İSTANBUL UNIVERSITY PRESS

Acta Infologica
acin 2024, 8 (1), 11–22
DOI: 10.26650/acin.1349544

Research Article / Araştırma Makalesi

A Model Design Using Blockchain and Smart Contracts Against Cyberattacks in Smart Home Systems

Osman Güler[1]

[1] Tusaş Şehit Hakan Gülşen MTAL, Ankara, Türkiye

Corresponding author : Osman Güler
E-mail : h.osmanguler@gmail.com

ABSTRACT

The use of Internet of Things (IoT)-based smart home systems is rapidly becoming widespread today. The structure of smart devices and the inadequacy of security systems make these systems vulnerable to cyberattacks. Therefore, using a solid security mechanism is important for protecting personal data in smart home systems The main purpose of this study is to present a model that works on the blockchain and smart contract infrastructure to ensure the security of smart home systems against cyberattacks. This study is a design-based research that examines how blockchain and smart contracts can be integrated to increase smart home security. The blockchain technology used in the proposed model protects the integrity of data by providing a decentralized distributed ledger to eliminate possible attack vectors. Additionally, predefined security protocols are automatically executed thanks to the use of smart contracts, thus increasing the overall durability of the system. In this way, the proposed model effectively reduces security vulnerabilities in smart home systems, ensures the immutability of data, prevents unauthorized changes, and offers an effective security solution against possible cyberattacks. As a result, the proposed model can be said to be a robust, efficient security solution for IoT networks and smart home systems.

Keywords: Internet of Things, smart homes, smart contracts, blockchain, cybersecurity

Submitted	: 24.08.2023
Revision Requested	: 27.12.2023
Last Revision Received	: 02.03.2024
Accepted	: 04.03.2024
Published Online	: 25.06.2024

1. INTRODUCTION

With the developments in the field of information and communication technology (ICT), sensor-based technological devices that are able to communicate are being widely used in all areas of our lives. This technology is called the Internet of Things (IoT). IoT technology provides smart physical objects with Internet connection access and power to communicate (Panarello et al., 2018). These objects collect, store, and analyze data from sensors in order to increase efficiency, quality, and production in many areas such as IoT, smart factories, smart home systems, smart agriculture and irrigation, smart cities, smart logistics, and smart health (Gökrem & Bozuklu, 2016). Analyzing data needs to be done with smart and automated methods for performance and efficiency (Savaş et al., 2022b).

The biggest example of IoT technology being used in daily life is smart home systems. Smart homes are a type of housing integrated with IoT that provide comfort, security, convenience, and increased quality of life to their owners (Moniruzzaman et al., 2022). Smart homes refer to private houses that provide automatic smart services through various home devices such as home heating, home lighting, and white goods without human intervention that send and receive data to and from these devices in real-time (Park et al., 2019). Although smart homes provide great benefits to their owners, they are potentially at risk from malicious attacks, as the devices used are constantly connected to a network and offer vulnerable solutions to cyberattacks (Khan et al., 2020). Because IoT devices use a decentralized approach to network connectivity, using standard existing security techniques for inter-device communication is very complex (Alam, 2019). People have to take precautions to make their living spaces, homes, and workplaces safe and to keep their data secure in cyber environments (Savaş & Karataş, 2022a). To address these concerns, the proposal has emerged that using blockchain technology and smart contracts to secure the transactions between IoT devices is crucial for improving system security. This approach offers a robust layer of protection that addresses certain vulnerabilities by connecting to IoT devices using public or private keys and by providing secure identification and authentication rather than adhering to the rules of a central node or intermediary (Hassan et al., 2020). Blockchain technology is important for strengthening the security of communication between IoT devices. Blockchain is a decentralized distributed ledger that provides secure, transparent, and tamper-proof record keeping. Each transaction is encapsulated in a block of information that is cryptographically linked to the previous block, thus creating an unalterable chain of information.

Blockchain technology plays an important role in solidifying a security system, as it works as a distributed ledger and makes data difficult to change. Blockchain enables system components to communicate and share data securely, making difficulty for an attacker trying to modify, delete, copy, or deceive data in a blockchain-enabled system (Tekin et al., 2020; Kodym et al., 2020). Smart contracts are programs that set terms between two or more components and automatically execute certain actions when these conditions are met (Restuccia et al., 2019). When used in conjunction with blockchain technology, smart contracts govern the cooperation and interactions among security system components.

Blockchain and smart contracts are important technologies in the design of smart home security systems. The use of blockchain and smart contracts in smart home systems provides benefits in such areas as secure data sharing by ensuring data integrity, reducing the risk of data manipulation, and increasing system security. Thanks to these technologies, the smart home security has increased, providing homeowners with a safer and more comfortable life.

