A Detailed Review on IoT Security and Management: Challenges, Recent Prospects and Solutions using Blockchain Methodology

Srivalli Ch[1], Dr.Vinay Chavan[2]

1Assistant Professor, Institute of Insurance and Risk Management, Gachibowli, Hyderabad.

2Professor, Seth Kesarimal Porwal College, Kamptee, Nagpur

Abstract:

Internet of Things (IoT) is one of the emerging and popular digital technology extensively used in applications like smart home, smart city, smart grids, etc. Also, it connects the different types of entities/objects at anytime and anywhere with the help of sensors and wireless mediums. However, it is essential to protect IoT objects from malware and cyber-attacks. Due to the immutable nature and associated security, blockchain technology is highly deployed in various IoT systems to ensure privacy and secrecy. But, satisfying all the security requirements of IoT systems remains one of the challenging issues yet to be resolved. This paper intends to conduct a detailed review for analyzing IoT systems' challenges and security requirements with suitable blockchain solutions. Also, it examines the significant effects of applying the blockchain methodology in IoT systems. Moreover, it investigates the efficacy and performance of the conventional blockchain-based security methodologies with their distinct features, essential solutions, benefits and limitations. The purpose of this paper is to satisfy the privacy-preserving requirements of IoT systems with the use of blockchain. In addition, the different types of blockchain access controlling techniques are reviewed for limiting the access to the entities or users according to the system rules and policies.

Keywords: Blockchain, Internet of Things (IoT), Smart Systems, Security, Access Controlling Methods, Authentication, and Consensus Algorithms

DOI: 10.24297/j.cims.2023.11.6

1. Introduction

Internet of Things (IoT) [1, 2] is an emerging and evolutionary technology increasingly used in different types of application domains. In IoT systems, each device/entity has its own identity for communicating with others. Also, the IoT is extensively [3] applied in all kinds of application systems like smart home, smart city, smart network, and etc due to their unique features and beneficiaries to the users. In this technology [4], the objects are embedded with the sensory devices using the communication machineries, which helps to establish the communication with other through internet. Among other benefits, the main reason deploying the IoT technology [5] is its low computing power, hence it is acknowledged and expanded widely. Moreover, it connects multiple devices or entities at anytime and anywhere using the communication standards. However, providing security to IoT systems is one of the complex and highly important tasks yet to be resolved. Due to the centralized architecture [6], it has the limitations of low interoperability, high cost, and single gateway. Blockchain is the most suitable option used for strengthening the security of IoT systems [7], which is a kind of distributed ledger technology that comprises the sequence of blocks for maintaining the digital transactions. Also, it enables the decentralized peer to peer communication over the network without human intervention. It has the distributed database for storing all transactions [8] in the form of immutable records, which are distributed across many participating nodes [9, 10]. By using this technology, the security is guaranteed by using the cryptographic models and decentralization strategies. Typically, the blocks are very difficult to create, because which requires some specific sensors [11] and certain time duration. Moreover, generating the block and tampering it with the previous block are highly complex, hence it is considered tamper-resistant. In the existing works, the different types of security blockchain based security methodologies [12, 13] are developed for securing IoT systems, and the general working model of blockchain methodology is shown in Fig 1. The conventional IoT security approaches [14, 15] limit with the following problems:

1.Lack of confidentiality and secrecy – Most of the IoT applications in recent days intend to receive the customized services.
2.Resource restraints – The IoT devices are limits with the bandwidth and memory capacity, which does not satisfy the complicated security problems.
3.Centralized nature – The present IoT devices are centralized in nature, which are individually monitored, and identified. Also, these are interlinked with the cloud servers, so there may be an increased possibility for the scalability problems. It creates certain failures, and interrupts the normal operation of the network.

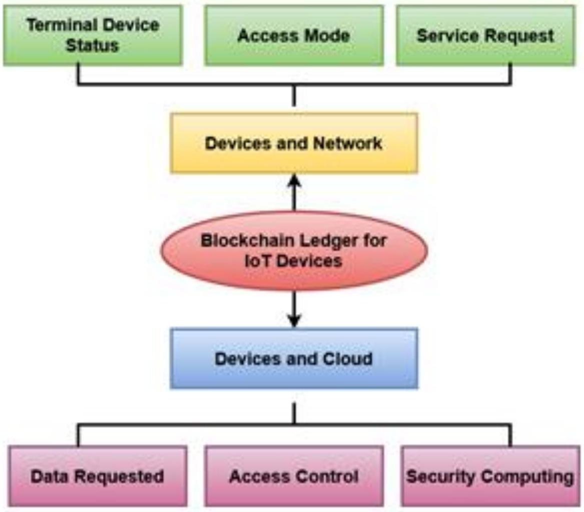

Fig 1. General working model of blockchain

The major objectives of this research work are as follows:

- To analyze the security challenges and problems associated to the IoT smart systems.
- To examine the major effects of using blockchain methodologies for addressing the security requirements of the IoT systems.
- To review the different types of existing blockchain methodologies with their distinct characteristics, benefits and limitations for strengthening the overall security of smart systems.
- To conduct the brief analysis for comparing the performance and efficiency of the existing **blockchain security models.**

The remaining portions of this paper are structuralized as follows: Section II reviews the conventional blockchain based security methodologies used in the IoT systems. Section III discusses the important properties, security challenges, and blockchain based access controlling mechanisms used in the existing works. Section IV validates the performance and efficiency of the conventional blockchain methods according to their security requirements and solutions. Finally, the overall paper is summarized with the obtainments and future scope in Section V.

