted on public blockchains, which are often used for dAPPs and cryptocurrency transactions. For example, a survey [128] attempts to provide a thorough picture of dAPPs, beginning with definitions of dAPPs and then common dAPPs architectures, in addition to presenting future research opportunities. Federated blockchains are managed by a pre-selected group of nodes that can be organizations or individuals. They allow public read access, but writing access is restricted to preselected nodes. Studies conducted on federated blockchains are often used by organizations with a common goal, such as improving supply chain efficiency or reducing fraud [162]. Private blockchains are fully restricted systems with limited read-and-write access. They are typically owned by a single organization and are often used for sensitive data or applications, where privacy and control are paramount. Numerous commercial applications, including supply chain management, identity management, and asset monitoring, can be implemented using private blockchains [163].

In addition to accessibility and governance, blockchain applications may differ by platform, customization, and consensus mechanisms [164]. The term “platform” describes the underlying blockchain technology, such as Hyperledger Fabric, Ethereum, or Bitcoin. Each platform had distinct features and security attributes. For example, Bitcoin is known for its security owing to its decentralized Proof-of-Work consensus mechanism, whereas Ethereum is more flexible and allows the development of smart contracts that can add new security features to applications.

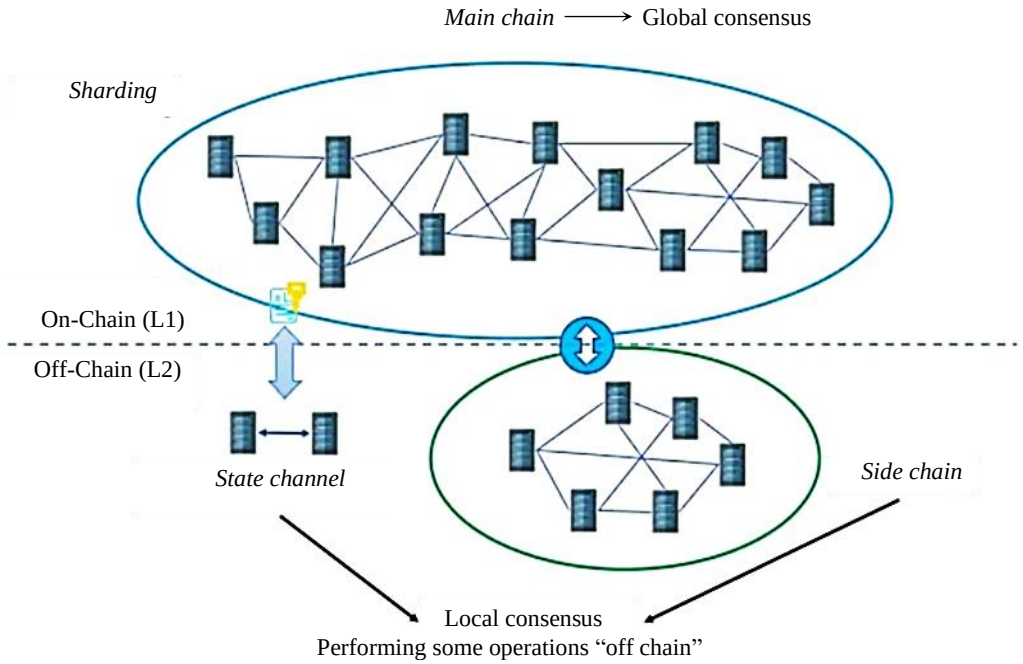

Figure 8. On-chain versus off-chain consensus.

Table 6. Summary of blockchain transaction types.

Feature	Public blockchain	Hybrid blockchain	Private blockchain
Access	Anyone can join and participate	A pre-selected set of nodes can join and participate	Only members of the organization can join and participate
Read access	Anyone can read all transactions	Anyone can read all transactions, or only authorized nodes can read specific transactions	Anyone can read all transactions, or only authorized nodes can read specific transactions
Security	Very secure, difficult to tamper with	May be less secure than a public blockchain, but more secure than a private blockchain	May be less secure than a public or consortium blockchain
Consensus	Permissionless, anyone can participate in consensus	Permissioned, only authorized nodes can participate in consensus	Permissioned, only authorized nodes can participate in consensus
Efficiency	Low, due to the need to incentivize miners to validate transactions	High, due to the fact that there is no need to incentivize miners	High, due to the fact that there is no need to incentivize miners

Table 7. Blockchain classification with consensus mechanisms.

Type	Consensus mechanism	Efficiency	Security	Decentralization
Public	Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake, Byzantine Fault Tolerance	Low	High	High
Federated	BFT, Proof-of-Authority, Proof-of-Reputation	Medium	Medium	Medium
Private	Byzantine Fault Tolerance, Proof-of-Authority, Centralized	High	Low	Low

Customization refers to modifications or adaptations that have been made to the blockchain platform. These customizations can be made to improve the security of the platform or add new features and functionality. For example, some organizations may choose to customize blockchain platforms to implement additional security measures, such as multi-signature wallets or access control lists [165]. The process by which an agreement is reached on the blockchain's current state is referred to as the consensus mechanism. PoW, PoS, and BFT are the most commonly used consensus techniques [166]. Each consensus method has unique security advantages and disadvantages. For instance, PoS is more energy efficient but may be more susceptible to specific types of attacks, whereas PoW is more secure but may be energy intensive. Table 7 explains the blockchain classification with consensus mechanisms. Table 8 presents a comprehensive taxonomy that provides a structured framework for classifying blockchain-based security approaches based on their key components and functionalities, enabling researchers, practitioners, and policymakers to better understand the landscape of blockchain-based security solutions and identify the most appropriate approaches for specific IoT applications.

Blockchain-Based Security Applications

Blockchain technology has the potential to revolutionize the security of IoT devices and networks by providing a decentralized and tamper-proof ledger that can be used to implement a wide range of security measures, such as access control, data integrity, and firmware updates. An example of a blockchain-based security solution for IoT is the decentralized access control system proposed [167]. This system consists of two layers: a top layer that manages access control policies for communication with other organizations and a bottom layer that includes IoT devices that rely on a blockchain gateway to enforce access control policies. This semi-centralized approach is necessary because IoT devices typically do not have the computing resources to apply the rules themselves. The proof-of-concept implementation of this system runs on the Bitcoin blockchain and uses a wallet interface to connect users. However, this currency requirement limits the affordability of the system and can become burdensome as the number of nodes increases. Another example of a blockchain-based security solution for IoT is the firmware update system proposed [168]. In this study, firmware information and IoT devices were securely managed by the proposed firmware update system through four processes: firmware registration/update, firmware update request, firmware update, and subscriber registration. Public-key encryption communication can be used to securely update the firmware of IoT devices and UAVs.

Table 8. Taxonomy of blockchain-based security approaches.

