2023

A Review of IoT Security and Privacy Using Decentralized Blockchain Techniques

Vinay Gugueoth
University of the Cumberlands

Sunitha Safavat
Howard University

Sachin Shetty
Old Dominion University, sshetty@odu.edu

Danda Rawat
Howard University

Original Publication Citation
Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IoT security and privacy using decentralized blockchain techniques. *Computer Science Review*, *50*, 1-16, Article 100585. https://doi.org/10.1016/j.cosrev.2023.100585

Computer Science Review 50 (2023) 100585

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review article

A review of IoT security and privacy using decentralized blockchain techniques

Vinay Gugueoth [a,*], Sunitha Safavat [b], Sachin Shetty [c], Danda Rawat [b]

[a] Department of Computer and Information Science, University of the Cumberlands, Williamsburg, USA
[b] Department of Electrical Engineering and Computer Science, Howard University, Washington Dc, USA
[c] Department of Computational, Modeling and Simulation Engineering, Old Dominion University, Norfolk, USA

ARTICLE INFO

Article history:
Received 24 January 2023
Received in revised form 2 August 2023
Accepted 14 August 2023
Available online xxxx

Keywords:
Internet of things
Blockchain
Security
Privacy
Consensus protocols

ABSTRACT

IoT security is one of the prominent issues that has gained significant attention among the researchers in recent times. The recent advancements in IoT introduces various critical security issues and increases the risk of privacy leakage of IoT data. Implementation of Blockchain can be a potential solution for the security issues in IoT. This review deeply investigates the security threats and issues in IoT which deteriorates the effectiveness of IoT systems. This paper presents a perceptible description of the security threats, Blockchain based solutions, security characteristics and challenges introduced during the integration of Blockchain with IoT. An analysis of different consensus protocols, existing security techniques and evaluation parameters are discussed in brief. In addition, the paper also outlines the open issues and highlights possible research opportunities which can be beneficial for future research.

Contents

* Corresponding author.
E-mail addresses: vinayg@ieee.org (V. Gugueoth), sunitha.safavat@howard.edu (S. Safavat), sshetty@odu.edu (S. Shetty), db.rawat@ieee.org (D. Rawat).

https://doi.org/10.1016/j.cosrev.2023.100585

1. Introduction

The significance of the Internet of Things (IoT) in the development of smart applications is increasing in recent times. IoT transforms the conventional applications into smart applications by incorporating advanced and sophisticated technologies and thereby helps in improving the productivity and quality of the service. With the increase in the adaptability of IoT systems, the concerns related to the security and privacy of IoT data is also increasing [1]. The smart devices used in the IoT architecture are resource constrained in nature and are vulnerable to various types of security attacks [2]. The IoT devices communicate through a centralized server which increases the risk of single point of failure [3]. Each layer in the IoT architecture suffers from different security issues and hence it is difficult to design a security model considering the heterogeneity of the IoT architecture. In addition to this, the security attacks are getting more sophisticated day by day. Some of the prominent attacks in the IoT architecture are malicious node injection, impersonation, physical attacks, phishing, jamming and data leakage [4]. It requires robust technology to cope with these security attacks. The security system designed to identify these attacks must satisfy the fundamental criteria such as confidentiality, integrity, and availability. Since IoT devices are characterized by the limited storage capacity and high energy consumption, it is not feasible for conventional cryptographic techniques to provide enough security [5]. Designing an efficient security model for IoT is a challenging task considering the continuous evolution of security threats in IoT. This research emphasizes Blockchain technologies for ensuring the security and privacy of IoT data.

1.1. Security threats in IoT

Security is one of the prominent aspects in the design and development of IoT devices. When an attack occurs in IoT devices, all sensors and actuators associated with the device will be compromised. In such cases, it is advised to replace all the sensors and hardware devices [6]. Replacing the compromised devices in real-time applications is not feasible since it is labor intensive and expensive. It is challenging to develop a security architecture which can overcome this limitation using traditional methods such as access control, encryption, user authentication etc. The taxonomy of the security threats in IoT is illustrated in Fig. 1. The security threats in IoT are broadly categorized as access control [7], impersonation attack, eavesdropping attack [8] and denial of service (DoS) and routing attack [9].

1.1.1. Access control

Access control refers to the identity management of the users and authentication of IoT devices. The heterogeneity of IoT devices makes it challenging to provide better access control and maintain the confidentiality of the IoT data. There are three different aspects of access control namely; authorization, confidentiality, and authentication.

- *Authorization:* Authorization is one of the important security parameters which allows the users to access files, services, application data etc. Blockchain based authorization techniques can be used for developing a multi-layered security network and can provide privacy preserving authorization for IoT devices [10].
- *Confidentiality:* Privacy or confidentiality helps in maintaining the privacy of various Blockchain based applications. Blockchain employs different techniques such as symmetric encryption, asymmetric encryption, and tokenization for maintaining confidentiality. Symmetric methods use the same keys for encrypting and decrypting the IoT data and asymmetric methods use different keys for encryption and decryption [11]. On the other hand, tokenization converts the valuable information into digital tokens which can be executed on a Blockchain platform [12]. Advanced encryption standard (AES), Data encryption standard (DES), Triple DES, and Rivest Cipher 4 (RC 4) are the examples of symmetric encryption methods. Correspondingly, Diffie–Hellman, Elliptic curve cryptography (ECC), Digital signature algorithm (DSA), and RSA encryption algorithm are categorized as asymmetric encryption algorithms [13]. For IoT, encryption techniques allow secure communication between two entities and thereby ensure data confidentiality. Though confidentiality is ensured, the risks related to privacy are still an open problem. Implementation of Attribute-based encryption (ABE) techniques [14]is considered as a potential tool for improving the privacy in Blockchain applications [15].
- *Authentication:* The decentralized architecture of Blockchain ensures authentication by default since the nodes and blocks are verified before initiating the transaction [16]. In the authentication process, the node is activated only if it has an appropriate private key for the public key. Since it involves a lot of complexities to develop a robust centralized authentication approach, [17] proposed a decentralized authentication technique called the Bubble of Trust for authenticating the nodes. In this process, a ticket is issued to the nodes for authentication and an encrypted object ID is created using a private key, which is further used for identifying the authenticated nodes.

1.1.2. Impersonation

Impersonation attack occurs when an attacker conceals his identity to access the valuable information [18]. Impersonation attack can be introduced in different forms; by tampering the node, by injecting malicious node into the IoT network, and by introducing man-in-the-middle attack wherein the attacker illegally intercepts and transmits the information communicated between two entities.

- *Node tampering:* Node tampering is an adversarial attack which controls the sensor node via physical attack. Node tampering usually occurs in the physical layer of an IoT system wherein the actual node is modified or exploited by the attackers and is replaced with a malicious node. By replacing the infected node, the attacker tries to gain illegal access to the IoT network [19].
- *Malicious node injection:* In this attack, the intruder attempts to inject a malicious code into the application module and thereby inject compromised information into the database. Due to the injection of malicious code, the nodes carrying the information are also infected and pose a significant threat to the privacy and security of the IoT system [20].
- *Man in the middle (MiTM) attack:* The MiTM attack is the most common attack in IoT applications [21]. MiTM attacks include spoofing and impersonation attacks which disrupt

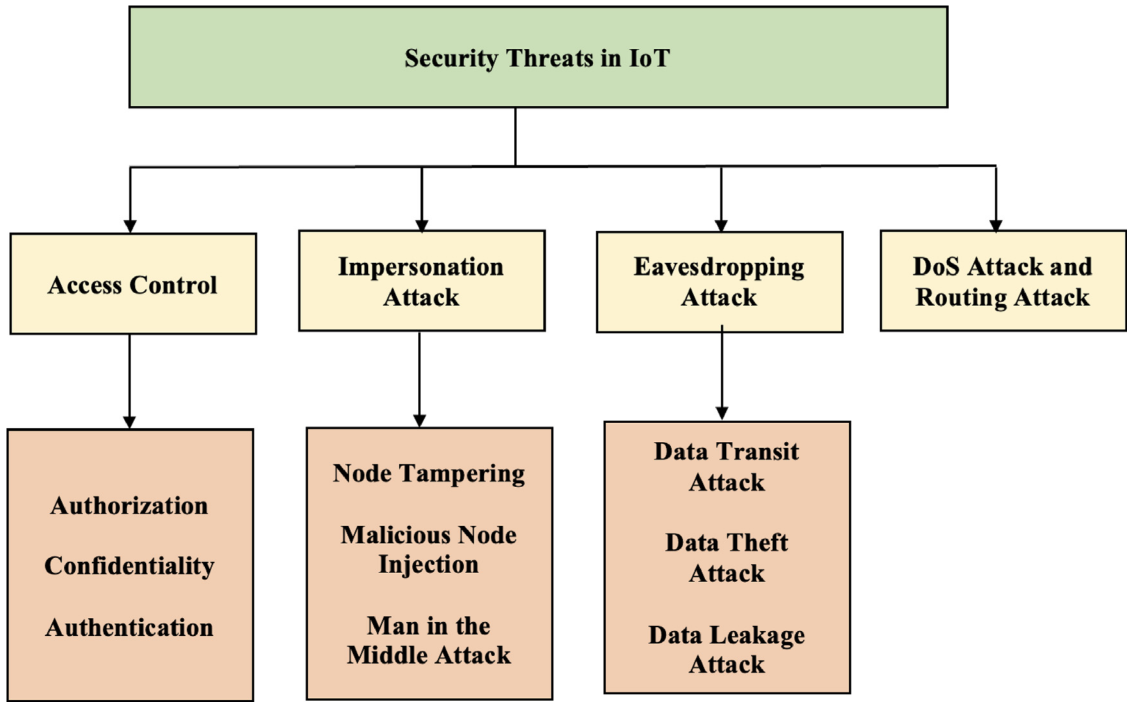

Fig. 1. Block diagram of the proposed framework.

the communication by concealing the identity of the user. For instance, a node A attempts to communicate with end user X while user X might be communicating with the MiTM attackers who impersonate themselves as end user X. This leads to serious security issues since there are high chances of data leakage to the attacker.

1.1.3. Eavesdropping attack

In this type, the attacker attempts to gain illegal access to the network data via device spoofing. Eavesdropping can result in data transit attack, data theft, and data leakage.

- *Data transit attack:* In data transit attack, the intruder attacks the communication channel by monitoring the data packets distributed throughout the network and attempts to exploit it. Sniffing and MiTM attacks are the most commonly occurring data transit attacks.
- *Data theft:* Data theft is an attempt to steal valuable information from the Blockchain network. This can be done by eavesdropping the communication that is carried out between two entities.
- *Data Leakage:* This attack refers to the leakage of confidential data from the Blockchain system to third party entities using a physical or wireless communication channel. Several confidential information such as electronic health records, sensitive user data, personal details, financial transactional data etc can be leaked.

1.1.4. DoS attack

DoS Attack is a serious effort to disturb, corrupt or prevent authentic users from accessing the network data. DoS attacks make the systems more vulnerable towards security threats posing significant challenges to the network security [22]. DoS attacks (single and multiple sources) are straightforward to orchestrate and bring havoc to the target a specific system, the reason being the simplicity in design and user interface, without requiring any significant knowledge or expertise or resource for their functioning. Though DoS attack does not cause any loss in the sensitive data, it can cause significant damage to the system in terms of operational cost.

1.1.5. Routing attack

Routing attacks usually occur in the network layer wherein the attacker injects the affected or compromised nodes which can tamper the routing paths during the communication process. By modifying the routes, the attacker disrupts the entire communication process.