2. Related Works

Mohanty, et al [16] introduced an Efficient Lightweight Integrated Blockchain (ELIB) model for supporting the security of IoT systems. The contribution of this work was to utilize the blockchain based Certificateless Cryptography (CC) methodology for ensuring the security of smart home applications. Typically, the smart home comprises the distinct IoT devices that are controlled by the local blockchain model. Here, the local immutable ledger technology has been utilized to control the smart home with ensured security. Qian, et al [17] implemented a high-level security management framework incorporated with the blockchain methodology for improving the security of smart home and transportation applications. Here, some of the open issues correlated to the abnormal traffic management, and identity verification in IoT systems have been investigated. Based on this analysis, it is studied that the machine learning is one of the most suitable technology for an abnormal traffic management. In addition to that, the different types of security problems associated to the layers of IoT systems are discussed in this work, which includes the application, network, and perception layers.

Alfandi, et al [18] examined the different types of privacy and security issues in the IoT systems with its appropriate blockchain solutions. It includes the problems of unauthorized data access, insecure service providence, unknown risk, and malicious insiders in the network. Moreover, it investigated about the types of blockchain chain methodologies used in the current application systems, which comprises the types of private, public, and consortium. The private blockchain is a kind of decentralized architecture, where the information exchange among the nodes is allowed in a specific or a particular application environment. Then, the consortium blockchain is also termed as the semi-private blockchain model, where the block verification has been performed by using the multi-signature scheme. Moreover, the public blockchain is an open-source medium, which does not has any pre-conditions for the privileges. Khan, et al [19] conducted a parametric analysis for investigating the security threats with its possible solutions to strengthen the IoT systems. The major security requirements of the IoT systems are as follows: data integrity, privacy, secrecy, authentication, authorization, service availability, and energy efficacy. Here, the different types of security threats have been categorized according to its characteristics as depicted in Fig 2.

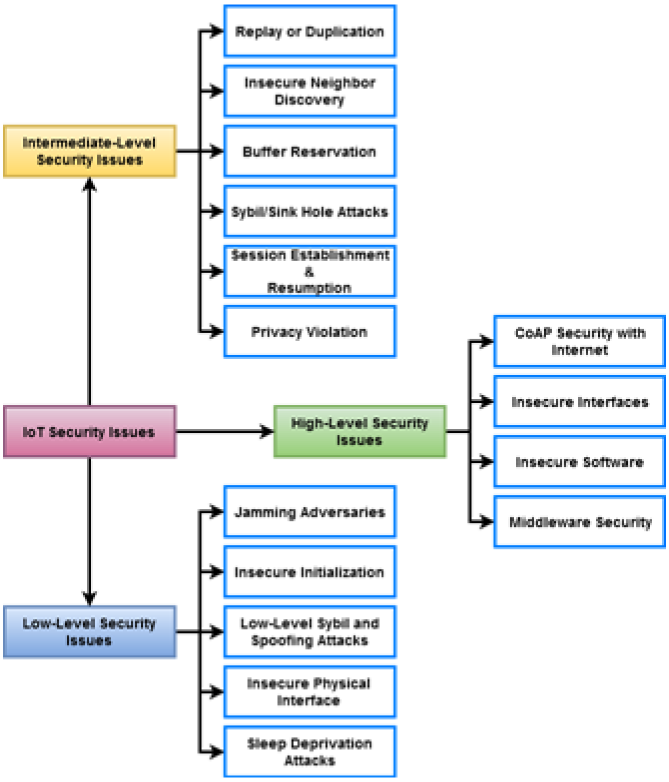
Replay or Duplication
Insecure Neighbor Discovery
Intermediate-Level Security Issues
Buffer Reservation
Sybil/Sink Hole Attacks
Session Establishment & Resumption
Privacy Violation
CoAP Security with Internet
Insecure Interfaces
IoT Security Issues
High-Level Security Issues
Insecure Software
Middleware Security
Jamming Adversaries
Insecure Initialization
Low-Level Security Issues
Low-Level Sybil and Spoofing Attacks
Insecure Physical Interface
Sleep Deprivation Attacks

Fig 2. Various IoT security issues

Dorri, et al [20] implemented a Lightweight Scalable Blockchain (LSB) methodology for assuring the security and privacy of IoT systems. Here, it was mentioned that the conventional blockchain methodologies are not more adaptable for the IoT context, due to the following problems:

1. Increased overhead and minimal scalability
2. High resource consumption
3. Increased latency and reduced throughput

In this work, the LSB methodology is mainly developed for the smart home application systems, which efficiently optimized the resource consumption. Moreover, the symmetric encryption methodology is also used for encrypting the transactions in order to ensure the security of data communication. Then, two fundamental elements of block manager, and transactions are highly concentrated in this work. Roy, et al [21] presented a comprehensive review about the prospects and challenges of using blockchain methodology in IoT systems. The purpose of this paper is to satisfy the privacy preserving requirements of IoT systems with the use of blockchain. Also, the major characteristics of using blockchain methodology were also discussed in this work, which includes security, autonomy, transparency, and collective verification.

3. Research Methodology

This section discusses about the major impacts of using blockchain methodology in IoT systems. Also, it investigates the security requirements of IoT, and different types of access controlling based blockchain methodologies for ensuring the security. The typical architecture of the blockchain based IoT security framework is shown in Fig 3.