Category	Subcategory	Description
Consensus Mechanisms	Proof-of-Work	Uses computational power to solve cryptographic puzzles, ensuring network security and transaction validation.
Proof-of-Stake	Rely on cryptocurrency holdings to validate transactions and maintain network consensus	
Proof-of-Authority	Employees trusted nodes with predefined authority to validate transactions and maintain network consensus	
Byzantine Fault Tolerance	Employs a distributed consensus mechanism to ensure network resilience and transaction validation even in the presence of faulty nodes	
Data Management	On-chain Data Storage	Stores data directly on the blockchain, providing tamper-proof and transparent data storage.
Off-chain Data Storage	Stores data external to the blockchain, reducing transaction costs and improving scalability	
Hybrid Data Storage	Combines on-chain and off-chain data storage strategies, balancing security and scalability requirements	
Access Control Mechanisms	Role-Based Access Control (RBAC)	Defines access permissions based on user roles and privileges.
Attribute-Based Access Control (ABAC)	Grants access based on user attributes, device characteristics, and contextual factors	
Policy-Based Access Control (PBAC)	Enforces access control rules defined in centralized policies	
Cryptographic Techniques	Public-key Cryptography	Employs asymmetric cryptography to secure data confidentiality, integrity, and authenticity.
Symmetric-key Cryptography	Utilizes shared secret keys for efficient encryption and decryption of data	
Hash Functions	Generates unique and unpredictable values from data, ensuring data integrity and authenticity	
Digital Signatures	Provide non-repudiation and authenticity for digital transactions	
Privacy-Preserving Techniques	Differential Privacy	Adds noise to data to protect individual privacy while preserving statistical utility.
Zero-Knowledge Proofs	Allow entities to prove their knowledge or ownership without revealing the underlying data	
Homomorphic Encryption	Enables computations on encrypted data without decrypting it, preserving data privacy	
Threat Detection and Prevention	Intrusion Detection Systems (IDS)	Monitor network traffic and system logs to detect anomalous activities and potential attacks.
Intrusion Prevention Systems	Actively block or mitigate detected intrusions to prevent damage or data breaches	
Anomaly Detection	Identifies deviations from normal patterns in system behavior or data to detect potential threats	
Signature-Based Detection	Utilizes known attack signatures to identify and block malicious activities	
Machine Learning Based Detection	Employs machine learning algorithms to analyze network traffic and system logs to detect suspicious behavior and potential attacks	

The public key of the IoT device and the Bloom filter were used for verification. The security of the proposed method was demonstrated by a security study based on the STRIDE model, and the blockchain network's performance was assessed through simulation on the Hyperledger.

In a further study [169], a blockchain-based end-to-end secure software update delivery framework for IoT devices was proposed. The goal of the framework is to transfer cryptographic computations from IoT devices with limited resources to a decentralized blockchain system while maintaining the availability, efficiency, secrecy, integrity, and auditability of certified software delivery. This study uses Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to create personalized authorization policies that greatly minimize the computational burden of key generation and delivery on the manufacturer side while ensuring that software updates can only be installed and decrypted on approved IoT devices. Similarly, a recent study [170] proposes a blockchain-enabled plan to achieve smooth and simultaneously flexible A&A within and across domains. In addition to a consortium blockchain, a contract-based mutual access control agreement was created, which allows domain managers to control access permissions independently of trusted third parties. The agreement serves as the basis for proposing an additional secure and privacy-preserving authentication protocol that enables anonymous access to authorized IoT domains by IoT devices by adapting one-out-of-many-proof techniques. This study used a threshold-based cryptosystem to further design a voting-based protocol. Finally, two proof-of-concept prototypes are built based on an open-source blockchain platform running on a virtual machine and a physical testbed to demonstrate the efficiency of our scheme in terms of computational and communication overhead.

A recent study [171] also proposed a new blockchain-based solution for IoT, where the authors proposed PBidm, a blockchain-based identity management system for the Industrial IoT (IIoT) that protects privacy. PBidm uses a blockchain to fully support the desired properties of immutability, tamper-proofness, auditability, revocability, and public verifiability. In addition, the authors provide a security analysis to ensure an appropriate level of security assurance and a performance evaluation of the proposed scheme to show that it is feasible for IIoT applications. Another study analyzed the firmware of 32,000 embedded devices and found that nearly 2,000 devices contained backdoors, such as hard-coded Telnet passwords [172].

Their study included routers that have other vulnerabilities and software bugs that increase the likelihood of being affected by common cyberattacks. Similarly, a recent study [173] presented a novel approach for a large-scale IoT system based on a permission-based blockchain that optimizes data storage and provides users with a lightweight authentication mechanism. The proposed approach has advantages in terms of scalability and ideal storage for most blockchain-based applications. Furthermore, IoT data are encrypted at the user end and uploaded to the cloud using homomorphic encryption. Another study provides a tamper-proof and secure smart contract for access control and information management of digital twin stakeholders, as well as a blockchain-based solution for digital twins using the Ethereum blockchain. Compared with state-of-the-art technologies, the proposed system uses 8% fewer resources in terms of transaction costs. The cost of Ethereum was 93% lower than that of previous methods, despite a 10% increase in execution costs [174]. A recent study [175] suggested hybrid centralized and blockchain-based architecture authentication to offer efficient authentication for IoT systems while reducing the usage of IoT resources. A local Ethereum blockchain network is used to present the design. By comparing the proposed approach with centralized and blockchain-based authentication schemes, the results show that it provides a significant improvement in terms of computational cost, execution time, and power consumption for IoT.

A study [176] provides a framework for enhancing the security and privacy of smart farms by utilizing the decentralized nature of blockchain technology. In addition to offering safe and unbreakable data storage, the distributed ledger architecture used by the framework to store and manage data from IoT devices placed on smart farms ensures data validity and integrity. This study automates the

implementation of pre-established norms and regulations using a variety of technologies, including the Ethereum Rinkeby smart contract mechanism, AWS cloud, ESP32, and smart farm security monitoring framework. By instantly identifying and reacting to security risks, the system has demonstrated its effectiveness in improving the security of smart farms in a proof-of-concept deployment. For smart farms, an IoT-based framework was proposed to increase the crop productivity [177]. This framework presents an AI-based precision model that can be used in conjunction with data from remote sensors to accurately predict crop growth in smart agriculture. According to the results, the random forest model performed better than the logistic regression model (84%), K-Nearest Neighbors (KNN) (90%), and Support Vector Classifier (SVC) (93%). Through blockchain-based supply chain management, technology can improve the economic context for farmers by reducing expenses and improving the overall quality of agricultural processes and product management. The evaluation of blockchain performance considers the latency, throughput, execution time, and gas consumption. Similarly, another study [178] proposed a framework using the blockchain smart contract concept. Each organization involved in the blockchain-based supply chain network manages parties' transactions. Every transaction was recorded to guarantee superior transparency and traceability across the supply chain environment. A group signature mechanism is used in the event of fraud. The overall performance of the system is measured using three metrics: transaction efficiency, system risk reduction, and participant confidence. Once the framework is implemented, the gas cost, average execution time, throughput, and latency are used to quantify the transaction efficiency. Based on these measures, the system operates at a satisfactory level. Even though the number of publications on IoT blockchains has almost doubled in the last three years, there are still some IoT needs that have not been fully addressed. A relatively large number of studies have proposed blockchain-based solutions for cloud integration, IoT storage, availability, integrity, privacy, and access control. However, there has not been much focus on plans for a secure execution, prevention, and detection environment. Retailers, researchers, and bad actors are focusing a lot of attention on personal and private devices because they make up more than half of all IoT devices and are predicted to reach over 75 billion devices by the year 2025. In addition, a recent study by IHS Markit, a global leader in critical information, analytics, and solutions, predicted that there will be 125 billion connected IoT devices worldwide by 2030, a staggering annual growth rate of 12% [179]. As of 2017, there were approximately 27 billion IoT devices in the world. As a result, security needs to be addressed from both the technical and policy perspectives.

