

Integrating blockchain technology for secure access control in smart home environments: A comprehensive review

Tariq Bishtawi^a, Mohammad Shehab^{a*}, Reem Alzub^b, Ayman Ghaben^c and Suaad M. Alenzi^d

^aCollege of Information Technology, Amman Arab University, Amman 11953, Jordan

^bCollege of Information Technology, Al-Balqa Applied University, Amman, Jordan

^cCollege of Computer Sciences and Informatics, Amman Arab University, Amman 11953, Jordan

^dCollege of Computer science and engineering, University of Hail, Hail, KSA

CHRONICLE

Article history:

Received October 31, 2024

Received in revised format March 10, 2025

Accepted April 24 2025

Available online

April 30 2025

Keywords:

Blockchain

Access control

Smart home

IoT

Cryptographic techniques

ABSTRACT

Smart home technologies have revolutionized modern living by enhancing convenience, efficiency, and security. In contrast, many interconnected devices introduce significant security and privacy challenges. This comprehensive review investigates the integration of blockchain technology as a robust solution for secure access control in smart home environments. The decentralized and tamper-resistant nature of blockchain technology effectively solves important problems, including device authentication, data integrity, and access management, through the use of cryptography and distributed ledgers. The study synthesizes findings from 52 research papers, categorizing them into three thematic areas: blockchain in access control systems, its applications in IoT, and specific implementations for smart homes. It highlights the transformative potential of blockchain in mitigating vulnerabilities inherent in centralized systems, fostering trust, and enhancing security frameworks. Despite its promising applications, challenges such as scalability, interoperability, and energy consumption persist, warranting further research. This paper stresses the necessity of collaboration to tackle these limitations and enhance blockchain-based access control solutions for smart homes, setting the stage for more secure and user-focused smart environments.

1. Introduction

Smart home technology has transformed the home automation sector over time due to technological evolution. This technology allows for multiple sensors and devices in the household to be connected and operated from a smartphone or computer (Rasras et al., 2023). Smart home technology is beneficial to the homeowner by providing effective energy use and additional convenience and security through the automation of tasks such as adjusting the thermostat, switching on lights, or monitoring security cameras (Veneruso et al., 2023). Modern trends in home automation have resulted in the emergence of modern and more sophisticated automated homes, previously referred to as smart homes. These environments provide added convenience by enabling the user to control various systems and devices remotely, increasing energy efficiency and security (Alakbarova, 2023). Using specialized devices and sensors, a smart home enhances the convenience of house residents, who can control all functions in a particular area with ease. Technological development has brought significant changes to the way we operate, and smart home technology has gained an edge over the years. Due to these technologies, the efficiency of modern houses has seen remarkable advancements. By using remote control and automation of actions, personalization and convenience that homeowners have never imagined possible is made available by smart home technologies. Some of the key components of smart home systems include smart appliances, sensors, controllers, and an intelligent interface for efficient managing and interaction. The systems are extended with the aid of integrating mobile applications, including Google

* Corresponding author

E-mail address moh.shehab12@gmail.com (M. Shehab)

Assistant, that allow operating the system with voice commands as well as providing mechanisms for home monitoring (Bethel et al., 2023). In addition, web-based and SMS systems are also available which, together with mobile and Arduino-based central controllers form a rich array of products in the field of home automation designed to meet specific needs of the clients (Mladenova & Cankov, 2023).

The advancement of technology has enabled a new way of securely and openly transmitting and storing data, and that is Thanks to Blockchain Technology. It comprises a range of activities designed such that everything is secure while allowing everyone involved to verify the information using a distributed ledger (Gadekallu et al., 2021). The records consist of a series of information that are stored in a distributed environment, which ensures that nothing can be altered once it has been entered. Several distinctive types of blockchains exist, each type comes with certain pros and cons, these include private and public blockchains. Every blockchain contains blocks and nodes and employs cryptographic algorithms as well as agreement mechanisms, Miners are also included (Singh et al., 2023). In this study, the author describes the current achievements and status of blockchain-based applications. Different industry sectors with their growing revolution are highlighted along with the sheer potential for economical and innovative impact. The development of blockchain technology, its basic tenets and first principles, as well as potential uses in healthcare and other sectors, are all covered in this research. The trends, threats, and prospects in the field of Blockchain are examined during review of literature on the subject. And many more in between are discussed, such as its effects on the financial and healthcare sectors as well as the supply chain management industry. The technology finds its use in finance addressing core challenges such as secure and transparent transactions while ensuring interoperability and scalability (Cole et al., 2019). Integrating blockchain technology into smart home systems is designed to improve security and privacy through effective access control mechanisms. Both researchers and developers are working to establish secure and trustworthy access methods. This will help safeguard data and smart home devices from unauthorized access or tampering, utilizing the tamper-resistant and distributed features of blockchain. This method seems to be capable of addressing critical security challenges associated with sophisticated homes such as insecure device-to-device communication, user and device verification, and fine-grained access control.

The review is generally focused on presenting observations regarding how blockchain technology applications may efficiently resolve issues of authorization and access control on the Internet of Things spaces and thus create reliability and reduce security management overhead using the features inherent in the technology including transparency, data encryption, and resilience to tampering conditions (Siller et al., 2022).

The remaining tasks are arranged as follows: First, in Section 2, we display the aggregated data, and discuss blockchain technology related to the access control system in Section 3. Section 4, describes the blockchain technology related to the Internet of Things. Also reviews the blockchain technology related to the smart home in Section 5. Section 6 contains the discussion session. Finally, the paper concludes in Section 7.

2. Collective data

This section illustrates the mechanism of collecting and organizing related publications including two main steps. First, a list of key search expressions was used to ensure the retrieval of relevant literature. For instance, “Blockchain technology,” “Blockchain technology with access control systems,” “Blockchain technology with IoT,” and “Blockchain technology with smart home.” These expressions were specifically chosen to capture the specific aspects of blockchain applications, especially in relation to access control systems and IoT-based smart home environments. The next step involved utilizing various academic databases, including Google Scholar, Springer, IEEE Xplore, and Elsevier. Initially, 75 articles were identified through this process. These publications were then carefully filtered based on the research objectives, with priority given to those offering meaningful insights into the application of blockchain technology. Therefore, 50 articles were chosen for detailed analysis. These articles were categorized into three sections, Blockchain technology related to access control systems, Blockchain technology related to IoT, and Blockchain technology related to Smart Home.