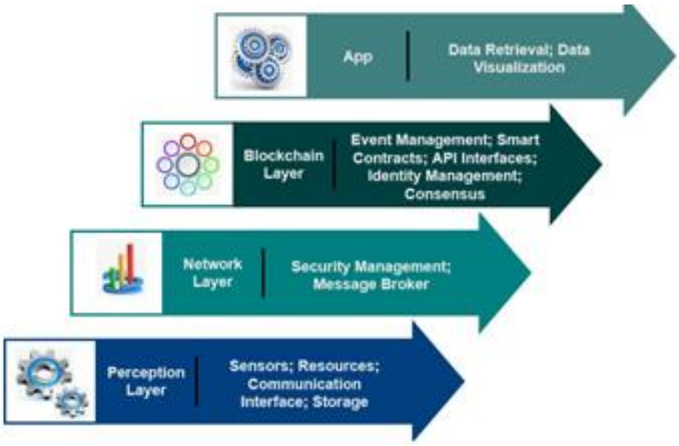
App
Data Retrieval; Data Visualization
Blockchain Layer
Event Management; Smart Contracts; API Interfaces; Identity Management; Consensus
Network Layer
Security Management; Message Broker
Perception Layer
Sensors; Resources; Communication Interface; Storage

Fig 3. Blockchain based IoT framework

A. Security Requirements in IoT

In IoT systems, some of the major requirements [22] are required to be satisfied for assuring the privacy and security of communication, which includes the followings:

1. Access Control – The distributed access controlling is one of the important requirements of IoT systems, because the entire networking system could be vulnerable, if it does not has the proper access controlling mechanism. Recently, the smart contracts based access controlling techniques are increasingly used to address this problem.
2. Authorization – It is also considered as the major security measure that is defined as the rights of user over the resources like services, product, data, applications, and etc.

In most of the smart-application environments, the blockchain based authorization techniques are used to validate the users.

3. Availability – In a trusted environment, availability in IoT systems is entirely depends on managing the requests received from the authorized persons. Moreover, it is more essential to satisfy the availability of requested data or service received from the trusted entities.
4. Authentication – In a decentralized environment, each participating entity or node is validated by others for ensuring the authenticity. In a smart home application systems, the lightweight security blockchain methodology is used to validate all the participants involved in the transactions. Normally, the authenticity of users is validated based on their signature, ID, private and public key pair used for identification.
5. Confidentiality – There may be an increased possibility for the malicious activities in the IoT systems, hence the confidentiality of data/service should be assured for the valid/trusted communication. In the recent works, the different types of encryption techniques like Advanced Encryption Standard (AES), Rivest Shamir Adlemann (RSA), and Elliptic Curve Cryptography (ECC) based cryptosystems are developed for assuring the data privacy while communicating with other devices. By using the blockchain model, the entities or nodes can be easily acknowledged for communication.
6. Identity – In most of the cybersecurity IoT systems, the identity verification and validation is treated as the major problem, due to the large number of interconnected devices in the network. By using the blockchain model, the identity management operations could be more reliable and scalable, due to its heterogeneity and mobility. Moreover, the identity of the particular entity or device is validated based on its intrinsic features/properties.
7. Non-Repudiation – It is defined as the transparent transaction of logging system that acknowledges the entities (i.e. sender and receiver) while communicating with each other. In a public blockchain based IoT systems, all transactions are recorded and logged in the public systems.
8. Third Party – In the centralized IoT environment, the central third party auditor can collect and maintain the data, so there may be an increased possibility for the data misuse.

9. Single Point of Failure – Due to the rapid growth of centralized networks, there may be a chance for the single point failure of the systems. In this environment, all the collected data are stored and maintained by the centralized authority, so if it goes down or fails, the entire networking system has been affected.
10. Scalability – Typically, the IoT can connect the large number of sensors and devices for sharing information or data with others. Due to its dynamic structure, the network scalability is one of the important measure need to be addressed in the IoT systems.

B. Blockchain Based IoT

The blockchain is one of the recent and most popular technology extensively used in many smart applications for assuring the system security. Generally, the blockchain is transactions in the blockchain network. The typical architecture of blockchain methodology is shown in Fig 4, which comprises the fields of block header, and transaction counter.

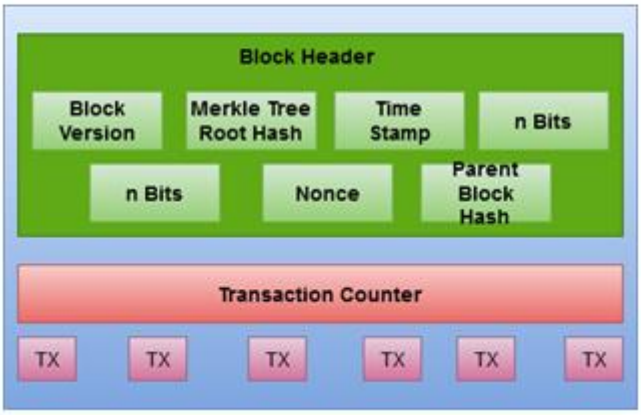

Fig 4. Structure of blockchain

In the IoT-enabled blockchain network, the communication between the entities is carried out by using the set of private and public key pair. Moreover, the user can use their own private key for signing the transactions and accessing the network. After that, the transaction verification process is performed by all the communicating entities exist in the blockchain network, where the invalid transactions are eliminated after verification. Then, the legitimate transactions are gathered for the fixed time, and the Proof of Work (PoW) is implemented for identifying the nonce with its block. Based on the newly generated block, the legal transactions are verified and updated with the hash value. During the verification process, the duplication problems are eliminated by using the cryptographic techniques that comprises the private and public key pair. Typically, the public key is shared with other entities, but the private key is maintained as secret. The developmental cycle of blockchain technology is represented in Fig 5.

