5

Design and Implementation of an IoT-Integrated Smart Home System with End-to-End Security Using Blockchain Technology

G. RAMESH[1], B. ANIL KUMAR[2], AND J. PRAVEEN[3]

[1]*Associate Professor, Department of Computer Science and Engineering, GRIET, Hyderabad, Telangana, India*
[2]*Associate Professor, Department of Electronics and Communication Engineering, GRIET, Hyderabad, Telangana, India*
[3]*Professor, Department of Electrical and Electronics Engineering, GRIET, Hyderabad, Telangana, India*

Contents

5.1 Introduction

The concept of smart homes is gaining popularity in cities, as it provides smart access to the infrastructure of homes and it can be

DOI: 10.1201/9781003269991-5

controlled from a smart hand-held device from a remote place. Smart homes can help the owners and residents of a house to have accessibility to their homes and can control bulbs, doors, and other electronic devices from a distant place. It is possible to have smart cities as well due to the emergence of technologies like cloud computing, Internet of Things, and distributed technologies. The problem with existing smart home systems, as explored in [1–5], is that end-to-end security may be at stake in certain cases where security loopholes are exploited by adversaries. When security is compromised, it can cause many issues, as unauthorized people can enter into the home and do unexpected things. Therefore, there is a need for more security in smart homes.

IoT-integrated smart applications like smart homes create security and privacy challenges. They are as follows. Scalability is the main problem, as the current centralized IoT platforms have message-routing mechanisms that create bottlenecks in scaling up to a large number of devices used in IoT. There is the security problem that a huge number of devices are participating to generate data and such a setup may be subjected to distributed denial of service (DDoS) attacks. Lack of data standards is another cause of concern as it leads to challenges and interoperability problems. As IoT-integrated solutions are associated with a huge number of devices, cost is another important concern. The integration with a centralized cloud may prove to be a bottleneck in the case of any disruption of services from the cloud for any reason.

This is the rationale behind taking up this work, which is aimed at designing and implementing a smart home with IoT and cloud integration, besides the use of blockchain technology that provides end-to-end security. Blockchain, as explored in [6], is a technology that refers to a distributed ledger of transactions and peer-to-peer communication among participating nodes that meet security needs and address security challenges thrown by IoT-integrated smart applications. In the blockchain network, each participant is granted access to an up-to-date copy of the encrypted ledger so as to help the node to have read/write and validate transactions. Though blockchain is initially used in the financial domain, it is now gaining popularity and acceptance for end-to-end security in IoT-integrated smart applications. The vision of decentralized IoT is realized with blockchain technology.

It facilitates end-to-end secure transactions among the participating devices and coordination among them.

In this context, IoT and blockchain technology offer a promising solution to a smart home system, as the system can provide end-to-end security and overcome the problems aforementioned. The usage of an open-standard distributed IoT solution can solve many problems that are associated with centralized approaches. As the blockchain technology is nothing but a distributed ledger of transactions, it offers direct communication to connected devices. Such devices collect data, and that can be accessed by all legitimate participants. Thus, decentralized blockchain networks can provide improved security of IoT-based solutions. Blockchain technology ensures end-to-end security by executing predefined smart contracts and taking care of specific consensus mechanisms that identify actions of compromised devices. In essence, the blockchain-enabled IoT-integrated smart home system can secure devices and data collected by them. It is possible as all facility management suppliers participate in a private blockchain in a distributed environment to provide timely service and automate the activities related to security.

5.2 Related Work

This section provides review of literature on the related topics of the proposed work. In the literature, it is found that the smart homes concept has been around for some years. However, there lacks an end-to-end security guarantee due to the number of connected devices and diversified technologies that form IoT and lack of standardization. Smart home literature found in [1,2], [6–10] reveals this fact. Since the smart home concept is realized based on IoT technology, it is important to ensure that there is end-to-end security. The IoT integration with smart homes and other use cases is found in [3], [11–15]. It is also true that blockchain in the technology is in the distributed environment, and it can be easily integrated with IoT, as studied in [4], [16–20]. The blockchain technology that provides a distributed ledger of transactions is suitable for helping IoT devices to achieve security benefits, as discussed in [5,21], and [22]. The integration of an IoT smart home with blockchain provides an end-to-end security guarantee, and the smart

home product that serves this privacy and security purpose is a need of society.