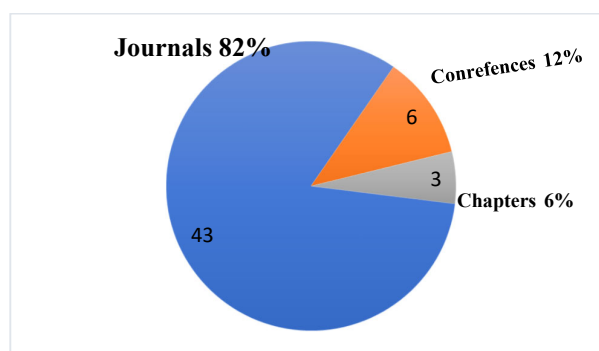


Fig. 1. Classification of the Publications

The classification of the publications is illustrated in Fig. 1, which shows their distribution by type. Journals account for the majority at 82%, followed by conference proceedings at 12%, and book chapters at 6%. This pie chart visually highlights the dominance of journal articles in the selected publications, reflecting their significant role in disseminating research within the field. Fig. 2 illustrates the annual trend of scholarly publications in the field of blockchain-based access control systems and IoT applications. The chart demonstrates steady growth in research contributions from 2020 to 2024, with a notable increase in publications in 2023 and 2024, reflecting the rising interest and intensified research efforts in this domain over recent years.

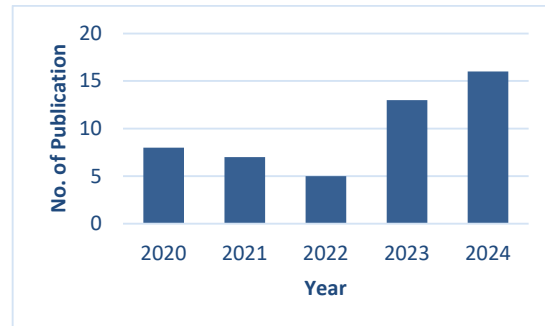


Fig. 2. Growth of Publications

3. Blockchain technology related to access control system

Zhang and Yan (2021) developed a blockchain-based system for smart home access control. This system utilizes Hyperledger Fabric and smart contracts to enforce access control measures. It ensures secure access for both local devices and remote user-initiated access via the Internet by creating a hybrid access control system that integrates dynamic attribute-based access control with a fixed access control matrix. To bolster security, Hussain et al. (2024) developed a dynamic access control system that employs machine learning algorithms and the fixed characteristics of Blockchain technology, particularly Ethereum. This system features machine learning techniques like neural networks and support vector machines (SVM). To further enhance performance and minimize latency, a caching mechanism based on the Ethereum Blockchain is also included. For smart home settings, Zhang and Xie (2024) suggested a trustworthy data access control system built on blockchain technology and attribute-based encryption. To accomplish fine-grained data access control, increase the effectiveness of data sharing, and safeguard user privacy, the approach blends symmetric encryption algorithms with attribute-based encryption algorithms. The blockchain stores the hash value that the cloud generates. The system will transmit a matching proof transaction to the blockchain whenever a user initiates an access transaction. To mitigate cybersecurity threats in smart home situations, Liu (2024) suggested a device access solution built on a zero-trust network architecture. The suggested method achieves mutual authentication between the newly connected device and the central control device (CCD) without compromising device privacy by using a zero-knowledge identity verification technique based on quadratic residues. Khan et al. (2024) put forward a solution that leverages smart contracts on Ethereum and Zerynth, explaining how Blockchain technology can be applied to secure IoT devices. By using Remix IDE and Infura, the development process is made easier and quicker. The ProVerif tool is utilized for formal verification of the correctness of user access control mechanisms in schema analysis. The paper emphasizes the benefits of security, transparency, scalability, speed, and data integrity, which are key advantages of integrating Blockchain systems with IoT devices. Güler (2024) has introduced a blockchain and smart contract-based approach to enhancing cyber security in smart home systems. The proposed system is designed to maintain data integrity and immutability within smart networks in households. Moreover, it has the potential to significantly boost security, privacy, and efficiency by streamlining the automation and coordination of various devices in a smart home context. A strategy for smart home authentication and access control using decentralized identifiers (DIDs) was presented by Zhao et al. (2023). This system features an improved capability-based access control approach that eases the complexity of authentication and simplifies user identity verification. DIDs are also utilized for uniquely identifying all the stakeholders within the smart home network, which includes users and smart devices.

The work detailed in (Alruwaili, 2024) introduces a Blockchain-based Deep Learning in the Secure Smart Home Network (BPDLS-SHN) on an IoT-cloud platform. This technique employs blockchain technology to enhance data privacy within the smart home framework. Additionally, BPDLS-SHN incorporates various methods for detecting malicious activities, including feature selection through the Binary Fox Optimization Algorithm (BFOA), classification via Attention-based Long Short-Term Memory (ALSTM), and hyperparameter tuning using Harbor Seal Whiskers Optimization (HSWO). Awais et al. (2024) offered a multi-agent system supervised by Blockchain Communities Management as an effective, decentralized, and creative way to improve IoT access control security. It incorporates a number of technologies, such as fog nodes, locally IoT devices, and cloud services. The decentralized and irreversible ledger characteristics of blockchain technology can be effectively utilized to address significant security issues in IoT systems, such as data leaks and cyberattacks, as demonstrated by Kumar et al. (2025). It explores the potential integration of blockchain technology with the IoT, highlighting how its security models and consensus procedures can enhance the overall security of IoT networks. To improve the effectiveness of access validations and policy management for Internet of Things systems, Huang et al. (2024) proposed a Pruned Blockchain based Access Control (PBAC) protocol. Because IoT devices are decentralized, standard centralized access control techniques have drawbacks that this protocol overcomes.

Given the sensitive nature of the data being handled, Sarkar et al. (2024) highlighted the growing significance of security in IoT. Also, access control protocols were separated into three groups to aid in a deeper comprehension: those that depend on certificates, those that do not, and those that are intended to use blockchain technology. A detailed assessment of a few current systems and a comparison of the transmission and computation costs were given for each category. A strategy to control access to IoT devices using Non-Fungible Tokens (NFTs) is presented in (2023).