Various studies have been conducted on the use of blockchain technology for security in smart home systems. Dorri et al. (2016) proposed an architecture based on blockchain technology that includes a smart home, an overlay network, and cloud storage devices. The proposed architecture uses blockchain technology in networked device-to-device transactions and uses reliable distributed methods to ensure the decentralization of the architecture. Because bitcoin requires computational overhead, the proposed method is manageable for low-resource IoTs. In another study, Dorri et al. (2017) equipped their smart home system with a device called a *miner* that is always online and responsible for the communication among all devices in the system. A native private blockchain is used to provide secure access control for mining IoT devices and data. In the proposed system, the miner has a list of communicating devices and gives a key to these devices to ensure user control, thus securing inter-device communication. In addition, the blockchain creates a fixed time-ordered transaction history that can be linked to other layers to provide specific services. Although these blockchain-based approaches are suitable for providing decentralized security and privacy, they are not suitable for use with low-capacity IoT devices because they involve significant amounts of energy, latency, and computational overhead. Dand and Nguyen (2018) proposed an approach using blockchain technology called smart home-based IoT- blockchain. Their proposed architecture was used to create an experimental scenario among the user, the service provider, and the smart home using Ganache, Remix, and Web3.js. This approach proposes a blockchain technology that uses three types of smart contracts (i.e., access control contract [ACC], judge contract [JC], and registration contract [RC]) to ensure secure access control and IoT deployment. According to the test results, the proposed architecture identified and solved challenges in the smart home system such as data privacy, secure access control, and extension capability.

Singh et al. (2019) proposed an architecture for system security in smart homes that uses a multivariate correlation analysis technique to analyze network traffic and determine the relationship between different traffic characteristics. The proposed model consists of four components: the smart home layer, a blockchain network, cloud computing, and service layer. As a result of their tests, the proposed architecture was seen to provide smart homes with a network attack detection and response system. Arif et al. (2020) examined smart home architectures and security situations that use blockchain. They proposed a simple, secure smart home architecture with an improved blockchain called a consortium blockchain, which is a combination of public and private blockchains. The user's role in the blockchain process is eliminated; instead, IoT devices are defined as miners in the system. In this way, previously selected nodes now participate in block creation and consensus. This structure makes the proposed system unique compared to the current state of the art. Zhang and Yan (2021) proposed a blockchain-based smart home access control scheme using Hyperledger Fabric to provide access control with smart contracts. They used a hybrid access control model based on dynamic attribute-based access control and a static access control matrix. This system rejects access requests over the network from malicious attackers or devices not defined in the device list. In this way, user-initiated remote access control and access control between local devices are simultaneously guaranteed. Baucas et al. (2021) proposed a smart home design using proprietary blockchain technology and localization through trilateration based on the received signal strength indicator (RSSI) using the Raspberry Pi 3 model. This system consists of two components and focuses on low-quality access-level implementation. First, it identifies unrecognized devices trying to gain access using the blockchain; secondly, it uses localization to determine the source of the attack and the general location of the device and to obtain more information.

This study proposes a smart home system design using blockchain and smart contracts in order to provide secure communication in IoT and smart home systems and to prevent cyberattacks. The study uses a design-based research method. Design-based research refers to the process of developing a solution-oriented model that can be applied to an existing problem. This model proposal involves design research that examines how blockchain and smart contracts can be integrated to increase smart home security. The theoretical and practical contributions of this study are as follows:

- The study proposes a comprehensive model designed for smart home systems that integrates blockchain technology into the security framework of IoT devices.
- The study's inclusion of smart contracts as part of the model contributes to the theoretical understanding of automated security protocols.
- The proposed model offers a practical solution for strengthening the security of smart home systems against cyberthreats. The research provides practical insights into mitigating the vulnerabilities associated with constant device connectivity and possible cyberattacks through the application of blockchain and smart contract technology.
- As the basis of this research, the combination of blockchain and smart contracts provides a holistic security solution for IoT designed specifically for smart homes.

The second section of the study explains IoT technology, smart home systems, blockchain, and smart contract technologies. The third section presents information about the types of cyberattacks against IoT and the precautions that can be taken. The fourth section explains the proposed blockchain-based smart home automation approach. The fifth section evaluates IoT and Blockchain technologies and makes some suggestions.

2. CONCEPTUAL BACKGROUND AND METHOD

The IoT devices commonly used in smart home systems present a number of security challenges. The fact that these devices are always online, communicate with each other, and exchange data makes these systems vulnerable to cyberattacks. The interactions among blockchain, smart contracts, and IoT form the basis of the security system to be created against cyberattacks in smart home systems. Designed primarily as a decentralized distributed ledger for securing data transactions in IoT systems, blockchain offers a transformative approach. Blockchain is crucial for security, as IoT devices communicate and exchange data automatically, with every transaction being recorded in a cryptographically linked block creating an immutable chain. Integrating blockchain into IoT security preserves the integrity of the data by providing data transactions through a reliable transparent ledger. Every transaction is verified through authentication mechanisms on the network, increasing the security and reliability of the data. Blockchain's decentralized immutable nature reduces the risks associated with unauthorized access, thus ensuring the reliability of the data transmitted between IoT devices in smart home systems. Smart contracts are used to automate security protocols. These programmable contracts perform predetermined actions when certain conditions are met. Smart contracts running on a blockchain ensure that predetermined rules are automatically implemented. This allows security protocols to be automated and human intervention to be reduced.

2.1. The Internet of Things

With the widespread use of Internet technologies, users can access data and communicate whenever and wherever they want. IoT involves a set of systems that allow physical objects consisting of smart objects and sensors to automatically connect and communicate with each other without requiring personal intervention or manual data entry thanks to network connections and Internet access (Can et al., 2016; Gündüz & Daş, 2018). IoT systems consist of four main components: objects, communication, data, and users (Gündüz & Daş, 2018; Oral & Çakır, 2017). Fig. 1 shows the IoT components.