As explored in [1,2], [6–10], the smart home concept is not yet integrated with the sophisticated security infrastructure of blockchain technology. This is the reason, in the area of smart homes and smart IoT applications, of the need for an end-to-end security guarantee that can be provided by blockchain as per its claims. It is therefore essential to investigate the need for blockchain technology integration with IoT-enabled smart homes. The most relevant references found in the literature on the security issues of smart homes with present schemes are [1,2], [6–10]. They reveal the fact that security to smart homes is very important as loopholes in security can cause many issues. The emergence of blockchain technology provides a distributed ledger of transactions that is accessible to IoT devices or connected devices that participate in smart home IoT applications. There is a need for integration of blockchain technology with IoT-enabled connected devices of smart homes to ensure that both devices and the data collected by them are secured against privacy and security attacks.

5.3 Security Challenges

Smart homes with IoT and cloud integration have many security challenges and scalability issues. The reason behind security issues is that the environment is distributed in nature and thousands of devices may participate in the network. When any device is compromised or when security credentials are stolen, the whole system will be exposed to security risks. The existing solutions to the problem of security in smart homes are not scalable, and they do have loopholes like lack of standards and are prone to DDoS attacks and other attacks. They are not able to provide end-to-end solutions to the transactions in IoT-enabled smart homes. There is a need for end-to-end security in such systems. The aim of this chapter is to design and implement an IoT-enabled smart home system with blockchain technology for end-to-end security, irrespective of the make and platform of applications and devices that participate in distributed computing. Since blockchain is the distributed ledger of transactions that is accessible to all legitimate devices, it can help

devices to be smart enough to prevent any security attacks. In other words, the smart home, with all its participating devices and data, is protected with blockchain technology integration.

5.4 Methodology

The methodology used in this chapter is described here. The research starts with review of literature to know the insights required to design and implement the proposed work (Figure 5.1).

In the analysis and design phase, the researcher will identify more accurate requirements and finalize them. Then the researcher designs the system. Afterwards, the design is converted into a working solution with a prototype application. Once a smart home prototype is built with IoT and cloud integration, it will be integrated with blockchian technology. After integrating with blockchain, the system is evaluated for end-to-end security and intended communications. The evaluation mainly focuses on device security and data security. Once the effectiveness of the blockchain with respect to end-to-end security is proved, the prototype is converted into an out-of-the-box commercial solution.

As shown in Figure 5.2, it is evident that the smart home devices and gateway of smart home are integrated with IoT and cloud platform using MQTT protocol. In turn, it is integrated with

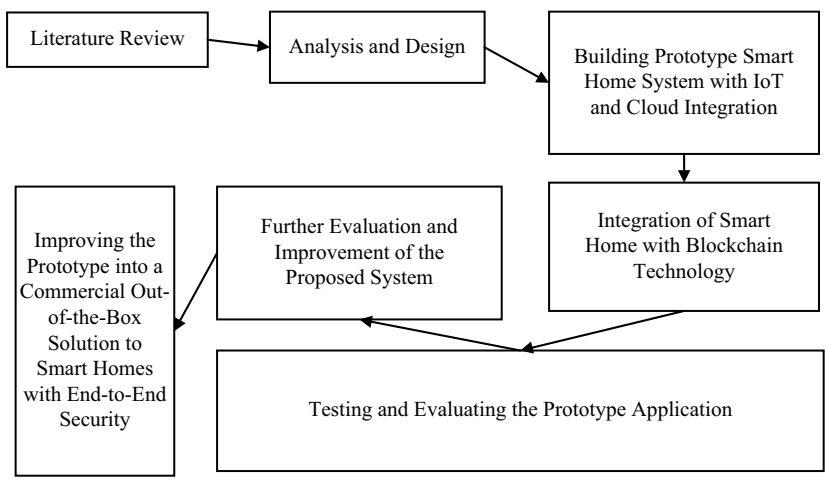

Figure 5.1 Conceptual design of the proposed research.