Table 1
Summary of Blockchain technology related to access control system

Ref.	Description	Strength	Weaknesses
Zhang & Yan, 2021	Control access to your smart home with Blockchain using Hyperledger Fabric.	Attribute-based access via smart contracts	Privacy risks depending on blockchain type
Hussain et al., 2024	Dynamic access control leveraging ML and Ethereum	Real-time adaptability	High computational needs for IoT devices
Zhang & Xie, 2024	Blockchain with attribute-based encryption for smart homes	Storage efficiency with cloud integration	Key management vulnerabilities
Liu, 2024	Zero-trust network architecture for device access	Novel security via mutual authentication	Efficiency concerns for low-power
Khan, 2024	Applied blockchain for IoT security using Ethereum and Zerynth	Strong ECC-based security	Slower access control procedures
Güler, 2024	Used blockchain and smart contracts for smart home security	Data integrity and immutability	Lacks real-world validation
Zhao et al., 2023	Decentralized identifiers for smart home access control	Simplified access via a single registration	Technical implementation challenges
Alruwaili, 2024	Deep learning integrated with blockchain for IoT-cloud security	High performance in threat detection	Complex implementation
Awais et al., 2024	Multi-agent blockchain for IoT access control	Secure fog node connections	Delays in time-sensitive applications
Dinesh et al., 2025	Real-world blockchain applications for IoT	Industrial case studies	Generic results
Huang et al., 2024	Pruned blockchain protocol for access control	Faster access by 43%	Limited flexibility in diverse IoT
Sarkar et al., 2024	Comprehensive IoT access control categorization	Clarifies access techniques	Theoretical focus without evidence
Sharma & Goveas, 2023	NFT-based IoT device access control	Empirical validation of efficiency	Energy and scalability issues
Bobde et al., 2024	Simulated attacks for blockchain-IoT	Robust security framework	Scalability challenges
Hussain et al., 2023	Ethereum-based IoT access control (Ether-IoT)	Decentralized data storage	Potential performance lags
Yang et al., 2021	Blockchain with square root algorithm for IoT authentication	Usability and security validation	Overlooked scalability concerns
Yang, 2024	Proxy re-encryption for IoT blockchain	Efficient transmission and coding	Lengthy re-encryption key generation

It demonstrated how this method may be applied to prevent unwanted access, add new users to the device access list, and grant access to the device only to those who are permitted. To directly address security issues, Bobde et al. (2024) suggested a thorough strategy that incorporates blockchain integration and experimental methods. To find weaknesses in IoT security solutions, the researchers run extensive simulations of real-world attacks. These assaults were replicated in order to find system weaknesses. The foundation of the suggested security framework is blockchain technology, in addition to experimental methods. Hussain et al. (2023) proposed Ether-IoT as a solution to the challenges posed by conventional centralized systems. This Internet of Things access control system utilizes the Ethereum Blockchain to create a decentralized framework. By combining Attribute-Based Access Control (ABAC) with Blockchain, Ether-IoT facilitates decentralized, fine-grained, and dynamically scalable management of IoT access control. To overcome the difficulties, a novel blockchain-based authentication system is put forth by Yang et al. (2021). The suggested technique achieves an effective authentication process by combining blockchain technology with the widely used square root algorithm. Lin et al. (2024) used proxy re-encryption technology to convert the data collected by IoT devices into ciphertext. Then the encrypted IoT data is stored on the blockchain. This study also combined Blockchain and Proxy Re-Encryption (BCPRE) technology to propose a secure data sharing method for IoT. The proposed IoT data security sharing method has the advantages of high security, fast encryption speed and good stability, which helps to improve the security performance of IoT. Parmar and Shah (2023) discussed a diverse IoT and blockchain environment that keenly senses and records data after ensuring its accuracy through a decentralized blockchain network. Their study presents a comprehensive method to tackle the potential data security challenges related to safeguarding information throughout its journey. This is achieved through proper authorization, access control policies, device-to-device data protection, and maintaining data integrity, particularly when transferring data from IoT devices to the blockchain network. Albulayhi et al. (2023) introduced an innovative lightweight blockchain-based framework for the Internet of Things aimed at enhancing the efficiency of IoT data communication. They proposed a versatile smart contract that facilitates

controlled and straightforward sharing of IoT data among various stakeholders within IoT systems, along with the capacity for automatic interaction based on a straightforward publish/subscribe model. A blockchain-based lightweight security framework created especially for information exchange in the IoT is presented in (Aljumah & Ahanger, 2023). Additionally, it used a dual chain strategy, combining blockchain technology for transactions and data to guarantee distributed storage and data tamper-proofing.

4. Blockchain technology related to Internet of Things

Wazid et al. (2020) presented a blockchain strategy for managing secure authentication keys in the IoT environment. It focused on future research options including challenges associated with using this technology in communications. It also discussed different types of blockchains and some of the most commonly used consensus algorithms. Umer et al. (2023) developed a system that employs sensors to handle a database for each device via a 5V relay circuit and a Raspberry Pi server. The Android app connects to the Raspberry Pi through an Apache server using an HTTP web interface. To verify its effectiveness, the home automation system was subjected to laboratory tests focusing on both performance and real-time functionality. This study emphasized the accessibility, simplicity, and scalability of the technology and hardware utilized in this setup. In (Ghadekar et al., 2019), the authors introduced a secure Ethereum Blockchain technology tailored for lightweight IoT environments. This technology enhances the IoT architecture by making it decentralized and lightweight, thereby eliminating the need for single-point authentication in IoT networks. The smart home system exemplifies potential use cases for other IoT applications as well. This technology offers measurable features like temperature readings and intrusion detection, with qualitative assessments indicating that the proposed architecture effectively counters various attack scenarios. Lee et al. (2023) introduced a method that employs CP-ABE for managing data access and key agreement, thereby enhancing data security in blockchain-based systems. Their solution utilized blockchains to guarantee data non-repudiation, accountability, and verification. The research assessed the security, functionality, computational, and communication costs of earlier systems. Additionally, cryptographic calculations were performed to evaluate the system's practical application. A qualitative assessment of the proposed architecture demonstrated its effectiveness in mitigating various attacks. In (Mbarek et al., 2020), the authors combined blockchain technology with IoT networks (BAC) to facilitate access to the control system. To boost the efficiency of blockchain management, they implemented an agent-based policy. The study further validated the proposed access control solution by applying it in a parental control context and assessed its performance and feasibility within a simulated smart home environment. Zhang and Yan (2021) used distributed ledger with blockchain cryptography to provide a tamper-resistant access control system through user authentication, device authorization, and audit trails. This study combined blockchain, IoT, and smart home technologies to build secure access control methods for connected homes. Gopalan et al. (2024) proposed an innovative strategy aimed at mitigating deauthentication threats within IoT environments. This methodology is based on research surrounding the development and implementation of the BBMDA framework, followed by a comparison with current techniques and a detailed evaluation. The BBMDA framework outperformed existing methods, including SVM, KNN, and CNN, in terms of accuracy, false positive rate, false negative rate, precision, recall, and F1 score. In (Yang et al., 2021), the authors provided a novel blockchain-based authentication mechanism to address the challenges by combining standard square root algorithms and blockchain technology to achieve excellent authentication. It demonstrated the security and utility of the proposed approach through comprehensive security analysis and experimentation. Shakarami et al. (2022) utilized a publish-subscribe model for access management within smart home IoT systems to introduce a decentralized ledger-based architecture. Their work emphasized the assignment of operational permissions and was backed by a proof-of-concept implementation that employs smart contracts to maintain governance integrity, taking advantage of the transparency and distribution features inherent in blockchain technology.