1.2. Blockchain for IoT security

Recently, Blockchain is regarded as one of the most effective technologies which can provide security against various malicious security threats [23,24]. Blockchain provides a decentralized platform for IoT applications which avoids the chances of a single point of failure. In general, Blockchain technology is defiant to data modification. In other words, the changes made in one of the ledgers are distributed to all the nodes participating in the transaction and the modified data is updated in the ledger. Once the transaction is authenticated from all the nodes in the network, it is impossible to modify the transaction without modifying the data in the previous blocks [25]. This nature of Blockchain is termed as immutable and irreversible. Each block in the network is linked with other blocks using a chain and each block contains the hash value of the previous block. The decentralized and distributed nature of Blockchain technology along with cryptographic properties makes it a potential candidate for addressing the security challenges in IoT. However, it is challenging to integrate Blockchain with IoT owing to the challenges such as complexity, high computation cost, throughput and delays. The challenges associated with Blockchain when implemented for IoT are described in Fig. 2 and are discussed in below points.

- *Heterogeneity of IoT devices*: With a system of modest sensors and interconnected things, IoT devices use different communication mediums to interact with other devices. Being the network of different devices, the heterogeneous and distributed nature of IoT devices makes the integration of IoT with Blockchain more complicated and challenging. The heterogeneity of IoT devices poses difficulty in facilitating communication between Blockchain and IoT.

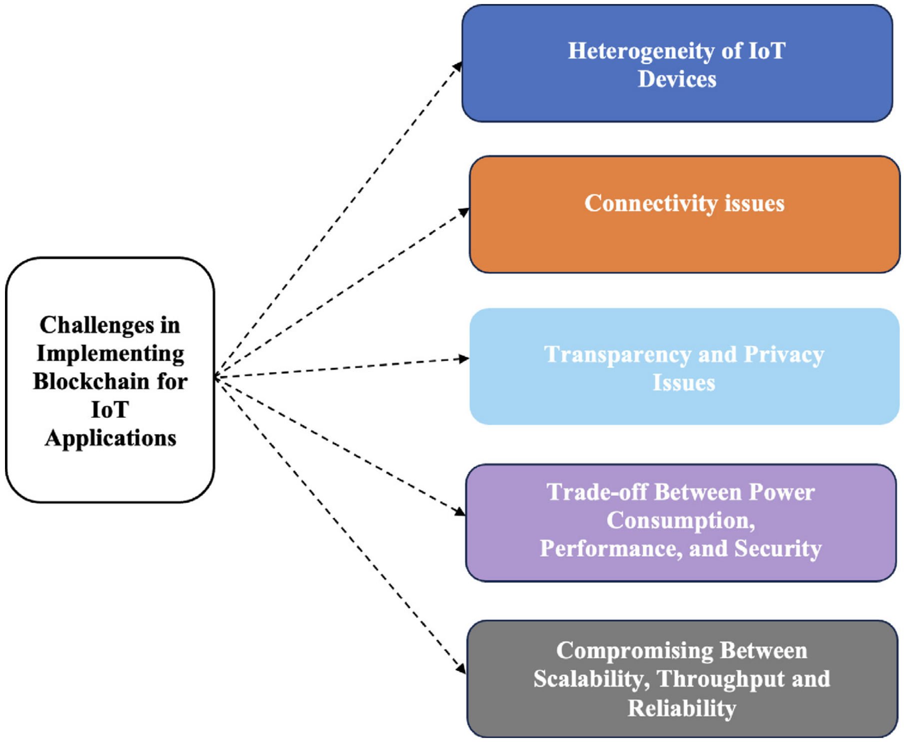

Fig. 2. Challenges of Implementing Blockchain with IoT.

- *Connectivity Issues*: IoT devices are expected to connect with multiple networking systems and share potential information with stakeholders. However, the limited storage capacity makes it difficult to connect these devices with Blockchain for providing new business opportunities and services in different applications [26].
- *Transparency and Privacy Issues*: Blockchain ensures transparency in its transactions. However, in most of the critical applications, it affects the privacy and confidentiality of the users while sharing and accessing data from IoT systems such as healthcare and banking applications [27]. For achieving an appropriate balance between transparency and privacy, it is essential to develop an effective access controlling framework for IoT using Blockchain.
- *Performance, Security, and Power Consumption*: Blockchain algorithms are often characterized with their high computation and high power consumption. This restricts the adoption of Blockchain for resource constrained applications such as IoT and raises the concerns about the performance of Blockchain in processing the IoT data. Researchers have suggested the optimization of Blockchain consensus algorithms to maximize the number of blocks per second and increase the speed of transaction [28,29]. For example, elimination of the proof-of-work (PoW) consensus algorithm can inflate the performance of Blockchain by reducing the power consumption [30]. Conversely, PoW secures the system against vicious threats and Sybil attacks, thereby making the Blockchain platform tamper-proof. This necessitates the need to achieve a balanced tradeoff between the security, performance, and power conversion.
- *Scalability, throughput, and reliability*: There is a continuous streaming of data in IoT systems which increases the concurrency. The complexity of Blockchain cryptography limits the throughput and affects the operational efficiency of the consensus protocols. In addition, the increased number of blocks in a chain demands a higher bandwidth to improve the throughput. However, increasing the throughput might affect the scalability and reliability of Blockchain platforms [31], which is an alarming concern.

1.3. Related works

Integration of Blockchain technology with IoT applications has gained a lot of prominence in recent years with respect to data security and data privacy in networking systems. Blockchain offers a distributed ledger technology which stores the data in blocks. These blocks are connected with each other in the form of a chain that makes it computationally impossible to modify the data stored in the blocks [32]. This nature of Blockchain makes it immutable, decentralized, fault-tolerant, transparent, verifiable, auditable and trustworthy [23,33]. Most commonly, Blockchain platforms are categorized as public, private, and consortium. Public or permission less Blockchain are accessible to everyone [34] and private or permissioned Blockchain are accessible only to verified entities who can validate the transactions and thereby reach a consensus. A novel security and privacy enhancement approach for IoT-based healthcare system is presented in [35]. The study leveraged Blockchain technology for formulating a decision matrix with enhanced security and privacy attributes such as access control, data availability, privacy and anonymity. Results validate the efficacy of the Blockchain based approach provides robust access control and integrity. An advanced Blockchain framework is implemented in [36] which is designed to manage IoT devices and secure their data. The proposed approach is built using a hash function which are independent of large hard forks. It is ensured that the hash code is not modified or tampered and the ephemeral trapdoor along with hash functions prevent the IoT data from being exploited. An enhanced approach for securing healthcare data in IoT systems known as EHDHE is presented in [37]. A Proposed Application (PA) based on Blockchain is implemented for generating, maintaining and validating healthcare certificates. The PA is responsible for establishing a secure communication between the Blockchain platform and end-user

Table 1
List of papers leveraging Blockchain for IoT security.

Reference	Security threats	IoT application	Observations
[39]	Collaborative security, predictive IoT security, and Intrusion-prevention	Internet-of-military things, Wireless sensor networks	Presents different Blockchain based solutions for IoT security
[40]	Denial of Service (DoS), Man in the Middle (MitM) and Sybil attacks	Cryptocurrency	Analyses the challenges and issues associated with the implementation of Blockchain for IoT
[41]	Attacks to end devices, attacks to communication channels, attacks to network protocols, attacks to sensory data, DoS attack and software attacks	Multiple applications	Discusses the layer-wise attacks in IoT and corresponding Blockchain solutions along with issues such as programming fraud, vulnerability of smart contract, and leakage of private key
[42]	Denial of Service (DoS) attacks, DDoS attacks and Access control	Multiple applications	Identifies the current challenges faced by the centralized IoT models and outlines the recent advancements done in Blockchain based decentralized models
[43]	Privacy concerns due to third party management, single points of failure, and firmware attacks	Cloud IoT, Fog IoT, and Smart IoT devices	Outlines the recent advancements and potential solutions for Blockchain in cloud and fog based IoT applications and centralized cloud servers

Table 2
Blockchain mechanisms for IoT Security.

Security areas in IoT	Proposed solutions	Blockchain features
Access control	[44]	Blockchain based decentralized public key infrastructure (PKI)
	[45]	Certificate revocation and status verification system
	[46]	Fortified chain and selective ring based access control (SRAC)
	[47,48]	Smart contracts for access control
	[49,50]	Attribute-based access control, Blockchain managers for access control
Data integrity	[51]	Bilinear mapping based Data Integrity Scheme
	[52]	EC-ElGamal, Bilinear pairing, and signature verification for preserving data integrity
	[53]	A Trusted Consortium Blockchain (TCB) for securing the integrity of big data
	[54]	Blockchain based third party auditing scheme.
	[55]	Distributed edge computing architecture
Data confidentiality	[56]	Interplanetary File System (IPFS) for storing and streaming IoT data
	[57]	Yugula- A Blockchain based encrypted cloud storage for storing IoT data
	[58]	A hash value generating encryption system for encrypting the IoT data.
	[59]	Blockiotintelligence — Blockchain with artificial intelligence
Data availability	[60]	AutAvailChain — Automatic and secure data availability in Blockchain.
	[61]	Blockchain infrastructure using LoRa and Ethereum

applications such as hospitals and medical centers. The PA used in this research creates and verifies healthcare certificates and strengthens the access control using smart contracts. A systematic review of privacy challenges related to IoT-based Blockchain is discussed in [38]. The review states that the Blockchain can overcome the complexities associated with data security and privacy. In addition, Blockchain can also ensure distributed storage, trustworthiness, and transparency which are essential parameters for IoT systems. However, Blockchain-based solutions are characterized by low scalability, high overhead bandwidth and computational complexity. Several survey papers have been published highlighting the significance of Blockchain technologies. The list of survey papers and existing Blockchain mechanisms for IoT security and privacy leveraging Blockchain are presented in Tables 1 and 2 respectively.

Several security frameworks have been proposed in existing literary works to ensure data security and privacy in IoT. [61] investigated the types of security attacks in IoT systems. It was observed that the sensitive data stored in the distributed storage service was tolerant to the faults and attacks such as distributed denial of service (DDOS) attacks in the network systems. The data management system was developed using a decentralized Blockchain network which employs LoRa network service providers as the networking mechanism and was executed using the Ethereum platform. The proposed approach ensured robust data security with minimized security risks. An empirical analysis on the integration of IoT with Blockchain was presented by [62]. The preliminary aim of this review is to outline the current approaches that use Blockchain technology for security of IoT systems. The current trends incorporate the concept of blockchain to integrate with IoT devices and techniques. This paper covers various domains and organizes the previous works based on the applications. An IoT based blockchain technology was proposed by [63] to enhance the data security mechanisms in the decentralized IoT environment. The main concern addressed in the study is data transparency which plays an important role in forensic investigation to validate the authenticity of the image information. Several Blockchain based IoT security are discussed in Table 3.

The main contributions of this research are summarized as follows:

- This survey presents a detailed analysis of Blockchain, types of Blockchain platforms, and consensus algorithms. The security characteristics, analysis of different consensus algorithms is investigated in detail.
- This paper discusses the integration of Blockchain for IoT, the advantages, challenges, and different techniques used for the security evaluation of IoT.
- A brief overview of different evaluation parameters such as latency, communication and computation overhead, storage

Table 3
Taxonomy of existing IoT security solutions based on Blockchain.