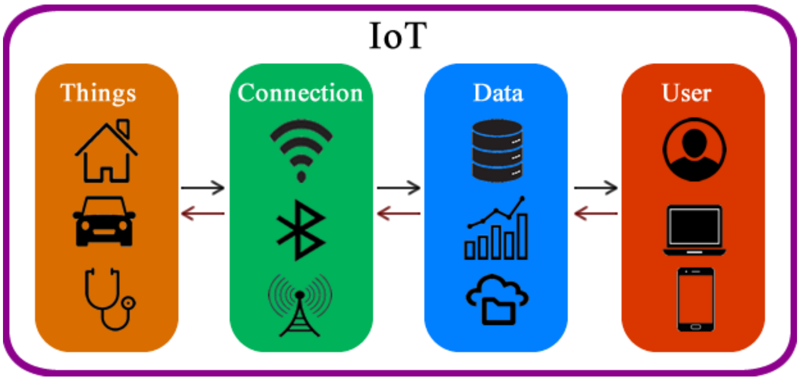

Figure 1. IoT Components

Objects consist of smart devices, sensors, and detectors used in IoT systems. Wired and wireless communication infrastructures such as Bluetooth, infrared, radio frequency identification (RFID), Zigbee, ethernet, and wi-fi are used for inter-object communication and sharing (Gökrem & Bozuklu, 2016). The data component consists of the data collected by the sensors, detectors, and objects in the environment, as well as the processors for these data. The user component consists of the users using the system and the interface programs used for access.

IoT technology is mostly used in daily life. For example, IoT technology can remotely control the ambient temperature, lighting, security systems, and even home appliances such as ovens and washing machines in smart home systems. IoT devices are also used in a variety of industries, including smart cities, smart healthcare, smart agriculture, and smart industrial applications.

2.2. Smart home systems

With the introduction of IoT technologies into daily life, smart technologies have begun being used in every area. One of these is in the home, where people spend their daily lives. Smart home systems are houses equipped with technologies that facilitate the life of the user, increases the comfort environment, provides energy efficiency, and provides a better-quality environment for people (İlkbahar et al., 2021). Electrical appliances, white goods, lighting and heating systems, audio and video systems, and security and camera systems in smart homes can communicate with each other and the user thanks to the wired or wireless network infrastructure (Kuncan & Çaça, 2019). The home owner can use the interface program to connect to smart home systems, control electrical appliances, adjust the temperature of the house, operate white goods, and see inside the house thanks to the cameras. When security threats such as intrusion, gas leakage, fire, or flooding occur, a message can be sent to the landlord and relevant institutions. With technological developments, smart homes now have artificial intelligence (AI) that can learn by themselves, monitor the user's daily life, and redevelop the program according to the user's needs (Avcı, 2022). Data on the user's daily activities at home are collected and used by such things as fuzzy logic, artificial neural networks, and machine learning algorithms. By processing the data with AI algorithms, the user's next behavior can be predicted (Güneş et al., 2019) and thus becomes able to produce unique solutions for home owners.

2.3. Blockchain

Blockchain technology is a decentralized distributed database management system that uses cryptographic techniques and does not require third-party verification (Novo, 2018). This technology involves a network formed of blocks containing encrypted transactions storing interconnected data. The blockchain is created by recording each block and adding it to the previous block; these blocks are linked chronologically and shared among all participants in the network

(Yıldız & Baştuğ, 2018). Once created, a block cannot be deleted or changed. Each block header in the blockchain contains the hash value of the previous block, a nonce (a temporary value used to generate the hash), a Merkle root (hash of all previous hashes), and timestamp information (Wu et al., 2020). Fig. 2 shows the blockchain structure.

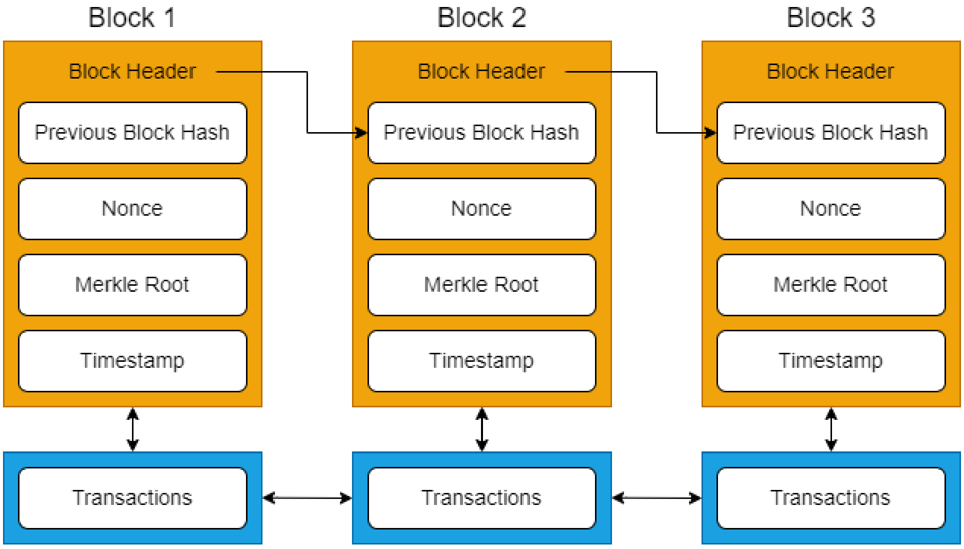

Figure 2. Blockchain architecture

Blockchain technology provides reliable, transparent, and sustainable database management due to the absence of a central authority. In addition, it has a structure that increases security thanks to the encrypted storage and distribution of data. In this way, it protects the accuracy and integrity of the data and prevents data tampering.