CONCLUSION

Various solutions, including encryption techniques, access control mechanisms, and intrusion detection systems, have been developed to address IoT security challenges. Moreover, blockchain technology offers promising solutions for enhancing IoT security by ensuring data integrity, enabling transparent transactions, and facilitating secure communication. Categorizing IoT services and operationalizing blockchains in specific security applications further bolsters the effectiveness of blockchain-based security solutions. As IoT continues to expand, it is crucial to adopt robust security measures, including blockchain-based solutions, to protect the privacy and integrity of IoT devices and their data. The contributions of this study can be summarized as follows:

1. Provision of a detailed classification of blockchain-based security approaches covering different consensus mechanisms, data management strategies, access control techniques, cryptographic methods, taxonomy, and privacy preservation techniques.
2. A systematic analysis of the existing limitations, problems, and difficulties associated with implementing blockchain-based security solutions in the IoT context highlights the need for tailored solutions that address the unique challenges of resource-constrained devices and decentralized networks.
3. Provision of insights for practitioners to improve the design of blockchain-based security techniques.

Recommendations

As IoT ecosystems continue to evolve, future research should focus on developing lightweight blockchain-based security frameworks tailored to resource-constrained devices. Collaboration among

academia, industry, and regulatory bodies is essential to standardize blockchain integration in IoT applications, ensuring seamless interoperability, scalability, and low latency. Additionally, exploring the convergence of blockchain with emerging technologies, such as AI and quantum computing, could unlock new potential for predictive security, real-time threat detection, and more efficient data management, ultimately enhancing the overall robustness of IoT networks.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest in this work.

Data Availability Statement

Data sharing does not apply to this article, as no new data were created or analyzed in this study.

REFERENCES

1. Pandey R, Goundar S, Fatima S, editors. Distributed Computing to Blockchain: Architecture, Technology, and Applications. Amsterdam: Elsevier Science; 2023.
2. Singh S. Consensus algorithms in blockchain technology: A comparative study. Asian J Multidimens Res. 2022;11:43–8. doi:10.5958/2278-4853.2022.00238.5.
3. Yadav AS, Singh N, Kushwaha DS. Evolution of blockchain and consensus mechanisms & its real-world applications. Multimed Tools Appl. 2023;82:34363–408. doi:10.1007/s11042-023-14624-6.
4. Rushita D, Sood K, Yadav US. Cryptocurrency and digital money in the new era. In: Grima S, Thalassinos E, Noja GG, Stamataopoulos TV, Vasiljeva T, Volkova T, editors. Digital Transformation, Strategic Resilience, Cyber Security and Risk Management. Bingley, United Kingdom: Emerald Publishing Limited; 2023. p. 179–90. doi:10.1108/S1569-37592023000111B013.
5. Panda SK, Sathya AR, Das S. Bitcoin: Beginning of the cryptocurrency era. In: Panda SK, Mishra V, Dash SP, Pani AK, editors. Intelligent Systems Reference Library. New York: Springer International Publishing; 2023. p. 25–58. doi:10.1007/978-3-031-22835-3_2.
6. Elaiyaraja A. A revolutionary impact on cryptocurrency. In: Kesavan D, Anand NM, editors. Emerging Insights on the Relationship between Cryptocurrencies and Decentralized Economic Models. Hershey (PA): IGI Global; 2023. p. 183-97. doi: 10.4018/978-1-6684-5691-0.ch012.
7. Taherdoost H. Blockchain and machine learning: A critical review on security. Information. 2023;14:295. doi:10.3390/info14050295.
8. Ajayi O, Saadawi T. Blockchain-based architecture for secured cyber-attack features exchange. 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), New York, NY, USA. 2020. p. 100–7. doi:10.1109/CSCloud-EdgeCom49738.2020.00025.
9. Yalçınsoy KÖ, Güngör A, Karakaya D, Özdal L, Kılıç M, Özdamar Erol Y, Çakar Özdal P. Tubulointerstitial nephritis and uveitis syndrome during the COVID-19 pandemic: a case series. Turk J Ophthalmol. 2024;54(1):5-10. doi: 10.1080/01969722.2023.2175153.
10. Sapra N, Shaikh I, Dash A. Impact of proof of work (PoW)-based blockchain applications on the environment: A systematic review and research agenda. J Risk Financ Manag. 2023;16:4. doi:10.3390/jrfm16040218.
11. Peng P, Ji S, Tian Z, Jiang H, Zheng W, Zhang X. Locality sensitive hashing for optimizing subgraph query processing in parallel computing systems. Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining; 2023 Aug 6–10; Long Beach, CA, USA. New York (NY): Association for Computing Machinery; 2023. p. 1885-96. doi: 10.1145/3580305.3599419.
12. Balani N, Chavan P. Design of heuristic model to improve blockchain-based sidechain configuration. Int J Comput Sci Eng. 2023;26:372–84. doi:10.1504/IJCSE.2023.132154.

13. Zhang Y, Zhao M, Li T, Wang Y, Liang T. Achieving optimal rewards in cryptocurrency stubborn mining with state transition analysis. Inf Sci. 2023;625:299–313. doi:10.1016/j.ins.2022.12.093.
14. Matsuo S, Gudgeon L, Klages-Mundt A, Perez Hernandez D, Werner S, Haines T, Sala M, editors. Financial Cryptography and Data Security. FC 2022 International Workshops: CoDecFin, DeFi, Voting, WTSC, Grenada, May 6, 2022. Revised Selected Papers. Cham: Springer; 2023. 690 p. (Lecture Notes in Computer Science). doi: 10.1007/978-3-031-32415-4.
15. Arslanian H. The Book of Crypto: The Complete Guide to Understanding Bitcoin, Cryptocurrencies and Digital Assets. Cham: Springer International Publishing; 2022. doi:10.1007/978-3-030-97951-5.
16. Sun G, Jiang M, Khooi XZ, Li Y, Li J. NeoBFT: accelerating Byzantine fault tolerance using authenticated in-network ordering. In: Proceedings of the ACM SIGCOMM 2023 Conference; 2023 Aug 28–Sep 1; New York, NY, USA. New York (NY): Association for Computing Machinery; 2023. p. 239–54. doi: 10.1145/3603269.3604874.
17. Chen Z, Gul OM, Kantarci B. Practical byzantine fault tolerance based robustness for mobile crowdsensing. Distrib Ledger Technol Res Pract. 2023;2:1–24. doi:10.1145/3580392.
18. Ahmadjee S, Mera-Gómez C, Bahsoon R, Kazman R. A study on blockchain architecture design decisions and their security attacks and threats. ACM Trans Softw Eng Methodol. 2022;31:1–45. doi:10.1145/3502740.
19. Chaganti R, Varadarajan V, Gorantla VS, Gadekallu TR, Ravi V. Blockchain-based cloud-enabled security monitoring using Internet of things in smart agriculture. Future Internet. 2022;14:9. doi:10.3390/fi14090250.
20. Fujihara A. Theoretical Considerations on Bitcoin Scalability Problem and Block Size Distribution. In: Proc Blockchain Kaigi 2022 (BCK22). J Phys Soc Jpn. 2023. doi:10.7566/JPSCP.40.011007.
21. Vaddadi VR, Vardhan Raj Annepu P, Gollapalli N, Challa A, Andhavarapu SB, Kumar Botta P. Exploiting cyber threats and protecting cryptocurrencies toward bitcoin exchanges. 2023 5th Biennial International Conference on Nascent Technologies in Engineering (ICNTE), Navi Mumbai, India, 2023. p. 1–6. doi:10.1109/ICNTE56631.2023.10146649.
22. Goel A, Suseela G. A step towards blockchain scalability resolution. Adv Sci Technol. 2023;124:635–43. doi:10.4028/p-6287yh.
23. Castellon CE, Khatib T, Roy S, Dutta A, Kreidl OP, Bölöni L. Energy-efficient blockchain-enabled multi-robot coordination for information gathering: Theory and experiments. Electronics. 2023;12:20. doi:10.3390/electronics12204239.
24. Wang F, Lu Y, Zhang Q, Liu Y, Liu L, Zhang Z. SoK: research status and challenges of blockchain smart contracts. Proceedings of the 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure; 2023 Jul 3–7; Melbourne, VIC, Australia. New York (NY): Association for Computing Machinery; 2023. p. 145–7. doi: 10.1145/3594556.3594620.
25. Velasco GC, Vaz NAP, Carvalho ST. Challenges and opportunities in smart contract development on the Ethereum virtual machine: a systematic literature review. In: Anais do 6º Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain); 2023 Sep 25–29; Brasília, DF, Brazil. Porto Alegre: Sociedade Brasileira de Computação; 2023. p. 15–28. doi: 10.5753/wblockchain.2023.756.
26. Chu H, Zhang P, Dong H, Xiao Y, Ji S, Li W. A survey on smart contract vulnerabilities: Data sources, detection and repair. Inf Softw Technol. 2023;159:107221. doi:10.1016/j.infsof.2023.107221.
27. Junaid A, Nawaz A, Usmani MF, Verma R, Dhanda N. Analyzing the performance of a DAPP using blockchain 3.0. 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India. 2023. p. 209–13. doi: 10.1109/Confluence56041.2023.10048887.
28. Wright SA. DAOs & ADSs. 2023 IEEE 15th International Symposium on Autonomous Decentralized System (ISADS), Mexico City, Mexico, 2023. p. 1-6. doi: 10.1109/ISADS56919.2023.10091973.
29. Imamura M, Omote K. Analysis of the features and structure behind availability in blockchain using altcoin. IEEE Access. 2022;10:98683–99. doi:10.1109/ACCESS.2022.3204697.