References	Threat	Application	Blockchain used	Blockchain type	Consensus	Security	Limitations
[64]	Data integrity	Cyber physical system	Ethereum	Public	Proof of trust	Data security and key management	User security is not addressed
[65]	Man in the middle attack (MITM)	Logistics	Ethereum	Public	Proof of delivery	Key management	Process is less secure since it does not address user security and data security
[66]	DDoS, ICMP flooding, and TCP flooding	Software Defined Networking (SDN)	Ethereum	Public	NA	Attack detection	Data privacy and user security are not addressed
[67]	MITM, Impersonation, and replay attacks	Internet of Intelligent Things (IoIT)	Bitcoin and Litecoin	Public	Proof of work	Key management	High storage, communication and computation cost
[68]	Transaction validation and security	Software Defined Networking (SDN)	Ethereum	Public and Private	Proof of work	Key management	The model is not suitable for handling uncertain, time-varying, and complex functionalities
[69]	Access control system	Fabric-IoT	Hyperledger Fabric	Private	Proof of work	Data security and privacy	Scalability and Reliability are not addressed
[70]	Privacy preservation	Healthcare systems	Hyperledger Fabric	Permissioned	Proof of authority	User privacy, Data integrity and Security	The scalability of Blockchain is questionable
[71]	Confidentiality, Integrity and Authorization	Smart homes	Hyperledger Fabric	Private and permissioned	NA	User security and Data security	Consensus protocols are not used to identify complex smart home settings and security threat scenarios

overhead, storage cost, scalability etc. is presented with an emphasis on performance evaluation of Blockchain.

- The challenges related to security and privacy in the Blockchain-IoT paradigm are listed along with open issues and future directions.

2. Overview of Blockchain

This section will provide a comprehensive analysis of Blockchain technology which includes the functioning of Blockchain along consensus algorithms and different Blockchain based security techniques such as P2P network, smart contracts, encryption, and cryptography based methods. One of the prominent characteristic abilities of Blockchain is its ability to form a decentralized P2P network and it is crucial to understand the mechanism involved in the P2P network formation which makes use of different consensus algorithms/protocols. This section outlines different aspects of Blockchain technology such as workflow of the Blockchain process, types of Blockchain, different consensus algorithms and its security characteristics. These aspects provide a clear analysis of the Blockchain mechanism and helps in understanding the concept of Blockchain and its corresponding feature while implementing for a specific application.

2.1. Functioning of Blockchain

The concept of Blockchain technology was developed based on Distributed Ledger Technology (DLT). Blockchain works on interlinking of devices and data transactions in the clusters. In general, Blockchain consists of a series of time stamped transactions which are controlled using advanced algorithms [25]. Every single entity participating in the transaction is called a node and each node in the sequence consists of the same data and is called a digital ledger. The nodes in the Blockchain network store the transactional details in the form of multiple consecutive blocks and use a common algorithm to reach consensus [72]. Each transaction is stored in the nodes in a distributed P2P network and each block will have details of the transaction such as timestamp, hash value of the previous block, nonce value, version number and merkle root. Version number helps in tracking the updates and changes made during the transaction. Nonce is an arbitrary value used by the miners during mining and hash is a cryptographic function which helps in securing the transaction [73]. On the other hand, timestamp is employed for understanding the occurrence of a particular transaction and Merkle root is obtained via hashing. A P2P network is created along with the users while implementing the Blockchain technology wherein the communication between users and platform is carried out through Blockchain [73]. Two keys namely private and public keys are used for communicating wherein public key can be accessed by all and private key is disclosed only to authorized entities in the network. In other words, a private key is used as the signature of the user to access the transactional information. The security of the data is ensured using cryptography methods [74] which prevents unverified access and data tampering using private keys. Any transaction in Blockchain is initiated by the nodes after securing it with a private key and the transactional information is published to the peer nodes after verification. Verification is carried out using different consensus algorithms or protocols which are designed to serve different objectives [75]. After verification, the miners collect the details of the transaction for creating a block and each block is provided with a unique timestamp and ID

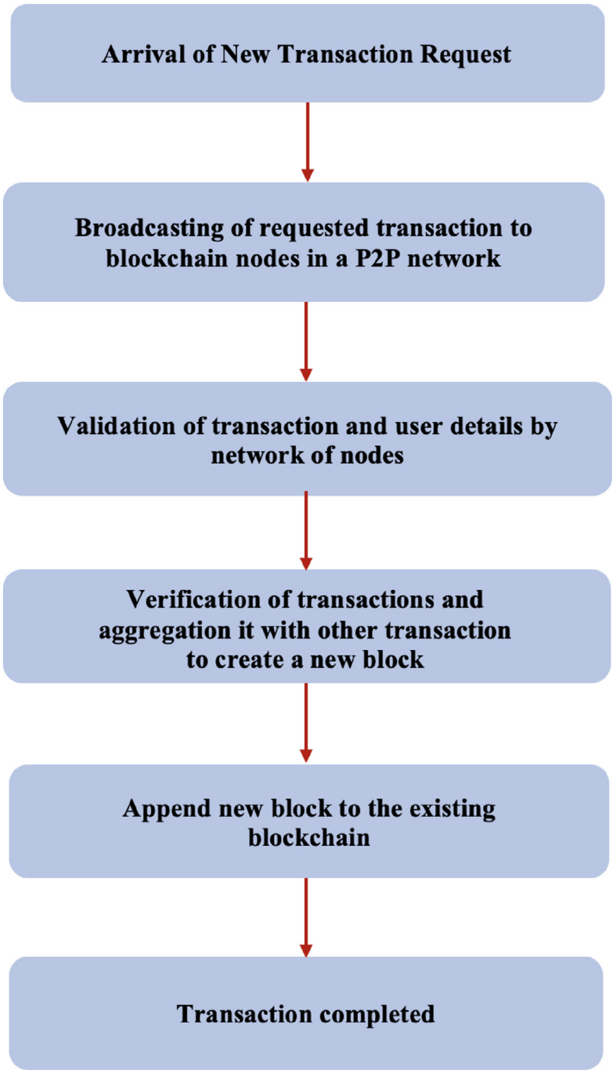

Fig. 3. Workflow of the Blockchain Process.

(hash value) to prevent any modification. The block which is created gets included in the Blockchain and the newly added block is linked to previous blocks using hash value and this process continues until all the blocks are added into the network [76]. The fundamental workflow of the Blockchain process is illustrated in Fig. 3.

2.2. Classification of Blockchain platforms

In general, Blockchain is categorized into three types namely public, private, and hybrid or consortium Blockchain [77]. They are categorized based on their ability to give permission to the users for interacting with the Blockchain network.

- *Public Blockchain:* They are also called permission less Blockchain since they allow all entities to participate in the transaction. The cost of transaction in public Blockchain is lesser compared to private because of the incentive based mining process which motivates the miners to mine blocks. However, public Blockchain require more time to complete a transaction compared to private Blockchain due to lack of connectivity among the peer nodes [77]. Some of the prominent examples of public Blockchain are Ethereum, Bitcoin, and Litecoin.
- *Private Blockchain:* These Blockchain are also called as permissioned Blockchain wherein the identity of each miner node is known. This ensures that only selected and verified minor nodes are allowed to participate in the transaction. Since only authorized users are given access to the transaction data, the security, confidentiality and privacy of the user information is strengthened compared to private Blockchain platforms [78]. Multichain [79], Quorum are examples of private Blockchain.
- *Consortium Blockchain:* Consortium Blockchain are hybrid Blockchain which combine the characteristics of both public and private Blockchain [80]. Consortium Blockchain are advantageous because of semi-decentralized nature with a multi-party consensus attribute which selects unique predefined nodes for carrying out a particular transaction. These nodes are managed by a specific group of entities which are also responsible for managing the transactions in a supervised manner [81]. Ethermint and Hyper ledger Fabric are some of the examples of hybrid or consortium Blockchain.

The comparison of different types of Blockchain are discussed in Table 4 [78–82].

2.3. Consensus algorithms

Consensus algorithms are an integral part of the Blockchain technology which are responsible for maintaining the integrity, confidentiality, and security of the Blockchain platform. Consensus algorithms help the Blockchain to reach a common agreement despite differences in their operational process. Consensus algorithms are different for different Blockchain. The most prominent consensus algorithms are illustrated in Fig. 4 and are discussed in below points.

1. *Proof of Work (POW):* PoW is the widely used consensus algorithm for Blockchain technology. In this mechanism, the miner solves the mathematical computations on the new block before validating the block to the ledger [83].
2. *Proof of stake (PoS):* PoS is an alternate mechanism for PoW. It requires less number of computations for mining compared to PoW, and in PoS, the creator of a new block is selected depending on its wealth (stake) [84]. There is no block reward in PoS, and the miners charge transaction fees. Delegated PoS and Leased PoS are the types of PoS whose voting process makes them more democratic than PoS.
3. *Byzantine fault-tolerant (BFT):* BFT consensus is used in case of Byzantine failure [85]. This mechanism uses 'general concept' wherein, the general manages the current information status. The message received by the general undergoes a computation process. In this process, every individual general is asked to provide feedback on the message, and after the conclusion, the general shares the decision with other generals in the system. The subclasses of BFT are categorized as pBFT (Practical Byzantine fault-tolerant) and dpBFT as shown in Fig. 4.
4. *Proof of Authority (PoA):* PoA is considered as an advanced alternative for PoW and PoS. PoA is faster and achieves consensus based on the identity as a stake [86]. Proof of Authentication (PoAh) [87] is a type of PoA which helps in authenticating the blocks after following the fundamental consensus algorithm.
5. *Proof of Elapsed Time (PoET):* PoET is the most popular choice for permissioned Blockchain. PoET is advantageous because of its permissioned Blockchain network where permission from the Blockchain is required to access the network [88]. Proof of Bandwidth is similar to PoET which reaches consensus based on relay bandwidth.

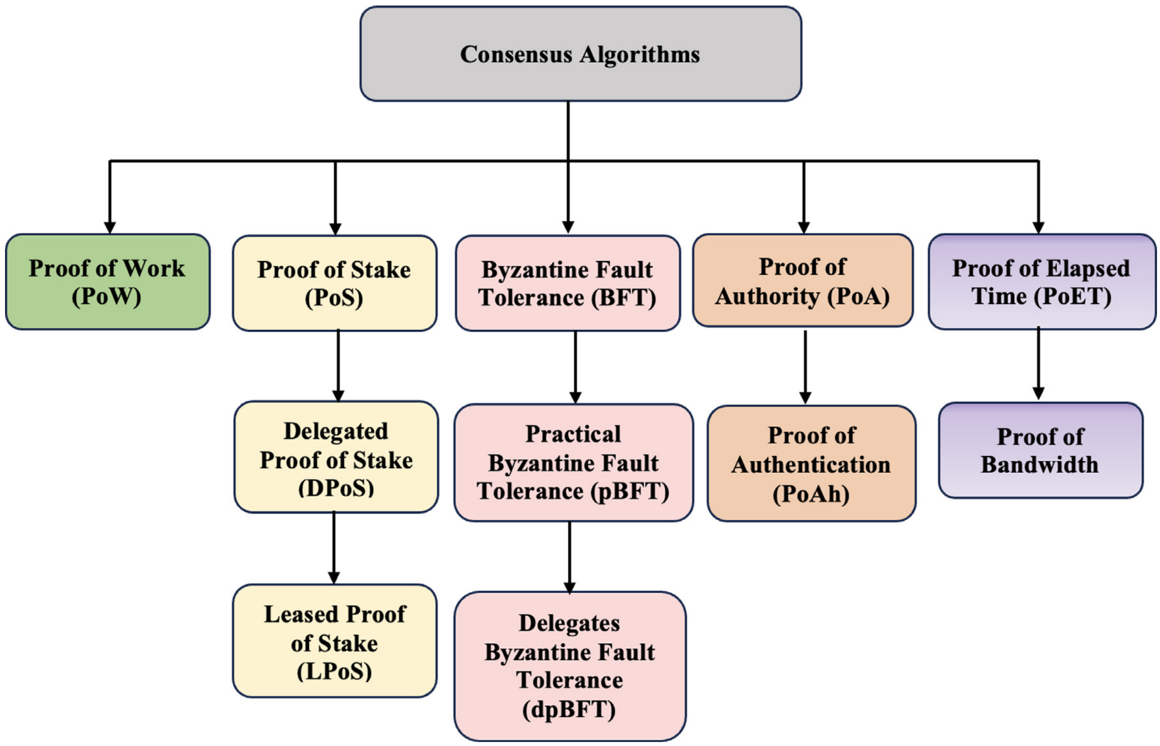

Fig. 4. Taxonomy of consensus algorithms.