Ruzbahani (2024) presented the application of AI techniques to blockchain-enabled IoT devices, which improves data confidentiality and integrity across networks. The impact of integrating blockchain with AI is that it can automate and improve security operations in the face of increasing cyber threats. This dual advantage also increases the resilience of the network against cyber-attacks. In (Raj & Ghosh, 2023), the authors offered an improvement to the security issues of Fusion Chain architecture by developing access policies for all data elements and the proposed model is named Fusion Chain-S. To ensure fault tolerance, the study used COAP (Constrained Application Protocol) as a security channel. The security of the framework is analyzed using BAN logic. Maesa et al. (2017) introduced a groundbreaking solution for establishing regulations that allow the distributed transfer and access to rights among users, leveraging blockchain technology. This approach makes policies and the exchange of rights transparent on the blockchain, enabling any user to easily view the relevant policy connected to a resource and the entities that have access rights. The main proposal is to record access permissions for a resource on the blockchain and manage them via "transactions". Ali et al. (2021) exploited the phenomenon known as blockchain to eliminate data security issues. The manufacturing technology was used to secure IoT devices and data as a Hyperledger blockchain framework. To evaluate data security solutions due to the diversity of IoT devices, an IoT-based smart home setup was chosen. In (Gopal, 2020), the Ethereum platform is used in the blockchain by providing the applications used to secure the server. The hardware and software are also carefully examined for their functional and non-functional requirements. To improve the quality of life, technology and services are managed over the network and because smart home systems are based on the IoT so that multiple home facilities can be managed remotely with a single mobile device, this increases their popularity. Singh et al. (2023) presented a proposed blockchain-based smart home gateway that provides protection against potential attacks on smart home gateways. To meet the security needs of smart home gateways, the proposed decentralized architecture uses Ethereum blockchain technology which increases confidentiality, integrity and authentication. The SHA-2 hash algorithm can be used to store the data generated by the network nodes or kept in databases based on specific information. Agrawal and Dhaou (2022) highlighted the significance of privacy and security while using the IoT to access data. It also

highlighted the difficulties developers experience in protecting user data because of the decentralized and diverse nature of IoT environments. Additionally, it criticized current access control models that depend on centralized structures, highlighting the security issues with these systems, particularly in light of the dynamic interactions between IoT devices.

Table 2
Summary of Blockchain technology related to Internet of Things

Ref.	Description	Strength	Weaknesses
Wazid et al., 2020	IoT authentication using blockchain	Integrates blockchain with IoT challenges	Limited practical validation
Umer et al., 2023	Sensors via Raspberry Pi and Android app	Combines blockchain and deep learning	high computational demands
Ghadekar et al., 2019	Secure Ethereum Blockchain for IoT	Resilience to attacks	High energy use
Lee et al., 2023	CP-ABE for blockchain security in IoT	Fine-grained access control	Limited real-world testing
Mbarek et al., 2020	Agent-based IoT access control with blockchain	Accurate access control	Lack of real-world validation
Zhang and Yan, 2021	Tamper-resistant cryptography for IoT	Effective security	Weak real-world implementation
Gopalan et al., 2024	BBMDA framework to prevent IoT threats	Adaptable to various IoT applications	Lack of testing
Yang et al., 2021	Blockchain authentication using algorithms	Reduced latency	Integration challenges
Shakarami et al., 2022	Decentralized ledger for IoT management	Reduced fraud risk	High computing
Ruzbahani, 2024	AI-based blockchain for IoT data confidentiality	Real-time threat detection	Privacy concerns
Raj and Ghosh, (2023)	Fusion Chain-S for scalable IoT access	Efficient resource use	Security trade-offs
Maesa et al. (2017)	Improved IoT access control via blockchain	Transparency	Integration and design challenges
Ali et al., 2021	Hyperledger for IoT data security	Smart contracts	Contract vulnerabilities
Gopal, 2020	Ethereum for IoT server security	Enhances privacy	High power
Singh et al., 2023	Smart home gateway with blockchain	Decentralization and privacy	Integration complexity
Namane and Dhaou, 2022	Privacy and security challenges in IoT	Highlights privacy	Limited practical examples