2.4. Smart contracts

Smart contracts are self-executing programmable contracts that run on blockchain technology. Thanks to these contracts, code pieces that can automatically run themselves, save data, keep values, and perform various calculations can be added to blocks when a certain situation occurs (Karaarslan & Akbaş, 2017). Smart contracts prevent the errors that occur in classical contracts and facilitate the checks and balances of the system and other contracts. At the same time, smart contracts are more reliable, work faster, have the ability to automatically execute, and save on operating costs compared to conventional contracts.

3. IoT CYBERATTACK DANGER

IoT technology connects billions of devices to the Internet. Many personal and business data are transmitted and stored on the Internet through these devices. As with any device with an Internet connection, IoT devices are a big target for cyberattacks. Information transmitted on IoT networks by unauthorized persons may be able to access and damage the network. Therefore, taking security measures and monitoring traffic continuously for cyberattacks are imperative (Dissanayake, 2021). This section discusses the types of cyberattacks that can be made against IoT devices, as well as the precautions that can be taken against cyberattacks.

3.1. DDoS Attacks

Distributed denial-of-service attacks (DDoS) are attacks that prevent a network from working by connecting many devices to that network. DDoS in an IoT network involves an attack that targets the availability of servers by flooding the communication channel by impersonating requests from the distributed IoT devices (Vishwakarma & Jain, 2020). By targeting IoT devices, these attacks can crash or render IoT applications or devices inoperable.

3.2. Man-in-the-Middle Attacks

One of the most popular attacks against IoT devices involves Man-in-the-Middle (MITM) attacks. MITM (or on-path) attacks are when an attacker gets between two nodes and interrupts communications, thus allowing the attacker to act as a proxy (Kuzlu & Güler, 2021). By appearing as a proxy in this way, the attacker can control incoming and outgoing messages.

3.3. Password Cracking Attacks

Most IoT devices are protected by default passwords that are simple and easy to guess. This facilitates attackers' ability to take control of devices. Attackers crack the current user password using dictionary attacks, which try possible letter and number combinations to guess user passwords, or by brute force attacks, which try all possible password combinations to find valid passwords (Abomhara & Køien, 2015).

3.4. Node Attacks

These attacks can damage a sensor node and involve the attacker physically replacing all or part of a node in order to access and modify sensitive information such as shared cryptographic keys (Islam & Aktheruzzaman, 2020). Attackers can disrupt the functionality of devices by preventing them from communicating with each other.

3.5. Social Engineering

While attackers do target IoT devices, they can also target humans. They do this by collecting information about the target person or institutions, with or without using technological tools (Irmak &Reis, 2018). One example of a social engineering attack involves the method of obtaining people's personal information or passwords by sending an email or message, which is known as phishing.

Many cyber security threats occur on the Internet, such as obtaining personal and corporate data, disclosing private information, and disabling commercial services (Savaş & Savaş, 2022). Because IoT devices in particular are always open to cyberattack, the security of these devices is very important. While using IoT devices, one needs to be aware of security vulnerabilities and take the necessary precautions. For this reason, the first of the measures that can be taken against cyberattacks is to change the default passwords of the devices and use strong passwords. In addition, regularly changing password and using different passwords on different devices are important. Monitoring for updates that eliminate devices' security vulnerabilities and installing manufacturer-provided updates are necessary. One's network system security should be increased, and firewall and antivirus software should be used. Devices that run on the network should be monitored regularly, and when unusual activity is observed, the devices should be turned off and their software and passwords should be updated immediately. Intrusion detection systems can be used to regularly monitor a network. One of the most important measures that can be taken against cyberattacks is to raise user and employee awareness about device security, cyberattacks, and the dangers of cyberattacks.

4. THE BLOCKCHAIN-BASED SMART HOME AUTOMATION APPROACH

This study aims to develop a model that uses smart contracts and blockchain technology to ensure data security against cyberattacks that might occur in smart home systems. The simple design diagram of the proposed system is shown in Fig. 3.

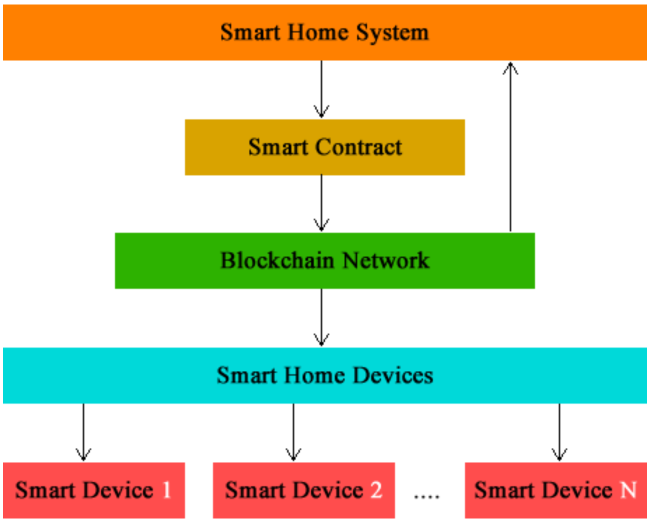

Figure 3. Suggested model design

Figure 3 shows a smart home model consisting of *N* smart devices (e.g., Smart Device 1, Smart Device 2, . . . , Smart Device N). These devices connect to a network system and communicate through a smart contract running on the blockchain network. In this way, the smart devices communicate with the smart contract by means of the blockchain network, exchanging data, receiving instructions, and providing real-time information. With this system, seamless automation and control of smart home devices is ensured based on predefined conditions determined by the smart contract. Fig. 4 presents the flow diagram of the smart home system using blockchain and smart contracts for the proposed system, with Algorithm 1 showing the details.