Table 4
Comparison of Blockchain types.

Features	Public Blockchain	Private Blockchain	Consortium Blockchain
Architecture	Completely decentralized	Partially decentralized	Partially decentralized
Permission	Permission less	Permissioned	Permissioned
Security	Low	Moderate	High
Consensu	PoW, PoS	Ripple	PoA, PBFT, PoET
Immutability	Immutable	Can be modified	Partially immutable
Flexibility	Low	High	High
Throughput	Less	High	High
Execution speed	Slow	Fast	Fast
Traceability	Completely traceable	Completely traceable	Partially traceable
Efficiency	Low	High	High

Table 5
Comparison of different consensus algorithms.

Consensus algorithms	Blockchain type	Scalability	Latency	Throughput	Suitability for IoT
PoW	Permission less	High	High	Low	Low
PoS	Permissioned and Permission less	High	Medium	High	Medium
DPoS	Permissioned and Permission less	High	Medium	High	Medium
LPoS	Permission less	High	Medium	Low	Low
PBFT	Permissioned	Low	Low	High	High
PoA	Permission less	High	Medium	Low	Low
PoET	Permissioned and Permission less	High	Low	Medium	High

Additionally, the comparison of different types of consensus algorithms are discussed in Table 5

2.4. Security characteristics

Blockchain incorporates three main security characteristics that makes it a potential candidate for providing security to IoT systems. The security characteristics are broadly categorized as follows: P2P network, smart contract, and cryptography [89–91]. These characteristics provide an automated, efficient, robust, reliable, and secure Blockchain platform for IoT security. A brief overview of these characteristics are discussed as follows:

- *P2P network:* A distributed P2P network allows communication between the peer nodes and helps the nodes to self-organize themselves to complete a particular task. Blockchain platforms employ a resilient, balanced and decentralized P2P network instead of adopting a fundamental centralized client–server architecture which is susceptible to malicious attacks [92]. A P2P network manages the interactions between different entities related to how and when to carry out transactions, number of participants, payment, and settlement etc.
- *Smart Contract:* Smart contracts are defined as the set of digital agreements which allows the execution of specific tasks among multiple users in the Blockchain. In smart contracts,

all the transactional details, conditions, and obligations of both the parties are defined clearly. After satisfying all the conditions, the contract will be executed automatically and once it is executed it cannot be altered or modified [93]. Blockchain implements smart contracts without the involvement of any third-party entity. These characteristics make it suitable for several information-sensitive applications such as IoT, finance, supply chain and healthcare systems.
- *Cryptography:* Cryptography is a method for securely transmitting data against unauthorized attackers. Encryption and decryption are the two primary cryptographic operations. Before delivering the image data to the receiver, it is encrypted to safeguard the information, and the encrypted data is decrypted and the data is restored to its original state. The two primary forms of encryption used in cryptography are symmetric and asymmetric [94]. Private key or symmetric encryption refers to cryptographic techniques that use the same key for encryption and decryption, while public key or asymmetric encryption refers to cryptographic techniques that use a separate key for encryption and decryption. [95]. The prominent elements of cryptography are key management, identity management, user security, trusted hardware, and advanced digital signatures.
- *Distributed Ledger:* Blockchain is characterized by its distributed ledger technology (DLT). Unlike conventional techniques which use centralized database operations such as addition and deletion of data, querying, modification etc, Blockchain allows only two operations namely adding and querying. In DLT based Blockchain, the data is analyzed using different data structures. This allows the Blockchain system to ensure privacy, integrity, and authenticity [96]. In addition, DLT also helps Blockchain to achieve data provenance. This helps in strengthening the security of Blockchain algorithms. The distributed ledger also increases the fault tolerance ability of Blockchain and makes them resilient to adversarial threats and attacks [96]. Furthermore, DLT in Blockchain also helps the system to achieve consensus without requiring any third party entity even in a byzantine environment.

3. Integration of Blockchain with IoT

Blockchain technology has the potential of transforming the centralized IoT systems. Blockchain is used to develop a secured, trusted and decentralized autonomous IoT network system for enhancing the reliability, stability and security of the IoT infrastructure and its applications, especially for analyzing the data transmission in IoT networks. With the integration of IoT and Blockchain, the security level can be strengthened significantly due to high immutability [97] and resilience to security attacks.

3.1. Need for integration

The complexities associated with IoT such as heterogeneity, resource constraintment, high vulnerability to adversarial attacks, privacy and confidentiality issues can be resolved using Blockchain [98]. The Blockchain-IoT integration offers various advantages which are discussed in below points:

- *Enhanced security:* A huge amount of data is collected from the IoT devices which needs to be secured using Blockchain since it can secure the data using encryption and cryptography methods. In addition, the integration of Blockchain and IoT facilitate the automatic update software's in IoT systems without compromising on security and privacy of IoT system data. By ensuring the security, the integration also minimizes the risk of security breaches and hence strengthens the immunity of the IoT system [99]. The work mentioned in [100] proposed a novel group theory (GT)-based binary spring search (BSS) algorithm which incorporates a hybrid deep neural network model. A Blockchain based privacy preservation approach is designed to detect unauthorized intrusions in the IoT systems. Securing patient information is a crucial factor in cryptographic applications which ensures the security of IoMT. The proposed approach enables the users to encrypt the patient information and upload it to the distributed ledger without relying on the Blockchain manager. A novel chaotic encryption technique based on IoT-Blockchain architecture is implemented in [101] to ensure security and privacy of IoT data. The proposed technique is evaluated using different IoT sensor data with respect to different evaluation metrics such as Number of Pixel Change Rate (NPCR), Unified Averaged Changed Intensity (UACI), Correlation Coefficients, and entropy under different attack scenarios. Results show that the chaotic encryption method achieved a NPCR and UACI values of 99.65% and 34% respectively. Results ensure that the proposed architecture effectively mitigates the security attacks in IoT.
- *Enhanced interoperability:* Consequently, Blockchain can offer improved interoperability in IoT networks by recording user and transaction information into Blockchain. The decentralized Blockchain platform allows the transformation, processing, mining and modification of different types of IoT datasets and helps in establishing secure communication between multiple platforms or applications [99]. The research work presented in [102] proposed a hierarchical Blockchain platform to enhance the integrity of the IoT data along with Blockchain interoperability. A decentralized Blockchain-of-Blockchains (BoBs) is introduced to simultaneously ensure the integrity and interoperability. The proposed approach is implemented using a Hyperledger Fabric and Ethermint for analyzing the potentiality of this concept.
- *Automatic interactions:* Majority of the IoT devices are capable of interacting automatically with other devices. This excellent feature can be enhanced and secured using Blockchain technology. Blockchain allows autonomous interaction using a Decentralized Autonomous Corporations (DACs) [103] which prevents the involvement of traditional agencies and entities. DACs are accompanied with smart contracts and are capable of working automatically. Since they do not require any manual intervention, the cost of implementation can be reduced significantly. Automatic interaction can be advantageous for IoT systems to adopt device-agnostic applications.
- *Reliability:* In general Blockchain is said to be highly reliable. Reliability plays an important role in Blockchain-IoT applications since it validates the effectiveness of the distributed network which can authenticate the information and ensure that the data has not been tampered. Along with reliability, the integrated Blockchain-IoT framework can also ensure the traceability and accountability of IoT sensor data.
- *Secure Code Deployment:* The secure and safe deployment of code for IoT systems can be benefitted from the immutable nature of Blockchain. This attribute assists the IoT system in updating the software's from different sources in a secured manner [104].
- *Traceability:* Traceability allows the users to access, verify, and validate the data whenever they want. All transactions stored in Blockchain are traceable and hence ensures the easy availability of the required information [105].
- *Service Market:* : Service market enables the transactions between multiple entities without depending on any centralized authority. The independence increases the speed

Table 6
Challenges in the integration of Blockchain with IoT.

References	Key areas	Challenges
[106,107]	Data security	Susceptibility to attacks such as MITM and eavesdropping Resource constrainment makes IoT susceptibility to attacks Risk of service rejection Risk of corrupt data entering the chain.
[108]	Consensus algorithms	Incompatibility of IoT devices to different consensus algorithms Complexity of implementation
[109]	Smart contracts	Difficulty in verifying and validating the smart contracts Complex data retrieval process can overburden smart contracts Require more number of resources for processing large scale IoT data
[110,111]	Scalability and Storage capacity	Generation of huge amount of data from IoT devices Require advanced and sophisticated techniques for processing, and normalizing the data
[112]	Anonymity and Privacy of IoT data	Issues related to privacy can increase the complexity of the Blockchain operation Security can be compromised. Limited availability of computation resources due to lack of economic feasibility
[113]	Legislative problems	Most of the legislative laws are obsolete and are inappropriate for current applications

of execution in IoT systems and increases the adaptability of IoT systems in service markets. This also allows the implementation of smaller services without increasing the computational burden and enables secure communication in a full-proof environment.

Despite the advantages, there are several challenges that are encountered while integrating IoT with Blockchain. Some of the prominent challenges associated with the integration of Blockchain with IoT are discussed in Table 6.