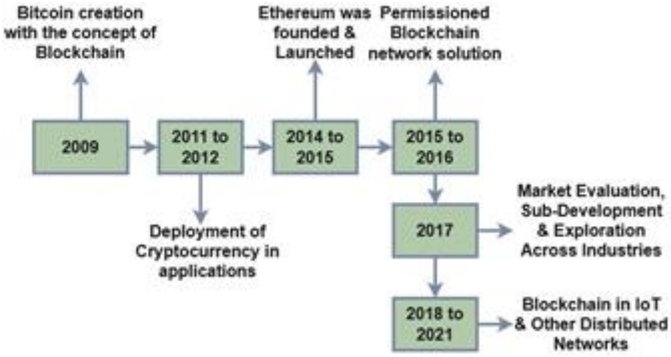
Bitcoin creation with the concept of Blockchain
Ethereum was founded & Launched
Permissioned Blockchain network solution
2009
2011 to 2012
2014 to 2015
2015 to 2016
2017
2018 to 2021
Deployment of Cryptocurrency in applications
Market Evaluation, Sub-Development & Exploration Across Industries
Blockchain in IoT & Other Distributed Networks

Fig 5. Development cycle of blockchain

The consenus algorithms are treated as the heart of blockchain methodology, because which helps to assure the privacy and security of network. It is a technique mainly used for solving the problems to verify the trustworthiness of data. Typically, the mathematical problems require more computational power for finding the solutions, and its output of hash is used to validate the transactions. Also, the consenus algorithms are blockchain platforms as illustrated in Fig 6.

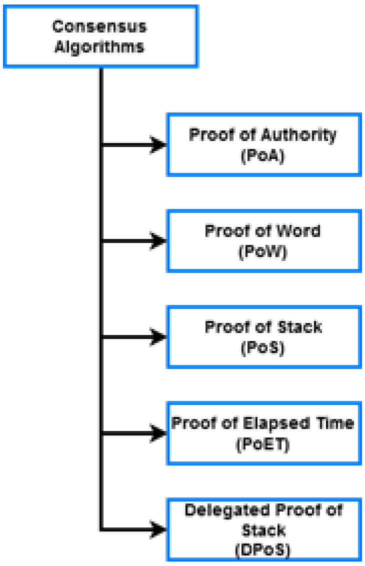

Fig 6. Types of Consensus algorithms

C. Blockchain based Access Controlling Methods

Due to the rapid growth of networking technology and communication systems, the IoT systems are highly attracted by many researchers in recent times. In this domain, various smart devices are interconnected with each other through the internet, which is highly beneficial for the IoT users in terms of remote monitoring, easy to use, adaptability, and data sharing. Still, the centralized structure is one of the major problems faced by the IoT systems, because there may be an increased chance for the system failure due to its lack of trust between the communicating devices. Therefore, various blockchain based access controlling techniques are developed in the conventional works, which comprises the following models:

- Attribute based access controlling
- Distributed access controlling
- Token based access controlling
- Distributed key management
- Smart contract based access controlling

1) Attribute Based Access Controlling (ABAC)

This kind of blockchain methodology is mainly developed to make the access management process as more simple in the IoT systems. Rouhani, et al [23] implemented an ABAC based blockchain methodology for protecting the IoT devices from the unauthorized users. The main beneficiaries of using this technique are listed in below: Fined grained and flexible access controlling, efficient access controlling policies, and makes the complex policies as more simple and reliable. Moreover, it includes the components of policy decision point, administration point, and information point. Generally, the ABAC is a kind of logical access controlling technique that provides the access to the entities or users according to the system rules and policies. Ren, et al [24] deployed an attribute based access controlling mechanism for the proper permission management of SDN-IoT systems. Also, the SILedger technology was utilized in this work for enabling an effective authorization in the heterogeneous environment.

This type of access controlling technique is mainly interlinked with the distributed network, which is the mixture of smart contract, sensor network, agent node, management hubs, and blockchain network. In paper [25], the Ethereum based distributed access controlling technique is deployed for securing the IoT systems against the malicious users. Here, the smart contract based system model is developed for that holds the components of subject attribute management, object attribute management, and policy management. The key benefits of using this model are reduced time and cost with simple computational operations.

3) Token based access controlling

Abdi, et al [26] presented a comprehensive review about the different types of blockchain based access controlling methodologies used in the IoT systems. Typically, the tokenization is a kind of digital signature used to access the system privileges based on proper authentication and access controlling policies. Xu, et al [27] implemented a robust identity based token management methodology for propagating the access permissions in the IoT systems. Moreover, it deployed the smart contracts for managing the tokens in the blockchain network. In addition to that, the capability based access right authorization was performed to in the blockchain network. When the user requests the service to the server, the cached token data is extracted from the storage for validating the authorization of user. The token based access controlling schemes are easy to implement, and it has the reduced communication overhead.

4) Distributed Key Management

Ma, et al [28] utilized a hierarchical access controlling mechanism incorporated with the distributed key management strategy for IoT systems. In this framework, the blockchain based key management technique is mainly used for assuring the security requirements of IoT, which includes extensibility, fine-grained access controlling, and decentralization. During key management, the computational operations like initialization, query accessing, record accessing, key updation, and revocation have been performed. Moreover, the transaction signature is also verified based on the hash value of present and previous transactions. The key benefits of using this approach are minimal processing time, mining time, and communication overhead. Panda, et al [29] used an authentication based distributed key management mechanism for IoT security. Here, the one way hash chain has been utilized to create the cryptographic keys, which provides the seed for generating the set of hash values to make a chain.

