



Leveraging Blockchain-Based Approaches for IoT Security

Ahmed Abubakar Aliyu 

Department of Secure Computing, Kaduna State University, Nigeria.
Email: ahmed.aliyu@kasu.edu.ng



Abstract

Blockchain technology is transforming various sectors, including the Internet of Things (IoT), by providing a decentralized and secure framework for data management and transaction processing. However, securing IoT devices and networks remains challenging due to their vulnerabilities and the increasing complexity of cyber threats. Blockchain-based solutions offer promising avenues to enhance IoT security, yet their adoption is hindered by the lack of a unified taxonomy and comprehensive architectural analysis. To advance the field, a standardized classification system is essential for comparing different blockchain security models and identifying the most suitable options for specific IoT applications. Additionally, deeper architectural evaluations are needed to examine trade-offs related to security, scalability, and efficiency. Empirical assessments are also crucial to test how these models perform under various threat scenarios and operational environments. This paper addresses these gaps by proposing a structured taxonomy, conducting systematic architectural evaluations, and providing empirical performance assessments. These efforts aim to support the development of secure, efficient, and scalable blockchain-based security solutions tailored to the unique challenges of IoT systems. Ultimately, this work seeks to strengthen trust and reliability in the integration of blockchain technologies within the IoT ecosystem.

Keywords: Blockchain technology, Cybersecurity, Internet of things (IoT), IoT Security, IoT Security Taxonomy, Intrusion detection systems.

Citation | Aliyu, A. A. (2025). Leveraging Blockchain-Based Approaches for IoT Security. *International Review of Applied Sciences*, 11(1), 1-21.

History:


Received: 6 May 2025

Revised: 27 July 2025

Accepted: 29 July 2025

Published: 1 August 2025

Licensed: This work is licensed under a [Creative Commons](https://creativecommons.org/licenses/by/4.0/)

Attribution 4.0 License 

Publisher: Asian Online Journal Publishing Group

Funding: The research is supported by the School of Cyber Science and Engineering, Wuhan University.

Institutional Review Board Statement: Not Applicable

Transparency: The author confirms that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Competing Interests: The author declares that there are no conflicts of interests regarding the publication of this paper.

Contribution of this paper to the literature

This paper provides a structured taxonomy of blockchain-based IoT security solutions, critically analyzes architectural and implementation challenges, and offers empirical insights to guide model selection. It supports the development of scalable, efficient, and secure blockchain frameworks tailored to IoT environments, enhancing trust, resilience, and applicability in real-world use cases.

1. Introduction

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 their inherent vulnerabilities and the increasing sophistication of cyberattacks. Blockchain-based security approaches have emerged as promising solutions to address these challenges, but the lack of a comprehensive taxonomy and systematic studies on their architectural design and effectiveness hinder 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 effectively compare and evaluate different solutions. This lack of clarity hampers researchers, practitioners, and policymakers in identifying the most appropriate approaches for specific IoT scenarios. Second, the absence of systematic studies on the architectural design of blockchain-based security approaches limits our understanding of the trade-offs between security, performance, and scalability. A comprehensive understanding of design choices and their implications is crucial for developing efficient and secure IoT systems. Finally, there is an urgent need for empirical studies on 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 current literature is critical to 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.

1.1. Literature Search

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

1.2. Inclusion Criteria

The initial screening process focused on identifying literature directly related to the application of blockchain technology in IoT security. Only peer-reviewed journal articles, conference papers, and reputable research reports were considered for inclusion. The selected publications specifically addressed the use of blockchain technology in areas such as IDS.

1.3. Exclusion Criteria

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

1.4. Data Extraction

From the selected studies, key information was systematically extracted, including the authors, publication year, research objectives, methodologies, findings, and limitations. This data was organized to facilitate a comprehensive review.

1.5. Synthesis and Analysis

The extracted data were analyzed to identify recurring patterns, trends, and themes related to the use of blockchain technology in IoT security. Comparative analysis was employed to examine the findings across studies, enabling insights into current trends and future research directions.

1.6. 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 ensured the quality and robustness of the evidence presented in the reviewed literature.

1.7. Identification of Gaps

The 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 potential opportunities for future research.

2. Blockchain Technology and Its Evolution

The history of blockchain technology can be traced back to the early 1990s when cryptographer Pandey et al. [1] first proposed a blockchain-like protocol in their 1982 thesis. Further work on a cryptographically secured chain of blocks was described by Stuart Haber and W. Scott Stornetta in 1991 [2]. They wanted to implement a system where document timestamps could not be tampered with. In 1992, Haber, Stornetta, and Dave Bayer incorporated Merkle trees into the design, which improved its efficiency by allowing multiple document certificates to be collected in one block [3]. Under their company Surety, the hashes of their document certificates have been published in the

New York Times every week since 1995. Notably, the first decentralized blockchain was conceived in 2008 by a person (or group of people) known as Satoshi Nakamoto [4]. Nakamoto improved the design in important ways, using a hashcash-like method to timestamp blocks without requiring them to be signed by a trusted party, and introduced a difficulty parameter to stabilize the rate at which blocks are added to the chain. 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, non-fungible tokens (NFTs), as well as academic research [6].

As a decentralized database shared across computers on a network, blockchain can be defined as a distributed ledger system that enables the secure, transparent, and tamper-proof recording of transactions [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 computers in the network. The transaction is subsequently verified by the computers and added to their copy of the blockchain. An important aspect of the blockchain, which is security, is predicated on the fact that tampering with the data on the blockchain is extremely difficult [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. Since 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].

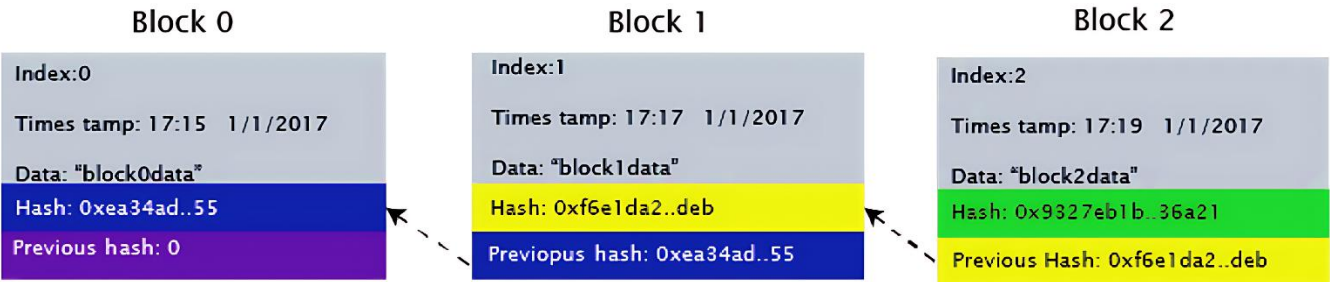


Figure 1. Blockchain illustration.

The computation required to obtain the appropriate nonce is proportional to the expected number of zeros. This means that it is very difficult to generate a new block, but once a block is generated, it is very easy to verify. This is because the nonce is a one-way function, meaning that it is easy to calculate the output of the function given the input, but very difficult to determine the input given the output [12]. Additionally, once a new block is generated, it is transmitted to other nodes in the network and verified. The miner who generated the block is rewarded with Bitcoins (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 indicates that the block is more likely to be valid. It is also more difficult for an attacker to declare a false transaction, as they would have to recalculate all subsequent blocks [15]. This would be a computationally intensive task that would be almost impossible to achieve.

In a nutshell, blockchain enables Byzantine fault tolerance (BFT) Sun et al. [16] by facilitating consensus in an unreliable environment, as well as decentralization, permanence, anonymity, and audibility. As a result of the decentralized structure, i.e., 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].

2.1. Blockchain's Original Limitations and Technical Response

The original blockchain faces technical challenges and limitations that could hinder its adoption as it evolves. One of these challenges is scalability [19]. Currently, Bitcoin's transaction rate is only seven transactions per second [20] which may be insufficient as the number of users increases. Another challenge is transaction time. Complete Bitcoin transactions take about 10 minutes [21] which is too long for many applications. Similarly, Bitcoin blocks are almost a megabyte in size, which can restrict the flow of information if it reaches the level of financial competition [22]. This can lead to bandwidth shortages. Furthermore, the security of Bitcoin is based on the assumption that most nodes in the network are functioning correctly, but there are known attacks that can exploit this weakness. In particular, Bitcoin mining consumes a lot of energy due to the trial and error involved in finding the correct nonce [23]. This is a major concern for some people because it raises environmental and sustainability issues. These limitations have led to the development of alternatives and changes to blockchain technology. For example, Ethereum introduces blockchains with an integrated Turing-complete programming language to enable the development of smart contracts and other decentralized applications [24]. Whereas Bitcoin and the underlying blockchain have the potential to transform many industries, they face technical challenges and limitations. It will also be important to address these issues to ensure the widespread adoption of blockchain technology as the technology advances.

The second version of the Ethereum blockchain uses a distributed virtual machine, called the Ethereum Virtual Machine (EVM), to execute smart contracts [25]. Ethereum smart contracts (in Figure 2) can be considered lightweight, decentralized applications, or dApps, which open the door to application research in various fields [26]. Similarly, Blockchain 3.0 [27] includes applications outside of 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 altcoins (Altcoin) [29] improve block timing, the 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].

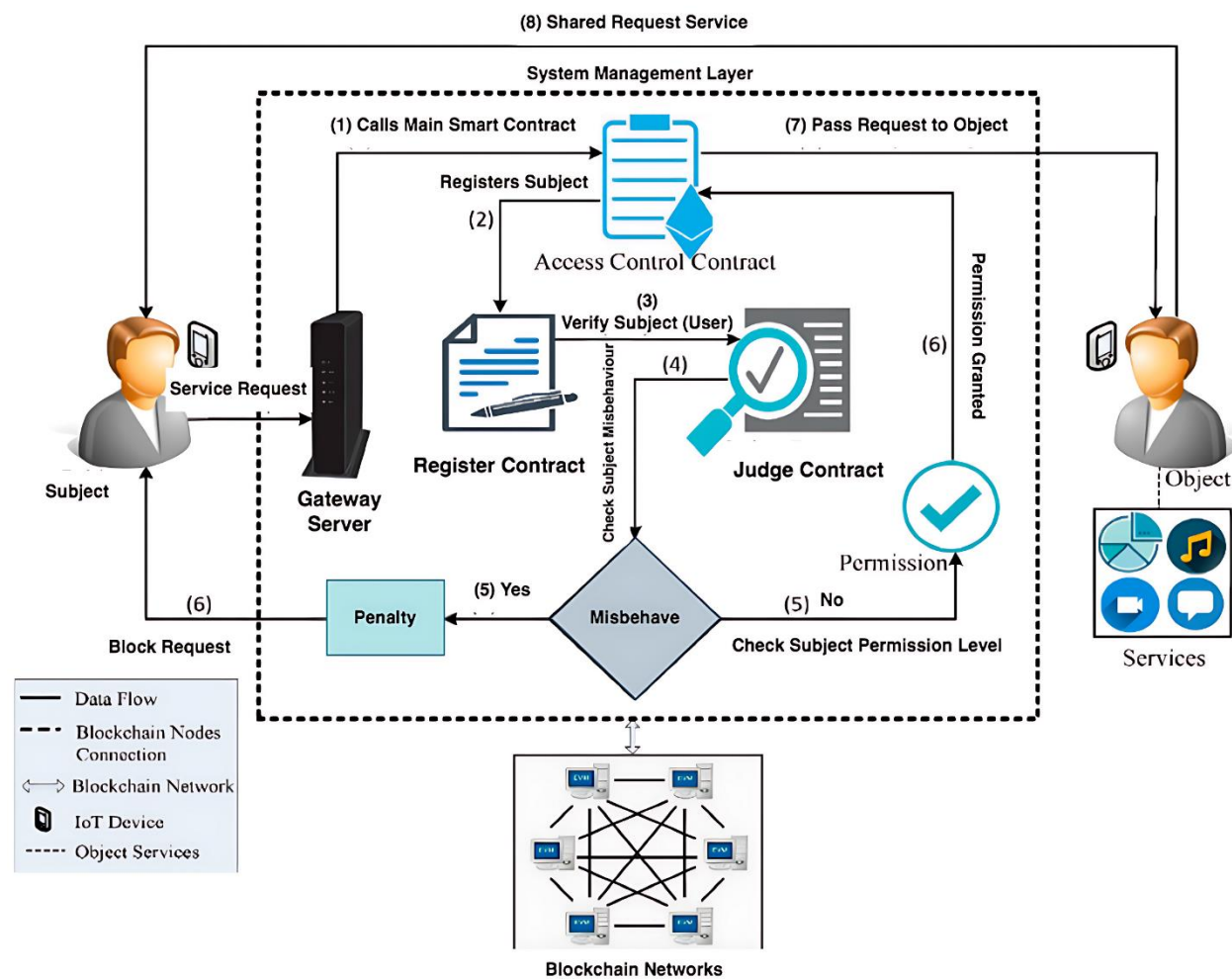


Figure 2. The smart contract.