3.2. Security analysis

There are different methods available for evaluating the security of integrated Blockchain-IoT framework. The prominent techniques used for the security evaluation are as follows:

- *Burrows, Abadi, and Needham (BAN) logic:* The BAN logic is one of the extensively used techniques for authentication and identity management processes. The main objectives of this logic are; robust privacy preservation, integrity of data, non-repudiation and traceability [114]. The BAN logic is used in [115] for preserving the privacy of medical data. The proposed Blockchain system consists of an authentication scheme along with a data transfer protocol. The authentication scheme employs an elliptic curve point multiplication for securely sharing the information between mobile devices and human sensors. The performance of a traceable Blockchain technology with smart contracts for securing IoT is evaluated in [116] using a BAN logic. The BAN logic validates mutual authentication between IoT and Blockchain. The verification provided by BAN logic helps in ensuring that the integrated system can withstand various security attacks, such as man-in-the-middle attacks, replay attacks, or impersonation attacks. The authentication mechanisms can be designed and evaluated to be resilient to these threats [117].
- *Game theory:* This is one of the natural techniques which can address the issues related to decentralization and decision making in IoT applications. There are different types of game theory approaches such as Stackelberg game, Noncooperative game, and Differential game [118]. The performance of Blockchain based framework for securing industrial IoT is evaluated using a game theory approach in [119]. One of the excellent attribute of this architecture is that the effect of the power of Blockchain nodes is reduced based on PoW and PoS consensus protocols. In addition, the game theory logic suggest that the authority and prominence of the nodes on the Blockchain network is determined by their behavior in the network. A novel distributed Blockchain based security architecture for IoT is presented in [120] which depends on the gateway nodes for securing the data stored in the Blockchain. The data shared through the nodes is secured using the middleware servers for analyzing and processing IoT data. The efficacy of the model is analyzed using a game theory model and results show that the proposed approach is robust, secure and efficient for ensuring the security and privacy of IoT data. In this context, game theory provides a strategic framework for modeling the interactions between different entities within the Blockchain-IoT framework. By leveraging the advantages of game theory, researchers can design and develop a secure authentication mechanism for the evolving landscape of Blockchain-IoT integrated framework [121].
- *Theory analysis:* The theory analysis mainly focuses on proving that the security framework can serve multiple objectives such as (a) ensuring the reliability, (b) secure privacy-preservation, and (c) providing fair incentives [122]. A theory-based analysis is implemented in [123] for classifying and analyzing the solutions designed for integrating IoT with Blockchain technology. The proposed approach states that most of the lightweight solutions developed for integrating IoT with Blockchain handles the issues related to energy or security separately. The theoretical based analysis is evaluated using real-time integration scenarios of Blockchain with IoT. Theory analysis is suitable for most of the Iot application and hence is used extensively in evaluating security approaches.
- *AVISPA tool:* This tool is one of the formal security verification tools which can effectively authenticate and validate the security methods for IoT systems [124]. It can offer various advantages such as formal verification, protocol analysis, automated testing, vulnerability detection and reduction of false positive rates while assessing the security aspects of such integrated frameworks.

Apart from the above mentioned security techniques, there are other characteristics which are essential for evaluating the security of integrated Blockchain-IoT frameworks. The essential characteristics are as follows: privacy, integrity, confidentiality, authentication, identity and location privacy, non-repudiation, traceability, trust management, unforgeability, access control, data auditability, and unlinkability. Table 7 discusses the security techniques used for different IoT applications.

Table 7
Security techniques for different IoT applications.

References	IoT application	Security technique
[125]	IoT based microgrids	Game theory
[126]	IoT based smart homes	Theory analysis
[127]	IoT based edge computing	Game theory
[128]	Cryptocurrencies	Theory analysis
[129]	Internet of drones	AVISPA tool
[130]	Internet of vehicles	Theory analysis
[131]	Healthcare applications	BAN logic
[132]	Cloud computing	Game theory
[133]	Internet of vehicles	BAN logic
[134]	Agriculture	AVISPA tool
[135]	Internet of vehicles	Pro verif tool

3.3. Evaluation parameters

The performance and effectiveness of the Blockchain for IoT applications are evaluated using different evaluation parameters which are listed in below points:

- *Consensus delay (Latency):* Latency is defined as the time consumed by the Blockchain for completing a transaction along with approval of the user and publication [136].
- *Communication and computation cost:* The communication cost includes the cost of communication rounds in a transaction including required parameters, verification request, and approval message. On the other hand, the computation cost includes the cost of resources required for the security such as key size, hash values, mining, transaction server etc. [137].
- *Storage overhead:* The storage overhead is measured in terms of storage cost and individual transaction during the verification process [138].
- *Storage size:* The storage size depends on the number of keys required, number of sessions, and amount of information to be stored [139].
- *Blockchain update time overhead* (ms): The block update time measures the time required by the Blockchain to update the transaction details [140]. The update time increases with the decrease in the size of the sliding window.
- *Effect of Blockchain consensus rate:* This parameter defines the charge rate of the consensus algorithms [141].
- *Average throughput (requests per second):* Throughput is the rate at which the Blockchain can handle multiple transaction or service requests within a defined period of time [142].
- *Scalability:* Scalability defines the capability of Blockchain to handle a large number of transactions without affecting the latency and throughput [143].
- *Transaction generation time* (ms): Transaction time is defined as the time taken by the Blockchain to generate a transaction which also includes the measurement of information retrieval time [144].

4. Challenges, open issues and future research directions

A brief overview of the open issues and research opportunities are discussed in this section.

4.1. Challenges related to security and privacy in Blockchain-IoT paradigm

As discussed in previous sections, the heterogeneous devices connected through Blockchain are highly susceptible to the security attacks which can deteriorate the quality of services provided by the integrated Blockchain-IoT paradigms. The prominent privacy and security challenges that needs to be addressed are summarized as follows:

4.1.1. Challenges related to Blockchain

Blockchain implementation comes with several challenges which must be addressed for ensuring successful adoption. In addition to issues such as scalability, interoperability, privacy, and confidentiality there are certain prominent challenges concerning Blockchain adoption which are as follows:

- *Regulatory Compliance:* Blockchain implementation should adhere to certain legal and regulatory compliances. The decentralized and immutable nature of Blockchain might deviate with certain data protection and privacy regulations which can lead to compliance issues.
- *Security Issues:* Although Blockchain is adopted for strengthening the security of the end applications, it is also susceptible to potential attacks. Smart contract vulnerability, attacks in consensus Blockchain such as proof-of-work, and hacking of cryptocurrency exchanges are some of the specific security concerns suffered by the Blockchain network.
- *High Energy Consumption:* Certain consensus protocols used in the Blockchain network consume more energy and this raises concerns about the environmental impact and sustainability of such networks.
- *User Experience:* The experience of the user while interacting with Blockchain-based applications can be complicated and challenging for non-technical users and it is essential to improve the accessibility and user interface for enhancing the experience in real-time applications.
- *Upgrade and Fork Management:* Updating and managing the network forks in Blockchain models can be contended and complex. It is challenging to coordinate network upgrades while maintaining consensus among network participants.
- *Lack of Awareness:* Since Blockchain is a relatively new technology there is a lack of understanding and awareness about its potential benefits and limitations. There is a need to educate the stakeholders for successfully implementing Blockchain for IoT security.

4.1.2. Challenges across different layers of IoT

The heterogeneous nature of IoT increases the complexity of implementing Blockchain-IoT solutions and there are several challenges across different layers of IoT such as, the perception layer (IoT devices), the network layer (communication infrastructure), and the application layer (services and applications).

- *Perception Layer:* The challenges in this layer are mainly related to IoT devices such as limited computational power, memory, and energy resources. It is a tedious task to implement robust Blockchain protocols on such resource-constrained devices. In addition, it is strenuous to ensure the identity and authentication of IoT devices for preventing unauthorized access to the device data.
- *Network Layer:* With the increase in the number of IoT devices, the pressure on the Blockchain for handing a large volume of data transactions also increases. This can raise the concern on the stability of the Blockchain protocols. Besides, the Blockchain transactions can exhibit a higher latency compared to conventional centralized systems. This can be problematic for real-time IoT applications that require low latency. Although this problem is discussed in several existing works, it is often challenging to ensure a consistent and reliable connectivity between IoT devices while maintaining the scalability and latency in dynamic and heterogeneous IoT environments.

- *Application Layer:* The application layer in a Blockchain-IoT environment consists of multiple factors of Blockchain such as deployment of smart contracts and consensus protocols, identity management, ensuring data integrity, and interoperability. The deployment of smart contracts on the integrated Blockchain-IoT platform must be thoroughly checked to mitigate the potential threats which can affect the security of the IoT applications. In addition, it is challenging to deploy an appropriate consensus mechanism which helps in achieving a balanced tradeoff between different Blockchain parameters such as security, efficiency, and scalability for IoT applications. Most of the Blockchain-based IoT application suffers from identity management issues and it is crucial to manage the identities of both IoT devices and participants in the Blockchain network for establishing a trusted ecosystem.

4.1.3. Challenges related to the integration of Blockchain with IoT

The integration of Blockchain with IoT raises critical security concerns and this section summarizes come of the challenges observed while integration Blockchain with IoT.

- *Lack of consensus protocols for Blockchain-IoT:* Existing consensus protocols have a common problem i.e., these protocols work on probability mechanisms and are not final. The lack of finality among the consensus protocols affects the development of permanent blocks which delays the confirmation of transaction. Due to the transaction delay, the adaptability of the integrated Blockchain-IoT paradigm for instantaneous IoT systems is restricted. A comprehensive analysis of consensus protocols is required to integrate them in IoT applications to improve the fault tolerance and make them resilient against DoS attacks.
- *Transaction validation::* In general, the transactions are validated by identifying the user identity, signature, and transaction details before initiating the process in Blockchain platforms. However, validating the transactions can be difficult in the Blockchain-IoT paradigm due to the distributed nature and heterogeneity of IoT devices which accepts data from multiple sources in different formats. Correspondingly, several other validation techniques need to be explored which can handle the heterogeneity of IoT data [145].
- *Device integration:* The main aim of integrating IoT devices to Blockchain network is to enhance the integrity of the data collected by the IoT devices. Though Blockchain incorporates an immutable DLT, the data collected from the IoT devices are vulnerable to potential threats. Besides, IoT devices use an external library web3.js as an interface to establish communication between other sensory devices, which increases the threat due to SQL and XSS attacks. It is highly essential to validate the authenticity of the data and make them tamper proof in order to integrate the devices with Blockchain platforms.
- *Software update:* IoT system requires continuous software updates in order to satisfy the varying application requirements and to handle the novel security attacks. However, threats such as ransomware attacks will encrypt the entire system data including files and stored data. To overcome this problem, it is essential to update the firmware on a periodic basis in order to ensure that all the device data is updated and are resistant to the attacks. However, it becomes difficult to update the software in Blockchain due to the decentralized nature. In the integrated Blockchain-IoT framework, most of the IoT devices work without updating the software and hence are exposed to several attacks.
- *Interoperability:* In Blockchain technology, interoperability refers to the ability of the Blockchain platforms to share and communicate with other Blockchain models. This will allow the Blockchain networks to gain or access the data and create new products leveraging the advantages of multiple Blockchain networks simultaneously. However, interoperability in Blockchain incorporates various issues such as poor security, trust, confidentiality, and data privacy issues. In particular, security threats are exacerbated by the presence of multiple Blockchain and possible multiple administrators. This problem becomes more complicated in integrated Blockchain-IoT applications. This is mainly due to the difficulty in coordinating between the transactions from different Blockchain and different IoT devices because of different properties.
- *Network Performance:* Most of the IoT based applications are designed to provide real-time services with better quality of service to ensure the satisfaction of the customers. To achieve better performance in terms of computation speed, integrity, and security, Blockchain is considered in IoT applications which achieves better throughput. Throughput defines the ability of the Blockchain network to validate the number of transactions in a second. However, with the increase in the demand for sophisticated IoT applications that tend to use micro payments for financial transactions like Bitcoin or cryptocurrency, it becomes difficult to achieve better network performance in terms of throughput. This is mainly due to the fact that Blockchain consensus protocols require more time and consume more power to validate the transactions. Hence achieving a balanced tradeoff between the network performance and integration efficiency is still a major challenge.