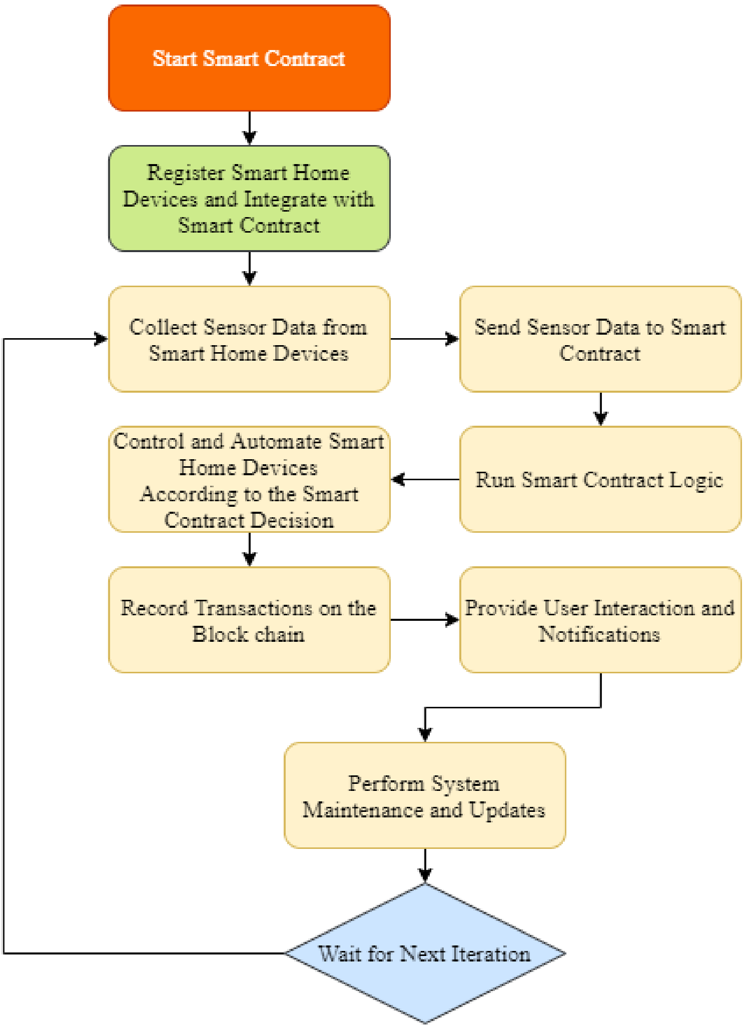
Start Smart Contract
Register Smart Home Devices and Integrate with Smart Contract
Collect Sensor Data from Smart Home Devices
Send Sensor Data to Smart Contract
Control and Automate Smart Home Devices According to the Smart Contract Decision
Run Smart Contract Logic
Record Transactions on the Block chain
Provide User Interaction and Notifications
Perform System Maintenance and Updates
Wait for Next Iteration

Figure 4. Flow diagram of Smart Contract and Blockchain structure

Algorithm 1: Blockchain and Smart Contract-Based Smart Home System

```
Start Smart Contract
Register Smart Home Devices and Integrate with Smart Contract
while(true)
  Collect Sensor Data from Smart Home Devices
  Send Sensor Data to Smart Contract
  Run Smart Contract Logic
  Control and Automate Smart Home Devices Based on Smart Contract Decision
  Record Transactions on the Blockchain
  Provide User Interaction and Notifications
  Perform System Maintenance and Updates
  Wait for Next Iteration
End While
```

- **Start Smart Contract:** A blockchain network is specially designed for the smart home system. The smart contract is deployed in the blockchain network by defining the necessary variables, functions, and conditions within the smart contract for controlling the smart devices.
- **Register Smart Home Devices and Integrate with Smart Contract:** Smart home devices are assigned unique identifiers using blockchain technology. They are registered and integrated into the smart contract, and the device information is stored in the smart contract.
- **Collect Sensor Data from Smart Home Devices:** Sensor data such as temperature, motion, light intensity, and humidity are continuously collected from the smart home devices.
- **Send Sensor Data to Smart Contract:** The sensor data collected from smart home devices is sent to the smart contract for processing and decision making.
- **Run Smart Contract Logic:** Incoming sensor data is evaluated against predefined conditions and rules in the smart contract, triggering appropriate actions or decisions.
- **Control and Automate Smart Home Devices According to the Smart Contract Decision:** Instructions or commands are sent by the smart contract to smart home devices for controlling operations such as turning lights on and off, adjusting thermostat settings, and activating security systems.
- **Record Transactions on the Blockchain:** The smart contract records the interactions, transactions, and decisions on the blockchain to ensure the transparency, immutability, and auditability of the system's activities.
- **Provide User Interaction and Notifications:** User interfaces (e.g., mobile apps, web interfaces) are provided for homeowners to interact with the smart home system. Homeowners are allowed to monitor and control smart home devices, view sensor data, and receive notifications/alerts. Access to devices is controlled using blockchain technology. In this way, only authorized users can access the devices, and in case of any unauthorized access, alarm systems are activated. Access rights to devices at home are managed using blockchain technology. A different access authorization can be defined for each user. For example, only certain devices may be authorized for children.
- **Perform System Maintenance and Updates:** The smart contract and blockchain network is regularly checked and updated to fix bugs and vulnerabilities or to implement system enhancements.
- The same operations are repeated as long as the system is running.