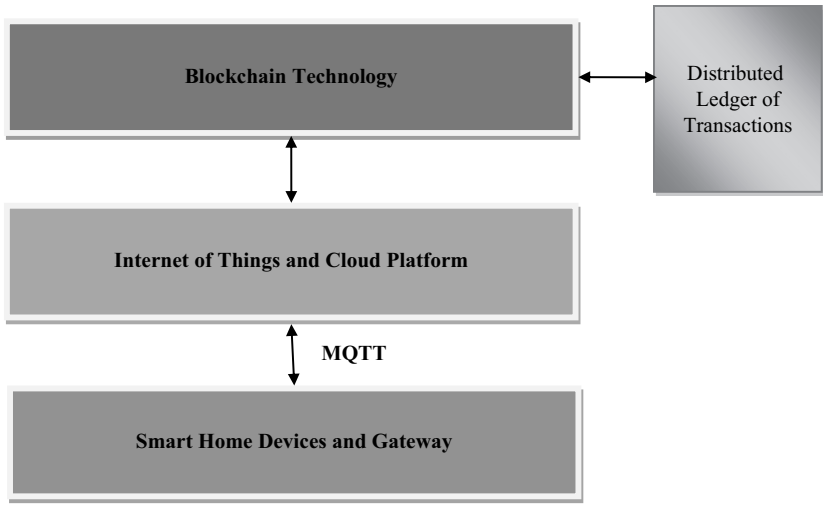

Figure 5.2 Outline of the proposed methodology.

blockchain technology using REST technology, which is interoperable in nature. The blockchain technology is equipped with a distributed ledger of transactions that is the important means of achieving end-to-end technology.

As shown in Figure 5.3, the blockchain technology has many components like Contracts API, Certificates API, Blockchain API, and Chaincode Registry. The security business logic is encapsulated in smart contracts. Such contracts are built using contracts API.

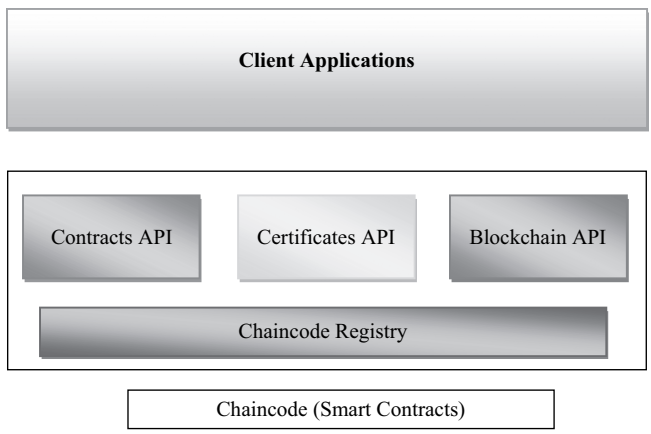

Figure 5.3 Blockchain technology components.

Blockchain API is the client API invoked by blockchain applications. Certificates API are used in the security process.

As shown in Figure 5.4, it is evident that the proposed system has integration with IoT, cloud, and blockchain technology. The smart home has plenty of electronic devices with sensors that are integrated with the IoT platform. The data collected by devices are sent to cloud storage. Such data are subjected to big data analytics to have essential business intelligence related to the usage of various resources at home and the behaviour of housemates. This business intelligence can help in making well-informed decisions. The devices participating in the computing are integrated with blockchain technology that enables storage of transactions in a distributed ledger. This ledger is made available to all participating devices so as to let them quickly validate transactions and identify compromised nodes, if any. The end-to-end security in the smart home is thus made possible.