4.2. Open issues and future directions

This section identifies the open issues and potential research directions which can help in exploring different aspects of Blockchain-IoT integration. Despite the availability of numerous survey papers in the literary works, there were some research gaps that needed more attention. For instance, the authors in [3] discussed prominent security threats for IoT. A layer-wise security problems are identified and corresponding solutions for resolving security threats are analyzed. However, very little focus is given to the privacy and security challenges associated with integrated Blockchain-IoT architecture. The current review attempts to fulfill this research gap by identifying issues related to the availability of consensus protocols for Blockchain-IoT, issues related to transaction validation, device integration, software update and interoperability. The work proposed in [73] provided a comprehensive analysis of IoT security using Blockchain. Although the paper addresses most of the security aspects, it does not focus on some of the techniques used for the security evaluation such as game theory, BAN logic and AVISPA tools. Besides, the study does not emphasize on the evaluation metrics. The current review sheds light on these aspects and fulfills the observed research gap. The authors [146] discuss different IoT — Blockchain approaches. However, it does not provide detailed analysis of security threats and existing security solutions. This constitutes one of the major research gaps, which is addressed in the current research. The survey presented in [147] reviewed the architecture of IoT and highlighted the significance of Blockchain for IoT systems. As observed, the study focused mainly on the network attacks and architectural details and very little focus is given on the possible solutions and need for Blockchain integration with IoT to strengthen the security. This limitation is addressed in the current review and the solutions with its limitations are discussed. In addition to these research gaps, there are other issues which need to be addressed.

The summarized issues and opportunities can improve the potential of Blockchain based IoT security.

- *Blockchain for intrusion detection systems (IDS):* Recently, several research works have implemented Blockchain for developing IDS in IoT [148,149]. IDS are implemented to identify the unauthorized intrusions in the systems and thereby prevent the adversarial security attacks using machine learning models. Blockchain in IDS verifies the integrity of the data and ensures transparency. However, it is challenging to identify appropriate cyber security datasets for Blockchain-based IDS [150] and it is also complicated to create a new dataset.
- *Developing effective consensus protocols:* Most of the widely used consensus protocols are PoW, PoS and PBFT. However, these protocols do not consider the threshold limit for storage and computation and hence their effectiveness is affected. Hence it is essential to consider various characteristics such as processing speed, computational requirements and trustworthiness while developing a suitable consensus protocol. For future research, hybrid consensus algorithms can be developed which integrate the advantages to two or more consensus protocols.
- *Blockchain based SDN for IoT:* Though there are several research studies available that combine Blockchain for SDN, there are certain challenges that are still intact when applied for practical IoT applications. Lack of a robust cryptography and encryption method can be a critical challenge which violates the privacy and confidentiality of the data communicated between two entities [151]. Besides, the issue of tackling attacks such as MITM and DoS in Blockchain based SDN in IoT are still prevalent.
- *5G-enabled Blockchain-based IoT networks:* 5G is one of the upcoming technologies which can transform the current IoT applications. With the increasing prominence, the issues of privacy leakage also increases in 5G networks. It can surely be challenging to develop an effective security framework considering the novelty, volatility, and susceptibility of 5G networks. Some promising techniques such as privacy aware deep learning [152], reinforcement learning, and game theory [153] can be used for strengthening the security in 5G-based Blockchain-IoT networks.
- *Secure Blockchain ledgers at Fog computing:* The implementation of distributed ledgers in fog computing is the most reliable and cost effective way to reduce the latency issue in Blockchain-IoT networks [154]. However, it is challenging to preserve the confidentiality of Blockchain ledgers. Securing the ledgers in fog computing applications needs to consider multiple factors such as selection of trusted fog nodes, ensuring confidentiality of ledgers etc [155]. Hence, carrying out researchers in this aspect is one of the critical challenges and the development of a secure, robust, reliable and resilient approach for the security of Blockchain based fog computing applications can be a potential research opportunity.

5. Conclusion

This paper presented a comprehensive analysis on the application of Blockchain for IoT systems and various threats that affect the security and privacy of the IoT data. This review discusses the taxonomy of different security threats in IoT and briefly discusses the existing works that leverage Blockchain for the security of IoT. The functioning of Blockchain is discussed in detail along with the security and privacy characteristics, consensus algorithms, and their comparison. Further, this review focuses on discussing the integration of Blockchain with IoT and the advantages, challenges, security techniques and performance evaluation parameters are outlined. It can be inferred from this review that Blockchain technology is one of the promising technologies which can offer numerous advantages in terms of enhancing the security and privacy of IoT data and contribute to the extension of IoT for various applications. The identified issues suggest that the deployment of Blockchain for IoT is still in its infant stage and there is an increasing demand for research works to address the challenges and complexities associated with the integration of Blockchain with IoT. In this context, this review identifies some of the prominent open issues and possible future research directions which can contribute to the researchers aiming to integrate Blockchain and IoT.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article

Acknowledgments

This work is supported in part by DoD Center of Excellence in AI and Machine Learning (CoE-AIML), USA under Contract Number W911NF-20-2-0277 with the U.S. Army Research Laboratory.

References

[1] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S.A. Kondaveeti, S. Shekhar, Continuous security in IoT using blockchain, in: 2018 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP, IEEE, 2018, pp. 6423–6427.
[2] M.A. Al-Garadi, A. Mohamed, A.K. Al-Ali, X. Du, I. Ali, M. Guizani, A survey of machine and deep learning methods for internet of things (IoT) security, IEEE Commun. Surv. Tutor. 22 (3) (2020) 1646–1685.
[3] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.
[4] B.K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, A.H. Gandomi, Addressing security and privacy issues of IoT using blockchain technology, IEEE Internet Things J. 8 (2) (2020) 881–888.
[5] S. Roy, M. Ashaduzzaman, M. Hassan, A.R. Chowdhury, Blockchain for IoT security and management: Current prospects, challenges and future directions, in: 2018 5th International Conference on Networking, Systems and Security (NSysS), IEEE, 2018, pp. 1–9.
[6] B.K. Mohanta, U. Satapathy, S.S. Panda, D. Jena, A novel approach to solve security and privacy issues for iot applications using blockchain, in: 2019 International Conference on Information Technology, ICIT, IEEE, 2019, pp. 394–399.
[7] W. Jiang, E. Li, W. Zhou, Y. Yang, T. Luo, IoT access control model based on blockchain and trusted execution environment, Processes 11 (3) (2023) 723.
[8] Q. Fan, J. Chen, L.J. Deborah, M. Luo, A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain, J. Syst. Archit. 117 (2021) 102112.
[9] S.M. Almeghlef, A.A.-M. AL-Ghamdi, M.S. Ramzan, M. Ragab, Application layer-based denial-of-service attacks detection against IoT-CoAP, Electronics 12 (12) (2023) 2563.
[10] M.A. Rashid, H.H. Pajooh, A security framework for IoT authentication and authorization based on blockchain technology, in: 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2019, pp. 264–271.
[11] A. Goel, A. Agarwal, M. Vatsa, R. Singh, N. Ratha, DeepRing: Protecting deep neural network with blockchain, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2019.

[12] X. Li, X. Wu, X. Pei, Z. Yao, Tokenization: Open asset protocol on blockchain, in: 2019 IEEE 2nd International Conference on Information and Computer Technologies, ICICT, IEEE, 2019, pp. 204–209.

[13] S. Chandel, W. Cao, Z. Sun, J. Yang, B. Zhang, T.-Y. Ni, A multi-dimensional adversary analysis of RSA and ECC in blockchain encryption, in: Future of Information and Communication Conference, Springer, 2020, pp. 988–1003.

[14] H. Zheng, J. Shao, G. Wei, Attribute-based encryption with outsourced decryption in blockchain, Peer-to-Peer Netw. Appl. 13 (5) (2020) 1643–1655.

[15] H. Guo, W. Li, E. Meamari, C.-C. Shen, M. Nejad, Attribute-based multi-signature and encryption for ehr management: A blockchain-based solution, in: 2020 IEEE International Conference on Blockchain and Cryptocurrency, ICBC, IEEE, 2020, pp. 1–5.

[16] D. Li, W. Peng, W. Deng, F. Gai, A blockchain-based authentication and security mechanism for IoT, in: 2018 27th International Conference on Computer Communication and Networks, ICCCN, IEEE, 2018, pp. 1–6.

[17] M.T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of Trust: A decentralized blockchain-based authentication system for IoT, Comput. Secur. 78 (2018) 126–142.

[18] Z. Haddad, M.M. Fouda, M. Mahmoud, M. Abdallah, Blockchain-based authentication for 5G networks, in: 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), IEEE, 2020, pp. 189–194.

[19] N. Kolokotronis, S. Brotsis, G. Germanos, C. Vassilakis, S. Shiaeles, On blockchain architectures for trust-based collaborative intrusion detection, in: 2019 IEEE World Congress on Services, Vol. 2642, SERVICES, IEEE, 2019, pp. 21–28.

[20] L.K. Ramasamy, F.K. KP, A.L. Imoize, J.O. Ogbebor, S. Kadry, S. Rho, Blockchain-based wireless sensor networks for malicious node detection: A survey, IEEE Access 9 (2021) 128765–128785.

[21] D. Swinhoe, What is a man-in-the-middle attack? How MitM attacks work and how to prevent them, Portal CSO 13 (2019).

[22] A. Bose, G.S. Aujla, M. Singh, N. Kumar, H. Cao, Blockchain as a service for software defined networks: A denial of service attack perspective, in: 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), IEEE, 2019, pp. 901–906.

[23] H.-N. Dai, Z. Zheng, Y. Zhang, Blockchain for Internet of Things: A survey, IEEE Internet Things J. 6 (5) (2019) 8076–8094.

[24] T. Sharma, S. Satija, B. Bhushan, Unifying blockchian and IoT: security requirements, challenges, applications and future trends, in: 2019 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS, IEEE, 2019, pp. 341–346.

[25] P. Patil, M. Sangeetha, V. Bhaskar, Blockchain for IoT access control, security and privacy: a review, Wirel. Pers. Commun. 117 (3) (2021) 1815–1834.

[26] H.F. Atlam, G.B. Wills, Technical aspects of blockchain and IoT, in: Advances in Computers, Vol. 115, Elsevier, 2019, pp. 1–39.

[27] T. Yu, X. Wang, Y. Zhu, Blockchain technology for the 5g-enabled internet of things systems: Principle, applications and challenges, in: 5G-Enabled Internet of Things, CRC Press, 2019, pp. 301–321.

[28] S.M.H. Bamakan, A. Motavali, A.B. Bondarti, A survey of blockchain consensus algorithms performance evaluation criteria, Expert Syst. Appl. 154 (2020) 113385.

[29] C. Fan, S. Ghaemi, H. Khazaei, P. Musilek, Performance evaluation of blockchain systems: A systematic survey, IEEE Access 8 (2020) 126927–126950.

[30] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, An efficient selective miner consensus protocol in blockchain oriented IoT smart monitoring, in: 2019 IEEE International Conference on Industrial Technology, ICIT, IEEE, 2019, pp. 1135–1142.

[31] Q. Zhou, H. Huang, Z. Zheng, J. Bian, Solutions to scalability of blockchain: A survey, IEEE Access 8 (2020) 16440–16455.

[32] G. Chapron, The environment needs cryptogovernance, Nature 545 (7655) (2017) 403–405.

[33] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.

[34] T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001.

[35] S. Qahtan, K.Y. Sharif, A. Zaidan, H. Alsattar, O. Albahri, B. Zaidan, H. Zulzalil, M. Osman, A. Alamoodi, R. Mohammed, Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 systems, IEEE Trans. Ind. Inform. 18 (9) (2022) 6415–6423.

[36] C. Chauhan, M.K. Ramaiya, Advanced model for improving IoT security using blockchain technology, in: 2022 4th International Conference on Smart Systems and Inventive Technology, ICSSIT, IEEE, 2022, pp. 83–89.

[37] P. Sharma, S. Namasudra, R.G. Crespo, J. Parra-Fuente, M.C. Trivedi, EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain, Inform. Sci. 629 (2023) 703–718.