30. Sasikumar A, Ravi L, Devarajan M, Vairavasundaram S, Selvalakshmi A, Kotecha K, et al. A decentralized resource allocation in edge computing for secure IoT environments. IEEE Access. 2023;11:117177–89. doi:10.1109/ACCESS.2023.3325056.
31. Galhotra B, Lowe D, Seth S. Blockchain technology in education: The perspective, challenges, and concerns. Open Access Res J Eng Technol. 2023;5:39–46. doi:10.53022/oarjet.2023.5.1.0075.
32. Kamau CG, Yavuzaslan A. African Journal of Commercial Studies. Afr J Commer Stud. 2023;3:Art. no. 2. doi:10.59413/ajocs/v3.i2.3.
33. Caldarelli G. Before Ethereum. The origin and evolution of blockchain oracles. IEEE Access. 2023;11:50899–50917. doi:10.1109/ACCESS.2023.3279106.
34. Hamdi A, Fourati L, Ayed S. Vulnerabilities and attacks assessments in blockchain 1.0, 2.0 and 3.0: Tools, analysis and countermeasures. Int J Inf Secur. 2024;23:713–757. doi:10.1007/s10207-023-00765-0.
35. Wang Q, Li C, Xia T, Ren Y, Wang D, Zhang G, Choo KK. Optimal Selfish Mining-Based Denial-of-Service Attack. IEEE Trans Inf Forensics Secur. 2024;19:835–850. doi:10.1109/TIFS.2023.3326386.
36. Notland JS, Nowostawski M, Li J. Runtime evolution of bitcoin's consensus rules. IEEE Trans Softw Eng. 2023;49:4477–4495. doi:10.1109/TSE.2023.3304851.
37. Rani P, Sachan RK, Kukreja S. A systematic study on blockchain technology in education: Initiatives, products, applications, benefits, challenges, and research direction. Comput. 2024;106:405–447. doi:10.1007/s00607-023-01228-z.
38. Tyagi AK, Dananjayan S, Agarwal D, Thariq Ahmed HF. Blockchain-Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. Sensors. 2023;23:Art. no. 2. doi:10.3390/s23020947.
39. Tao X, Das M, Zheng C, Liu Y, Wong PKY, Xu Y, Liu H, Gong X, Cheng JCP. Enhancing BIM security in emergency construction projects using lightweight blockchain-as-a-service. Autom Constr. 2023;150:104846. doi:10.1016/j.autcon.2023.104846.
40. Kumar Jha AK. Hybrid consensus mechanism (HCM): Achieving efficient and secure consensus in blockchain networks. SSRN Electron J. 2023. doi:10.2139/ssrn.4413290.
41. Zhang T, Huang Z. FPoR: Fair proof-of-reputation consensus for blockchain. ICT Express. 2023;9:45–50. doi:10.1016/j.icte.2022.11.007.
42. Tang J, Lu X, Xiang Y, Shi C, Gu J. Blockchain search engine: Its current research status and future prospect in Internet of things network. Future Gener Comput Syst. 2023;138:120–141. doi:10.1016/j.future.2022.08.008.
43. Motwani D, Sonawane S. Modeling Blockchain Technology-Driven Practices to Be Integrated in Fintech for Creating Reliable Business Processes. Scand J Inf Syst. 2023;35:Art. no. 1.
44. Aliyu AA. Improving Cloud data Security by hybridization of zero-knowledge proof and time-based one-time password. KASU J Math Sci KJMS. 2020;1:116–126.
45. Abu-Faraj M, Al-Hyari A, Obimbo C, Aldebei K, Altaharwa I, Alqadi Z, Almanaseer O. Protecting digital images using keys enhanced by 2D chaotic logistic maps. Cryptography. 2023;7(2):Art. no. 2. doi:10.3390/cryptography7020020.
46. Lin GN, Jianbing LI, Kunlong Y, Xuesong W. Research on the motion and scattering characteristics of intermittent long chaff. Chin J Radio Sci. 2023;38:114–122. doi:10.12265/j.cjors.2022005.
47. Solomon R, Weber R, Almashaqbeh G. smartFHE: Privacy-preserving smart contracts from fully homomorphic encryption. In: Proceedings of the 8th European Symposium on Security and Privacy (EuroS&P); 2023 May 10–12; Vienna, Austria. IEEE; 2023. p. 309–331. doi:10.1109/EuroSP57164.2023.00027.
48. Krichen M. Strengthening the security of smart contracts through the power of artificial intelligence. Comput. 2023;12:Art. no. 5. doi:10.3390/computers12050107.
49. Goel S, Verma A, Jain VK. CRA-RPL: A novel lightweight challenge-response authentication-based technique for securing RPL against dropped DAO attacks. Comput Secur. 2023;132:103346. doi:10.1016/j.cose.2023.103346.