5. Blockchain technology related to Smart Home

Lee et al. (2020) introduced blockchain technology in a smart home system based on a gateway architecture to improve data integrity and avoid data forgery in smart home environments. The technology guaranteed that IoT device data administration in smart home systems was safe and impenetrable. The gateway mechanism controls the flow of information between the blockchain and the limitations of IoT devices. The results showed the proposed architect solved the cyber security threats of safe smart home systems. Majeed et al. (2020) provided a system as an Android app that integrated two mechanisms SVM and blockchain in home automation systems. SVM was used for intelligent decision-making based on two states on, and off while blockchain was used for authentication of IoT devices. The system is based on Raspberry Pi as a database server and HTTP interface with Apache server for communication between App and Raspberry Pi. The proposed system was evaluated in real life and conveniently showed usefulness and usability besides high security, privacy, and reality in smart home applications. A blockchain-based smart home (BSH) control system architecture built on cloud-based services and blockchain technology was presented by Liao (2022). Cloud services were used to control and manage smart home devices. BSH access control was made safe and effective with blockchain technology. Adhering to the policy on access control, the suggested schema inspected every resource visitor and completed requests using an SM2 threshold signature. The Hyperledger Fabric alliance chain-building platform was used to evaluate the schema, ensuring that resource suppliers could take part in all access control procedures and reduce the possibility of unwanted access. The findings demonstrated the BSH access control scheme's strong suitability for use in a smart home scenario. Lee and Kim (2021) examined the effectiveness of blockchain technology on cyber defense designing through the security and privacy of decentralized data, avoiding tampering. It points to some issues such as improved identification and authentication data, and safeguards for IoT and communication protocols. The study concludes that blockchain has a lot of potential for combating cyber threats, further development is required to fully realize its potential in workable, effective, and legal implementations. Arif et al. (2020) addressed Blockchain technology's potential as an effective solution to the security challenges applied to smart home systems. The study presented a straightforward safe smart home architecture design based on the Consortium blockchain, a refined form of blockchain. By combining blockchain technology with IoT resources that are limited, the study enhanced security by enabling trusted peer-to-peer communication and immutable data logs. The model was evaluated and tested by testbed using a few household IoT devices and concluded blockchain provides a solution for improving smart home protection.

Qashlan et al. (2021) identified an authentication method that establishes a secure framework for Internet of Things devices within smart home ecosystems. This approach combines attribute-based access control, smart contracts, and edge computing. The authors proposed a privacy-preserving technique that ensures secure data transfer and storage by leveraging the decentralized and immutable features of blockchain technology. By employing cryptographic methods to anonymize user data, this system safeguards sensitive information while maintaining functionality. The study demonstrated how blockchain can mitigate privacy risks and enhance trust in smart home environments. In another study, the authors in (Pancari et al., 2023) discussed the deployment of attribute-based access control (ABAC) in an Internet of Things smart home setting, focusing on two widely used blockchain platforms: Ethereum and Hyperledger Fabric. They analyzed the advantages and disadvantages of each platform. Ethereum is deemed a more suitable network for building an ABAC environment due to its flexible architecture, which allows for the integration of a greater number of real IoT devices. On the other hand, Hyperledger Fabric offers a much faster implementation process, thanks to its test networks and chain code availability. Noor et al. (2022) investigated how blockchain technology might improve smart agricultural systems' security and transparency. The framework implements decentralized access control to address concerns such as data privacy, unauthorized access, and trust in multi-stakeholder settings. Farmers, sensors, and service providers may share data safely thanks to blockchain's immutable ledger, which reduces dependency on centralized authority. Only authorized users will be able to communicate with the system thanks to the suggested solution's automation of access management through smart contracts. This approach enhances the security, scalability, and efficiency of smart farming apps, while promoting sustainable agriculture practices. In order to enhance energy efficiency and security during remote green lightning situations, Huang (2024) integrated blockchain-based technologies into smart home systems. The author's purpose was enhancing the system's functionality and security to satisfy rural communities' lighting requirements and support sustainable development by optimizing the energy usage in IoT via smart home systems. The results showed the developing rural environments as smart home system by used blockchain technology in IoT devices. Gopal (2020) integrated smart contract as a blockchain mechanism in smart home systems. Smart contracts support the transaction to happen without third parties, also the person can retrieve stored data with public and private keys. Blockchain and smart contracts were used in the construction of a home automation control system that regulates the ON and OFF states of the equipment in a smart house. The GPIO emulator was used to view the outcome of this design. Park and Chang (2022) suggested an improved device management system that uses zero-knowledge proof and smart blockchain contracts to authenticate each device in a smart home, hence improving security. The objective of this paper is to protect the public keys of home network devices and their communication with one another. The proposed model, when executed three times on Rinkeby, one of Ethereum's test networks, showed an improvement of about 10 seconds over the block generation-based method. Sisi and Souri (2021) introduced a secure and efficient remote mutual authentication system featuring fine-grained access control. This system combined digital signatures and blockchain technology to verify users, activate the domestic gateway, and ensure reliable auditing of changes to access policies, access histories, and device credentials. The findings showed that the system significantly enhanced the security of smart home systems. Xue et al. (2018) developed a private blockchain-based access control system for efficiently and securely managing access in the context of smart homes. A private blockchain that prioritizes secure storage and security against data manipulation, stores access logs, and significantly lowers communication and processing overhead. The system demonstrated that PBAC is practical and effective in smart home ecosystems. Ghadimi et al. (2024) introduced a non-linear model applied to smart home systems. The model identified the regulations, user concerns, and elements that comprise the security of IoT devices in smart homes. The model stored the security rules as a script inside the blockchain using blockchain technology. The findings demonstrated a high degree of statistical features, including distribution and interoperability, and a low degree of time-related features, such as verifying the object's authenticity. Johari and Alsaqour (2022) developed a model aimed at enhancing security within smart home networks. They examined various security threats tied to these networks through a qualitative lens, including detailed case study analysis. By integrating blockchain technology, the authors proposed ways to bolster safety and security in smart home environments. Their findings suggest that this model significantly enhances ongoing access control and adaptability in security architecture. Song et al. (2020) presented an innovative approach that merges the Attribute-Based Access Control (ABAC) model with blockchain technology. The system employs PDP and PIP smart contracts to facilitate effective access control decisions. In the realm of open IoT, this framework promises distributed, dynamic, and reliable access management. Conducting three experiments, the schema simulated an access control scenario within a smart home setting, demonstrating the practical feasibility of access control decisions made through their proposed system.

6. Discussion

This review paper discussed and evaluated the integration of secure access control and blockchain technology in the context of smart home environments. To understand the different blockchain-based secure access control systems, we gathered 52 research papers from various academic sources and categorized them into three groups. According to the literature review, blockchain offers a safe, decentralized, and impenetrable method that can enhance access control. Even if the future looks bright, issues like scalability, interoperability, and security still need to be resolved, which means more research and development is needed. But according to the reviewed literature, blockchain is starting to gain traction as a practical way to boost security and foster confidence in smart home settings. To solve the current issues and improve the state of blockchain-based access control, researchers and practitioners should work together. By examining the strengths of earlier research, we believe that incorporating blockchain technology for secure access control in smart home settings offers a promising way to improve security and privacy in IoT systems. Overall, attention should be directed towards the challenges and unresolved issues concerning latency, scalability, and other critical factors that influence the deployment of blockchain-based access control systems in smart homes.