However, the technical hurdles and limitations of Bitcoin and its original blockchain hinder its adaptation as it evolves [31]. Firstly, Bitcoin's current maximum throughput is only seven transactions per second, which may limit its scalability over time as the number of users increases. Secondly, the time required to complete a transaction is approximately 10 minutes [32] and the time required to mine a block is often tied to the number of zeros required for PoW, with a latency that makes the original blockchain unsuitable for applications that rely on immediacy. Thirdly, as 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. Lastly, 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] has described three different realistic attacks on Bitcoin security involving block manipulation and transaction delivery. Also, the Sybil attack relies on IP address control and rapid financial intervention. Another study [35] shows 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 even effectively launching double-spending attacks. In addition, software problems have been discovered in Bitcoin software, 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 the PoW, it requires a significant amount of computing power.

The limitations and weaknesses of Bitcoin have prompted the search for alternatives or modifications to the original method to enhance the application and scope of blockchain technology. The first and subsequent versions of blockchain have been classified based on their potential activities. The blockchain community has defined three categories: 1.0, 2.0, and 3.0 [37]. Blockchain 1.0 is the original blockchain technology implemented by Bitcoin. It is primarily focused on cryptocurrency and digital payments. Blockchain 2.0 is an extension of Blockchain 1.0 that introduces smart contracts and dApps. Smart contracts are self-executing contracts stored on the blockchain, while dApps are applications that run on the blockchain and are not controlled by a single entity. Blockchain 3.0 is a future vision of blockchain technology that aims to expand its capabilities beyond cryptocurrency and smart contracts. Blockchain 3.0 is expected to be more scalable, secure, and efficient than previous versions of blockchain technology. Lastly, 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 while Table 2 compares Blockchain's key performance from the literature.

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%

Note: Essentially, we can divide consensus algorithms into three categories.

2.1.1. Traditional Consensus Algorithms

Paxos and its variants: These algorithms, like Raft, are commonly used in distributed systems to ensure consistency and fault tolerance. They work by a designated leader proposing values and other nodes voting on them.

Byzantine Fault Tolerance (BFT): This family of algorithms is designed to tolerate malicious Byzantine failures, where nodes can fail in arbitrary ways. BFT algorithms are typically more complex than Paxos but can provide stronger guarantees.

Proof-of-Work (PoW): This is the consensus algorithm used by Bitcoin and other blockchains. Miners compete to solve cryptographic puzzles, and the first to find a solution gets to add the next block to the chain. PoW is secure but can be energy-intensive and slow.

2.1.2. Blockchain-Based Consensus Algorithms

Proof-of-Stake (PoS): This algorithm replaces miners with validators, who stake their cryptocurrency to participate in the consensus process. Validators are selected based on the amount of cryptocurrency they stake, and they vote on new blocks. PoS is less energy-intensive than PoW but can be more vulnerable to attacks.

Delegated Proof-of-Stake (DPoS): This is a variant of PoS where users delegate their voting power to a small number of representatives. DPoS can be faster and more efficient than PoS, but it can also be more centralized.

Proof-of-Authority (PoA): This algorithm uses a pre-defined set of validators who are trusted to act honestly. PoA is fast and efficient but can be less secure than other consensus algorithms.

2.1.3. Emerging Consensus Algorithms

Proof-of-Elapsed Time (PoET): This algorithm uses elapsed time as a means of measuring consensus. Nodes compete to generate a random number, and the first to do so gets to add the next block to the chain. PoET is less energy-intensive than PoW but may be more vulnerable to attack [40].

Proof of Activity (PoA): This algorithm rewards nodes for performing useful activities, such as storing data or processing transactions. PoA can be more efficient than PoW and PoS but can be more complex to implement.

Proof-of-Reputation (PoR): This is a new reputation-based consensus algorithm that addresses the security, performance, and centralization concerns of existing permissionless blockchain consensus algorithms. PoR achieves a balance between scalability, security, and decentralization by combining BFT, reputation, reward, and punishment mechanisms [41].

Sharding: This is a technique that can be used with other consensus algorithms to improve scalability. Sharding divides the blockchain into smaller pieces, called shards, which can be processed independently. This allows more transactions to be processed per second.

In summary, the original limitations of blockchain include scalability, security, energy consumption, and usability. Scalability refers to the ability of a blockchain network to process large numbers of transactions quickly and efficiently. Current blockchain networks are often slow and expensive to use, especially for high-volume applications [42]. In addition, security is another concern with blockchain networks, as they can be vulnerable to attacks such as 51% attacks and double spending attacks. Blockchain networks can also consume a significant amount of energy due to the computing power required to mine and validate transactions. This raises environmental and sustainability issues, which are major concerns for some. Another limitation is that blockchain technology can be complex and difficult for non-technical users to operate effectively [43]. This may limit its adoption in some industries.

2.2. 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 are recommended [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]. This framework includes a compiler that converts scripts into cryptography-based

protocols. Because 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, there are flaws in the technical and functional principles of smart contracts. A study highlights 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, which is used to manipulate the results of transactions executed by the contract. This study also simulates a DAO attack [49] in which an attacker steals money by exploiting a flaw in the payout function after a fallback. Another current challenge identified in a recently published paper is four significant security flaws in blockchain systems. These are transaction order dependency, timestamp dependency, anomaly mishandling, and re-internalization [50]. These flaws can also be exploited by attackers to steal funds, disrupt the network or even bring down the system.

The potential of blockchain, however, 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 perception of time [51], which allows for the extension of services to other areas, especially security. Beyond financial applications, there are some out-of-the-box benefits of blockchain, according to one study [52] such as Distributed P2P Networks, Fault Tolerance, Practical consensus, and Predictable, trustless participation.

Data invariance and data 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 anything of value [54]. However, not all security solutions are suitable for replacement or supplementation by blockchain applications. A recent study [55] proposes 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 not being entirely trusted; (3) the first 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 not being fully trusted. Furthermore, other works call for a comprehensive technological strategy before incorporating blockchain into diverse solutions [56-58]. Despite its limitations, blockchain technology has the potential to revolutionize the security landscape [59]. Its unique characteristics, such as decentralization, immutability, and transparency, make it well-suited for a wide range of security applications [60]. One area where blockchain is already having a significant impact is in data storage, as blockchain-based data storage solutions offer a number of advantages over traditional centralized systems, including enhanced security, improved transparency, and increased efficiency [61]. Additionally, blockchain is also being used to improve the security of protected health information (PHI) [62]. Blockchain-based PHI management solutions can help give patients 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 also being used to improve the security of various other applications, including data control, DDoS defense, file protection, and general IoT security [63]. In summary, blockchain technology has the ability to 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.

3. Intrusion Detection Systems

An Intrusion Detection System (IDS) is a security tool that monitors network traffic or system activities for signs of malicious behavior, unauthorized access, or policy violations [64]. When suspicious activity is detected, the IDS logs the event and alerts administrators, helping organizations respond quickly to potential threats. Detection methods include signature-based systems that recognize known attack patterns and anomaly-based systems that flag deviations from normal behavior. Unlike firewalls, which block unauthorized access, IDSs are primarily designed to detect and report threats rather than prevent them, making them an essential component of a layered cybersecurity strategy.

3.1. Traditional Intrusion Detection Systems

IDSs can detect a variety of attacks, including DoS attacks, malware infections, and unauthorized access attempts. Furthermore, IDSs work by analyzing network traffic for patterns that indicate malicious activity. These patterns can be based on specific characteristics of malicious traffic, such as unusual packet sizes or traffic patterns. IDSs can be used in various ways, such as monitoring network traffic at the perimeter of a network or deploying on individual hosts to monitor traffic for that host [65]. Moreover, an IDS is a critical reactive security measure that detects potential attacks in progress on a host system [66]. Also, 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 attacks that could be harmful or looming threats of violations of computer and network security policies is known as an IDS, shown in Figure 3 [65].

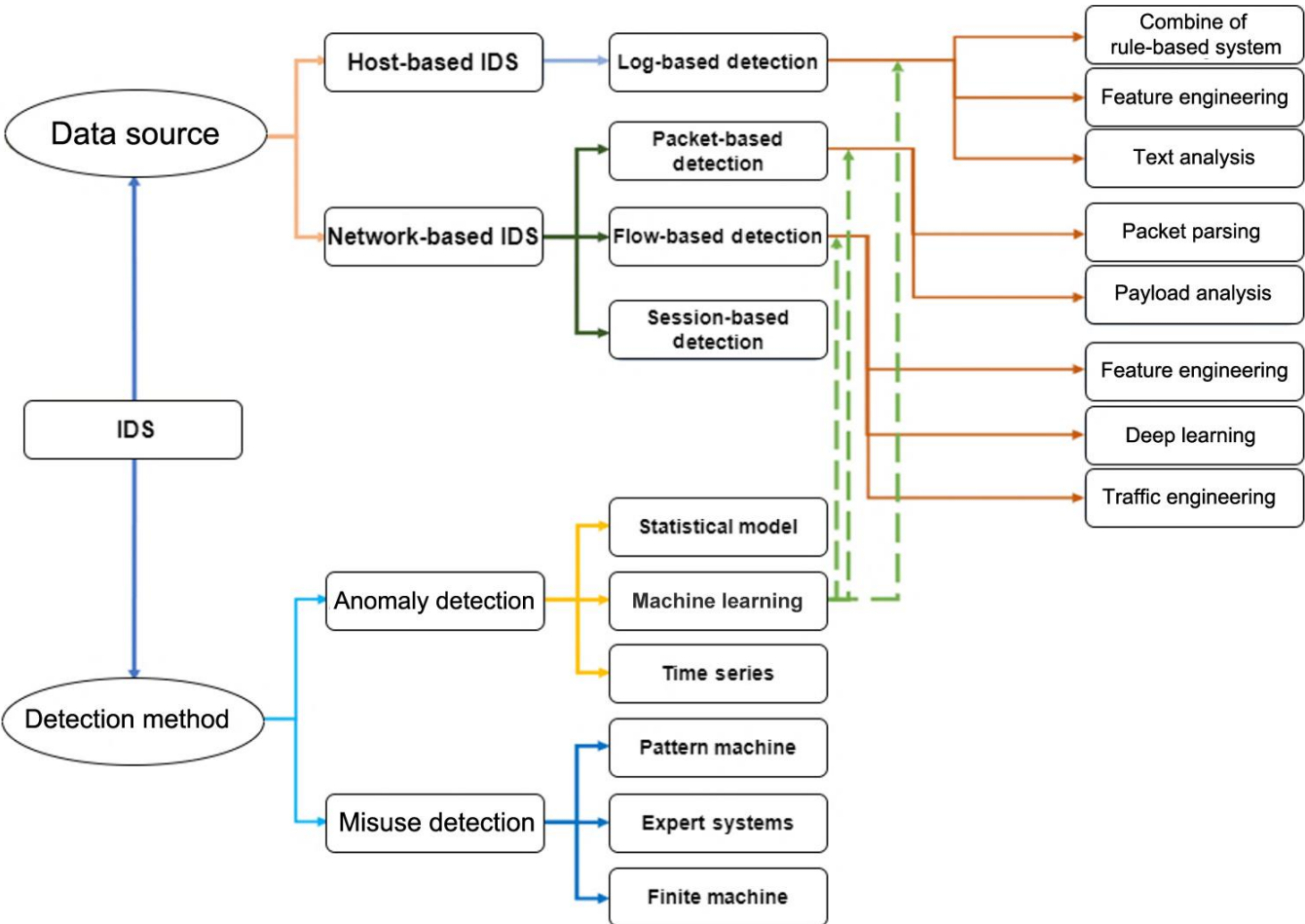


Figure 3. The traditional IDS structure.

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 strive to detect and alert on normal or abnormal networking activities. Intruders may attempt to damage, compromise, or devastate systems using wirelessly communicated packets. Recently, several IDSs have been integrated into cybersecurity systems to detect and mitigate malicious traffic from legitimate ones. IDSs are traditionally classified into five types, as outlined below [69].