5) Smart Contract based Access Controlling

Sultana, et al [30] integrated the access controlling mechanism with the blockchain smart contracts for increasing the security of IoT devices. In the blockchain methodology, the smart contracts are mainly used to eradicate the participation of other third-parties. Typically, it is defined as the computerized programs, which forms the rules for enabling the valid transactions between two entities. Moreover, the transactions are not completed, until it satisfy all the agreements of smart contracts. The smart contract based access controlling mechanism prevents the IoT system from the single point of failure. Zhang, et al [31] deployed a smart contract based access controlling framework for the IoT systems. In this framework, policies, which includes the fields of resource, action, permission, and time of least request. Moreover, it incorporates the operations of other contracts such as access control contract, register contract, and judge contract.

4. Results And Discussion

This section validates the security properties and efficiency of the conventional approaches used in the IoT smart systems. Table 1 validates the different types of security properties that are successfully addressed by the conventional blockchain approaches. It includes the parameters of privacy, scalability, decentralization, extensibility, and computational overhead. According this evaluation, it is analyzed that the extensibility could not be highly addressed by the existing works. Also, most of techniques mainly focused on to satisfy the property of decentralization, then privacy and scalability measures. The computational overhead is also does not mainly focused by the existing works. The successful blockchain methodology should satisfy all these requirements for ensuring the strong security of IoT systems. Similarly, some other general and essential measures satisfied by the existing blockchain methodologies are also listed in Table 2. Based on the results, it is analyzed that the security level of blockchain mechanism is mainly determined based on these parameters of anonymity, authentication, access control, availability, and immutability.

Table 1. Security properties addressed by the conventional approaches

References	Privacy	Scalability	Decentralization	Extensibility	Computational overhead
[32]	Yes	Yes	Yes	NA	Yes
[33]	Yes	Yes	Yes	NA	Yes
[34]	Yes	Yes	Yes	Yes	No
[35]	No	Yes	No	NA	NA
[28]	Yes	Yes	Yes	Yes	No
[36]	No	No	Yes	Yes	No
[37]	Yes	Yes	Yes	No	NA
[38]	No	No	Yes	No	NA
[39]	No	Yes	Yes	No	Yes
[40]	Yes	Yes	Yes	NA	Yes
[41]	Yes	No	Yes	NA	Yes
[30]	Yes	No	Yes	NA	NA

Table 2. Comparative analysis among the conventional approaches based on IoT security requirements with the blockchain methodology

Security Measures	[42]	[43]	[44]	[45]	[46]	[47]
Anonymity	Yes	Yes	Yes	Yes	No	Yes
Authentication	Yes	Yes	Yes	Yes	No	Yes
Availability	Yes	No	No	Yes	No	Yes
Access Control	No	No	Yes	Yes	Yes	No
Confidentiality	Yes	No	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes	Yes	Yes
Immutability	Yes	Yes	Yes	Yes	Yes	Yes
Privacy	Yes	Yes	Yes	No	Yes	Yes
Non-	Yes	Yes	Yes	Yes	Yes	Yes

Table 3 investigates the different types of problems associated to the IoT systems with the appropriate characteristics of blockchain. Among other, the illegal use, scalability, and accessaddressed by the existing works. Ensuring the properties of smart contracts, anonymity, and scalability helps to solve the most of the challenges in the IoT systems. Table 4 compares the existing blockchain integrated security models with distinct characteristics, pros and cons.

Table 3. IoT problems Vs Blockchain characteristics

Characteristics of Blockchain	IoT Problems							
	Privacy	Integrity	Third party	Trusted data origin	Access control	Single point of failure	Scalability	Illegal use
Decartelization	Yes	Yes	No	Yes	No	Yes	No	Yes
Persistency	No	Yes	No	Yes	No	No	No	No
Anonymity	Yes	No	No	No	No	No	No	No
Scalability	No	No	No	No	No	No	Yes	No
Resilience	No	No	Yes	No	No	Yes	No	No
High efficiency	No	No	Yes	No	Yes	Yes	No	No
Transparency	No	No	No	Yes	Yes	No	No	No
Smart Contract	Yes	Yes	No	No	Yes	No	No	No

Table 4. Comparative analysis

Authors & Year	**Security Mechanism**	**Description**	**Advantages**	**Disadvantages**
Mohanty, et al & 2020 [16]	Efficient Lightweight Integrated Blockchain (ELIB)	The purpose of this technique is to satisfy the security requirements of IoT based smart home application systems.	1. Minimal processing time 2. Reduced energy consumption 3. Optimized overhead	1. Complex mathematical operations
Dorri, et al & 2019 [20]	Lightweight Scalable Blockchain (LSB) model	In this paper, an effective blockchain methodology has been implemented to assure the privacy and security of IoT systems.	1. High fault tolerance capability 2. Minimal imperceptible delay	1. Increased overhead 2. High processing time
Zhang, et al & 2018 [31]	Smart contract blockchain methodology	Here, the smart contract based security framework is developed for identifying the misbehavior nodes in the network using the access control contracts.	1. Trustworthy access controlling 2. Minimal transaction delay	1. Time consuming task 2. Complexity in updating rules
Xu, et al & 2018 [27]	Blend CAC	This paper developed a blockchain enabled decentralized capability based access controlling mechanism for securing the IoT systems.	1. Better scalability 2. Lightweight model 3. Centralized policy decision support	1. Role explosion 2. High resource utilization