By following this algorithm, the blockchain and smart contract-based smart home system can effectively automate and coordinate the transactions of various devices while providing transparency, security, and privacy to the interactions between devices and homeowners. Some similarities and differences occur between the proposed approach and other studies in the literature. Some studies in the literature have used blockchain alone, with various approaches such as device communication occurring through a miner or through the use of a hybrid access control model. Other studies have used smart contract logic for access control and data privacy and to secure IoT deployment. The current study's proposed model uses blockchain and smart contracts for decentralization and security, similar to the studies in the literature. The model in this study uses blockchain technology for smart contract access control based on sensor data. In this model, the system maintenance and updates step plays an important role for security. Although not explicitly stated in the studies conducted in the literature, regular checks and updates have been implied as being necessary for ensuring system security. Figures of the architectures suggested in the literature are shown in Fig. 5.

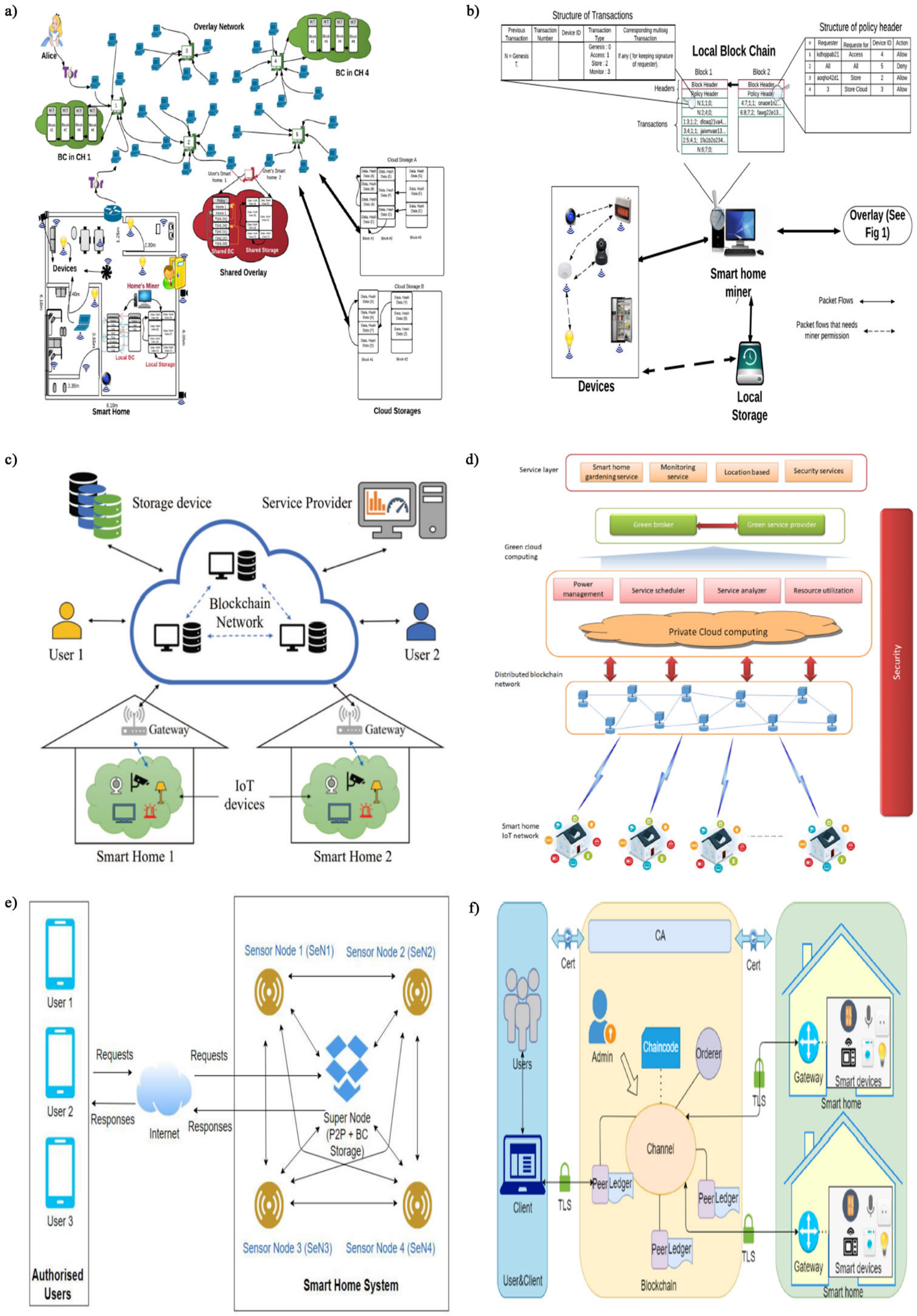

Figure 5. Previously proposed architectures: a) Dorri et al. (2016); b) Dorri et al. (2017); c) Dand & Nguyen (2018); d) Singh et al. (2019); e) Arif et al. (2020); and f) Zhang & Yan (2021)

This study' proposed model appears to be compatible with many concepts presented in the literature, such as the use of blockchain for security, smart contract logic for decision-making, and user interaction. The integration of smart devices with unique identifiers and the continuous monitoring of sensor data can be mentioned as examples of the contributions this study's proposed system presents to the literature.