50. He D, Wu R, Li X, Chan S, Guizani M. Detection of vulnerabilities of blockchain smart contracts. IEEE Internet Things J. 2023;10:12178–12185. doi:10.1109/JIOT.2023.3241544.
51. Salem Balobaid A, Alagrash YH, Hussein Fadel A, Hasoon JN. Modeling of blockchain with encryption based secure education record management system. Egypt Inf J. 2023;24:100411. doi:10.1016/j.eij.2023.100411.
52. Bovenzi G, Aceto G, Persico V, Pescapé A. Blockchain performance in Industry 4.0: Drivers, use cases, and future directions. J Ind Inf Integr. 2023;36:100513. doi:10.1016/j.jii.2023.100513.
53. Peyrone N, Wichadakul D. A formal model for blockchain-based consent management in data sharing. J Log Algebr Methods Program. 2023;134:100886. doi:10.1016/j.jlamp.2023.100886.
54. Sharma G, Gandhi P. A framework of secured system using blockchain in healthcare industry. AIP Conf Proc. 2023;020003. doi:10.1063/5.0154721.
55. Toufaily E. An integrative model of trust toward crypto-tokens applications: A customer perspective approach. Digit Bus. 2022;2:100041. doi:10.1016/j.digbus.2022.100041.
56. Gad AG, Mosa DT, Abualigah L, Abohany AA. Emerging trends in blockchain technology and applications: A review and outlook. J King Saud Univ Comput Inf Sci. 2022;34:6719–6742. doi:10.1016/j.jksuci.2022.03.007.
57. Sanka AI, Cheung RCC. A systematic review of blockchain scalability: Issues, solutions, analysis and future research. J Netw Comput Appl. 2021;195:103232. doi:10.1016/j.jnca.2021.103232.
58. Marchesi L, Marchesi M, Tonelli R, Lunesu MI. A blockchain architecture for industrial applications. Blockchain: Res Appl. 2022;3:100088. doi:10.1016/j.bcra.2022.100088.
59. Akshatha PS, Dilip Kumar SMD. MQTT and blockchain sharding: An approach to user-controlled data access with improved security and efficiency. Blockchain: Res Appl. 2023;4:100158. doi:10.1016/j.bcra.2023.100158.
60. Jia X, Wang L, Cheng K, Jing P, Song X. A blockchain-based privacy-preserving and collusion-resistant scheme (PPCR) for double auctions. Digit Commun Netw. 2025;11:116–125. doi:10.1016/j.dcan.2023.05.002.
61. Liu R, Yu X, Yuan Y, Ren Y. BTDSI: A blockchain-based trusted data storage mechanism for Industry 5.0. J King Saud Univ Comput Inf Sci. 2023;35:101674. doi:10.1016/j.jksuci.2023.101674
62. Guimarães T, Duarte R, Pinheiro B, Faria D, Gomes P, Santos MF. Blockchain analytics – Real-time log management in healthcare. Procedia Comput Sci. 2022;201:702–707. doi:10.1016/j.procs.2022.03.094
63. Malik V, Mittal R, Mavaluru D, Narapureddy BR, Goyal SB, Martin RJ, Srinivasan K, Mittal A. Building a secure platform for digital governance interoperability and data exchange using blockchain and deep learning-based frameworks. IEEE Access. 2023;11:70110–70131. doi:10.1109/ACCESS.2023.3293529
64. Abdulganiyu OH, Ait Tchakoucht T, Saheed YK. A systematic literature review for network intrusion detection system (IDS). Int J Inf Secur. 2023;22:1125–1162. doi:10.1007/s10207-023-00682-2
65. Abbas SH, Naser WAK, Kadhim AA. Subject review: Intrusion detection system (IDS) and intrusion prevention system (IPS). Glob J Eng Technol Adv. 2023;14:155–158. doi:10.30574/gjeta.2023.14.2.0031
66. Goyal A, Han X, Wang G, Bates A. Sometimes you aren't what you do: Mimicry attacks against provenance graph host intrusion detection systems. Proceedings of the Network and Distributed System Security (NDSS) Symposium; 2023 Feb 27–Mar 3; San Diego, CA, USA. San Diego, CA: Internet Society; 2023. p. 1–12. doi: 10.14722/ndss.2023.24207.
67. Aliyu AA. Information security: An effective tool for sustainable Nigerian national security and development. Paper presented at: Annual International Conference on Peace Building: The Role of Faith-Based Organizations; 2022 Mar 19–20; Abuja, Nigeria. Directorate of Peace and Conflict Resolution, Fityanul Islam of Nigeria; 2022.
68. Riley I, Marshall A, Quirk L, Gamble R. An architectural design to address the impact of adaptations on intrusion detection systems. Proceedings of the 56th Hawaii International Conference on System Sciences; 2023 Jan 3; Hawaii, USA. p. 6873. DOI: 10.24251/HICSS.2023.832.

69. Helixstorm. (2022). Understanding the 5 Types of Intrusion Detection Systems. [online] Helixstorm. Available from: https://www.helixstorm.com/blog/types-of-intrusion-detection-systems/
70. Wu C, Chen S. A heuristic intrusion detection approach using deep learning model. In: Int Conf Inf Netw (ICOIN); 2023. p. 438–442. doi:10.1109/ICOIN56518.2023.10049024.
71. Sophos. (2020). What are Signatures and How Does Signature-Based Detection Work? [online] Sophos. Available from: https://home.sophos.com/en-us/security-news/2020/what-is-a-signature
72. Techslang. What is Signature-Based Detection? A short definition of Signature-Based Detection. [Online] Techslang. Available from: https://www.techslang.com/definition/what-is-signature-based-detection/
73. Al-E'mari S, Anbar M, Sanjalawe Y, Manickam S, Hasbullah I. Intrusion detection systems using blockchain technology: A review, issues and challenges. Comput Syst Sci Eng. 2022;40:87–112. doi:10.32604/csse.2022.017941
74. Bhavsar M, Roy K, Kelly J, Olusola O. Anomaly-based intrusion detection system for IoT application. Discov Internet Things. 2023;3:5. doi:10.1007/s43926-023-00034-5
75. Alem S, Espes D, Nana L, Martin E, De Lamotte F. A novel bi-anomaly-based intrusion detection system approach for industry 4.0. Future Gener Comput Syst. 2023;145:267–283. doi:10.1016/j.future.2023.03.024
76. Landauer M, Wurzenberger M, Skopik F, Hotwagner W, Höld G. AMiner: A modular log data analysis pipeline for anomaly-based intrusion detection. Digit Threat Res Pract. 2023;4:1–16. doi:10.1145/3567675
77. Chakraborty A, Biswas A, Khan AK. Artificial intelligence for cybersecurity: threats, attacks and mitigation. In: Biswas A, Semwal VB, Singh D, editors. Artificial Intelligence for Societal Issues. Intelligent Systems Reference Library, vol 231. Cham: Springer; 2023. p. 1. DOI: 10.1007/978-3-031-12419-8_1.
78. Priya VSD, Chakkaravarthy SS. Containerized cloud-based honeypot deception for tracking attackers. Sci Rep. 2023;13:1. doi:10.1038/s41598-023-28613-0. PubMed: 36697488
79. Javadpour A, Pinto P, Ja'fari F, Zhang W. DMAIDPS: A distributed multi-agent intrusion detection and prevention system for cloud IoT environments. Cluster Comput. 2023;26:367–384. doi:10.1007/s10586-022-03621-3
80. Kably S, Benbarrad T, Alaoui N, Arioua M. Multi-zone-wise blockchain based intrusion detection and prevention system for IoT environment. Comput Mater Continua. 2023;74:253–278. doi:10.32604/cmc.2023.032220
81. Babu ES, Bkn S, Nayak SR, Verma A, Alqahtani F, Tolba A, Mukherjee A. Blockchain-based intrusion detection system of IoT urban data with device authentication against DDoS attacks. Comput Electr Eng. 2022;103:108287. doi:10.1016/j.compeleceng.2022.108287
82. Singh D. Internet of Things. In: Singh CD, Kaur H, editors. Factories of the Future: Technological Advancements in the Manufacturing Industry. Hoboken, New Jersey, United States: John Wiley & Sons; 2023. p.195–227. doi:10.1002/9781119865216.ch9
83. Falayi A, Wang Q, Liao W, Yu W. Survey of distributed and decentralized IoT securities: Approaches using deep learning and blockchain technology. Future Internet. 2023;15:5. doi:10.3390/fi15050178
84. Dong W, Wang H, Wang R. A study on the technique for recognizing IoT devices using FTP messages. Proc SPIE. 2023 Jun 14;12708:127080P. DOI: 10.1117/12.2683980.
85. Mahdi OA, Alazab A, Bevinakoppa S, Ali N, Khraisat A. Enhancing IoT intrusion detection system performance with the diversity measure as a novel drift detection method. In: 9th Int Conf Inf Technol Trends (ITT); 2023. p. 50–54. doi:10.1109/ITT59889.2023.10184268
86. Memos VA, Psannis KE, Lv Z. A secure network model against bot attacks in the edge-enabled industrial Internet of things. IEEE Trans Ind Inform. 2022;18:7998–8006. doi:10.1109/TII.2022.3162837
87. Taha K. Proactive measures for cyber-physical systems cybersecurity. IEEE Int Conf Cyber Secur Resilience (CSR); 2023. p. 353–358. doi:10.1109/CSR57506.2023.10224929