Table 3
Summary of Blockchain technology related to Smart Home

Ref.	Description	Strength	Weaknesses
Lee et al., 2020	Introduced blockchain in smart homes using gateway architecture	Tamper-proof data for IoT ecosystems	Cost trade-offs
Majeed et al., 2020)	Developed an Android app integrating SVM and blockchain for home automation	Authentication of IoT devices	Difficulty scaling for large IoT ecosystems
Liao, 2022	Use blockchain-based access control schema with cloud services	Improved privacy with reduced centralization	Complexity in integrating blockchain and cloud services
Lee and Kim, 2021	Examined blockchain efficiency in cybersecurity	Transparency enhances cyber defense	Lack of practical evidence
Arif et al., 2020	Explored public and private blockchain solutions	Improved security and tamper resistance	Absence of AI mechanisms
Qashlan et al., 2021	Designed an authentication method combining ABAC	Scalability through edge servers	High complexity for small-scale smart home
Pancari et al., 2023	Assessed Hyperledger Fabric's and Ethereum for ABAC in IoT	Detailed evaluation of platform strengths	Lack real-world implementation
Noor et al., 2022	Investigated blockchain for improving security	Simplifies access control	Performance decreases as transactions
Huang, 2024	Applied blockchain to improve energy performance and security	Focused on sustainable energy	Limited technical resources
Gopal, 2020	Integrated smart contracts for secure and efficient smart home	Reduced human error	Complexity in adoption by non-technical users
Park and Chang, 2022	Using zero-knowledge proof and smart contracts	Improved security and privacy of user	Higher energy consumption
Sisi and Souri, 2021	Integrating digital signatures and blockchain	Fine-grained access control	Higher deployment and maintenance costs
Xue et al., 2018	Created a private access control mechanism based on blockchain technology.	Private blockchains enhance scalability	Lacked practical prototype
Ghadimi et al., 2024	Proposed a nonlinear model for identifying IoT security risks	Accounts for complex attack vectors	Limited application of nonlinear models

7. Conclusion

Integrating blockchain technology for secure access control in smart home environments offers numerous benefits, including enhanced security, transparency, and privacy. Despite challenges, ongoing research and development efforts are driving innovations to overcome technical, regulatory, and usability barriers. By harnessing the transformative potential of blockchain technology, smart homes can achieve greater security, efficiency, and user-centricity in the digital age. In order to create reliable and sustainable blockchain-based access control systems for smart home settings, future research should concentrate on these issues.

This article explores the pros and cons of blockchain security, along with its historical use in cash and digital asset transactions. It also compares various previous studies on how blockchain technology can be integrated for secure access management in smart home environments, aiming to envision the future of smart living. The implementation of such autonomous smart settings could greatly simplify and enhance human life. Blockchain technology offers essential features like automation, security, and privacy, which are crucial for IoT applications in smart environments. In this paper, we illustrate how blockchain technology has addressed specific challenges and limitations across these technologies.

References

- Alakbarova, I. (2023). Development of a model for the analysis of human behavior in a smart home environment. *Problems of Information Society*, 14(1), 75–84. <https://doi.org/10.25045/jpis.v14.i1.08>
- Albulayhi, A. S., & Alsukayti, I. S. (2023). A Blockchain-Centric IoT architecture for effective smart Contract-Based management of IoT data communications. *Electronics*, 12(12), 2564. <https://doi.org/10.3390/electronics12122564>
- Ali, R. F., Muneer, A., Dominic, P., & Taib, S. M. (2021). Hyperledger Fabric Framework with 5G Network for Blockchain-based Security of IoT Smart Home Applications. 2021 International Conference on Decision Aid Sciences and Application (DASA), 1109–1114. <https://doi.org/10.1109/dasa53625.2021.9682263>
- Aljumah, A., & Ahanger, T. A. (2023). Blockchain-Based information sharing security for the internet of things. *Mathematics*, 11(9), 2157. <https://doi.org/10.3390/math11092157>
- Alruwaili, F. F. (2024). Blockchain-Powered Deep Learning for Internet of Things with Cloud-Assisted Secure Smart Home Networks. *IEEE Access*, 12, 119927–119936. <https://doi.org/10.1109/access.2024.3450796>