Thanks to the proposed blockchain and smart contract-based smart home system, malicious access requests and cyberattacks are preventable. The smart contracts that make up the smart home system are resistant to data manipulation attacks because they are recorded on the blockchain in a transparent, unchangeable, and auditable manner. This means that monitoring and modifying any datum in the system are difficult. Blockchain technology protects against unauthorized access attacks by preventing unauthorized changes to the smart contracts and limiting unauthorized access to the smart home devices. Only authorized users can interact with the system through the smart contracts. The blockchain's transparent recording of the order and timestamping of the transactions prevents attackers from violating timestamps or changing the order of transactions. Smart contracts and the blockchain network undergo regular security updates and maintenance. This ensures that any known vulnerabilities are fixed and that the system remains up to date.

The defense mechanisms the proposed model will display against the cyberattacks described in Section 3 are stated below.

- Because data and transactions are spread over a distributed network using blockchain technology, no single point of the system can be focused on, thus effectively preventing DDoS attacks.
- Because security is provided using cryptographic keys and digital signatures, the system is resistant to password cracking attacks.
- The system is resistant to Man-in-the-Middle (on-path) attacks thanks to the transparent and encrypted recording of transactions using blockchain technology, as well as the use of secure encryption protocols in the communication between smart contracts.
- Because blockchain networks work with distributed and consensus algorithms (Proof of Work [PoW]/Proof of Stake [PoS]), the security of the network increases, and attacks against individual nodes become difficult.
- Social engineering attacks generally occur by manipulating the users. In blockchain-based smart home systems, security can be combined with technical measures such as cryptographic keys and digital signatures to ensure resistance to social engineering attacks.

This approach provides resistance to a series of cyberattacks on the system thanks to the features offered by blockchain and smart contracts. However, factors such as implementation, configuration errors, user errors, or vulnerabilities in the system design can affect the security of the system. Conducting ongoing security assessments and updating security measures are important.

5. CONCLUSION

Security in IoT systems is a field of study that has been emphasized in recent years. With the developments in technology, IoT devices have entered every aspect of life. These devices are connected to networks and the Internet and thus are vulnerable to cyberattacks. In order to protect the integrity and immutability of data in smart home networks, this study has proposed a model that uses blockchain and smart contracts for cyber security in smart home systems.

The proposed blockchain and smart contract-based smart home system has been designed to ensure the integrity and immutability of data in smart home networks. The study has also explained the algorithm and flow chart of the system. The proposed smart home system enables automation and coordination of various devices in the smart home environment while also significantly increasing security, privacy, and overall efficiency.

In comparison to prior research efforts in this field, the proposed model addresses the unique challenges posed by smart home systems. While previous studies have explored various blockchain-based approaches, such as those proposed by Dorri et al. (2016, 2017), Dand and Nguyen (2018), Singh et al. (2019), Arif et al. (2020), Zhang and Yan (2021), and Baucas et al. (2021), the current study's model seeks to strike a balance between energy efficiency and security, making it particularly suitable for low-capacity IoT devices.

In future research, the aim will be to test the model's performance against cyberattacks by actually implementing it. In this way, valuable information will be provided about the practical performance and robustness of the proposed blockchain and smart contract-based security framework in the context of smart home systems. The research is thus expected in this way to contribute to the evolving landscape of IoT security, especially in the field of smart home technology.

Peer Review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Grant Support: The author declared that this study has received no financial support.

ORCID IDs of the author

Osman Güler 0000-0003-3272-5973

REFERENCES

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.

Alam, T. (2019). Blokzincir and its Role in the Internet of Things (IoT). International Journal of Scientific Research in Computer Science, Engineering and Information Technology. Vol 5(1). DOI: 10.32628/CSEIT195137

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.

Avcı, İ. (2022). Akıllı evlerde IoT teknolojileri ve siber güvenlik. Avrupa Bilim ve Teknoloji Dergisi, (34), 226- 233.

Baucas, M. J., Gadsden, S. A., & Spachos, P. (2021). IoT-based smart home device monitor using private blockchain technology and localization. *IEEE Networking Letters, 3*(2), 52-55.

Can, O., Sezer, E., Bursa, O., & Ünalir, M. O. (2016). Nesnelerin interneti ve güvenli bir sağlık bilgi modeli önerisi. In *4th International Symposium on Innovative Technologies in Engineering and Science (ISITES2016) 3-5 Nov 2016 Alanya/Antalya-Turkey*.

Dang, T. L. N., & Nguyen, M. S. (2018). An approach to data privacy in smart home using blockchain technology. In *2018 International Conference on Advanced Computing and Applications (ACOMP)* (pp. 58-64). IEEE.

Dissanayake, M. B. (2021). Feature Engineering for Cyber-attack detection in Internet of Things. *International Journal of Wireless and Microwave Technologies, 11*(6), 46-54.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops* (PerCom workshops) (pp. 618-623). IEEE.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blokzincir in internet of things: challenges and solutions. *arXiv preprint arXiv:1608.05187*.