88. Municio E, Latré S, Marquez-Barja JM. Extending network programmability to the things overlay using distributed industrial IoT protocols. IEEE Trans Ind Inform. 2021;17:251–259. doi:10.1109/TII.2020.2972613
89. Thomas V, Terence S, Agrawal B, Immaculate J. In: 4th Int Conf Signal Process Commun (ICSPC); 2023. p. 225–228. doi:10.1109/ICSPC57692.2023.10125704
90. Wasnik P, Chavhan N. A review paper on designing intelligent intrusion detection system using deep learning. 11th Int Conf Emerg Trends Eng Technol Signal Inf Process (ICETET – SIP); 2023. p. 1–6. doi:10.1109/ICETET-SIP58143.2023.10151563.
91. Zhang S, Cao D. A blockchain-based provably secure anonymous authentication for edge computing-enabled IoT. J Supercomput. 2024;80:6778–808. doi:10.1007/s11227-023-05696-0.
92. Ameyed D, Jaafar F, Petrillo F, Cheriet M. Quality and security frameworks for IoT-architecture models evaluation. SN Comput Sci. 2023;4:1–17. doi:10.1007/s42979-023-01815-z.
93. Paolone G, Iachetti D, Paesani R, Pilotti F, Marinelli M, Di Felice P. A Holistic Overview of the Internet of Things Ecosystem. IoT. 2022;3:Art. no. 4. doi:10.3390/iot3040022.
94. Aaqib M, Ali A, Chen L, Nibouche O. IoT trust and reputation: A survey and taxonomy. J Cloud Comput. 2023;12:42. doi:10.1186/s13677-023-00416-8.
95. Askar NA, Habbal A, Alden FZ, Wei X, Alaidaros H, Guo J, et al. Forwarding strategies for named data networking based IoT: Requirements, taxonomy, and open research challenges. IEEE Access. 2023;11:78363–83. doi:10.1109/ACCESS.2023.3276713.
96. Santos R, Eggly G, Gutierrez J, Chesñevar CI. Extending the IoT-stream model with a taxonomy for sensors in sustainable smart cities. Sustainability. 2023;15:Art. no. 8. doi:10.3390/su15086594.
97. Alahmadi S, Rojas P, Idriss H, Bayoumi M. Taxonomy of consumer and industrial IoTSoutheastCon 2023, Orlando, FL, USA. 2023. p. 418–24. doi:10.1109/SoutheastCon51012.2023.10115217.
98. Karie NM, Sahri NM, Yang W, Valli C, Kebande VR. A review of security standards and frameworks for IoT-based smart environments. IEEE Access. 2021;9:121975–95. doi:10.1109/ACCESS.2021.3109886.
99. El-Kady AH, Halim S, El-Halwagi MM, Khan F. Analysis of safety and security challenges and opportunities related to cyber-physical systems. Process Saf Environ Prot. 2023;173:384–413. doi:10.1016/j.psep.2023.03.012.
100. Kampourakis V, Gkioulos V, Katsikas S. A systematic literature review on wireless security testbeds in the cyber-physical realm. Comput Secur. 2023;133:103383. doi:10.1016/j.cose.2023.103383.
101. Wang D, Zhou J, Masdari M, Qasem SN, Sayed BT. Security in wireless body area networks via anonymous authentication: Comprehensive literature review, scheme classification, and future challenges. Ad Hoc Netw. 2024;153:103332. doi:10.1016/j.adhoc.2023.103332.
102. Marshoodulla SZ, Saha G. An approach towards removal of data heterogeneity in SDN-based IoT framework. Internet Things. 2023;22:100763. doi:10.1016/j.iot.2023.100763.
103. Kaur B, Dadkhah S, Shoeleh F, Neto ECP, Xiong P, Iqbal S, et al. Internet of things (IoT) security dataset evolution: Challenges and future directions. Internet Things. 2023;22:100780. doi:10.1016/j.iot.2023.100780.
104. Collaguazo A, Villavicencio M, Abran A. An activity-based approach for the early identification and resolution of problems in the development of IoT systems in academic projects. Internet Things. 2023;24:100929. doi:10.1016/j.iot.2023.100929.
105. Makhdoom I, Abolhasan M, Franklin D, Lipman J, Zimmermann C, Piccardi M, et al. Detecting compromised IoT devices: Existing techniques, challenges, and a way forward. Comput Secur. 2023;132:103384. doi:10.1016/j.cose.2023.103384.
106. Sami MA, Khan TA. Forecasting failure rate of IoT devices: A deep learning way to predictive maintenance. Comput Electr Eng. 2023;110:108829. doi:10.1016/j.compeleceng.2023.108829.
107. Schiller E, Aidoo A, Fuhrer J, Stahl J, Ziörjen M, Stiller B. Landscape of IoT security. Comput Sci Rev. 2022;44:100467. doi:10.1016/j.cosrev.2022.100467.