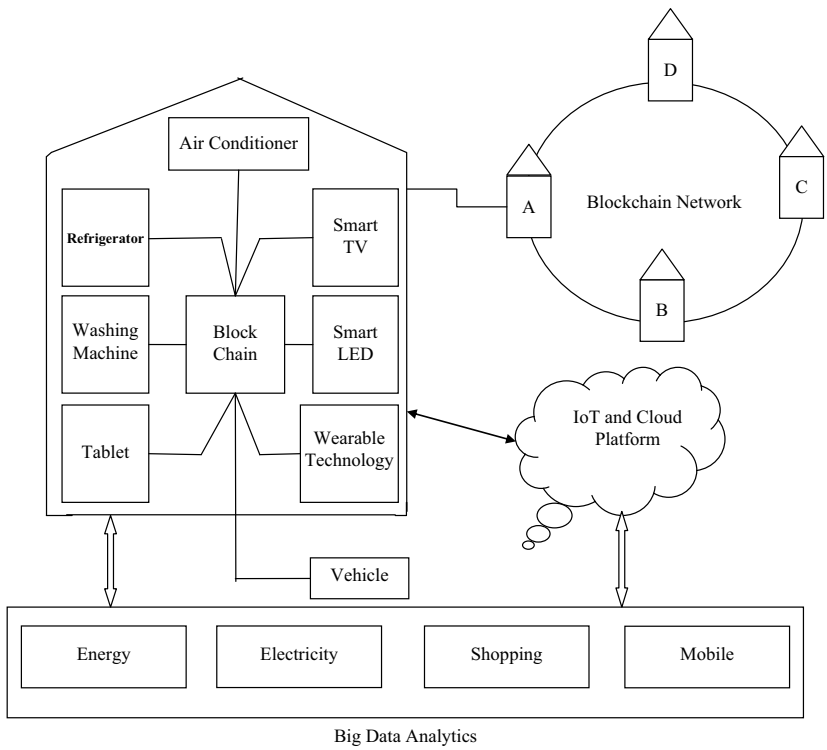

Figure 5.4 The proposed system with smart home system integrated with IoT, cloud, and blockchain technology.

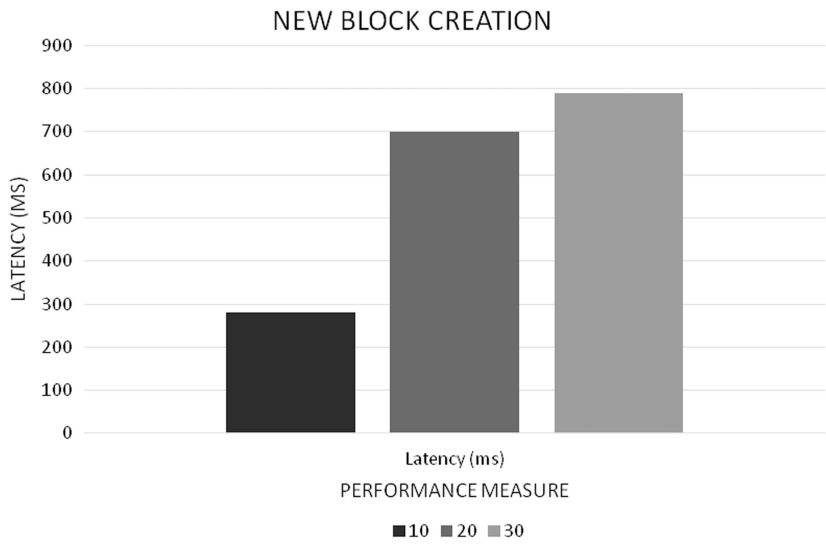

Figure 5.5 Shows performance of the system to create a new block in terms of latency.