(1) A network-based IDS (NIDS) is a system that monitors the entire network through one or more points of contact. To deploy a NIDS, you typically need to install it on a hardware device within the network infrastructure [44]. When the NIDS is installed, it samples every packet (a collection of data) that passes through it. A standard NIDS is capable of scanning all traffic that passes through it. (2) A network node-based IDS (NNIDS) is a subset of a NIDS, but because it works differently, we will classify it as a separate type of IDS [70]. The packets that pass through a NNIDS are also analyzed. Instead of relying on a centralized device to monitor all network traffic, the system monitors each node connected to your network. This distinction has some advantages, such as faster speeds and the use of fewer resources. (3) A Host IDS (HIDS) extends the device independence of NNIDS. HIDS can be used to install IDS software on all network-connected devices. HIDSs work by taking 'snapshots' of the device to which they are assigned. By comparing the latest snapshot with previous records, HIDS can detect differences that could indicate an 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 protect the web server by monitoring inbound and outbound traffic. (5) Another type of IDS that focuses on the security of software applications is an application protocol-based IDS (APIDS). APIDSs, sometimes called Host-based IDSs (HIDSs), monitor communication between applications and the server. An APIDS is typically installed on groups of servers. Moreover, an APIDS is unlikely to meet all the 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:

- Signature-based IDS.
- Anomaly-based IDS.
- Hybrid IDS.

A signature is a common footprint or pattern that can take the form of unauthorized software execution, unauthorized network access, unauthorized directory access, or anomalies in the use of network privileges [71]. It can also be a sequence of bytes in a file or network traffic associated with a malicious attack on a computer network or system. 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 to achieving this level of protection [72]. Signature-based detection is used by antivirus software to identify malicious software threats. It is also recognized as a fundamental 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 models and Rule-based models [73]. Despite the fact that 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. To detect malware, pattern-matching models use single or multiple pattern-matching algorithms. In contrast, rule-based approaches have a set of rules that are compared to network traffic or audit data. If the rules match, they can detect any attack. The hybrid model is a combination of the two.

Anomaly-based IDSs identify malicious activity by detecting deviations from normal behavior. This approach contrasts with signature-based IDSs, which detect malicious activity by matching known attack patterns. Anomaly-based IDSs 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 activity as malicious if it deviates from normal behavior. There are a number of different approaches to 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 then flag any activity that deviates from normal behavior as malicious [75]. Another approach is to use statistical methods to identify deviations from normal behavior [76]. For example, an anomaly-based IDS might track the number of packets sent between two hosts over a period of time. If the number of packets sent between the two hosts suddenly increases, the anomaly-based IDS might 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 the advantages include detecting new and emerging threats and flexibility. Its disadvantages include being more prone to false positives and also being more difficult to configure and maintain.

3.2. Blockchain-Based Intrusion Detection Systems

Blockchain-based IDSs represent a new generation of security mechanisms that leverage blockchain technology to enhance the detection and prevention of malicious activities. These systems incorporate innovative techniques for malware identification and integrate protective measures such as firewalls, quarantine protocols, and blacklists [77]. One key application of blockchain in IDSs is the development of distributed reputation systems that monitor malware behavior and suspicious activity across multiple networks, enabling more effective threat detection and mitigation [78].

However, implementing blockchain in IDSs poses challenges. It requires significant technical expertise and a deep understanding of blockchain architecture barriers for organizations with limited resources or skills. Additionally, blockchain systems can introduce new vulnerabilities, including 51% attacks, smart contract exploits, and consensus-related threats. Therefore, careful system design and robust implementation strategies are crucial to minimizing these risks.

For instance, Javadpour et al. [79] proposed a Distributed Multi-Agent Intrusion Detection and Prevention System (DMAIDPS) tailored for cloud-based IoT environments. Using a six-step detection process with KDD Cup 99 and NSL-KDD datasets, the system classifies network activity as either normal or under attack. Evaluation metrics such as recall, accuracy, and F-score demonstrated their effectiveness.

In another study, Kably et al. [80] introduced the Multi-Zone-Wise Blockchain (MZWB) model. It combines the Enhanced Blowfish Algorithm (EBA) for authenticating IoT nodes with a Bayesian Direct Acyclic Graph (B-DAG) for network management. Intrusion detection occurs in two stages: a Deep Convolutional Neural Network (DCNN) initially classifies data packets as normal, malicious, or suspicious, and a Generative Adversarial Network (GAN) further analyzes the suspicious packets. Finally, the Improved Monkey Optimization (IMO) algorithm is applied to reconstruct and mitigate the intrusion scenario.

Additionally, Babu et al. [81] developed a permissioned blockchain system utilizing lightweight technology and an arbiter PUF model to secure key pairs in IoT devices. Their collaborative detection approach uses machine learning-based ensemble techniques to identify DDoS attacks, achieving a higher detection rate and reduced false positives compared to existing methods. Alerts are securely distributed across authenticated IoT nodes using blockchain. Table 3 presents a comparative analysis of traditional versus blockchain-based IDS solutions.

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, can be expensive

4. Internet of Things

The IoT refers to the network of interconnected physical devices that are embedded with sensors, software, and other technologies to enable them to collect and exchange data [82]. These devices are often small and have limited resources, making them difficult to secure. As a result, the IoT is a prime target for cyberattacks [83]. One of the biggest challenges in securing the IoT is the sheer number of devices involved. A study Dong et al. [84] has predicted that there will be more than 75 billion IoT devices connected to the Internet by 2025, as shown in Figure 4. This large scale makes it difficult to track and manage all the devices and increases the likelihood that vulnerabilities will go unnoticed. Another challenge is the diversity of IoT devices [85]. IoT devices come in all shapes and sizes and are used for a variety of purposes. This diversity makes it difficult to develop security solutions that are effective across all types of IoT devices. In addition, IoT devices often collect and process sensitive data, such as personal or financial information. If this data is not properly secured, it could be stolen or compromised by attackers [86]. Despite these challenges, there are several measures that can be taken to enhance IoT security. One important step is to implement security measures at the device level [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 will help prevent attackers from gaining access to sensitive data on other networks. Finally, it is important to monitor the IoT network for suspicious activity [89]. This can be accomplished using

various tools and techniques, such as intrusion detection systems and security information and event management systems [90].

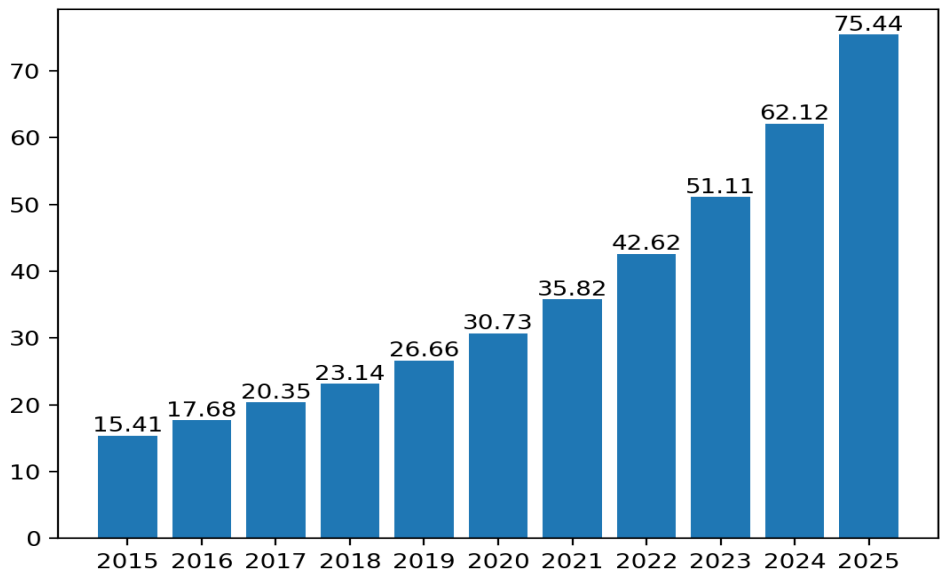


Figure 4. Prediction of the Global number of IoT devices from 2015 to 2025.
Source: Dong, et al. [84]

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 comprise the IoT. It is designed with modularity, flexibility, and extensibility in mind to accommodate the evolving and dynamic nature of the IoT ecosystem [91]. The IoT-RM offers a number of 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 layer, communication layer, edge layer, 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, a number of taxonomies have been proposed, each with its own focus and strengths [94]. A common approach to IoT taxonomy is to divide IoT into layers based on the architectural components of an IoT system. These layers include the device layer, communication layer, edge layer, and cloud layer [95]. Another approach to the 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, the IoT can also be classified based on the underlying technologies used to implement it. These technologies include Radio Frequency Identification (RFID), Wireless Sensor Networks (WSNs), cloud computing, artificial intelligence (AI), blockchain, edge computing, and fog computing [97].

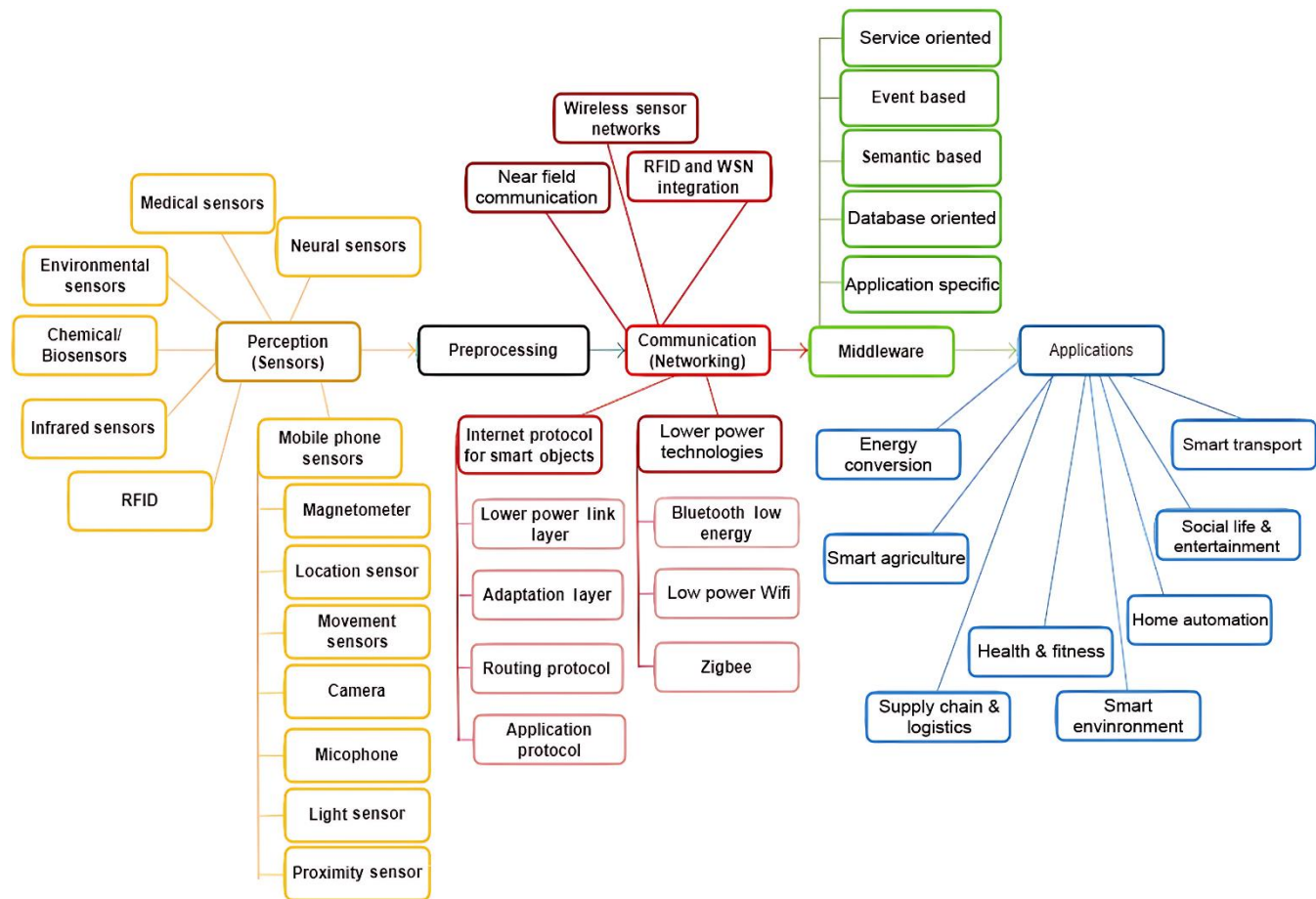


Figure 5. Architectural layer taxonomy of IoT technologies.

4.1. IoT Security Challenges

The rapid expansion of the IoT has exposed various security challenges that need to be addressed. One 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. The most common issues found in IoT devices include insecure network interfaces, inadequate authentication, insecure web services, poor privacy controls, inadequate security configurability, insecure software, and poor physical security [99].

At 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 the 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 and 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]. Internet network extensions from mobile non-IP sensors to cloud and fog computing, multiple entry points, and domain diversity (ownership, policy, and connectivity) add to the list of obstacles [108]. Furthermore, inadequate perimeter protection, host-based detection mechanisms, and patching procedures adapted to the IoT world are also important issues that need to be addressed [109]. Figure 6 shows the cyberattacks to which IoT devices are vulnerable.