- Arif, S., Khan, M. A., Rehman, S. U., Kabir, M. A., & Imran, M. (2020). Investigating smart home security: Is blockchain the answer? *IEEE Access*, 8, 117802–117816. <https://doi.org/10.1109/access.2020.3004662>
- Awais, M., Iqbal, M. W., Ahmad, S. Z., & Arif, S. (2024). Revolutionizing Access Control in IoT Systems through Blockchain Technology. *Bulletin of Business and Economics (BBE)*, 13(2), 1090–1095. <https://doi.org/10.61506/01.00434>
- Bethel, G. B., Reddy, M. S. R., Varma, M. K., Vamshi, D. S., & Stephen, P. (2023). Smart Home Application for Challenged Along with Human Temperature Detector. *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 1613–1617. <https://doi.org/10.1109/icscds56580.2023.10104600>
- Bobde, Y., Narayanan, G., Jati, M., Raj, R., Cvitić, I., & Peraković, D. (2024). Enhancing Industrial IoT Network Security through Blockchain Integration. *Electronics*, 13(4), 687. <https://doi.org/10.3390/electronics13040687>
- Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: implications for operations and supply chain management. *Supply Chain Management an International Journal*, 24(4), 469–483. <https://doi.org/10.1108/scm-09-2018-0309>
- Di Francesco Maesa, D., Mori, P., & Ricci, L. (2017). Blockchain based access control. In *Lecture notes in computer science* (pp. 206–220). https://doi.org/10.1007/978-3-319-59665-5_15
- Dinesh, K. K., Ravi, J., Nachiappan, B., Mohanraj, A., & Najmusher, H. (2025). Blockchain Technology for Secure and Trustworthy IoT Systems. In *Enhancing Security and Regulations in Libraries With Blockchain Technology* (pp. 39-68). IGI Global. <https://doi.org/10.4018/979-8-3693-9616-2.ch003>
- Gadekallu, T. R., Pham, Q., Nguyen, D. C., Maddikunta, P. K. R., Deepa, N., Prabadevi, B., Pathirana, P. N., Zhao, J., & Hwang, W. (2021). Blockchain for Edge of Things: applications, opportunities, and challenges. *IEEE Internet of Things Journal*, 9(2), 964–988. <https://doi.org/10.1109/jiot.2021.3119639>
- Ghadekar, P., Doke, N., Kaneri, S., & Jha, V. (2019). Secure Access Control to IoT Devices using Blockchain. *International Journal of Recent Technology and Engineering (IJRTE)*, 8(2), 3064–3070. <https://doi.org/10.35940/ijrte.f2273.078219>
- Ghadimi, N., Koozehkanani, Z. D., & Mortazavi, S. A. (2024). Presenting a blockchain-based nonlinear model for the security of smart home. *International Journal of Nonlinear Analysis and Applications*, 15(12), 333-341. DOI: <https://doi.org/10.22075/ijnaa.2023.31676.4703>
- Gopal, S. B. (2020). Secured Smart Home using Blockchain Technology. *Gedrag & Organisatie*, 33(02). <https://doi.org/10.37896/gor33.02/251>
- Gopalan, S. H., Manikandan, A., Dharani, N. P., & Sujatha, G. (2024). Enhancing IoT Security: A Blockchain-Based mitigation framework for deauthentication attacks. *The International Journal of Networked and Distributed Computing*, 12(2), 237–249. <https://doi.org/10.1007/s44227-024-00029-w>
- Güler, O. (2024). A Model Design Using Blockchain and Smart Contracts Against Cyberattacks in Smart Home Systems. *Acta Infologica*, 8(1), 11-22. <https://doi.org/10.26650/acin.1349544>
- Huang, Y. (2024). Smart home system using blockchain technology in green lighting environment in rural areas. *Heliyon*, 10(4), e26620. <https://doi.org/10.1016/j.heliyon.2024.e26620>
- Huang, Y., Yen, I., & Bastani, F. (2024). A Blockchain Embedded Peer-to-Peer Access Control Framework for IoT Systems. arXiv e-prints, arXiv-2407. DOI: <https://doi.org/10.48550/arXiv.2407.05506>
- Hussain, H. A., Mansor, Z., Shukur, Z., & Jafar, U. (2023). Ether-IoT: A realtime lightweight and scalable Blockchain-Enabled cache algorithm for IoT access control. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, 75(2), 3797–3815. <https://doi.org/10.32604/cmc.2023.034671>
- Hussain, H. A., Mansor, Z., Shukur, Z., & Jafar, U. (2024). Cost-Optimized dynamic access control policy using blockchain and machine learning for enhanced security in IoT smart homes. *ITM Web of Conferences*, 63, 01009. <https://doi.org/10.1051/itmconf/20246301009>
- Johari, A., & Alsaqour, R. (2022). Blockchain-Based model for smart home network security. *International Journal of Computer Networks and Applications*, 9(4), 497. <https://doi.org/10.22247/ijcna/2022/214509>
- Khan, N. S., Mir, R. N., Chishti, M. A., & Saleem, M. (2024). B-ERAC: Blockchain-Enabled Role-Based Access Control for secure IoT device communication. *Scalable Computing Practice and Experience*, 25(6). <https://doi.org/10.12694/scpe.v25i6.2936>
- Lee, J., Kim, M., Park, K., Noh, S., Bisht, A., Das, A. K., & Park, Y. (2023). Blockchain-Based Data Access control and key agreement system in IoT environment. *Sensors*, 23(11), 5173. <https://doi.org/10.3390/s23115173>
- Lee, S., & Kim, S. (2021). Blockchain as a Cyber Defense: opportunities, applications, and challenges. *IEEE Access*, 10, 2602–2618. <https://doi.org/10.1109/access.2021.3136328>
- Lee, Y., Rathore, S., Park, J. H., & Park, J. H. (2020). A blockchain-based smart home gateway architecture for preventing data forgery. *Human-centric Computing and Information Sciences*, 10(1). <https://doi.org/10.1186/s13673-020-0214-5>
- Liao, K. (2022). Design of the secure smart home system based on the blockchain and cloud service. *Wireless Communications and Mobile Computing*, 2022, 1–12. <https://doi.org/10.1155/2022/4393314>
- Liu, N. P. (2024). A blockchain empowered smart home access scheme based on zero-trust architecture. *Deleted Journal*, 20(3), 43–49. <https://doi.org/10.52783/jes.2356>
- Majeed, R., Abdullah, N. A., Ashraf, I., Zikria, Y. B., Mushtaq, M. F., & Umer, M. (2020). An intelligent, secure, and smart home automation system. *Scientific Programming*, 2020, 1–14. <https://doi.org/10.1155/2020/4579291>
- Mbarek, B., Ge, M., & Pitner, T. (2020). Blockchain-Based access control for IoT in smart home systems. In *Lecture notes*