Gökrem, L., & Bozuklu, M. (2016). Nesnelerin interneti: Yapılan çalışmalar ve ülkemizdeki mevcut durum. *Gaziosmanpaşa Bilimsel Araştırma Dergisi*, (13), 47-68.

Gündüz, M. Z., & Daş, R. (2018). Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 24*(2), 327-335.

Güneş, H., Bicakcı, S., Orta, E., & Akdaş, D. (2019). Akıllı evlerde kullanılan yapay zekâ teknikleri için simülasyon geliştirilmesi. *Gazi University Journal of Science Part C: Design and Technology, 7*(3), 554-563.

Hassan, M., Chen, J., Iftekhar, A., & Cui, X. (2020). Future of the internet of things emerging with blockchain and smart contracts. *International Journal of Advanced Computer Science and Applications*, 11(6).

Irmak, H., & Reis, Z. A. (2018). Sosyal Mühendislik Saldırılarına Karşı Web Tabanlı Bir Farkındalık Eğitimi. In 7th International Conference on *"Innovations in Learning for the Future": Digital Transformation in Education*, 108.

Islam, M. R., & Aktheruzzaman, K. M. (2020). An analysis of cybersecurity attacks against internet of things and security solutions. *Journal of Computer and Communications, 8*(4), 11-25.

İlkbahar, F., Şeyma, Ü., Karakaya, A. T., & Bayram, E. (2021). Akıllı Ev Sistemleri Üzerine Bir Model Önerisi. *AJIT-e: Academic Journal of Information Technology, 12*(45), 90-105.

Karaarslan, E., & Akbaş, M. F. (2017). Blokzinciri tabanli siber güvenlik sistemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 3*(2), 16-21.

Khan, M.A., Abbas, S., Rehman, A., Saeed, Y., Zeb, A., Uddin, M.I., Nasser, N. & Ali, A. (2020). A machine learning approach for blockchain -based smart home networks security. *IEEE Network, 35*(3), pp.223-229.

Kodym, O., Kubáč, L. & Kavka, L. (2020). Risks associated with Logistics 4.0 and their minimization using Blockchain. *Open Engineering,* 10(1), 74-85.

Kuncan, M. & Çaça, Ö. (2019). Akıllı Ev Teknolojisi için Kablosuz Akıllı Kit. *Avrupa Bilim ve Teknoloji Dergisi*, (17), 271-282.

Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of things, 1*, 1-14.

Moniruzzaman, M., Khezr, S., Yassine, A. & Benlamri, R. (2020). Blockchain for smart homes: Review of current trends and research challenges. *Computers & Electrical Engineering, 83*, p.106585.

Novo, O. (2018). Blokzincir meets IoT: An architecture for scalable access management in IoT. *IEEE internet of things journal, 5*(2), 1184-1195.

Oral, O., & Çakır, M. (2017). Nesnelerin interneti kavramı ve örnek bir prototipin oluşturulması. *Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 1*, 172-177.

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

Park, J. H., Salim, M. M., Jo, J. H., Sicato, J. C. S., Rathore, S., & Park, J. H. (2019). CIoT-Net: a scalable cognitive IoT based smart city network architecture. *Human-centric Computing and Information Sciences*, 9(1), 1-20.

Restuccia, F., Kanhere, S.D., Melodia, T. & Das, S.K. (2019). Blockchain for the internet of things: Present and future. *arXiv preprint arXiv:1903.07448*.

Savaş, S. & Karataş, S. (2022a). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review, 3*(1), pp.7-34. https://doi.org/10.1365/s43439-021-00045-4

Savaş, S., Duraklar, K., Çınar, O.A., Koç, M., Turan, A., Uslu, U., Doğanay, A.S., Özceyhan, O.G., Destan, M.Y. & Duşbudak, H. (2022b). Güneş Enerjisi Sistemlerinde Yenilikçi ve Akıllı Bakım Onarım. *Journal of Information Systems and Management Research, 4*(2), pp.35-49.

Savaş, T., & Savaş, S. (2022). Tekdüzen kaynak bulucu yoluyla kimlik avı tespiti için makine öğrenmesi algoritmalarının özellik tabanlı performans karşılaştırması. *Politeknik Dergisi*, 25(3): 1261-1270.

Singh, S., Ra, I. H., Meng, W., Kaur, M., & Cho, G. H. (2019). 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, 15*(4), 1550147719844159.

Tekin, M., Öztürk, D. & Bahar, İ. (2020). Akıllı lojistik faaliyetlerinde blokzincir teknolojisi. *Kent Akademisi, 13*(3), pp.570-583.

Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication systems, 73*(1), 3-25.

Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., & Rong, C. (2019). A comprehensive survey of blockchain: From theory to IoT applications and beyond. *IEEE Internet of Things Journal, 6*(5), 8114-8154.

Yıldız, R. Ö., & Baştuğ, S. (2018). Blok zincir teknolojisi kapsamında elektronik konşimento.(ss. 7-12). IV. Uluslararası Kafkasya–Orta Asya Dış Ticaret ve Lojistik Kongresi, Düzenleyen Adnan Menderes Üniversitesi. Aydın, 7 (8).

Zhang, W., & Yan, H. (2021). A blockchain -based access control scheme for smart home. In *Journal of Physics: Conference Series* (Vol. 1971, No. 1, p. 012049). IOP Publishing.

How cite this article

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