Rouhani, et al & 2021 [23]	Distributed attribute based access controlling model	It efficiently regulates the access permissions according to the characteristics of resources, subjects, and context.	1. High flexibility 2. Simple to implement 3. Fine-grained model	1. Possibility for the privacy leakage 2. Interoperability issues
Sultana, et al & 2020 [30]	Blockchain based Smart Contracts	Here, the blockchain based data sharing system is developed for enabling the proper authentication and access controlling in IoT systems.	1. Efficient access control management 2. Ensured trust	1. High execution and transaction cost 2. Inefficient data sharing
Sultan, et al & 2019 [48]	Blockchain for IoT systems	The authors investigated about the major impacts and challenges of deploying the blockchain methodology for IoT smart systems.	1. It provided some suitable suggestions for identifying the system	1. It failed to analyze the performance of blockchain methodology in IoT systems
Ammi, et al & 2021 [49]	Hyperledger blockchain methodology for IoT smart home security	It mainly objects to ensure the properties of availability, authorization, confidentiality, and privacy of smart home IoT systems.	1. Better transparency and Interoperability 2. High robustness	1. Increased computational overhead. 2. High energy delay.
Lin, et al & 2019 [50]	Secured mutual authentication based blockchain methodology	This approach integrates the functions of group signature, message authentication code, and user's access history for ensuring the security requirements of IoT	1. Better traceability and privacy preservation. 2. Reduced communication	1. Complex mathematical operations. 2. Possibility for data loss.
Khan, et al & 2020 [51]	Machine learning based blockchain framework	The main purpose of this work is to ensure the security of smart home systems by using the machine learning based decentralized blockchain	1. Better accuracy. 2. Minimal false positives.	1. High computational overhead. 2. Complex mathematical operations.
Singh, et al & 2019 [52]	Efficient and secured blockchain architecture for	The main contribution of this paper was to obtain an increased data integrity and confidentiality by using an encryption based hashing algorithm.	1. Ensured data privacyand availability. 2. Better system	1. Increased latency. 2. More energy consumption.

Fig 7 validates the error probability analysis of PoT and PoW methods with respect to different cycles of time. The error probability is mainly estimated to determine the efficacy of blockchain methodologies. Moreover, it should be reduced for ensuring the reliable and scalable system operations. Consequently, Fig 8 evaluates the size of blockchain in terms of (KB) with respect to varying number of requests received from the IoT systems. In this analysis, the blockchain size is estimated for both with allocation and without allocation of received requests. From the results, it is observed that the size of without allocation requests is greater than with allocation. Moreover, Fig 9 shows the average energy consumption of IoT- blockchain systems with respect to varying number of requests. The performance and lifetime of networks are highly depends on the energy consumption of devices, which must be minimized for ensuring the increased lifespan. According to the results, it is analyzed that the average energy consumption of with allocation is highly reduced, when compared to without allocation of requests. the problems like single point of failure, scalability, and access control are yet to be resolved. Based on this study, a lightweight and efficient blockchain security methodology can be implemented in the future work for ensuring highly strengthening the security of IoT systems. Also, the cryptographic techniques can also utilized in future for minimizing the memory usage and storage overhead of IoT systems.