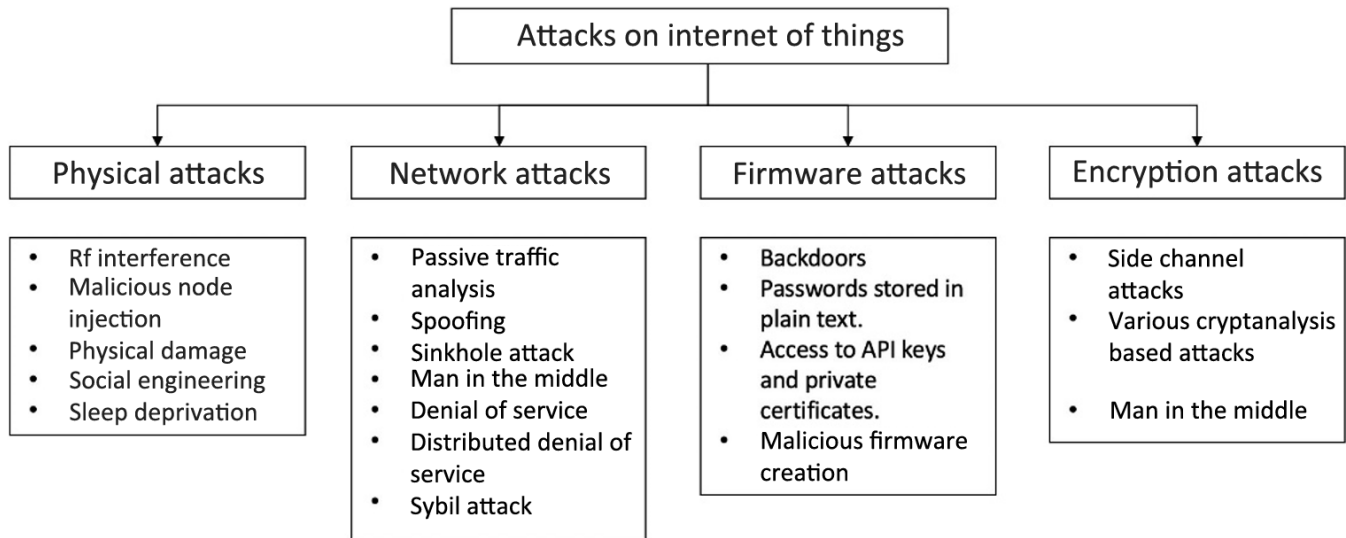


Figure 6. IoT devices are vulnerable to Cyberattacks.

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

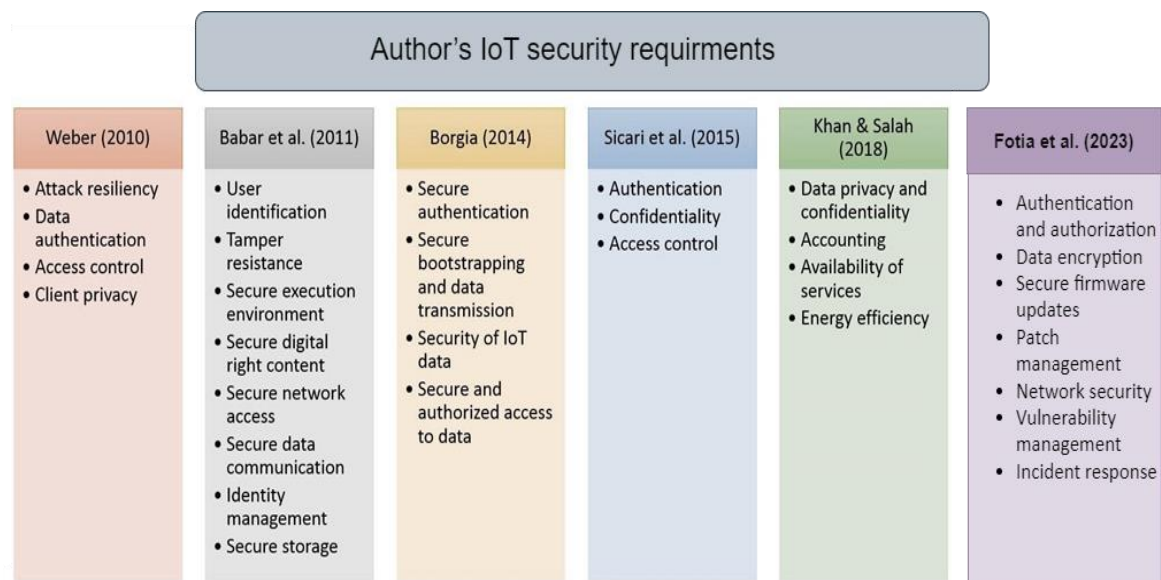


Figure 7. Author's IoT security requirements.

Researchers have proposed various security requirements for IoT devices [110-114]. For example, Lidia et al. [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. Barrera et al. [116] proposed a more detailed and structured set of security requirements based on IoT architectures. However, it is more acceptable to list 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 that are outside the security realm. Figure 7 explains the authors' IoT security requirements, while Table 4 shows the IoT security issues and architectural collaboration 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, and a 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, and availability.
Application	Malware, insecure cloud environments, weak passwords, inadequate security and privacy measures, antivirus software, unsafe software, inaccessible host-based classification and detection, and security education.	Researchers, cloud providers, and security vendors	Secure storage, privacy, secure cloud environments, secure execution environments, and security education programs.

4.2. 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 at the sensing layer [117]. These solutions rely on signal strength, packet transmission efficiency, correction codes, and frequency variation to avoid interference. Similarly, other researchers have developed similar solutions to detect and prevent forgery and spoofing attacks at the sensing layer [118]. In addition, solutions are also being 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 example, researchers have proposed compressed versions of the Authentication Header (AH) and Encapsulating Security Payload (ESP) mechanisms for WSNs [120]. They have also proposed similar IPsec approaches for IPv6 low-power wireless personal area networks (6LoWPAN). However, these approaches may incur energy overheads and increase response times. Researchers have also proposed new authentication and access control methods, such as authentication and ability-based access control (IACAC) [121]. IACAC considers the capabilities of IoT devices when making access control decisions. This approach can enhance 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. Also, Rao and Deebak [123] proposed a password-based

authentication scheme using smart cards and biometrics, with a standby solution in 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 with the cloud. Additionally, Malan et al. [126] proposed a cross-device authentication and key distribution scheme that does not require a central server. [127] has also proposed a context-based authentication and access control scheme that takes into account the fact that IoT devices are often managed by different users in the same location. In a recent study, Hosseini et al. [128] proposed a mutual trust approach that creates a centralized, token-based, object-level access control system has been proposed. Another study Foidl and Felderer [129] proposed a trust model that can calculate the trustworthiness of IoT devices based on various factors. Finally, Ashrif et al. [130] developed a security framework for securing 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 the IoT, including an 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 hop 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 Elsadig [136] proposed a service-oriented architecture that aims to prevent DDoS attacks on the 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 fix the 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 an 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, there are a number of complementary solutions that can improve the reliability and scalability of the system. For example, a recent study [140] proposes using 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 paper [141] presents 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, which can be used for distributed information sharing with other IoT gateways.

At 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, as different controls are required from a management perspective. However, policies must be adapted to the 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 and 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 how it responds to various attacks and resulting failures. Furthermore, some researchers [142] take this approach, proposing Markov models to better understand the results of simulated attacks on the vulnerability or availability of the various components of an IoT infrastructure without causing harm.

The IoT has found a place in the cloud to offload storage and compute capabilities that limited hardware cannot support. This introduces inherent threats and security issues associated with the 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 the challenge as a whole. Additionally, a study [143] has proposed a secure packet forwarding and privacy-preserving framework for cloud-based IoT (considered as a single environment) based on Threshold Credit-Based Incentive (TCBI) and Symmetric Homomorphic Mapping (SHM) encryption for packet forwarding and privacy protection through one-way trapdoor licensing. Furthermore, intrusion detection systems (IDS) and intrusion prevention systems (IPS) help identify and prevent potential 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, as well as scalability issues. However, these systems offer reliability because they have been under intense scrutiny by the security community for a long time; their limitations and shortcomings have been recognized and can be exploited in the right context.

4.3. Blockchain Security Solutions

Blockchain technology is a promising solution for improving authentication and access control in the 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 central trusted authority that can be exploited by attackers. Instead, trust is distributed across a network of nodes, making these systems more resilient to attacks. In addition, 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, FairAccess, and secure

communication within virtual security zones [147]. However, there are still several challenges that need to be addressed before blockchain-based authentication and access control systems can be widely deployed in the 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 control. In addition, blockchain-based systems are typically public, meaning that all access control transactions are visible to anyone [150]. This can be a problem for applications that require confidential access control decisions. Finally, blockchain technology is complex, and it can be 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 we secure IoT devices and networks. As blockchain technology continues to mature and become more scalable, we can expect to see more blockchain-based authentication and access control solutions deployed in the real world.

4.4. Blockchain-Based Security Solutions for IoT

4.4.1. IoT Service Classification

In order to explore different IoT security applications, it is useful to categorize IoT devices by operational domains and communication models. This is because the security requirements of IoT applications differ depending on the domain and model. Khang et al. [152] proposed three operational domains for IoT devices:

- i. Individual and Home.
- ii. Governmental and Utilities.
- iii. Industry and Enterprises.

Moreover, another study has added a fourth domain, which is the intelligent transport systems [153]. Each operational domain has its own unique security requirements. For example, privacy protection is an important security requirement for IoT devices in the individual and family domain, while scalability and collaboration capabilities are more important for IoT devices in the government and utilities domain. Similarly, a study proposed three communication models for IoT devices: device-to-device (D2D), device-to-cloud (D2C), and device-to-gateway (D2G) [154]. D2D is a communication model used when devices communicate directly with each other. However, D2C is the model used when devices communicate with a cloud server, while D2G is used when devices communicate with a gateway device, which then relays the communication to another device or network. However, these communication models are not mutually exclusive. For example, a D2C device can also communicate with other devices using the D2D communication model [155]. When designing IoT security applications, it is important to consider the operational domain and communication model of the devices involved. This will help ensure that the security requirements of the application are met. Table 5 gives the details of the IoT Security Applications Classification.

Table 5. A 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	Helps organizations comply with applicable IoT security regulations and standards.	Policy management systems, audit, and reporting tools
Smart homes security	Protects 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

4.4.2. Blockchain Operational Classification

Blockchain operations can be divided into on-chain and off-chain [156]. On-chain operations are those recorded on the blockchain and visible to all network participants. They typically involve the transfer of value or assets, such as cryptocurrency or tokens. On-chain operations can be further subdivided into state-changing and non-state-changing operations. State-changing operations alter the state of the blockchain, such as creating a new transaction or updating an existing account balance. Non-state-changing operations do not modify the blockchain's state, such as reading a transaction or querying the account balance [157]. Off-chain operations are those that are not recorded on the blockchain and are not visible to all participants in the network. They are typically used to improve the scalability and efficiency of blockchain networks. Off-chain operations can be further subdivided into payment channels, state channels, and layer-two solutions [158]. Payment channels allow participants to make payments to each other without having to broadcast each transaction to the blockchain, while state channels enable participants to execute smart contracts without broadcasting each state change to the blockchain. Layer two solutions, in addition, are protocols built on top of a blockchain to improve its scalability and efficiency.

While on-chain operations offer the benefits of transparency, security, and immutability, they can be slow and expensive to process, especially on popular blockchain networks [159]. In addition, on-chain operations can be used

to track user activity and expose sensitive information. Off-chain operations, on the other hand, offer the benefits of scalability, efficiency, and privacy. However, they can be more vulnerable to attacks than on-chain operations and may lead to centralization of power among the parties involved in the operation [160]. The best type of operation to use depends on the specific application. If security and transparency are paramount, then on-chain operations should be used. If scalability and efficiency are more important, then off-chain operations can be used. Figure 8 shows on-chain and off-chain blockchain consensus.