- in computer science (pp. 17–32). https://doi.org/10.1007/978-3-030-59051-2_2
- Mladenova, T., & Cankov, V. (2023, June). Smart Home Based on IoT-Architecture and Practices. In 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-5). IEEE.
- Namane, S., & Dhaou, I. B. (2022). Blockchain-Based access control techniques for IoT applications. *Electronics*, 11(14), 2225. <https://doi.org/10.3390/electronics11142225>
- Noor, N. M., Razali, N. a. M., Malizan, N. A., Ishak, K. K., Wook, M., & Hasbullah, N. A. (2022). Decentralized Access Control using Blockchain Technology for Application in Smart Farming. *International Journal of Advanced Computer Science and Applications*, 13(9). <https://doi.org/10.14569/ijacsa.2022.0130993>
- Pancari, S., Rashid, A., Zheng, J., Patel, S., Wang, Y., & Fu, J. (2023). A Systematic Comparison between the Ethereum and Hyperledger Fabric Blockchain Platforms for Attribute-Based Access Control in Smart Home IoT Environments. *Sensors*, 23(16), 7046.
- Park, J., & Chang, S. (2022). Secure device control scheme with blockchain in a smart home. *Measurement and Control*, 56(3–4), 546–557. <https://doi.org/10.1177/00202940221105855>
- Parmar, M., & Shah, P. (2023). Internet of things-blockchain integration: a robust data security approach for end-to-end communication. *Indonesian Journal of Electrical Engineering and Computer Science*, 32(2), 1050. <https://doi.org/10.11591/ijeecs.v32.i2.pp1050-1057>
- Qashlan, A., Nanda, P., He, X., & Mohanty, M. (2021). Privacy-Preserving mechanism in smart home using blockchain. *IEEE Access*, 9, 103651–103669. <https://doi.org/10.1109/access.2021.3098795>
- Raj, R., & Ghosh, M. (2023, March). A Lightweight Blockchain Framework for secure transaction in resource constrained IoT devices. In 2023 5th International Conference on Recent Advances in Information Technology (RAIT) (pp. 1-7). IEEE.
- Rasras, M., Marin, I., & Radu, S. (2023). Smart Home Environment Modelled with a Multi-Agent System. arXiv preprint arXiv:2304.08494. doi: <https://doi.org/10.48550/arxiv.2304.08494>
- Ruzbahani, A. M. (2024). AI-Protected Blockchain-based IoT environments: Harnessing the Future of Network Security and Privacy. arXiv preprint arXiv:2405.13847.
- Sarkar, S., Kakade, K., AK, S., & R, R. (2024). Utilising blockchain technology to implement a security control method for node access to the Internet of Things. *Intelligent Decision Technologies*, 18(2), 953–963. <https://doi.org/10.3233/iddt-230136>
- Sharma, R. K., & Goveas, N. (2023, March). Use of blockchain in securing iot systems with resource constrained devices. In 2023 IEEE 20th International Conference on Software Architecture Companion (ICSA-C) (pp. 216-223). IEEE.
- Shakarami, M., Benson, J., & Sandhu, R. (2022, April). Blockchain-based administration of access in smart home IoT. In *Proceedings of the 2022 ACM workshop on secure and trustworthy cyber-physical systems* (pp. 57-66).
- Sille, R., Mahdi, H. F., Choudhury, T., Sahoo, S., Kapoor, A., Nanda, I., & Sharma, A. (2022). Review Study on Blockchain Frameworks for Security issues in IoT Devices. *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, 10, 876–881. <https://doi.org/10.1109/ismsit56059.2022.9932744>
- Singh, A., Chauhan, S., Dargar, S. K., Tharewal, S., Gutte, V. S., Tiwari, P. K., & Gupta, S. (2023). Blockchain enabled security mechanism for preventing data forgery in IoT-based smart homes. *Journal of Discrete Mathematical Sciences and Cryptography*, 26(5), 1437–1446. <https://doi.org/10.47974/jdmsc-1769>
- Singh, R., Jain, S., & Gupta, S. (2023). Review Paper on Block-Chain Technology. *International Journal of Advanced Research in Science Communication and Technology*, 66–67. <https://doi.org/10.48175/ijarsct-10723>
- Sisi, Z., & Souri, A. (2021). Blockchain technology for energy-aware mobile crowd sensing approaches in Internet of Things. *Transactions on Emerging Telecommunications Technologies*, 35(4). <https://doi.org/10.1002/ett.4217>
- Song, L., Li, M., Zhu, Z., Yuan, P., & He, Y. (2020). Attribute-Based access control using smart contracts for the internet of things. *Procedia Computer Science*, 174, 231–242. <https://doi.org/10.1016/j.procs.2020.06.07>
- Umer, M., Sadiq, S., Alhebshi, R. M., Sabir, M. F., Alsubai, S., Hejaili, A. A., Khayyat, M. M., Eshmawi, A. A., & Mohamed, A. (2023). IoT based smart home automation using blockchain and deep learning models. *PeerJ Computer Science*, 9, e1332. <https://doi.org/10.7717/peerj-cs.1332>
- Veneruso, S., Bertrand, Y., Leotta, F., Serral, E., & Mecella, M. (2023). A model-based simulator for smart homes: Enabling reproducibility and standardization. *Journal of Ambient Intelligence and Smart Environments*, 15(2), 143–163. <https://doi.org/10.3233/ais-220016>
- Wazid, M., Das, A. K., Shetty, S., & Jo, M. (2020). A tutorial and future research for building a Blockchain-Based secure communication scheme for Internet of Intelligent Things. *IEEE Access*, 8, 88700–88716. <https://doi.org/10.1109/access.2020.2992467>
- Xue, J., Xu, C., & Zhang, Y. (2018). Private Blockchain-Based secure access control for smart home systems. *KSII Transactions on Internet and Information Systems*, 12(12). <https://doi.org/10.3837/tiis.2018.12.024>
- Yang, L. (2024). Internet of Things security design based on blockchain and identity re-encryption. *Journal of Cyber Security and Mobility*, 369–392. <https://doi.org/10.13052/jcsm2245-1439.1332>
- Yang, X., Yang, X., Yi, X., Khalil, I., Zhou, X., He, D., Huang, X., & Nepal, S. (2021). Blockchain-Based secure and lightweight authentication for internet of things. *IEEE Internet of Things Journal*, 9(5), 3321–3332. <https://doi.org/10.1109/jiot.2021.3098007>
- Yang, X., Yang, X., Yi, X., Khalil, I., Zhou, X., He, D., Huang, X., & Nepal, S. (2021b). Blockchain-Based secure and

- lightweight authentication for internet of things. *IEEE Internet of Things Journal*, 9(5), 3321–3332. <https://doi.org/10.1109/jiot.2021.3098007>
- Zhang, W., & Yan, H. (2021). A blockchain-based access control scheme for smart home. *Journal of Physics Conference Series*, 1971(1), 012049. <https://doi.org/10.1088/1742-6596/1971/1/012049>
- Zhang, X., & Xie, X. (2024). A combination of Attribute-Based encryption and blockchain access control scheme in smart home environment. *International Journal of Computer Science and Information Technology*, 4(1), 303–311. <https://doi.org/10.62051/ijcsit.v4n1.37>
- Zhao, X., Zhong, B., & Cui, Z. (2023). Design of a decentralized Identifier-Based Authentication and Access Control model for smart Homes. *Electronics*, 12(15), 3334. <https://doi.org/10.3390/electronics12153334>



© 2025 by the authors; licensee Growing Science, Canada. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (<http://creativecommons.org/licenses/by/4.0/>).