[38] W. Liang, N. Ji, Privacy challenges of IoT-based blockchain: a systematic review, Cluster Comput. 25 (3) (2022) 2203–2221.

[39] M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future for internet of things security: a position paper, Digit. Commun. Netw. 4 (3) (2018) 149–160.

[40] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. Challenges and opportunities, Future Gener. Comput. Syst. 88 (2018) 173–190.

[41] X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on blockchain for Internet of Things, Comput. Commun. 136 (2019) 10–29.

[42] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the Internet of Things: A comprehensive survey, IEEE Commun. Surv. Tutor. 21 (2) (2018) 1676–1717.

[43] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, A survey on the adoption of blockchain in iot: Challenges and solutions, Blockchain: Res. Appl. 2 (2) (2021) 100006.

[44] A. Papageorgiou, A. Mygiakis, K. Loupos, T. Krousarlis, DPKI: a blockchain-based decentralized public key infrastructure system, in: 2020 Global Internet of Things Summit (GIoTS), IEEE, 2020, pp. 1–5.

[45] Y.C.E. Adja, B. Hammi, A. Serhrouchni, S. Zeadally, A blockchain-based certificate revocation management and status verification system, Comput. Secur. 104 (2021) 102209.

[46] B.S. Egala, A.K. Pradhan, V. Badarla, S.P. Mohanty, Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control, IEEE Internet Things J. 8 (14) (2021) 11717–11731.

[47] W. Xiang, Z. Yuanyuan, Scalable access control scheme of internet of things based on blockchain, Procedia Comput. Sci. 198 (2022) 448–453.

[48] M. Khalid, S. Hameed, A. Qadir, S.A. Shah, D. Draheim, Towards SDN-based smart contract solution for IoT access control, Comput. Commun. 198 (2023) 1–31.

[49] S. Tegane, F. Semchedine, A. Boudries, An extended Attribute-based access control with controlled delegation in IoT, J. Inf. Secur. Appl. 76 (2023) 103473.

[50] S. Kaven, V. Skwarek, Poster: Attribute based access control for IoT devices in 5G networks, in: Proceedings of the 28th ACM Symposium on Access Control Models and Technologies, 2023, pp. 51–53.

[51] Z.A. Hussien, H.A. Abdulmalik, M.A. Hussain, V.O. Nyangaresi, J. Ma, Z.A. Abduljabbar, I.Q. Abduljaleel, Lightweight integrity preserving scheme for secure data exchange in cloud-based IoT systems, Appl. Sci. 13 (2) (2023) 691.

[52] Q. Zhao, S. Chen, Z. Liu, T. Baker, Y. Zhang, Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems, Inf. Process. Manage. 57 (6) (2020) 102355.

[53] M. Juma, F. Alattar, B. Touqan, Securing big data integrity for industrial IoT in smart manufacturing based on the trusted consortium blockchain (TCB), IoT 4 (1) (2023) 27–55.

[54] G. Dong, X. Wang, A secure IoT data integrity auditing scheme based on consortium blockchain, in: 2020 5th IEEE International Conference on Big Data Analytics, ICBDA, IEEE, 2020, pp. 246–250.

[55] H. Xue, D. Chen, N. Zhang, H.-N. Dai, K. Yu, Integration of blockchain and edge computing in internet of things: A survey, Future Gener. Comput. Syst. 144 (2023) 307–326.

[56] H.R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic, M. Omar, Trustworthy iot data streaming using blockchain and ipfs, IEEE Access 10 (2022) 17707–17721.

[57] S.P. Gochhayat, E. Bandara, S. Shetty, P. Foytik, Yugala: Blockchain based encrypted cloud storage for IoT data, in: 2019 IEEE International Conference on Blockchain (Blockchain), IEEE, 2019, pp. 483–489.

[58] G. Rathee, A. Sharma, H. Saini, R. Kumar, R. Iqbal, A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology, Multimedia Tools Appl. 79 (15) (2020) 9711–9733.

[59] S.K. Singh, S. Rathore, J.H. Park, Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence, Future Gener. Comput. Syst. 110 (2020) 721–743.

[60] G.F. Camilo, G.A.F. Rebello, L.A.C. de Souza, O.C.M. Duarte, AutAvailChain: Automatic and secure data availability through blockchain, in: GLOBECOM 2020-2020 IEEE Global Communications Conference, IEEE, 2020, pp. 1–6.

[61] K.R. Ozyilmaz, A. Yurdakul, Designing a Blockchain-based IoT with Ethereum, swarm, and LoRa: the software solution to create high availability with minimal security risks, IEEE Consum. Electron. Mag. 8 (2) (2019) 28–34.

[62] A. Panarello, N. Tapas, G. Merlino, F. Longo, A. Puliafito, Blockchain and iot integration: A systematic survey, Sensors 18 (8) (2018) 2575.

[63] J.H. Ryu, P.K. Sharma, J.H. Jo, J.H. Park, A blockchain-based decentralized efficient investigation framework for IoT digital forensics, J. Supercomput. 75 (8) (2019) 4372–4387.

[64] C. Machado, A.A.M. Fröhlich, IoT data integrity verification for cyber-physical systems using blockchain, in: 2018 IEEE 21st International Symposium on Real-Time Distributed Computing, ISORC, IEEE, 2018, pp. 83–90.
[65] H.R. Hasan, K. Salah, Blockchain-based proof of delivery of physical assets with single and multiple transporters, IEEE Access 6 (2018) 46781–46793.
[66] S. Rathore, B.W. Kwon, J.H. Park, BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network, J. Netw. Comput. Appl. 143 (2019) 167–177.
[67] M. Wazid, A.K. Das, S. Shetty, M. Jo, A tutorial and future research for building a blockchain-based secure communication scheme for internet of intelligent things, IEEE Access 8 (2020) 88700–88716.
[68] A.S. Hosen, S. Singh, P.K. Sharma, U. Ghosh, J. Wang, I.-H. Ra, G.H. Cho, Blockchain-based transaction validation protocol for a secure distributed IoT network, IEEE Access 8 (2020) 117266–117277.
[69] H. Liu, D. Han, D. Li, Fabric-IoT: A blockchain-based access control system in IoT, IEEE Access 8 (2020) 18207–18218.
[70] C. Stamatellis, P. Papadopoulos, N. Pitropakis, S. Katsikas, W.J. Buchanan, A privacy-preserving healthcare framework using hyperledger fabric, Sensors 20 (22) (2020) 6587.
[71] M. Ammi, S. Alarabi, E. Benkhelifa, Customized blockchain-based architecture for secure smart home for lightweight IoT, Inf. Process. Manage. 58 (3) (2021) 102482.
[72] Y. Wang, S. Cai, C. Lin, Z. Chen, T. Wang, Z. Gao, C. Zhou, Study of blockchains's consensus mechanism based on credit, IEEE Access 7 (2019) 10224–10231.
[73] S. Saxena, B. Bhushan, M.A. Ahad, Blockchain based solutions to secure IoT: background, integration trends and a way forward, J. Netw. Comput. Appl. 181 (2021) 103050.
[74] T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, J. Wang, Untangling blockchain: A data processing view of blockchain systems, IEEE Trans. Knowl. Data Eng. 30 (7) (2018) 1366–1385.
[75] S. Velliangiri, P. Karthikeyan, Blockchain technology: challenges and security issues in consensus algorithm, in: 2020 International Conference on Computer Communication and Informatics, ICCCI, IEEE, 2020, pp. 1–8.
[76] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: A state of the art survey, IEEE Commun. Surv. Tutor. 21 (1) (2018) 858–880.
[77] D. Dasgupta, J.M. Shrein, K.D. Gupta, A survey of blockchain from security perspective, J. Bank. Financ. Technol. 3 (1) (2019) 1–17.
[78] R. Andreev, P. Andreeva, L. Krotov, E. Krotova, Review of blockchain technology: types of blockchain and their application, Intellekt. Sist. Proizv. 16 (1) (2018) 11–14.
[79] Multichain, Open platform for Blockchain applications, 2020, https://www.multichain.com/.
[80] W. She, Z.-H. Gu, X.-K. Lyu, Q. Liu, Z. Tian, W. Liu, Homomorphic consortium blockchain for smart home system sensitive data privacy preserving, IEEE Access 7 (2019) 62058–62070.
[81] X. Zhang, X. Chen, Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network, IEEE Access 7 (2019) 58241–58254.
[82] GitHub, Bitcoin GitHub implementation, 2020, https://www.multichain.com/.
[83] A. Yazdinejad, G. Srivastava, R.M. Parizi, A. Dehghantanha, H. Karimipour, S.R. Karizno, SLPoW: Secure and low latency proof of work protocol for blockchain in green IoT networks, in: 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), IEEE, 2020, pp. 1–5.
[84] F. Yang, W. Zhou, Q. Wu, R. Long, N.N. Xiong, M. Zhou, Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism, IEEE Access 7 (2019) 118541–118555.
[85] O. Alfandi, S. Otoum, Y. Jararweh, Blockchain solution for iot-based critical infrastructures: Byzantine fault tolerance, in: NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2020, pp. 1–4.
[86] S. Alrubei, E. Ball, J. Rigelsford, Securing IoT-blockchain applications through honesty-based distributed proof of authority consensus algorithm, in: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), IEEE, 2021, pp. 1–7.
[87] D. Puthal, S.P. Mohanty, P. Nanda, E. Kougianos, G. Das, Proof-of-authentication for scalable blockchain in resource-constrained distributed systems, in: 2019 IEEE International Conference on Consumer Electronics, ICCE, IEEE, 2019, pp. 1–5.
[88] M.A. Kumar, V. Radhesyam, B. Srinivasarao, Front-End IoT application for the bitcoin based on proof of elapsed time (PoET), in: 2019 Third International Conference on Inventive Systems and Control, ICISC, IEEE, 2019, pp. 646–649.
[89] B.K. Mohanta, S.S. Panda, D. Jena, An overview of smart contract and use cases in blockchain technology, in: 2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT, IEEE, 2018, pp. 1–4.
[90] T. Sharma, S.K. Prasad, A.K. Gupta, A study-based review on blockchain technology for IoT, in: Emerging Technologies in Data Mining and Information Security, Springer, 2021, pp. 901–911.
[91] K. Yu, L. Tan, C. Yang, K.-K.R. Choo, A.K. Bashir, J.J. Rodrigues, T. Sato, A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings, IEEE Internet Things J. (2021).
[92] R.T. Frahat, M.M. Monowar, S.M. Buhari, Secure and scalable trust management model for IoT P2P network, in: 2019 2nd International Conference on Computer Applications & Information Security, ICCAIS, IEEE, 2019, pp. 1–6.
[93] T.M. Hewa, Y. Hu, M. Liyanage, S.S. Kanhare, M. Ylianttila, Survey on blockchain-based smart contracts: Technical aspects and future research, IEEE Access 9 (2021) 87643–87662.
[94] M. Al-Shabi, A survey on symmetric and asymmetric cryptography algorithms in information security, Int. J. Sci. Res. Publ. (IJSRP) 9 (3) (2019) 576–589.
[95] S. Zhai, Y. Yang, J. Li, C. Qiu, J. Zhao, Research on the application of cryptography on the blockchain, in: Journal of Physics: Conference Series, Vol. 1168, IOP Publishing, 2019, 032077.
[96] B. Bhushan, P. Sinha, K.M. Sagayam, J. Andrew, Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions, Comput. Electr. Eng. 90 (2021) 106897.
[97] R. Sethi, B. Bhushan, N. Sharma, R. Kumar, I. Kaushik, Applicability of industrial IoT in diversified sectors: evolution, applications and challenges, in: Multimedia Technologies in the Internet of Things Environment, Springer, 2021, pp. 45–67.
[98] S. Gupta, S. Sinha, B. Bhushan, Emergence of blockchain technology: Fundamentals, working and its various implementations, in: Proceedings of the International Conference on Innovative Computing & Communications, ICICC, 2020.
[99] M.H. Miraz, M. Ali, Integration of blockchain and IoT: an enhanced security perspective, 2020, arXiv preprint arXiv:2011.09121.
[100] A. Ali, M.A. Almaiah, F. Hajjej, M.F. Pasha, O.H. Fang, R. Khan, J. Teo, M. Zakarya, An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network, Sensors 22 (2) (2022) 572.
[101] R. Durga, E. Poovammal, K. Ramana, R.H. Jhaveri, S. Singh, B. Yoon, CES blocks—a novel chaotic encryption schemes-based blockchain system for an IoT environment, IEEE Access 10 (2022) 11354–11371.
[102] M.S. Rahman, M. Chamikara, I. Khalil, A. Bouras, Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city, J. Ind. Inf. Integr. 30 (2022) 100408.
[103] J. Wu, F. Xiong, C. Li, Application of Internet of Things and blockchain technologies to improve accounting information quality, IEEE Access 7 (2019) 100090–100098.
[104] X. Lin, J. Li, J. Wu, H. Liang, W. Yang, Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach, IEEE Trans. Ind. Inform. 15 (12) (2019) 6367–6378.
[105] S. Wang, D. Li, Y. Zhang, J. Chen, Smart contract-based product traceability system in the supply chain scenario, IEEE Access 7 (2019) 115122–115133.
[106] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2702–2733.
[107] S. Quincozes, T. Emilio, J. Kazienko, MQTT protocol: fundamentals, tools and future directions, IEEE Lat. Am. Trans. 17 (09) (2019) 1439–1448.
[108] M. Alaslani, F. Nawab, B. Shihada, Blockchain in IoT systems: End-to-end delay evaluation, IEEE Internet Things J. 6 (5) (2019) 8332–8344.
[109] S. Rouhani, R. Deters, Security, performance, and applications of smart contracts: A systematic survey, IEEE Access 7 (2019) 50759–50779.
[110] M. Mangia, A. Marchioni, F. Pareschi, R. Rovatti, G. Setti, Chained compressed sensing: A blockchain-inspired approach for low-cost security in IoT sensing, IEEE Internet Things J. 6 (4) (2019) 6465–6475.
[111] S. Qi, Y. Lu, Y. Zheng, Y. Li, X. Chen, CPDS: Enabling compressed and private data sharing for industrial internet of things over blockchain, IEEE Trans. Ind. Inform. 17 (4) (2020) 2376–2387.
[112] K.-K.R. Choo, Z. Yan, W. Meng, Blockchain in industrial IoT applications: Security and privacy advances, challenges, and opportunities, IEEE Trans. Ind. Inform. 16 (6) (2020) 4119–4121.
[113] M. Novak, Crypto-friendliness: Understanding blockchain public policy, J. Entrep. Public Policy (2019).
[114] D. Shin, K. Yun, J. Kim, P.V. Astillo, J.-N. Kim, I. You, A security protocol for route optimization in DMM-based smart home IoT networks, IEEE Access 7 (2019) 142531–142550.
[115] T.-F. Lee, H.-Z. Li, Y.-P. Hsieh, A blockchain-based medical data preservation scheme for telecare medical information systems, Int. J. Inf. Secur. 20 (2021) 589–601.