108. Gomez J, Kfoury EF, Crichigno J, Srivastava G. A survey on network simulators, emulators, and testbeds used for research and education. Comput Netw. 2023;237:110054. doi:10.1016/j.comnet.2023.110054.
109. Thabit F, Can O, Aljahdali AO, Al-Gaphari GH, Alkhzaimi HA. Cryptography algorithms for enhancing IoT security. Internet Things. 2023;22:100759. doi:10.1016/j.iot.2023.100759.
110. Weber RH. Internet of things – New security and privacy challenges. Comput Law Secur Rev. 2010;26:23–30. doi:10.1016/j.clsr.2009.11.008.
111. Babar SD, Mahalle PN, Prasad NR, Prasad R. Proposed on device capability based authentication using AES-GCM for Internet of Things (IoT). Proceedings of the 3rd Springer International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (Mobisec 2011); Aalborg University, Denmark. 2011.
112. Borgia E. The Internet of things vision: Key features, applications and open issues. Comput Commun. 2014;54:1–31. doi:10.1016/j.comcom.2014.09.008.
113. Sicari S, Rizzardi A, Miorandi D, Coen-Porisini A. Internet of things: Security in the keys. Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks. New York, NY, USA: ACM; 2016. p. 129–33. doi:10.1145/2988272.2988280.
114. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Gener Comput Syst. 2018;82:395–411. doi:10.1016/j.future.2017.11.022.
115. Fotia L, Delicato F, Fortino G. Trust in edge-based Internet of things architectures: State of the art and research challenges. ACM Comput Surv. 2023;55:no. 9, 1–34. doi:10.1145/3558779.
116. Barrera D, Bellman C, Van Oorschot P. Security Best Practices: A Critical Analysis Using IoT as a Case Study. ACM Trans Priv Secur. 2023;26:1–30. doi:10.1145/3563392.
117. Jouhari M, Saeed N, Alouini MS, Amhoud EM. A survey on scalable LoRaWAN for massive IoT: Recent advances, potentials, and challenges. IEEE Commun Surv Tutor. 2023;25:1841–76. doi:10.1109/COMST.2023.3274934.
118. Akhtar MS, Feng T. A systemic security and privacy review: attacks and prevention mechanisms over IoT layers. EAI Endorsed Trans Sec Saf. 2022;8(30):e5. doi:10.4108/eetss.v8i30.590.
119. Kumar V, Paul K. Device fingerprinting for cyber-physical systems: A survey. ACM Comput Surv. 2023;55:1–41. doi:10.1145/3584944.
120. Ashrif FF, Sundararajan EA, Ahmad R, Hasan MK, Yadegaridehkordi E. Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction. J Netw Comput Appl. 2024;221:103759. doi:10.1016/j.jnca.2023.103759.
121. Alkunidry D, Alhuwaysi S, Alharbi R. Security threads and IoT security. J Comput Commun. 2023;11:Art. no. 9. DOI: 10.4236/jcc.2023.119005.
122. Ali U, Idris MYIB, Frnda J, Ayub MNB, Khan MA, Khan N, Beegum TR, Jasim AA, Ullah I, Babar M. Enhanced lightweight and secure certificateless authentication scheme (ELWSCAS) for Internet of things environment. Internet Things. 2023;24:100923. DOI: 10.1016/j.iot.2023.100923.
123. Rao PM, Deebak BD. A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. Ad Hoc Netw. 2023;146:103159. DOI: 10.1016/j.adhoc.2023.103159.
124. Meng X, Yang C, Qi Y, Liang W, Xu Z, Li K, Deng H. A novel multi-party authentication scheme for FCN-based MIoT systems in natural language processing environment. ACM Trans Asian Low-Resource Lang Inf Process. 2023. DOI: 10.1145/3590149.
125. Chen J, Xiao H, Zheng Y, Hassan MM, Ianni M, Guzzo A, Fortino G. DKSM: A Decentralized Kerberos Secure Service-Management protocol for Internet of things. Internet Things. 2023;23:100871. DOI: 10.1016/j.iot.2023.100871.
126. Malan E, Peluso V, Calimera A, Macii E, Montuschi P. Automatic Layer Freezing for Communication Efficiency in Cross-Device Federated Learning. IEEE Internet Things J. 2024;11:6072-6083. DOI: 10.1109/JIOT.2023.3309691.
127. More P, Sakhare S. Context-aware device classification and clustering for smarter and secure connectivity in Internet of Things. EAI Endorsed Trans Ind Netw Intell Syst. 2023;10(3). doi:10.4108/eetinis.v10i3.3874.

128. Hosseini SM, Ferreira J, Bartolomeu PC. Blockchain-based decentralized identification in IoT: An overview of existing frameworks and their limitations. Electronics. 2023;12:Art. no. 6. DOI: 10.3390/electronics12061283.
129. Foidl H, Felderer M. An approach for assessing industrial IoT data sources to determine their data trustworthiness. Internet Things. 2023;22:100735. DOI: 10.1016/j.iot.2023.100735.
130. Ashrif F, Sundarajan E, Ahmed R, Hasan M. SLAE6: Secure and lightweight authenticated encryption scheme for 6LoWPAN networks. Proceedings of the 12th International Conference on Sensor Networks - SENSORNETS; 2023; SciTePress: INSTICC; 2023. p. 67-78. doi:10.5220/0011632200003399.
131. Ellamathy J. Securing LwM2M with mbed TLS in Contiki-NG. Accessed on 01 November, 2023. Available at https://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-500539.
132. Gilles O, Gracia Pérez D, Brameret PA, Lacroix V. Securing IIoT communications using OPC UA PubSub and trusted platform modules. J Syst Archit. 2023;134:102797. DOI: 10.1016/j.sysarc.2022.102797.
133. Rana S, Mondal MRH, Kamruzzaman J. RBFK cipher: A randomized butterfly architecture-based lightweight block cipher for IoT devices in the edge computing environment. Cybersecur. 2023;6:3. DOI: 10.1186/s42400-022-00136-7.
134. Krishnamoorthy N, Umarani S. Implementation and management of cloud security for industry 4.O – data using hybrid elliptical curve cryptography. J High Technol Manag Res. 2023;34:100474. DOI: 10.1016/j.hitech.2023.100474.
135. Devi U, Jacob A. Cryptographic validation of lightweight Block ciphers and hash functions. 2023 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA), Bangalore, India. 2023. p. 1-10. DOI: 10.1109/PKIA58446.2023.10262450.
136. Elsadig MA. Detection of denial-of-service attack in wireless sensor networks: A lightweight machine learning approach. IEEE Access. 2023;11:83537-83552. DOI: 10.1109/ACCESS.2023.3303113.
137. Alrubayyi H. (2023). Artificial immune systems for detecting unknown malware in the IoT. [Online]. Available from: https://qmro.qmul.ac.uk/xmlui/handle/123456789/84686.
138. Hammad M, Jillani RM, Ullah S, Namoun A, Tufail A, Kim KH, Shah H. Security framework for network-based manufacturing systems with personalized customization: An Industry 4.0 approach. Sensors. 2023;23:Art. no. 17. DOI: 10.3390/s23177555.
139. Mohamed D, Ismael O. Enhancement of an IoT hybrid intrusion detection system based on fog-to-cloud computing. J Cloud Comput. 2023;12:41. DOI: 10.1186/s13677-023-00420-y.
140. Qamar R, Zardari BA. A study of blockchain-based Internet of things. Iraqi J Comput Sci Math. 2022;4:Art. no. 1. DOI: 10.52866/ijcsm.2023.01.01.003.
141. Zang M, Zheng C, Dittmann L, Zilberman N. Toward Continuous Threat Defense: In-Network Traffic Analysis for IoT Gateways. IEEE Internet Things J. 2024;11:9244-9257. DOI: 10.1109/JIOT.2023.3323771.
142. Zhang X. Prediction of cyberspace security data based on the Markov chain model. Appl Math Nonlinear Sci. 2023;8(2):2539-2548. DOI: 10.2478/amns.2023.1.00434.
143. Mena DMM. Blockchain-based security framework for the Internet of things and home networks. Phys D. Accessed on 01 November, 2023. Available at https://www.proquest.com/docview/2838330313/abstract/8E92FAC47D9A4EFAPQ/1.
144. Ismail S, Reza H, Zadeh HK, Vasefi F. A blockchain-based IoT security solution using multichain. 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA. 2023. p. 1105-1111. DOI: 10.1109/CCWC57344.2023.10099128.
145. Chen Y, Tao L, Liang B, Sun L, Li Y, Xing B, Chen L. Capability and Blockchain-Based Fine-Grained and Flexible Access Control Model. IEEE Netw. 2023;37:197-205. DOI: 10.1109/MNET.127.2200414.
146. Liu C, Xu M, Guo H, Cheng X, Xiao Y, Yu D, Gong B, Yerukhimovich A, Wang S, Lyu W. TBAC: A Tokoin-Based Accountable Access Control Scheme for the Internet of Things. IEEE Trans Mob Comput. 2024;23:6133-6148. DOI: 10.1109/TMC.2023.3316622.