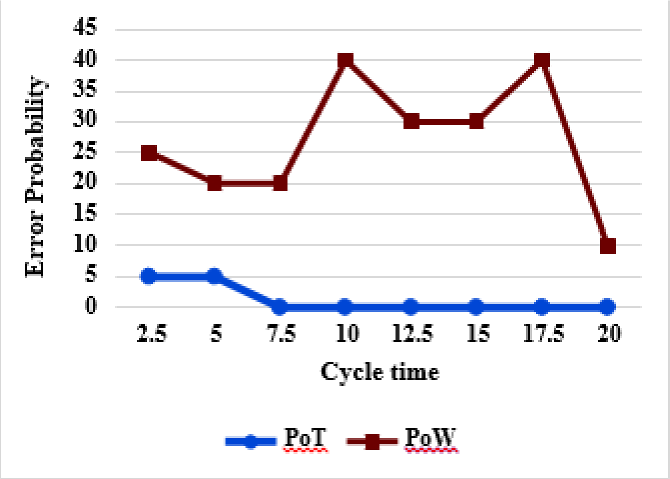

Fig 7. Error probability analysis

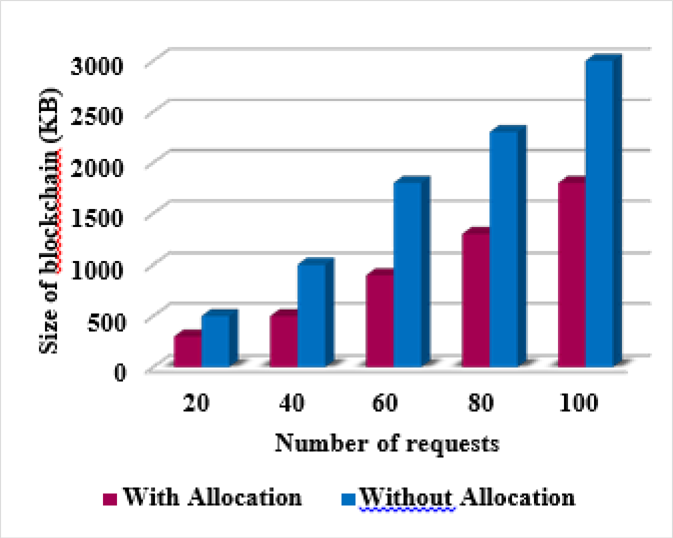

Fig 8. Blockchain size Vs number of requests

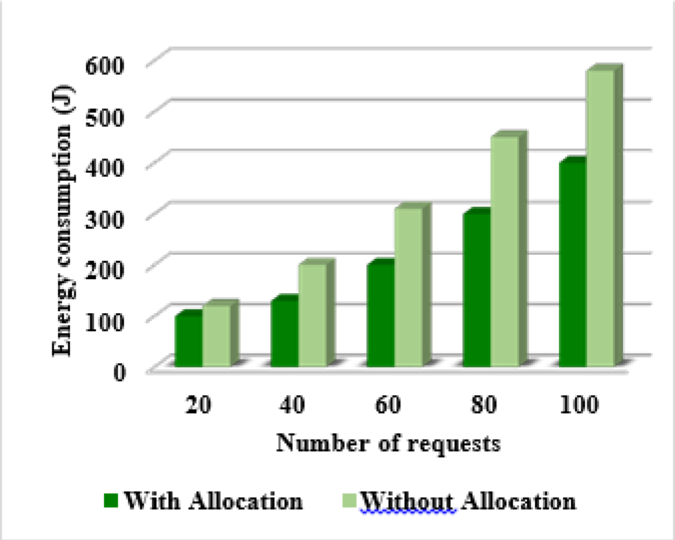

Fig 9. Analysis of energy consumption in blockchain-IoT systems

5. Conclusion

The purpose of this paper is to present a comprehensive analysis for analyzing the different types of blockchain methodologies used for strengthening the security of IoT systems. Typically, developing an efficient and simple blockchain methodology is one of the complicated tasks due to its increased computational complexity and cost consumption. According to this review, it is studied that a lightweight blockchain methodologies are more suitable for IoT security systems, because which has the benefits of minimal processing time and reduced computational overhead. Similarly, the smart contracts based blockchain technologies are extensively used in many security applications, which ensures an authentication based access controlling operations. Also, it is important to guarantee the properties of privacy, integrity, access control, scalability, resilience and efficiency during the design of security mechanisms. Most of existing works employed the consensus algorithms for ensuring the above properties, which uses the hash codes for validating the transactions. However, pp. 12-18, 2018.

References

1. Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," IEEE Wireless Communications, vol. 25, With Allocation Without Allocation
2. S. Dhar and I. Bose, "Securing IoT devices using zero trust and blockchain," Journal of Organizational Computing and Electronic Commerce, vol. 31, pp. 18-34, 2021.

3. M. El-Masri and E. M. A. Hussain, "Blockchain as a mean to secure Internet of Things ecosystems–a systematic literature review," Journal of Enterprise Information Management, 2021.
4. S. M. Muzammal and R. K. Murugesan, "A study on leveraging blockchain technology for IoT security enhancement," in 2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA), 2018, pp.1-6.
5. M. H. Miraz and M. Ali, "Blockchain enabled enhanced IoT ecosystem security," in International conference for emerging technologies in computing, 2018, pp. 38-46.
6. R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. Kondaveeti, et al., "Continuous security in IoT using blockchain," in 2018 IEEE international conference on acoustics, speech and signal processing (ICASSP), 2018, pp. 6423-6427.
7. M. Padmaja, S. Shitharth, K. Prasuna, A. Chaturvedi, P. R. Kshirsagar, and A. Vani, "Grow of artificial intelligence to challenge security in IoT application," Wireless Personal Communications, pp. 1-17, 2021.
8. N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," Procedia Computer Science, vol. 132, pp. 1815-1823, 2018.
9. Y. Gupta, R. Shorey, D. Kulkarni, and J. Tew, "The applicability of blockchain in the Internet of Things," in 2018 10th International Conference on Communication Systems & Networks (COMSNETS), 2018, pp. 561-564.
10. S. Choi and J.-H. Lee, "Blockchain-based distributed firmware update architecture for IoT devices," IEEE Access, vol. 8, pp. 37518-37525, 2020.
11. G. B. Mohammad, S. Shitharth, S. A. Syed, R. Dugyala, K. S. Rao, F. Alenezi, et al., "Mechanism of Internet of Things (IoT) Integrated with Radio Frequency Identification (RFID) Technology for Healthcare System," Mathematical Problems in Engineering, vol. 2022, 2022.
12. S. Singh, A. S. Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed iot network," IEEE Access, vol. 9, pp. 13938-13959, 2021.
13. M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges," IEEE access, vol. 8, pp. 32031-32053, 2020.
14. J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," Journal of Network and Computer Applications, vol. 149, p. 102481, 2020. D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G.