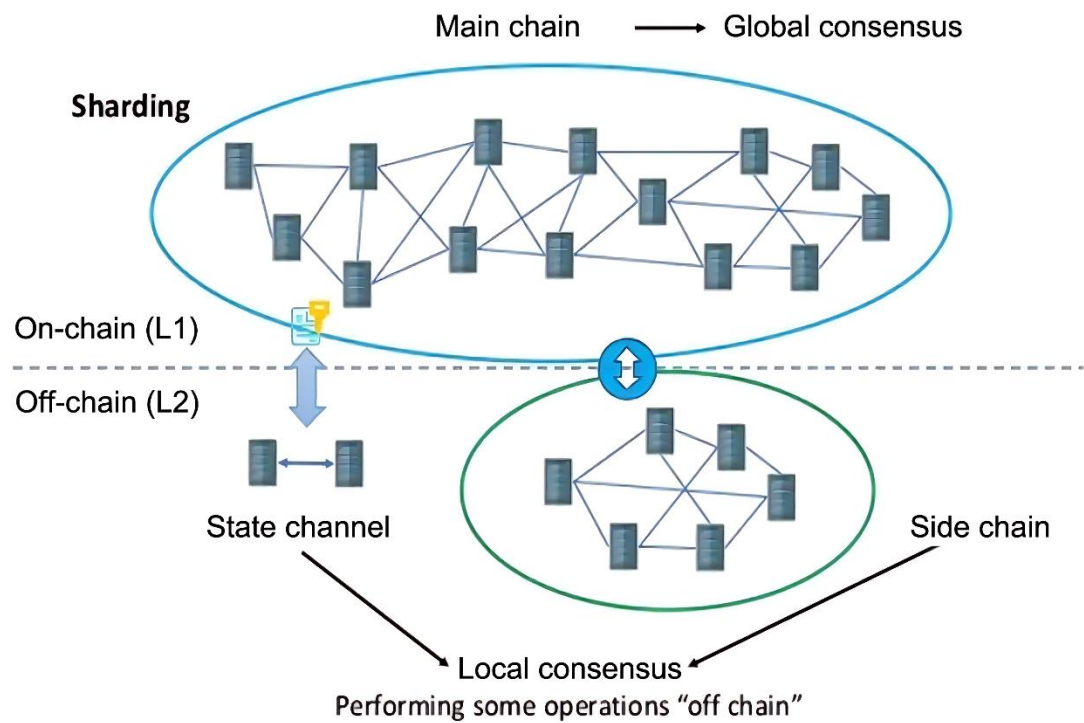


Figure 8. On-chain versus off-chain consensus.

Blockchain technology can also be categorized into three main types based on their accessibility and governance model, as shown in Table 6: public, federated, and private blockchains [161]. Public blockchains are accessible to anyone with an internet connection and allow users to interact with the blockchain without permission. They are secured by a distributed network of nodes that validate transactions and maintain the blockchain ledger.

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

There are several studies on public blockchains that 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 presentation of future research opportunities. Federated blockchains are managed by a pre-selected group of nodes, which can be organizations or individuals. They allow public read access, but write access is restricted to the pre-selected nodes. Studies conducted on federated blockchains are often used by consortia of 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. Private blockchains can be used to implement a variety of enterprise applications such as asset tracking, identity management, and supply chain management [163]. In addition to accessibility and governance, blockchain applications may also differ by platform, customization, and consensus mechanism [164]. Platform refers to the underlying blockchain technology used, such as Bitcoin, Ethereum, or Hyperledger Fabric. Each platform has its own unique features and security characteristics. For example, Bitcoin is known for its security due to its decentralized proof-of-work consensus mechanism, while Ethereum is more flexible and allows the development of smart contracts that can add new security features to applications. Furthermore, customization refers to any modifications or adaptations that have been made to the blockchain platform. These customizations can be made to improve the security of the platform or to add new features and functionality. For example, some organizations may choose to customize the blockchain platform to implement additional security measures, such as multi-signature wallets or access control lists [165]. Consensus mechanism refers to the method used to reach consensus on the state of the blockchain. The most common consensus mechanisms are PoW, PoS, and BFT [166]. Each consensus mechanism has its own strengths and weaknesses in

terms of security. For example, PoW is very secure but can be energy-intensive, while PoS is more energy-efficient but can be more vulnerable to certain types of attacks. Table 7 explains blockchain classification with consensus mechanisms. 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, is presented in Table 7. Furthermore, Table 8. presents the taxonomy of blockchain-based security approaches.

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

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	Relies on cryptocurrency holdings to validate transactions and maintain network consensus.	
Proof-of-authority	Employs trusted nodes with pre-defined 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.	

4.5. Blockchain-Based Security Applications

Blockchain technology holds significant promise for enhancing the security of IoT systems by enabling decentralized, tamper-proof mechanisms for access control, data integrity, and firmware updates. One notable example is the decentralized access control system proposed by Rizzardi et al. [167], which consists of two layers: a

top-level policy management system and a lower layer of IoT devices connected through a blockchain gateway. Due to the limited computational capacity of most IoT devices, this semi-centralized model shifts enforcement to the gateway, though its reliance on the Bitcoin blockchain and wallet-based user interface may introduce scalability and cost concerns. Similarly, Seo et al. [168] proposed a secure firmware update framework involving public key encryption and Bloom filters for verifying firmware authenticity across four key processes. Their STRIDE-based security analysis and Hyperledger simulation demonstrated its practical viability. Building on this, Solomon et al. [169] introduced a blockchain-based framework using Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to enable secure, end-to-end delivery of software updates while minimizing cryptographic burdens on IoT devices. Tong et al. [170] advanced this concept further with a mutual access control protocol supported by a consortium blockchain, integrating anonymous authentication via one-out-of-many proofs and threshold-based cryptographic voting protocols - successfully tested through virtual and physical prototypes.

Expanding beyond access control and updates, Bao et al. [171] developed PBidm, a blockchain-based identity management system tailored for the Industrial IoT, offering immutability, auditability, and privacy preservation. Additional research has uncovered vulnerabilities in over 2,000 embedded devices with backdoors, emphasizing the urgent need for secure architectures [172]. Al Hwaitat et al. [173] responded with a lightweight, permissioned blockchain framework combining homomorphic encryption and optimized data storage. Furthermore, a smart contract-based solution for digital twins on the Ethereum blockchain demonstrated efficiency gains and lower operational costs [174]. To improve authentication while conserving resources, another study proposed a hybrid centralized-blockchain model using a local Ethereum network with favorable performance results [175]. Aliyu and Liu [176] applied blockchain to smart farming, automating security processes via smart contracts and decentralized data management. Other frameworks have integrated AI for precision agriculture, demonstrating performance improvements with models such as Random Forest and SVC [177]. In supply chain contexts, blockchain ensures transparency, integrity, and traceability through smart contracts and group signatures according to Chatterjee and Singh [178]. While interest in blockchain-IoT integration is growing rapidly, key challenges remain, particularly in securing execution environments and improving intrusion detection. With over 75 billion IoT devices expected by 2025 and 125 billion by 2030 [179], addressing these security concerns from both technical and policy angles is increasingly critical.

5. Conclusion

Various solutions, including encryption techniques, access control mechanisms, and intrusion detection systems, have been developed to address these challenges of IoT security. Moreover, blockchain technology offers promising solutions to enhance IoT security by ensuring data integrity, enabling transparent transactions, and facilitating secure communication. Categorizing IoT services and operationalizing blockchain in specific security applications further bolsters the effectiveness of blockchain-based security solutions. As the 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:

- (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) Systematic analyses of the existing limitations, problems, and difficulties associated with implementing blockchain-based security solutions in the IoT context, highlighting 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.

5.1. Recommendations

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

References

- [1] R. Pandey, S. Goundar, and S. Fatima, *Distributed computing to blockchain: Architecture, technology, and applications*. Amsterdam, Netherlands: Elsevier, 2023.
- [2] S. Singh, "Consensus algorithms in blockchain technology: A comparative study," *Asian Journal of Multidimensional Research*, vol. 11, no. 10, pp. 43–48, 2022. <https://doi.org/10.5958/2278-4853.2022.00238.5>
- [3] A. S. Yadav, N. Singh, and D. S. Kushwaha, "Evolution of blockchain and consensus mechanisms & its real-world applications," *Multimedia Tools and Applications*, vol. 82, no. 22, pp. 34363–34408, 2023. <https://doi.org/10.1007/s11042-023-14624-6>
- [4] D. Rushita, K. Sood, and U. S. Yadav, "Cryptocurrency and digital money in the New Era," in digital transformation, strategic Resilience, cyber security and risk management " *Contemporary Studies in Economic and Financial Analysis*, vol. 111B, pp. 179–190, 2023. <https://doi.org/10.1108/S1569-37592023000111B013>
- [5] S. K. Panda, A. R. Sathya, and S. Das, "Bitcoin: Beginning of the cryptocurrency era," in recent advances in blockchain technology: Real-world applications, S. K. Panda, V. Mishra, S. P. Dash, and A. K. Pani, Eds., in Intelligent Systems Reference Library." Cham: Springer International Publishing, 2023, pp. 25–58.
- [6] A. Elaiyaraja, "A revolutionary impact on cryptocurrency. In Emerging insights on the relationship between cryptocurrencies and decentralized economic models." Hershey, PA: IGI Global, 2023, pp. 183–197.
- [7] H. Taherdoost, "Blockchain and machine learning: A critical review on security," *Information*, vol. 14, no. 5, p. 295, 2023. <https://doi.org/10.3390/info14050295>
- [8] O. Ajayi and T. Saadawi, "Blockchain-based architecture for secured cyber-attack features exchange," presented at the In 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud) / 2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 100–107). IEEE. <https://doi.org/10.1109/CSCloud-EdgeCom49738.2020.00025>, 2020.
- [9] N. Kumaran and J. S. S. Mohan, "BRDO: Blockchain-assisted intrusion detection using optimized deep stacked network," *Cybernetics and Systems*, pp. 1–22, 2023. <https://doi.org/10.1080/01969722.2023.2175153>