[116] C.-L. Chen, Z.-Y. Lim, H.-C. Liao, Y.-Y. Deng, A traceable and authenticated IoTs trigger event of private security record based on blockchain, Appl. Sci. 11 (6) (2021) 2843.
[117] J.J. Hathaliya, S. Tanwar, An exhaustive survey on security and privacy issues in Healthcare 4.0, Comput. Commun. 153 (2020) 311–335.
[118] M.A. Ferrag, L. Shu, The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial, IEEE Internet Things J. 8 (24) (2021) 17236–17260.
[119] F. Ghovanlooy Ghajar, A. Sikora, D. Welte, Schloss: Blockchain-based system architecture for secure industrial iot, Electronics 11 (10) (2022) 1629.
[120] H. Tian, X. Ge, J. Wang, C. Li, H. Pan, Research on distributed blockchain-based privacy-preserving and data security framework in IoT, IET Commun. 14 (13) (2020) 2038–2047.
[121] S. Khezr, A. Yassine, R. Benlamri, Towards a trustful game-theoretic mechanism for data trading in the blockchain-IoT ecosystem, J. Netw. Syst. Manage. 30 (4) (2022) 56.
[122] C. Lai, M. Zhang, J. Cao, D. Zheng, SPIR: A secure and privacy-preserving incentive scheme for reliable real-time map updates, IEEE Internet Things J. 7 (1) (2019) 416–428.
[123] S. Abed, R. Jaffal, B.J. Mohd, A review on blockchain and iot integration from energy, security and hardware perspectives, Wirel. Pers. Commun. 129 (3) (2023) 2079–2122.
[124] Automated, Automated validation of internet security protocols and applications, 2020, http://www.avispa-project.org/.
[125] J. Li, Z. Zhou, J. Wu, J. Li, S. Mumtaz, X. Lin, H. Gacanin, S. Alotaibi, Decentralized on-demand energy supply for blockchain in internet of things: a microgrids approach, IEEE Trans. Comput. Soc. Syst. 6 (6) (2019) 1395–1406.
[126] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, K.-K.R. Choo, Home-Chain: A blockchain-based secure mutual authentication system for smart homes, IEEE Internet Things J. 7 (2) (2019) 818–829.
[127] Y. Liu, F.R. Yu, X. Li, H. Ji, V.C. Leung, Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing, IEEE Trans. Veh. Technol. 68 (11) (2019) 11169–11185.
[128] L. Zhang, H. Li, Y. Li, Y. Yu, M.H. Au, B. Wang, An efficient linkable group signature for payer tracing in anonymous cryptocurrencies, Future Gener. Comput. Syst. 101 (2019) 29–38.
[129] B. Bera, D. Chattaraj, A.K. Das, Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment, Comput. Commun. 153 (2020) 229–249.
[130] B. Luo, X. Li, J. Weng, J. Guo, J. Ma, Blockchain enabled trust-based location privacy protection scheme in VANET, IEEE Trans. Veh. Technol. 69 (2) (2019) 2034–2048.
[131] X. Cheng, F. Chen, D. Xie, H. Sun, C. Huang, Design of a secure medical data sharing scheme based on blockchain, J. Med. Syst. 44 (2) (2020) 1–11.
[132] A. Wilczyński, J. Kołodziej, Modelling and simulation of security-aware task scheduling in cloud computing based on Blockchain technology, Simul. Model. Pract. Theory 99 (2020) 102038.
[133] J. Noh, S. Jeon, S. Cho, Distributed blockchain-based message authentication scheme for connected vehicles, Electronics 9 (1) (2020) 74.
[134] A. Vangala, A.K. Sutrala, A.K. Das, M. Jo, Smart contract-based blockchain-envisioned authentication scheme for smart farming, IEEE Internet Things J. 8 (13) (2021) 10792–10806.
[135] Z. Xu, W. Liang, K.-C. Li, J. Xu, H. Jin, A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles, J. Parallel Distrib. Comput. 149 (2021) 29–39.
[136] A. Arena, A. Bianchini, P. Perazzo, C. Vallati, G. Dini, BRUSCHETTA: An IoT blockchain-based framework for certifying extra virgin olive oil supply chain, in: 2019 IEEE International Conference on Smart Computing, SMARTCOMP, IEEE, 2019, pp. 173–179.
[137] H. Tan, I. Chung, Secure authentication and key management with blockchain in VANETs, IEEE Access 8 (2019) 2482–2498.
[138] P. Wei, D. Wang, Y. Zhao, S.K.S. Tyagi, N. Kumar, Blockchain data-based cloud data integrity protection mechanism, Future Gener. Comput. Syst. 102 (2020) 902–911.
[139] Y. Zhang, B. Li, B. Liu, J. Wu, Y. Wang, X. Yang, An attribute-based collaborative access control scheme using blockchain for IoT devices, Electronics 9 (2) (2020) 285.
[140] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, J. Ma, Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network, IEEE Trans. Veh. Technol. 68 (11) (2019) 11309–11322.
[141] C. Dang, J. Zhang, C.-P. Kwong, L. Li, Demand side load management for big industrial energy users under blockchain-based peer-to-peer electricity market, IEEE Trans. Smart Grid 10 (6) (2019) 6426–6435.
[142] S.M. Danish, M. Lestas, H.K. Qureshi, K. Zhang, W. Asif, M. Rajarajan, Securing the LoRaWAN join procedure using blockchains, Cluster Comput. 23 (3) (2020) 2123–2138.
[143] Q. Lu, X. Xu, Y. Liu, I. Weber, L. Zhu, W. Zhang, uBaaS: A unified blockchain as a service platform, Future Gener. Comput. Syst. 101 (2019) 564–575.
[144] M. Shen, Y. Deng, L. Zhu, X. Du, N. Guizani, Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach, IEEE Netw. 33 (5) (2019) 27–33.
[145] Q. Wang, X. Zhu, Y. Ni, L. Gu, H. Zhu, Blockchain for the IoT and industrial IoT: A review, Internet Things 10 (2020) 100081.
[146] D. Minoli, B. Occhiogrosso, Blockchain mechanisms for IoT security, Internet Things 1–2 (2018) 1–13.
[147] M. Alizadeh, K. Andersson, O. Schelén, A survey of secure internet of things in relation to blockchain, J. Internet Serv. Inf. Secur. (JISIS) 10 (3) (2020) 47–75.
[148] H. Liang, J. Wu, S. Mumtaz, J. Li, X. Lin, M. Wen, MBID: Micro-blockchain-based geographical dynamic intrusion detection for V2X, IEEE Commun. Mag. 57 (10) (2019) 77–83.
[149] O. Alkadi, N. Moustafa, B. Turnbull, K.-K.R. Choo, A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks, IEEE Internet Things J. 8 (12) (2020) 9463–9472.
[150] F. Hussain, R. Hussain, S.A. Hassan, E. Hossain, Machine learning in IoT security: Current solutions and future challenges, IEEE Commun. Surv. Tutor. 22 (3) (2020) 1686–1721.
[151] P. Mishra, A. Biswal, S. Garg, R. Lu, M. Tiwary, D. Puthal, Software defined internet of things security: properties, state of the art, and future research, IEEE Wirel. Commun. 27 (3) (2020) 10–16.
[152] X. Liu, H. Li, G. Xu, S. Liu, Z. Liu, R. Lu, PADL: Privacy-aware and asynchronous deep learning for IoT applications, IEEE Internet Things J. 7 (8) (2020) 6955–6969.
[153] Q. Xu, Z. Su, R. Lu, Game theory and reinforcement learning based secure edge caching in mobile social networks, IEEE Trans. Inf. Forensics Secur. 15 (2020) 3415–3429.
[154] M. Mukherjee, L. Shu, D. Wang, Survey of fog computing: Fundamental, network applications, and research challenges, IEEE Commun. Surv. Tutor. 20 (3) (2018) 1826–1857.
[155] R. Lu, L. Zhang, J. Ni, Y. Fang, 5G vehicle-to-everything services: Gearing up for security and privacy, Proc. IEEE 108 (2) (2019) 373–389.