5.5 Experimental Results

This section presents the experimental results of the proposed system with partial implementation. It measures the time taken for a new block creation in a distributed ledger and also the time taken to retrieve required data.

As presented in Figure 5.5, the experiments are made with block sizes 10, 20, and 30. Each time, the latency is observed. The latency for creation of a new block in the distributed ledger has its impact on the block size (Figure 5.6).

As presented in Figure 5.5, the experiments are made with block sizes 10, 20 and 30. Each time, the latency is observed. The latency for data retrieval from the distributed ledger has its impact on the block size.

5.6 Conclusion and Future Work

The main focus of this chapter is to design and implement an IoT- and cloud-enabled smart home system with blockchain technology for end-to-end security, besides bestowing benefits of smart home. Blockchain technology ensures that all participating devices in the distributed system can gain access to distributed

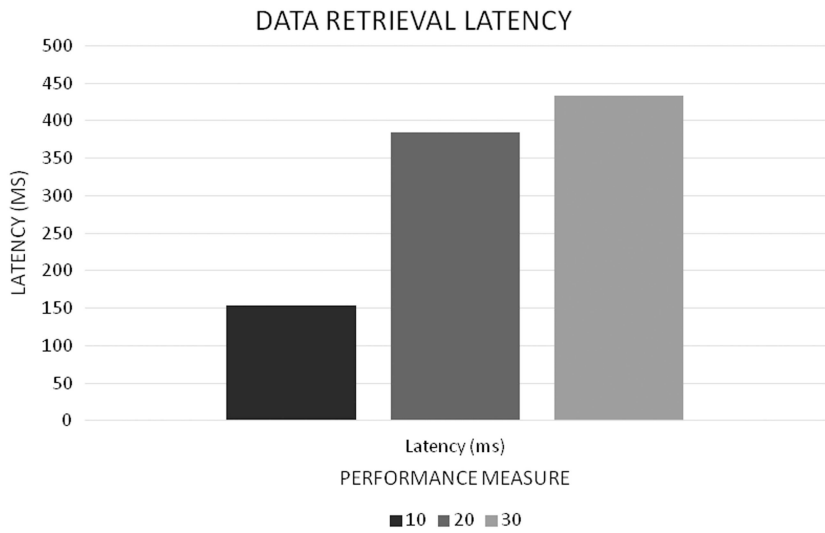

Figure 5.6 Shows performance of the system to retrieve required data.

ledger of transactions and quickly update and validate the transactions. In the process, they can easily detect compromised nodes. In this chapter, we proposed a methodology for smart home and blockchain integration for a higher level of security. The IoT-based smart home–related transactions are saved to a cloud-based distributed ledger in blockchain. The system has a provision to create a hash and encrypt the transactions prior to sending to the blockchain. An empirical study is made to have partial realization of the proposed system. The results revealed that the transactions in a smart home environment are immutable, and they have inherent security of blockchain. The latency for new transactions and data retrieval is observed. In the future, we intend to provide more implementation details and experimental results with improvements in the scope of this work.

References

[1] Dr. M. L. Ravi Chandra, B. Varun Kumar and B. Sureshbabu. (2017). Smart Home Automation Using Virtue of IoT. IEEE International Conference on Energy, Communication, Data Analytics and Soft Computing, P1–P5.

[2] Ioan Szilagyi and Patrice Wira. (2018). An Intelligent System for Smart Buildings Using Machine Learning and Semantic Technologies: A Hybrid Data-Knowledge Approach. *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, St. Petersburg, Russia, P20–P25.

[3] Yuanyu Zhang, Shoji Kasahara, Yulong Shen, Xiaohong Jiang and Jianxiong Wan. (2018). Smart Contract-Based Access Control for the Internet of Things. *IEEE*, 6(2), P1–P11.

[4] Konstantinos Christidis and Michael Devetsikiotis. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, P1–P12.