- [10] N. Sapra, I. Shaikh, and A. Dash, "Impact of proof of work (PoW)-Based blockchain applications on the environment: A systematic review and research agenda," *Journal of Risk and Financial Management*, vol. 16, no. 4, p. 218, 2023. <https://doi.org/10.3390/jrfm16040218>
- [11] P. Peng, S. Ji, Z. Tian, H. Jiang, W. Zheng, and X. Zhang, "Locality sensitive hashing for optimizing subgraph query processing in parallel computing systems," in *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (pp. 1885–1896). Long Beach, CA, USA: ACM.* <https://doi.org/10.1145/3580305.3599419>, 2023.
- [12] N. Balani and P. Chavan, "Design of heuristic model to improve blockchain-based sidechain configuration," *International Journal of Computational Science and Engineering*, vol. 26, no. 4, pp. 372-384, 2023. <https://doi.org/10.1504/IJCSE.2023.132154>
- [13] Y. Zhang, M. Zhao, T. Li, Y. Wang, and T. Liang, "Achieving optimal rewards in cryptocurrency stubborn mining with state transition analysis," *Information Sciences*, vol. 625, pp. 299-313, 2023. <https://doi.org/10.1016/j.ins.2022.12.093>
- [14] Matsuo S., S. Ghesmati, W. Fdhila, and E. Weippl, *Financial cryptography and data security: FC 2022 international workshops: CoDecFin, DeFi, Voting, WTSC, Grenada, May 6, 2022, revised selected papers (Vol. 13412). In lecture notes in computer science.* Cham, Switzerland: Springer International Publishing, 2023.
- [15] H. Arslanian, *The book of crypto: The complete guide to understanding bitcoin, cryptocurrencies and digital assets.* Cham: Springer International Publishing, 2022.
- [16] G. Sun, M. Jiang, X. Z. Khooi, Y. Li, and J. Li, "NeoBFT: Accelerating Byzantine fault tolerance using authenticated in-network ordering," in *Proceedings of the ACM SIGCOMM 2023 Conference (pp. 239–254). New York, NY, USA: ACM.* <https://doi.org/10.1145/3603269.3604874>, 2023.
- [17] Z. Chen, O. M. Gul, and B. Kantarci, "Practical byzantine fault tolerance based robustness for mobile crowdsensing," *Distributed Ledger Technologies: Research and Practice*, vol. 2, no. 2, pp. 1-24, 2023. <https://doi.org/10.1145/3580392>
- [18] S. Ahmadjee, C. Mera-Gómez, R. Bahsoon, and R. Kazman, "A study on blockchain architecture design decisions and their security attacks and threats," *ACM Transactions on Software Engineering and Methodology*, vol. 31, no. 2, pp. 1-45, 2022. <https://doi.org/10.1145/3502740>
- [19] R. Chaganti, V. Varadarajan, V. S. Gorantla, T. R. Gadekallu, and V. Ravi, "Blockchain-based cloud-enabled security monitoring using internet of things in smart agriculture," *Future Internet*, vol. 14, no. 9, p. 250, 2022. <https://doi.org/10.3390/fi14090250>
- [20] A. Fujihara, "Theoretical considerations on Bitcoin scalability problem and block size distribution," in *Proceedings of Blockchain Kaigi 2022 (BCK22) (Vol. 40, Article 011007). JPS Conference Proceedings. Journal of the Physical Society of Japan.* <https://doi.org/10.7566/JPSCP.40.011007>, 2023.
- [21] V. R. Vaddadi, P. V. R. Annepu, N. Gollapalli, A. Challa, S. B. Andhavarapu, and P. K. Botta, "Exploiting cyber threats and protecting cryptocurrencies toward Bitcoin exchanges," presented at the In 2023 5th Biennial International Conference on Nascent Technologies in Engineering (ICNTE) (pp. 1–6). <https://doi.org/10.1109/ICNTE56631.2023.10146649>, 2023.
- [22] A. Goel and G. Suseela, "A step towards blockchain scalability resolution," *Advances in Science and Technology*, vol. 124, pp. 635-643, 2023. <https://doi.org/10.4028/p-6287yh>
- [23] C. E. Castellon, T. Khatib, S. Roy, A. Dutta, O. P. Kreidl, and L. Bölöni, "Energy-efficient blockchain-enabled multi-robot coordination for information gathering: Theory and experiments," *Electronics*, vol. 12, no. 20, p. 4239, 2023. <https://doi.org/10.3390/electronics12204239>
- [24] W. Feng, L. Yang, Z. Qiang, L. Yang, L. Linlin, and Z. Zhiruo, "SoK: Research status and challenges of blockchain smart contracts," presented at the Proceedings of the 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure, Melbourne, VIC, Australia, 2023. [Online]. Available: <https://doi.org/10.1145/3594556.3594620>.
- [25] G. C. Velasco, N. A. P. Vaz, and S. T. Carvalho, "Challenges and opportunities in smart contract development on the ethereum virtual machine: A systematic literature review," in *Workshop on Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain)*, 2023: SBC, pp. 15-28, doi: <https://doi.org/10.5753/wblockchain.2023.756>.
- [26] H. Chu, P. Zhang, H. Dong, Y. Xiao, S. Ji, and W. Li, "A survey on smart contract vulnerabilities: Data sources, detection and repair," *Information and Software Technology*, vol. 159, p. 107221, 2023/07/01/ 2023. <https://doi.org/10.1016/j.infsof.2023.107221>
- [27] A. Junaid, A. Nawaz, M. F. Usmani, R. Verma, and N. Dhanda, "Analyzing the performance of a DAPP using blockchain 3.0," in *2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 19-20 Jan. 2023 2023, pp. 209-213.
- [28] S. A. Wright, "DAOs & ADSs," in *2023 IEEE 15th International Symposium on Autonomous Decentralized System (ISADS)*, 15-17 March 2023 2023, pp. 1-6.
- [29] M. Imamura and K. Omote, "Analysis of the features and structure behind availability in blockchain using altcoin," *IEEE Access*, vol. 10, pp. 98683-98699, 2022.
- [30] A. Sasikumar *et al.*, "A decentralized resource allocation in edge computing for secure iot environments," *IEEE Access*, vol. 11, pp. 117177-117189, 2023.
- [31] B. Galhotra, D. Lowe, and S. Seth, "Blockchain technology in education: The perspective, challenges, and concerns," *Open Access Research Journal of Engineering and Technology*, vol. 5, no. 1, pp. 39-46, 2023. <https://doi.org/10.53022/oarjet.2023.5.1.0075>
- [32] C. G. Kamau and A. Yavuzaslan, "CryptoAudit: Nature, requirements and challenges of Blockchain transactions audit," *African Journal of Commercial Studies*, vol. 3, no. 2, pp. 101-107, 2023. <https://doi.org/10.59413/ajocs/v3.i2.3>
- [33] G. Caldarelli, "Before ethereum the origin and evolution of blockchain oracles," *IEEE Access*, vol. 11, pp. 50899-50917, 2023.
- [34] A. Hamdi, L. Fourati, and S. Ayed, "Vulnerabilities and attacks assessments in blockchain 1.0, 2.0 and 3.0: Tools, analysis and countermeasures," *International Journal of Information Security*, vol. 23, no. 2, pp. 713-757, 2024/04/01 2024. [Online]. Available: <https://doi.org/10.1007/s10207-023-00765-0>
- [35] Q. Wang *et al.*, "Optimal selfish mining-based denial-of-service attack," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 835-850, 2024.
- [36] J. S. Notland, M. Nowostawski, and J. Li, "Runtime evolution of bitcoin's consensus rules," *IEEE Transactions on Software Engineering*, vol. 49, no. 9, pp. 4477-4495, 2023.
- [37] P. Rani, R. K. Sachan, and S. Kukreja, "A systematic study on blockchain technology in education: Initiatives, products, applications, benefits, challenges and research direction," *Computing*, vol. 106, no. 2, pp. 405-447, 2024/02/01 2024. [Online]. Available: <https://doi.org/10.1007/s00607-023-01228-z>
- [38] A. K. Tyagi, S. Dananjayan, D. Agarwal, and H. F. Thariq Ahmed, "Blockchain—internet of things applications: Opportunities and challenges for industry 4.0 and society 5.0," *Sensors*, vol. 23, no. 2.
- [39] X. Tao *et al.*, "Enhancing BIM security in emergency construction projects using lightweight blockchain-as-a-service," *Automation in Construction*, vol. 150, p. 104846, 2023/06/01/ 2023. <https://doi.org/10.1016/j.autcon.2023.104846>
- [40] A. Kumar Jha, "Hybrid consensus mechanism (HCM): Achieving efficient and secure consensus in blockchain networks," Retrieved: <https://ssrn.com/abstract=4413290>. [Accessed 2023.
- [41] T. Zhang and Z. Huang, "FPoR: Fair proof-of-reputation consensus for blockchain," *ICT Express*, vol. 9, no. 1, pp. 45-50, 2023/02/01/ 2023. <https://doi.org/10.1016/j.icte.2022.11.007>
- [42] J. Tang, X. Lu, Y. Xiang, C. Shi, and J. Gu, "Blockchain search engine: Its current research status and future prospect in Internet of Things network," *Future Generation Computer Systems*, vol. 138, pp. 120-141, 2023/01/01/ 2023. <https://doi.org/10.1016/j.future.2022.08.008>
- [43] D. Motwani and S. Sonawane, "Modelling blockchain technology-driven practices to be integrated in fintech for creating reliable business processes," *Scandinavian Journal of Information Systems*, vol. 35, no. 1, pp. 205-220, 2023.
- [44] A. A. Aliyu, "Improving cloud data security by hybridization of zero-knowledge proof and time-based one-time password," *KASU Journal of Mathematical Sciences*, vol. 1, no. 2, pp. 116-126, 2020.
- [45] M. a. Abu-Faraj *et al.*, "Protecting digital images using keys enhanced by 2d chaotic logistic maps," *Cryptography*, vol. 7, no. 2.
- [46] G. Lin, L. Jianbing, Y. Kunlong, and W. Xuesong, "Research on the motion and scattering characteristics of intermittent long chaff," *CHINESE JOURNAL OF RADIO SCIENCE*, vol. 38, no. 1, pp. 114-122, 2023. <https://doi.org/10.12265/j-cjors.2022005>
- [47] R. Solomon, R. Weber, and G. Almashaqbeh, "SmartFHE: Privacy-preserving smart contracts from fully homomorphic encryption," in *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, 3-7 July 2023 2023, pp. 309-331.

- [48] M. Krichen, "Strengthening the security of smart contracts through the power of artificial intelligence," *Computers*, vol. 12, no. 5.
- [49] S. Goel, A. Verma, and V. K. Jain, "CRA-RPL: A novel lightweight challenge-response authentication-based technique for securing RPL against dropped DAO attacks," *Computers & Security*, vol. 132, p. 103346, 2023/09/01/ 2023. <https://doi.org/10.1016/j.cose.2023.103346>
- [50] D. He, R. Wu, X. Li, S. Chan, and M. Guizani, "Detection of vulnerabilities of blockchain smart contracts," *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 12178-12185, 2023.
- [51] S. A. Balobaid, Y. H. Alagrash, A. Hussein Fadel, and J. N. Hasoon, "Modeling of blockchain with encryption based secure education record management system," *Egyptian Informatics Journal*, vol. 24, no. 4, p. 100411, 2023/12/01/ 2023. <https://doi.org/10.1016/j.eij.2023.100411>
- [52] G. Bovenzi, G. Aceto, V. Persico, and A. Pescapé, "Blockchain performance in industry 4.0: Drivers, use cases, and future directions," *Journal of Industrial Information Integration*, vol. 36, p. 100513, 2023/12/01/ 2023. <https://doi.org/10.1016/j.jii.2023.100513>
- [53] N. Peyrone and D. Wichadakul, "A formal model for blockchain-based consent management in data sharing," *Journal of Logical and Algebraic Methods in Programming*, vol. 134, p. 100886, 2023/08/01/ 2023. <https://doi.org/10.1016/j.jlamp.2023.100886>
- [54] G. Sharma and P. Gandhi, "A framework of secured system using blockchain in healthcare industry," in *Proceedings of the Recent Advances in Sciences, Engineering, Information Technology & Management (p. 020003)*. Jaipur, India. <https://doi.org/10.1063/5.0154721>, 2023.
- [55] E. Toufaily, "An integrative model of trust toward crypto-tokens applications: A customer perspective approach," *Digital Business*, vol. 2, no. 2, p. 100041, 2022/01/01/ 2022. <https://doi.org/10.1016/j.digbus.2022.100041>
- [56] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, "Emerging trends in blockchain technology and applications: A review and outlook," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 9, pp. 6719-6742, 2022/10/01/ 2022. <https://doi.org/10.1016/j.jksuci.2022.03.007>
- [57] A. I. Sanka and R. C. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *Journal of Network and Computer Applications*, vol. 195, p. 103232, 2021/12/01/ 2021. <https://doi.org/10.1016/j.jnca.2021.103232>
- [58] L. Marchesi, M. Marchesi, R. Tonelli, and M. I. Lunesu, "A blockchain architecture for industrial applications," *Blockchain: Research and Applications*, vol. 3, no. 4, p. 100088, 2022/12/01/ 2022. <https://doi.org/10.1016/j.bcr.2022.100088>
- [59] P. S. Akshatha and S. M. Dilip Kumar, "MQTT and blockchain sharding: An approach to user-controlled data access with improved security and efficiency," *Blockchain: Research and Applications*, vol. 4, no. 4, p. 100158, 2023/12/01/ 2023. <https://doi.org/10.1016/j.bcr.2023.100158>
- [60] X. Jia, L. Wang, K. Cheng, P. Jing, and X. Song, "A blockchain-based privacy-preserving and collusion-resistant scheme (PPCR) for double auctions," *Digital Communications and Networks*, vol. 11, no. 1, pp. 116-125, 2025/02/01/ 2025. <https://doi.org/10.1016/j.dcan.2023.05.002>
- [61] R. Liu, X. Yu, Y. Yuan, and Y. Ren, "BTDSI: A blockchain-based trusted data storage mechanism for Industry 5.0," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 8, p. 101674, 2023/09/01/ 2023. <https://doi.org/10.1016/j.jksuci.2023.101674>
- [62] T. Guimarães, R. Duarte, B. Pinheiro, D. Faria, P. Gomes, and M. F. Santos, "Blockchain analytics - real-time log management in healthcare," *Procedia Computer Science*, vol. 201, pp. 702-707, 2022/01/01/ 2022. <https://doi.org/10.1016/j.procs.2022.03.094>
- [63] V. Malik et al., "Building a secure platform for digital governance interoperability and data exchange using blockchain and deep learning-based frameworks," *IEEE Access*, vol. 11, pp. 70110-70131, 2023.
- [64] O. H. Abdulganiyu, T. Ait Tchakoucht, and Y. K. Saheed, "A systematic literature review for network intrusion detection system (IDS)," *International Journal of Information Security*, vol. 22, no. 5, pp. 1125-1162, 2023/10/01 2023. [Online]. Available: <https://doi.org/10.1007/s10207-023-00682-2>
- [65] S. Abbas, W. Naser, and A. Kadhim, "Subject review: Intrusion detection system (IDS) and intrusion prevention system (IPS)," *Global Journal of Engineering and Technology Advances*, vol. 2, no. 14, pp. 155-158, 2023. <https://doi.org/10.30574/gjeta.2023.14.2.0031>
- [66] X. M. Han-Vanbastelaer, "Sometimes, you aren't what you do: mimicry attacks against provenance graph host intrusion detection systems," Xueyuan Vanbastelaer, Retrieved: <https://www.vanbastelaer.com/publication/evasion/>, 2023.
- [67] A. A. Aliyu, "Information security: An effective tool for sustainable Nigerian national security and development," in *In Proceedings of the 1st Annual International Conference on Fitayanul Islam Nigeria, Abuja, Nigeria* <https://www.researchgate.net/publication/359369635>, 2022.
- [68] I. Riley, A. Marshall, L. Quirk, and R. Gamble, "An architectural design to address the impact of adaptations on intrusion detection systems," Retrieved: <https://hdl.handle.net/10125/103466>, 2023.
- [69] Understanding the 5 Types of Intrusion Detection Systems, "Understanding the 5 types of intrusion detection systems," helixstorm, Retrieved: <https://www.helixstorm.com/blog/types-of-intrusion-detection-systems/>, 2023.
- [70] C. s. Wu and S. Chen, "A heuristic intrusion detection approach using deep learning model," in *2023 International Conference on Information Networking (ICOIN)*, 11-14 Jan. 2023 2023, pp. 438-442.
- [71] What is Signature-Based Detection? — Techslang, "Techslang — tech explained in simple terms," Retrieved: <https://www.techslang.com/definition/what-is-signature-based-detection/>, 2023.
- [72] What is a Signature and How Can I detect it?, "What is a signature and how can I detect it?," Retrieved: <https://home.sophos.com/en-us/security-news/2020/what-is-a-signature>, 2023.
- [73] S. Al-E'mari, M. Anbar, Y. Sanjalawe, S. Manickam, and I. Hasbullah, "Intrusion detection systems using blockchain technology: A review, issues and challenges," *Computer Systems Science & Engineering*, vol. 40, no. 1, pp. 87-112, 2022. <https://doi.org/10.32604/csse.2022.017941>
- [74] M. Bhavsar, K. Roy, J. Kelly, and O. Olusola, "Anomaly-based intrusion detection system for IoT application," *Discover Internet of Things*, vol. 3, no. 1, p. 5, 2023/05/30 2023. [Online]. Available: <https://doi.org/10.1007/s43926-023-00034-5>
- [75] S. Alem, D. Espes, L. Nana, E. Martin, and F. De Lamotte, "A novel bi-anomaly-based intrusion detection system approach for industry 4.0," *Future Generation Computer Systems*, vol. 145, pp. 267-283, 2023.
- [76] L. Max, W. Markus, S. Florian, H. Wolfgang, and G. Höld, "AMiner: A modular log data analysis pipeline for anomaly-based intrusion detection," *Digital Threats*, vol. 4, no. 1, p. Article 12, 2023. [Online]. Available: <https://doi.org/10.1145/3567675>
- [77] A. Chakraborty, A. Biswas, and A. K. Khan, "Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation." Cham: Springer International Publishing, 2023, pp. 3-25.
- [78] V. S. D. Priya and S. S. Chakkaravarthy, "Containerized cloud-based honeypot deception for tracking attackers," *Scientific Reports*, vol. 13, no. 1, p. 1437, 2023/01/25 2023. [Online]. Available: <https://doi.org/10.1038/s41598-023-28613-0>
- [79] A. Javadpour, P. Pinto, F. Ja'fari, and W. Zhang, "DMAIDPS: A distributed multi-agent intrusion detection and prevention system for cloud IoT environments," *Cluster Computing*, vol. 26, no. 1, pp. 367-384, 2023/02/01 2023. [Online]. Available: <https://doi.org/10.1007/s10586-022-03621-3>
- [80] S. Kably, T. Benbarrad, N. Alaoui, and M. Arioua, "Multi-zone-wise blockchain based intrusion detection and prevention system for iot environment," *Computers, Materials & Continua*, vol. 74, no. 1, pp. 253-278, 2023. [Online]. Available: <http://www.techscience.com/cmc/v74n1/49846>
- [81] E. S. Babu et al., "Blockchain-based intrusion detection system of IoT urban data with device authentication against DDoS attacks," *Computers and Electrical Engineering*, vol. 103, p. 108287, 2022/10/01/ 2022. <https://doi.org/10.1016/j.compeleceng.2022.108287>
- [82] D. Singh, "Internet of things in factories of the future." Hoboken, NJ: John Wiley & Sons, Ltd, 2023, pp. 195-227.
- [83] A. Falayi, Q. Wang, W. Liao, and W. Yu, "Survey of distributed and decentralized iot securities: Approaches using deep learning and blockchain technology," *Future Internet*, vol. 15, no. 5.
- [84] W. Dong, H. Wang, and R. Wang, "A study on the technique for recognizing IoT devices using FTP messages," presented at the In 3rd International Conference on Internet of Things and Smart City (IoTSC 2023) (pp. 190-195). SPIE. <https://doi.org/10.1117/12.2683980>, 2023.