15. Muhammad, and J. Wang, "Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network- integrated approach," IEEE Internet of Things Journal, vol. 7, pp. 6143-6149, 2020.
16. S. N. Mohanty, K. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. Lakshmanaprabu, et al., "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy," Future Generation Computer Systems, vol. 102, pp. 1027-1037, 2020.
17. Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, et al., "Towards decentralized IoT security enhancement: A blockchain approach," Computers & Electrical Engineering, vol. 72, pp. 266-273, 2018.
18. O. Alfandi, S. Khanji, L. Ahmad, and A. Khattak, "A survey on boosting IoT security and privacy through blockchain," Cluster Computing, vol. 24, pp. 37-55, 2021.
19. M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future generation computer systems, vol. 82, pp. 395-411, 2018.
20. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT security and anonymity," Journal of Parallel and Distributed Computing, vol. 134, pp. 180-197, 2019.
21. S. Roy, M. Ashaduzzaman, M. Hassan, and 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), 2018, pp. 1-9.
22. R. Aluvalu, V. Uma Maheswari, K. K. Chennam, and S. Shitharth, "Data security in cloud computing using Abe-based access control," in Architectural wireless networks solutions and security issues, ed: Springer, 2021, pp. 47-61.
23. S. Rouhani, R. Belchior, R. S. Cruz, and R. Deters, "Distributed attribute-based access control system using permissioned blockchain," World Wide Web, vol. 24, pp. 1617-1644, 2021.
24. W. Ren, Y. Sun, H. Luo, and M. Guizani, "SILedger: A blockchain and ABE-based access control for applications in SDN-IoT networks," IEEE Transactions on Network and Service Management, vol. 18, pp. 4406-4419, 2021.
25. M. Yutaka, Y. Zhang, M. Sasabe, and S. Kasahara, "Using ethereum blockchain for distributed attribute- based access control in the internet of things," in 2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1-6.
26. A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi, and A. S. A.-M. Al-Ghamdi, "Blockchain platforms and access control classification for IoT systems," Symmetry, vol. 12, p. 1663, 2020.

27. R. Xu, Y. Chen, E. Blasch, and G. Chen, "Blendcac: A blockchain-enabled decentralized capability-based access control for iots," in 2018 IEEE International conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1027-1034.
28. M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario," IEEE access, vol. 7, pp. 34045-34059, 2019.
29. S. S. Panda, D. Jena, B. K. Mohanta, S.Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Authentication and key management in distributed iot using blockchain technology," IEEE Internet of Things Journal, vol. 8, pp. 12947-12954, 2021.
30. T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, "Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices," Applied Sciences, vol. 10, p. 488, 2020.
31. Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," IEEE Internet of Things Journal, vol. 6, pp.1594-1605, 2018.
32. S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," IEEE Access, vol. 7, pp. 38431-38441, 2019.
33. Y. Zhang, B. Li, B. Liu, J. Wu, Y. Wang, and X. Yang, "An attribute-based collaborative access control scheme using blockchain for IoT devices," Electronics, vol. 9, p. 285, 2020.
34. A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman,"FairAccess: a new Blockchain-based access control framework for the Internet of Things," Security and ommunication networks, vol. 9, pp. 5943-5964, 2016.
35. O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," IEEE internet of things journal, vol. 5, pp. 1184-1195, 2018.
36. N. Fotiou, I. Pittaras, V. A. Siris, S. Voulgaris, and G.C. Polyzos, "Secure IoT access at scale using blockchains and smart contracts," in 2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), 2019, pp. 1-6.
37. [A. Z. Ourad, B. Belgacem, and K. Salah, "Using blockchain for IOT access control and authentication management," in International Conference on Internet of Things, 2018, pp. 150-164.
38. H. Al Breiki, L. Al Qassem, K. Salah, M. H. U. Rehman, and D. Sevtinovic, "Decentralized access control for IoT data using blockchain and trusted oracles," in 2019 IEEE International Conference on Industrial Internet (ICII), 2019, pp. 248-257.

39. O. J. A. Pinno, A. R. A. Gregio, and L. C. De Bona, "Controlchain: Blockchain as a central enabler for access control authorizations in the iot," in GLOBECOM 2017-2017 IEEE Global Communications Conference, 2017, pp. 1-6.
40. G. Yu, X. Zha, X. Wang, W. Ni, K. Yu, P. Yu, et al., "Enabling attribute revocation for fine-grained access control in blockchain-IoT systems," IEEE Transactions on Engineering Management, vol. 67, pp. 1213-1230, 2020.
41. B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," Computer Communications, vol. 153, pp. 229-249, 2020.
42. A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in 2017 IEEE/ACM Second International Conference on Internet-of- Things Design and Implementation (IoTDI), 2017, pp. 173-178.
43. A. G. Abbasi and Z. Khan, "VeidBlock: Verifiable identity using blockchain and ledger in a software defined network," in Companion Proceedings of the10th International Conference on Utility and Cloud Computing, 2017, pp. 173-179.
44. D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," in 2017 Global Internet of Things Summit (GIoTS), 2017, pp. 1-6.
45. B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in 2017 IEEE International Conference on Web Services (ICWS), 2017, pp. 468-475.
46. M. Steichen, S. Hommes, and R. State, "ChainGuard—A firewall for blockchain applications using SDN with OpenFlow," in 2017 Principles, Systems and Applications of IP Telecommunications (IPTComm), 2017, pp. 1-8.
47. S. R. Basnet and S. Shakya, "BSS: Blockchain security over software defined network," in 2017 International conference on computing, communication and automation (ICCCA), 2017, pp. 720-725.
48. A. Sultan, M. A. Mushtaq, and M. Abubakar, "IOT security issues via blockchain: a review paper," in Proceedings of the 2019 International Conference on Blockchain Technology, 2019, pp. 60-65.
49. M. Ammi, S. Alarabi, and E. Benkhelifa, "Customized blockchain-based architecture for secure smart home for lightweight IoT," Information Processing & Management, vol. 58, p. 102482, 2021.
50. C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K.-K. R. Choo, "HomeChain: A blockchain-based secure mutual authentication system for smart homes," IEEE Internet of Things Journal, vol. 7, pp. 818-829, 2019.

51. M. A. Khan, S. Abbas, A. Rehman, Y. Saeed, A. Zeb, M. I. Uddin, et al., "A machine learning approach for blockchain-based smart home networks security," IEEE Network, vol. 35, pp. 223-229, 2020.
52. S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology," International Journal of Distributed Sensor Networks, vol. 15, p. 1550147719844159, 2019.