[5] Kamanashis Biswas and Vallipuram Muthukkumarasamy. (2016). Securing Smart Cities Using Blockchain Technology. IEEE International Conference on High Performance Computing and Communications, P1–P2.

[6] Waqar Ali, Ghulam Dustgeer, Muhammad Awais, and Munam Ali Shah. (2017). IoT Based Smart Home: Security Challenges, Security Requirements and Solutions. International Conference on Automation & Computing, University of Huddersfield, P1–P6.

[7] Vaibhavkumar Yadav, Shubham Borate, Soniya Devar, Rohit Gaikwad and A. B. Gavali. (2017). Smart Home Automation Using Virtue of IoT. IEEE International Conference for Convergence in Technology, P1–P5.

[8] Ms. Priti Vasant Kale, Dr. Samidha Dwivedi Sharma. (2014). Intelligent Home Security System Using Illumination Sensitive Background Model. *International Journal of Advance Engineering and Research Development*, 1(5), P1–P11.

[9] Arun Cyril Jose, and Reza Malekian. (2017). *Improving Smart Home Security; Integrating Logical Sensing into Smart Home*. IEEE, P1–P18.

[10] Dariusz Frejlichowski, Katarzyna Gosciewska, Paweł Forczmanski and Radosław Hofman. (2014). "Smartmonitor"—An Intelligent Security System for the Protection of Individuals and Small Properties with the Possibility of Home Automation. *Sensors*, 14(6), P1–P27.

[11] Timothy Malche and Priti Maheshwary. (2017). Internet of Things (IoT) for Building Smart Home System. IEEE International Conference on I-SMAC (IoT In Social, Mobile, Analytics and Cloud) (I-SMAC), P1–P6.

[12] S. Tanwar, P. Pately, K. Patelz, S. Tyagix, N. Kumar and M. S. Obaidat. (2017). An Advanced Internet of Thing Based Security Alert System for Smart Home. IEEE International Conference on Computer, Information and Telecommunication Systems, P1–P5.

[13] Dr. M. L. Ravi Chandra, B. Varun Kumar, B. Sureshbabu. (2017). IoT Enabled Home with Smart Security. International Conference on Energy, Communication, Data Analytics and Soft Computing, P1–P5.

[14] Joshua Streiff, Olivia Kenny, Sanchari Das, Andrew Leeth, and L. Jean Camp. (2018) Poster Abstract: Who's Watching Your Child Exploring Home Security Risks with Smart Toybears. IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation, P1–P2.

[15] Su Zin Zin Win, Zaw Min Minhtun, and Hlamyo Tun. (2016). Smart Security System for Home Appliances Control Based on Internet of Things. *International Journal of Scientific & Technology Research*, 5(6), P1–P6.

[16] Ali Dorri, Salil S. Kanhere, Raja Jurdaky and Praveen Gauravaram. (2017). Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. IEEE International Conference on Pervasive Computing and Communications Workshops (Percom Workshops), P1–P6.

[17] Ali Dorri, Salil S. Kanhere and Raja Jurdak. (2017). Towards an Optimized Blockchain for IoT. ACM Second International Conference on Internet-of-Things Design and Implementation, P1–P6.

[18] Ali Dorri, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. (2017) *A Light Weight Scalable Blockchain for IoT Security and Privacy*. IEEE, P1–P17.

[19] Raja Jurdak. (2017). *Blockchain for Internet of Things Security and Privacy*. Csiro, P1–P21.

[20] Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram. (2017). *Blockchain for IoT Security and Privacy*. IEEE, P1–P7.

[21] Jianjun Sun, Jiaqi Yan and Kem Z. K. Zhang. (2016). Blockchain-Based Sharing Services: What Blockchain Technology Can Contribute to Smart Cities. *Financial Innovation*, 2, P1–P9.

[22] Shiyong Yin, Jinsong Bao, Yiming Zhang and Xiaodi Huang. (2017). M2M Security Technology of CPS Based on Blockchains. *Symmetry*, 9(9), P1–P16.