- [85] O. A. Mahdi, A. Alazab, S. Bevinakoppa, N. Ali, and A. Khraisat, "Enhancing IoT intrusion detection system performance with the diversity measure as a novel drift detection method," presented at the In 2023 9th International Conference on Information Technology Trends (ITT) (pp. 50–54). <https://doi.org/10.1109/ITT59889.2023.10184268>, 2023.
- [86] V. A. Memos, K. E. Psannis, and Z. Lv, "A secure network model against bot attacks in edge-enabled industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 7998–8006, 2022.
- [87] K. Taha, "Proactive measures for cyber-physical systems cybersecurity," presented at the In 2023 IEEE International Conference on Cyber Security and Resilience (CSR), 353–358. <https://doi.org/10.1109/CSR57506.2023.10224929>, 2023.
- [88] E. Municio, S. Latré, and J. M. Marquez-Barja, "Extending network programmability to the things overlay using distributed industrial iot protocols," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 251–259, 2021.
- [89] V. Thomas, S. Terence, B. Agrawal, and J. Immaculate, "Internet of things control center," presented at the In 2023 4th International Conference on Signal Processing and Communication (ICSPC) (pp. 225–228). <https://doi.org/10.1109/ICSPC57692.2023.10125704>, 2023.
- [90] P. Wasnik and N. Chavhan, "A review paper on designing intelligent intrusion detection system using deep learning," presented at the In 2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP) (pp. 1–6). <https://doi.org/10.1109/ICETET-SIP58143.2023.10151563>, 2023.
- [91] S. Zhang and D. Cao, "A blockchain-based provably secure anonymous authentication for edge computing-enabled IoT," *The Journal of Supercomputing*, vol. 80, no. 5, pp. 6778–6808, 2024/03/01 2024. [Online]. Available: <https://doi.org/10.1007/s11227-023-05696-0>
- [92] D. Ameyed, F. Jaafar, F. Petrillo, and M. Cheriet, "Quality and security frameworks for iot-architecture models evaluation," *SN Computer Science*, vol. 4, no. 4, p. 394, 2023/05/15 2023. [Online]. Available: <https://doi.org/10.1007/s42979-023-01815-z>
- [93] G. Paolone, D. Iachetti, R. Paesani, F. Pilotti, M. Marinelli, and P. Di Felice, "A holistic overview of the internet of things ecosystem," *IoT*, vol. 3, no. 4, pp. 398–434.
- [94] M. Aaqib, A. Ali, L. Chen, and O. Nibouche, "IoT trust and reputation: A survey and taxonomy," *Journal of Cloud Computing*, vol. 12, no. 1, p. 42, 2023/03/22 2023. [Online]. Available: <https://doi.org/10.1186/s13677-023-00416-8>
- [95] N. A. Askar *et al.*, "Forwarding strategies for named data networking based iot: Requirements, taxonomy, and open research challenges," *IEEE Access*, vol. 11, pp. 78363–78383, 2023.
- [96] R. Santos, G. Eggly, J. Gutierrez, and C. I. Chesñevar, "Extending the IoT-stream model with a taxonomy for sensors in sustainable smart cities," *Sustainability*, vol. 15, no. 8.
- [97] AlahmadiS., P. Rojas, H. Idriss, and M. Bayoumi, "Taxonomy of consumer and industrial IoT," in *SoutheastCon 2023*, 1–16 April 2023 2023, pp. 418–424.
- [98] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. KEBANDE, "A review of security standards and frameworks for iot-based smart environments," *IEEE Access*, vol. 9, pp. 121975–121995, 2021.
- [99] A. H. El-Kady, S. Halim, M. M. El-Halwagi, and F. Khan, "Analysis of safety and security challenges and opportunities related to cyber-physical systems," *Process Safety and Environmental Protection*, vol. 173, pp. 384–413, 2023/05/01/ 2023. <https://doi.org/10.1016/j.psep.2023.03.012>
- [100] V. Kampourakis, V. Gkioulos, and S. Katsikas, "A systematic literature review on wireless security testbeds in the cyber-physical realm," *Computers & Security*, vol. 133, p. 103383, 2023/10/01/ 2023. <https://doi.org/10.1016/j.cose.2023.103383>
- [101] D. Wang, J. Zhou, M. Masdari, S. N. Qasem, and B. T. Sayed, "Security in wireless body area networks via anonymous authentication: Comprehensive literature review, scheme classification, and future challenges," *Ad Hoc Networks*, vol. 153, p. 103332, 2024/02/01/ 2024. <https://doi.org/10.1016/j.adhoc.2023.103332>
- [102] S. Z. Marshoodulla and G. Saha, "An approach towards removal of data heterogeneity in SDN-based IoT framework," *Internet of Things*, vol. 22, p. 100763, 2023/07/01/ 2023. <https://doi.org/10.1016/j.iot.2023.100763>
- [103] B. Kaur *et al.*, "Internet of things (IoT) security dataset evolution: Challenges and future directions," *Internet of Things*, vol. 22, p. 100780, 2023/07/01/ 2023. <https://doi.org/10.1016/j.iot.2023.100780>
- [104] A. Collaguazo, M. Villavicencio, and A. Abran, "An activity-based approach for the early identification and resolution of problems in the development of IoT systems in academic projects," *Internet of Things*, vol. 24, p. 100929, 2023/12/01/ 2023. <https://doi.org/10.1016/j.iot.2023.100929>
- [105] I. Makhdoom *et al.*, "Detecting compromised IoT devices: Existing techniques, challenges, and a way forward," *Computers & Security*, vol. 132, p. 103384, 2023/09/01/ 2023. <https://doi.org/10.1016/j.cose.2023.103384>
- [106] M. A. Sami and T. A. Khan, "Forecasting failure rate of IoT devices: A deep learning way to predictive maintenance," *Computers and Electrical Engineering*, vol. 110, p. 108829, 2023/09/01/ 2023. <https://doi.org/10.1016/j.compeleceng.2023.108829>
- [107] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Zörjen, and B. Stiller, "Landscape of IoT security," *Computer Science Review*, vol. 44, p. 100467, 2022/05/01/ 2022. <https://doi.org/10.1016/j.cosrev.2022.100467>
- [108] J. Gomez, E. F. Kfoury, J. Crichigno, and G. Srivastava, "A survey on network simulators, emulators, and testbeds used for research and education," *Computer Networks*, vol. 237, p. 110054, 2023/12/01/ 2023. <https://doi.org/10.1016/j.comnet.2023.110054>
- [109] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography algorithms for enhancing iot security," *Internet of Things*, vol. 22, p. 100759, 2023/07/01/ 2023. <https://doi.org/10.1016/j.iot.2023.100759>
- [110] R. H. Weber, "Internet of things – new security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010/01/01/ 2010. <https://doi.org/10.1016/j.clsr.2009.11.008>
- [111] S. D. Babar, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Proposed on device capability-based authentication using AES-GCM for internet of things (IoT)," in *Proceedings of the 3rd Springer International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec 2011)*, 2011.
- [112] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014/12/01/ 2014. <https://doi.org/10.1016/j.comcom.2014.09.008>
- [113] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, "Internet of things: Security in the keys," in *Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet '16)*, 129–133. New York, NY, USA: Association for Computing Machinery. <https://doi.org/10.1145/2988272.2988280>, 2016.
- [114] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018/05/01/ 2018. <https://doi.org/10.1016/j.future.2017.11.022>
- [115] F. Lidia, D. Flávia, and G. Fortino, "Trust in edge-based internet of things architectures: State of the art and research challenges," *ACM Computing Surveys*, vol. 55, no. 9, p. Article 182, 2023. [Online]. Available: <https://doi.org/10.1145/3558779>
- [116] D. Barrera, C. Bellman, and P. Van Oorschot, "Security best practices: A critical analysis using IoT as a case study," *ACM Transactions on Privacy and Security*, vol. 26, no. 2, pp. 1–30, 2023.
- [117] M. Jouhari, N. Saeed, M. S. Alouini, and E. M. Amhoud, "A survey on scalable lorawan for massive iot: Recent advances, potentials, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1841–1876, 2023.
- [118] M. S. Akhtar and T. Feng, "A systemic security and privacy review: Attacks and prevention mechanisms over IoT layers," *EAI Endorsed Transactions on Security & Safety*, vol. 8, no. 30, 2022. <https://eudl.eu/doi/10.4108/eetss.v8i30.590>
- [119] V. Kumar and K. Paul, "Device fingerprinting for cyber-physical systems: A survey," *ACM Computing Surveys*, vol. 55, no. 14s, pp. 1–41, 2023.
- [120] F. F. Ashrif, E. A. Sundararajan, R. Ahmad, M. K. Hasan, and E. Yadegaridehkordi, "Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction," *Journal of Network and Computer Applications*, vol. 221, p. 103759, 2024.
- [121] D. Alkunidry, S. Alhuwaysi, and R. Alharbi, "Security Threads and IoT Security," *Journal of Computer and Communications*, vol. 11, no. 9, pp. 76–83, 2023.
- [122] U. Ali *et al.*, "Enhanced lightweight and secure certificateless authentication scheme (ELWSCAS) for internet of things environment," *Internet of Things*, vol. 24, p. 100923, 2023.
- [123] P. M. Rao and B. D. Deebak, "A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions," *Ad Hoc Networks*, vol. 146, p. 103159, 2023.