147. Ghaffari F, Bertin E, Crespi N, Hatin J. Distributed ledger technologies for authentication and access control in networking applications: A comprehensive survey. Comput Sci Rev. 2023;50:100590. DOI: 10.1016/j.cosrev.2023.100590.
148. Gugueoth V, Safavat S, Shetty S, Rawat D. A review of IoT security and privacy using decentralized blockchain techniques. Comput Sci Rev. 2023;50:100585. DOI: 10.1016/j.cosrev.2023.100585.
149. Mu C, Ding T, Yang M, Huang Y, Jia W, Shen X. Peer-to-peer energy trading based on a hybrid blockchain system. Energy Rep. 2023;9:124-128. DOI: 10.1016/j.egyr.2023.09.123.
150. Luo M, Zhou J, Yang P. RATS: A regulatory anonymous transaction system based on blockchain. J Parallel Distrib Comput. 2023;182:104751. DOI: 10.1016/j.jpdc.2023.104751.
151. Tabatabaei MH, Vitenberg R, Veeraragavan NR. Understanding blockchain: Definitions, architecture, design, and system comparison. Comput Sci Rev. 2023;50:100575. doi:10.1016/j.cosrev.2023.100575
152. Khang A, Gupta SK, Rani S, Karras DA, SMART. Cities: IoT Technologies, Big Data Solutions, Cloud Platforms, and Cybersecurity Techniques. Boca Raton, Florida, United States: CRC Press; 2023.
153. Sęk J, Trojanowski P, Gilewicz Ł, Gapinski B, Evtuhov A. Implementation of intelligent transport systems in an urban agglomeration: A case study. In: Ivanov V, Trojanowska J, Pavlenko I, Rauch E, Piteľ J, editors. Advances in Design, Simulation and Manufacturing VI. Switzerland: Springer Nature; 2023. p. 152–61. doi:10.1007/978-3-031-32767-4_15
154. Srikanth GU, Geetha R, Prabhu S. An efficient key agreement and Authentication Scheme (KAAS) with enhanced security control for IIoT systems. Int J Inf Technol. 2023;15:1221–30. doi:10.1007/s41870-023-01173-2
155. Tahir A, Mashood K. Internet of things and big data in the contexts of education and science. Pak J Educ Res. 2023;6. doi:10.52337/pjer.v6i2.796
156. Cai T, Chen W, Psannis KE, Goudos SK, Yu Y, Zheng Z, et al. On-Chain and off-chain scalability techniques. In: Chen W, Zheng Z, Huang H, editors. Blockchain Scalability. New York: Springer Nature; 2023. p. 81–96. doi:10.1007/978-981-99-1059-5_3
157. Yu B, Feng L, Zhu H, Qiu F, Wan J, Yao S. MeHLDT: A multielement hash lock data transfer mechanism for on-chain and off-chain. Peer-to-Peer Netw Appl. 2023;16:1927–43. doi:10.1007/s12083-023-01491-z
158. Wang J, Li Y, Tan A, Gong Z, Wang Y. Multi-User On-Chain and Off-Chain Collaborative Query Optimization Based on Consortium Blockchain. In: Yuan L, Yang S, Li R, Kanoulas E, Zhao X, editors. Web Information Systems and Applications. Singapore: Springer Nature; 2023. p. 476–87. doi:10.1007/978-981-99-6222-8_40.
159. Selvadurai N. Mitigating the legal challenges associated with blockchain smart contracts: The potential of hybrid On-Chain/off-chain contracts. Wash Lee Law Rev. 2023;80:1163.
160. Khobragade P, Turuk AK. On-chain off-chain blockchain model for IoT using IPFS. IET Conf Proc. 2023;30–4. doi:10.1049/icp.2023.1452.
161. Afraz N, Wilhelmi F, Ahmadi H, Ruffini M. Blockchain and Smart contracts for telecommunications: Requirements vs. cost analysis. IEEE Access. 2023;11:95653–66. doi:10.1109/ACCESS.2023.3309423.
162. Zhu J, Cao J, Saxena D, Jiang S, Ferradi H. Blockchain-empowered federated learning: Challenges, solutions, and future directions. ACM Comput Surv. 2023;55:1–31. doi:10.1145/3570953.
163. Al-Sumaidaee G, Alkhudary R, Zilic Z, Swidan A. Performance analysis of a private blockchain network built on hyperledger fabric for healthcare. Inf Process Manag. 2023;60:103160. doi:10.1016/j.ipm.2022.103160
164. Saurabh K, Upadhyay P, Rani N. A study on blockchain-based marketplace governance platform adoption: A multi-industry perspective. Digit Policy Regul Gov. 2023;25:653–92. doi:10.1108/DPRG-04-2023-0053.
165. Mollajafari S, Bechkoum K. Blockchain technology and related security risks: Towards a seven-layer perspective and taxonomy. Sustainability. 2023;15(18):13401. doi:10.3390/su151813401.

166. Yadav AK, Singh K, Amin AH, Almutairi L, Alsenani TR, Ahmadian A. A comparative study on consensus mechanism with security threats and future scopes: Blockchain. Comput Commun. 2023;201:102–15. doi:10.1016/j.comcom.2023.01.018.
167. Rizzardi A, Sicari S, Miorandi D, Coen-Porisini A. Securing the access control policies to the Internet of things resources through permissioned blockchain. Concurr Comput Pract Exp. 2022;34:e6934. doi:10.1002/cpe.6934.
168. Seo JW, Islam A, Masuduzzaman M, Shin SY. Blockchain-based secure firmware update using an UAV. Electronics. 2023;12(10):2189. doi:10.3390/electronics12102189.
169. Solomon G, Zhang P, Brooks R, Liu Y. A secure and cost-efficient blockchain facilitated IoT software update framework. IEEE Access. 2023;11:44879–94. doi:10.1109/ACCESS.2023.3272899
170. Tong F, Chen X, Huang C, Zhang Y, Shen X. Blockchain-assisted secure intra/inter-domain authorization and authentication for Internet of things. IEEE Internet Things J. 2023;10:7761–73. doi:10.1109/JIOT.2022.3229676.
171. Bao Z, He D, Khan MK, Luo M, Xie Q. PBidm: Privacy-preserving blockchain-based identity management system for industrial Internet of things. IEEE Trans Ind Inform. 2023;19:1524–34. doi:10.1109/TII.2022.3206798
172. Chesser M, Nepal S, Ranasinghe DC. Icicle: A re-designed emulator for grey-box firmware fuzzing. Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis. ACM; 2023. p. 76–88. Available from: arXiv:2301.13346. doi:10.1145/3597926.3598039.
173. Al Hwaitat AK, Almaiah MA, Ali A, Al-Otaibi S, Shishakly R, Lutfi A, et al. A new blockchain-based authentication framework for secure IoT networks. Electronics. 2023;12(17):3618. doi:10.3390/electronics12173618.
174. Onwubiko A, Singh R, Awan S, Pervez Z, Ramzan N. Enabling trust and security in digital twin management: A blockchain-based approach with Ethereum and IPFS. Sensors. 2023;23(14):6641. doi:10.3390/s23146641
175. Khashan OA, Khafajah NM. Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems. J King Saud Univ Comput Inf Sci. 2023;35:726–39. doi:10.1016/j.jksuci.2023.01.011.
176. Aliyu AA, Liu J. Blockchain-based smart farm security framework for the Internet of things. Sensors. 2023;23(18):7992. doi:10.3390/s23187992.
177. Shreya S, Chatterjee K, Singh A. BFSF: A secure IoT based framework for smart farming using blockchain. Sustain Comput Inform Syst. 2023;40:100917. doi:10.1016/j.suscom.2023.100917
178. Chatterjee K, Singh A, Neha. A blockchain-enabled security framework for smart agriculture. Comput Electr Eng. 2023;106:108594. doi:10.1016/j.compeleceng.2023.108594.
179. Qadir Z, Le KN, Saeed N, Munawar HS. Towards 6G Internet of things: Recent advances, use cases, and open challenges. ICT Express. 2023;9:296–312. doi:10.1016/j.icte.2022.06.006.