- [124] X. Meng *et al.*, "A novel multi-party authentication scheme for FCN-based MIIoT systems in natural language processing environment," *ACM Transactions on Asian and Low-Resource Language Information Processing*, 2023.
- [125] J. Chen *et al.*, "DKSM: A decentralized kerberos secure service-management protocol for internet of things," *Internet of Things*, vol. 23, p. 100871, 2023.
- [126] E. Malan, V. Peluso, A. Calimera, E. Macii, and P. Montuschi, "Automatic layer freezing for communication efficiency in cross-device federated learning," *IEEE Internet of Things Journal*, vol. 11, no. 4, pp. 6072-6083, 2023.
- [127] P. More and S. R. Sakhare, "Context-Aware device classification and clustering for smarter and secure connectivity in internet of things," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 10, no. 3, p. 5, 2023.
- [128] S. M. Hosseini, J. Ferreira, and P. C. Bartolomeu, "Blockchain-based decentralized identification in iot: An overview of existing frameworks and their limitations," *Electronics*, vol. 12, no. 6, p. 1283, 2023.
- [129] H. Foidl and M. Felderer, "An approach for assessing industrial IoT data sources to determine their data trustworthiness," *Internet of Things*, vol. 22, p. 100735, 2023.
- [130] F. Ashrif, E. Sundarajan, R. Ahmed, and M. Hasan, "SLAE6: Secure and lightweight authenticated encryption scheme for 6LoWPAN networks," in *Proceedings of the 12th International Conference on Sensor Networks, Online Streaming, --- Select a Country ---: SCITEPRESS - Science and Technology Publications*, 2023.
- [131] J. Ellamathy, "Securing LwM2M with Mbed TLS in contiki-NG," 2023.
- [132] O. Gilles, D. G. Pérez, P.-A. Brameret, and V. Lacroix, "Securing iiot communications using opc ua pubsub and trusted platform modules," *Journal of Systems Architecture*, vol. 134, p. 102797, 2023.
- [133] S. Rana, M. R. H. Mondal, and J. Kamruzzaman, "RBFK cipher: A randomized butterfly architecture-based lightweight block cipher for IoT devices in the edge computing environment," *Cybersecurity*, vol. 6, no. 1, p. 3, 2023.
- [134] N. Krishnamoorthy and S. Umarani, "Implementation and management of cloud security for industry 4.0-data using hybrid elliptical curve cryptography," *The Journal of High Technology Management Research*, vol. 34, no. 2, p. 100474, 2023.
- [135] U. Devi and A. Jacob, "Cryptographic validation of lightweight block ciphers and hash functions," presented at the IEEE International Conference on Public Key Infrastructure and its Applications (PKIA) (pp. 1-10). IEEE, 2023.
- [136] M. A. Elsadig, "Detection of denial-of-service attack in wireless sensor networks: A lightweight machine learning approach," *IEEE Access*, vol. 11, pp. 83537-83552, 2023.
- [137] H. Alrubayyi, "Artificial immune systems for detecting unknown malware in the IoT," Retrieved: <https://qmr.qmul.ac.uk/xmlui/handle/123456789/84686>, 2023.
- [138] M. Hammad *et al.*, "Security framework for network-based manufacturing systems with personalized customization: an industry 4.0 approach," *Sensors*, vol. 23, no. 17, p. 7555, 2023.
- [139] D. Mohamed and O. Ismael, "Enhancement of an IoT hybrid intrusion detection system based on fog-to-cloud computing," *Journal of Cloud Computing*, vol. 12, no. 1, p. 41, 2023.
- [140] R. Qamar, "A study of blockchain-based internet of things," *Iraqi Journal For Computer Science and Mathematics*, vol. 4, no. 1, p. 3, 2023.
- [141] M. Zang, C. Zheng, L. Dittmann, and N. Zilberman, "Toward Continuous Threat Defense: in-Network Traffic Analysis for IoT Gateways," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 9244-9257, 2023.
- [142] X. Zhang, "Prediction of cyberspace security data based on the markov chain model," *Applied Mathematics and Nonlinear Sciences*, vol. 8, no. 2, pp. 2539-2548, 2023.
- [143] D. M. M. Mena, "Blockchain-based security framework for the internet of things and home networks," Retrieved: <https://www.proquest.com/docview/2838330313/abstract/8E92FAC47D9A4EFAPQ/1>, 2021.
- [144] S. Ismail, H. Reza, H. K. Zadeh, and F. Vasefi, "A blockchain-based IoT security solution using multichain," presented at the IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1105-1111). IEEE, 2023.
- [145] Y. Chen *et al.*, "Capability and blockchain-based fine-grained and flexible access control model," *IEEE Network*, vol. 37, no. 6, pp. 197-205, 2023.
- [146] C. Liu *et al.*, "Tbac: A tokoin-based accountable access control scheme for the internet of things," *IEEE Transactions on Mobile Computing*, vol. 23, no. 5, pp. 6133-6148, 2023.
- [147] F. Ghaffari, E. Bertin, N. Crespi, and J. Hatin, "Distributed ledger technologies for authentication and access control in networking applications: A comprehensive survey," *Computer Science Review*, vol. 50, p. 100590, 2023.
- [148] V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, "A review of IoT security and privacy using decentralized blockchain techniques," *Computer Science Review*, vol. 50, p. 100585, 2023.
- [149] C. Mu, T. Ding, M. Yang, Y. Huang, W. Jia, and X. Shen, "Peer-to-peer energy trading based on a hybrid blockchain system," *Energy Reports*, vol. 9, pp. 124-128, 2023.
- [150] M. Luo, J. Zhou, and P. Yang, "RATS: A regulatory anonymous transaction system based on blockchain," *Journal of Parallel and Distributed Computing*, vol. 182, p. 104751, 2023.
- [151] M. H. Tabatabaei, R. Vitenberg, and N. R. Veeragavan, "Understanding blockchain: Definitions, architecture, design, and system comparison," *Computer Science Review*, vol. 50, p. 100575, 2023.
- [152] A. Khang, S. K. Gupta, S. Rani, and D. A. Karras, *Smart cities: IoT Technologies, big data solutions, cloud platforms, and cybersecurity techniques*. CRC Press, 2023.
- [153] J. Sęk, P. Trojanowski, Ł. Gilewicz, B. Gapinski, and A. Evtuhov, *Implementation of intelligent transport systems in an urban agglomeration: A case study*, in *advances in design, simulation and manufacturing VI*, V. Ivanov, J. Trojanowska, I. Pavlenko, E. Rauch, and J. Pitel, Eds., in *Lecture Notes in Mechanical Engineering*. Cham: Springer Nature Switzerland, 2023.
- [154] G. U. Srikanth, R. Geetha, and S. Prabhu, "An efficient Key Agreement and Authentication Scheme (KAAS) with enhanced security control for IIoT systems," *International Journal of Information Technology*, vol. 15, no. 3, pp. 1221-1230, 2023.
- [155] A. Tahir and K. Mashood, "Internet of things and big data in the contexts of education and science," *Pakistan Journal of Educational Research*, vol. 6, no. 2, 2023.
- [156] T. Cai *et al.*, "On-chain and off-chain scalability techniques." Singapore: Springer Nature Singapore, 2023, pp. 81-96.
- [157] B. Yu, L. Feng, H. Zhu, F. Qiu, J. Wan, and S. Yao, "MeHLDT: A multielement hash lock data transfer mechanism for on-chain and off-chain," *Peer-to-Peer Networking and Applications*, vol. 16, no. 4, pp. 1927-1943, 2023.
- [158] J. Wang, Y. Li, A. Tan, Z. Gong, and Y. Wang, "Multi-user on-chain and off-chain collaborative query optimization based on consortium blockchain," in *web information systems and applications*, L. Yuan, S. Yang, R. Li, E. Kanoulas, and X. Zhao, Eds., in *lecture notes in computer science*. Singapore: Springer Nature, 2023, pp. 476-487.
- [159] N. Selvadurai, "Mitigating the legal challenges associated with blockchain smart contracts: The potential of hybrid on-chain/off-chain contracts," *Washington and Lee Law Review*, vol. 80, p. 1163, 2023.
- [160] P. Khobragade and A. K. Turuk, "On-chain off-chain blockchain model for IoT using IPFS," presented at the International Conference on Advanced Computing and Communications (ADCOM 2022) (Vol. 2023, pp. 30-34). IET, 2023.
- [161] N. Afraz, F. Wilhelm, H. Ahmadi, and M. Ruffini, "Blockchain and smart contracts for telecommunications: Requirements vs. cost analysis," *IEEE Access*, vol. 11, pp. 95653-95666, 2023.
- [162] J. Zhu, J. Cao, D. Saxena, S. Jiang, and H. Ferradi, "Blockchain-empowered federated learning: Challenges, solutions, and future directions," *ACM Computing Surveys*, vol. 55, no. 11, pp. 1-31, 2023.
- [163] G. Al-Sumaidae, R. Alkhudary, Z. Zilic, and A. Swidan, "Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare," *Information Processing & Management*, vol. 60, no. 2, p. 103160, 2023.
- [164] K. Saurabh, P. Upadhyay, and N. Rani, "A study on blockchain-based marketplace governance platform adoption: a multi-industry perspective," *Digital Policy, Regulation and Governance*, vol. 25, no. 6, pp. 653-692, 2023.
- [165] S. Mollajafari and K. Bechkoum, "Blockchain technology and related security risks: Towards a seven-layer perspective and taxonomy," *Sustainability*, vol. 15, no. 18, p. 13401, 2023.

- [166] A. K. Yadav, K. Singh, A. H. Amin, L. Almutairi, T. R. Alsenani, and A. Ahmadian, "A comparative study on consensus mechanism with security threats and future scopes: Blockchain," *Computer Communications*, vol. 201, pp. 102-115, 2023.
- [167] A. Rizzardi, S. Sicari, D. Miorandi, and A. Coen-Porisini, "Securing the access control policies to the Internet of Things resources through permissioned blockchain," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 15, p. e6934, 2022.
- [168] J. W. Seo, A. Islam, M. Masduzzaman, and S. Y. Shin, "Blockchain-based secure firmware update using an uav," *Electronics*, vol. 12, no. 10, p. 2189, 2023.
- [169] G. Solomon, P. Zhang, R. Brooks, and Y. Liu, "A secure and cost-efficient blockchain facilitated IoT software update framework," *IEEE Access*, vol. 11, pp. 44879-44894, 2023.
- [170] F. Tong, X. Chen, C. Huang, Y. Zhang, and X. Shen, "Blockchain-assisted secure intra/inter-domain authorization and authentication for Internet of Things," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7761-7773, 2022.
- [171] Z. Bao, D. He, M. K. Khan, M. Luo, and Q. Xie, "PBidm: Privacy-preserving blockchain-based identity management system for Industrial Internet of Things," *IEEE transactions on industrial informatics*, vol. 19, no. 2, pp. 1524-1534, 2022.
- [172] M. Chesser, S. Nepal, and D. C. Ranasinghe, "Icicle: A re-designed emulator for grey-box firmware fuzzing," in *Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis*, 2023, pp. 76-88.
- [173] A. K. Al Hwaitat *et al.*, "A new blockchain-based authentication framework for secure IoT networks," *Electronics*, vol. 12, no. 17, p. 3618, 2023.
- [174] A. Onwubiko, R. Singh, S. Awan, Z. Pervez, and N. Ramzan, "Enabling trust and security in digital twin management: a blockchain-based approach with ethereum and ipfs," *Sensors*, vol. 23, no. 14, p. 6641, 2023.
- [175] O. A. Khashan and N. M. Khafajah, "Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 2, pp. 726-739, 2023.
- [176] A. A. Aliyu and J. Liu, "Blockchain-based smart farm security framework for the internet of things," *Sensors*, vol. 23, no. 18, p. 7992, 2023.
- [177] S. Shreya, K. Chatterjee, and A. Singh, "BFSF: A secure IoT based framework for smart farming using blockchain," *Sustainable Computing: Informatics and Systems*, vol. 40, p. 100917, 2023.
- [178] K. Chatterjee and A. Singh, "A blockchain-enabled security framework for smart agriculture," *Computers and Electrical Engineering*, vol. 106, p. 108594, 2023.
- [179] Z. Qadir, K. N. Le, N. Saeed, and H. S. Munawar, "Towards 6G internet of things: Recent advances, use cases, and open challenges," *ICT express*, vol. 9, no. 3, pp. 296-312, 2023.