Int. J. Nonlinear Anal. Appl. In Press, 1–9
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2023.31676.4703

# Presenting a blockchain-based nonlinear model for the security of smart home

Nayereh Ghadimi, Ziaddin Daie Koozehkanani*, Seyed Amir Mortezavi

*Department of Electrical and Computer Engineering, Tabriz University, Tabriz, Iran*

*(Communicated by Mouquan Shen)*

**Abstract**

Using the Internet of Things technology, it will be possible to control the smart devices and appliances in a smart home. In this paper, the policies and concerns of users of smart devices and devices in homes and the factors that threaten privacy and access control in the Internet of Things are identified. In order to prevent the factors that cause these limitations, a non-linear model with its application in the smart home is presented. It is also investigated at which stage access to the Internet of Things weakens the security of smart homes and attacks by hackers. The independent variable of this research is the safe design of the smart home, and the variables of speed, time, usefulness, efficiency, ease of use, usability and security are dependent variables. The emphasis of this paper is on the use of blockchain technology to store the security rules in the form of a script inside the blockchain and the security rules are not concentrated in one place. Finally, a non-linear model is presented that can cover some of the security disadvantages of using the Internet of Things in smart homes and increase the security of the smart home.

Keywords: Non-linear model, Smart home, Blockchain, Security
2020 MSC: 68M25, 70K99, 94A62

## 1 Introduction

The Internet of Things is one of the new technologies in the current era, and after its widespread use, the issue of its security and confidentiality has attracted a lot of attention and has become a controversial issue in this field. Protecting the Internet of Things is a complex and difficult activity because the Internet of Things requires confidentiality, integrity, authentication, access control, privacy and trust among users in this area in a precise manner. Today, most of the advanced countries have invested the necessary financial resources and human resources for research and development on the home security system with Internet of Things technology. One of the important goals of smart homes is to establish more control and smart security in a house or even a large building. In fact, by using the Internet of Things, it is possible to control the devices and smart devices in a smart home, and in this way, it will be possible to establish better security in the smart home.

A smart home is a home or a technology-compliant environment that allows all home appliances and household electrical appliances to provide remote control to users by connecting to the Internet and other communication platforms [10]. There have been many advancements in technology as a result of which sensors, processors, transmitters,

*Corresponding author
*Email addresses:* nayereh.ghadimi@gmail.com (Nayereh Ghadimi), zdaei@tabrizu.ac.ir (Ziaddin Daie Koozehkanani ), sa.mortezavi@tabrizu.ac.ir ( Amir Mortezavi)

*Received:* July 2023 *Accepted:* September 2023

receivers etc. are now available at very cheap rates. Therefore, this equipment can be used in daily life [21]. The Internet of Things is a new technological thought process in which every physical object or object is connected to the Internet for a better quality of life in society [9]. Most companies are designing, developing and deploying smart objects and smart homes. Now and in the future in all smart homes, there will be computing, communication, monitoring and power control even over people [4]. The Internet of Things is a reliable technology for improving the quality of life in smart homes, which can appear through the provision of various automatic, interactive and convenient services [20].

Using the Internet of Things technology, it will be possible to control the smart devices and appliances in a smart home. In this article, the policies and concerns of users of smart devices and devices in homes and the factors that threaten privacy and access control in the Internet of Things are identified. In order to prevent the factors that cause these limitations, a non-linear model with its application in the smart home is presented. It is also investigated at which stage access to the Internet of Things weakens the security of smart homes and attackers' attacks on them. The independent variable of this research is the safe design of the smart home, and the variables of speed, time, usefulness, efficiency, ease of use, usability and security are dependent variables. The emphasis of this paper is on the use of blockchain technology to store the security rules in the form of a script inside the blockchain and the security rules are not concentrated in one place. Finally, a non-linear model is presented that can cover some of the security disadvantages of using the Internet of Things in smart homes and increase the security of the smart home.

## 2 Challenges of Internet of Things for Application in Smart Home

Security in the Internet of Things can be considered the most important challenge for the development of this technology. In this regard, various standards are being presented, but still the security threats and requirements of the Internet of Things and even its risks have not been well identified and analyzed. Two important factors of static and centralization are the problems of access control policy. In fact, many of the access control solutions proposed to date lead to unauthorized access and control of devices by collecting and analyzing user data for centralized entities. Unauthorized access control of devices may cause ethical problems and privacy violations, so it is necessary that the access control policy be studied and reviewed more carefully to increase security. The use of Internet of Things in smart homes faces challenges as shown in Table 1.

Vulnerabilities in the Internet of Things and smart home cause various threats. Some of these threats are presented in Table 2 based on the research done.

The reasons for the difference between the security of the Internet of Things and other devices include the following:

1. IoT devices often use slow processors. Most of these devices are driven by batteries. Today's cryptographic algorithms require fast computations, so they cannot communicate directly with these devices.
2. IoT devices have limited memory compared to mobile phones and laptops. Conventional security schemes are not designed for devices with limited memory.
3. IoT devices often use low-speed radio communications. Due to low bandwidth, traditional security plans cannot be connected to IoT-based systems.
4. Installing security packages on an IoT device may not be feasible because IoT-style operating systems may lack modules to receive and integrate new codes.
5. IoT mobile devices may connect to the network without prior configuration or may suddenly leave the network. This kind of sudden change in network topologies affects the performance of existing security programs. As a result, these designs cannot be applied to the Internet of Things environment.

Next, we will talk about the use of blockchain in the Internet of Things. The interesting feature of blockchain is that if a series of data is recorded and stored in it, it is not easy to change them. Features of blockchain technology include: advanced features such as smart contracts and smart home, potential financial applications such as private securities, internet insurance, applications including the Internet of Things, decentralized information storage, notarizations, and anti-fraud solutions.

In short, it can be stated that one of the other features of blockchain is that: 1- There is no centralized server. 2- The data of each node becomes an official report set with other nodes. 3- The data is recorded independently on each network node. Smart homes should be considered one of the main applications of the Internet of Things. By using this concept, users can be informed of their status instantly through communication with all types of household appliances used. For example, if the macro has finished its work, the user will be informed about this through notifications, and as a result, the productivity in the system will increase.

Table 1: Challenges of IoT in the field of smart home

| Challenge | Description | Refs. |
|---|---|---|
| Privacy | Preservation of privacy and related issues such as information security and disclosure of information and data | [10, 21, 9] |
| Communications | Strength, stability of security and many communication protocols and the heterogeneity of these communications | [4, 20] |
| Safety | Physical safety of objects, physical access and self-safety capability | [12, 2] |
| Network and security | Network through communication and the breadth and diversity of communication | [18, 14] |
| Security | Maintain security independently | [23, 13] |
| Trust | Trust mechanisms | [11, 16] |
| Confidentiality and encryption | Maintaining confidentiality and related solutions such as encryption and object restrictions | [7, 29] |
| Security of information | Maintaining the security of information against the Internet of Things due to the increase in the volume of information, the multiplicity of objects and heterogeneity | [25, 6] |
| Naming and identity management | Authentication of identities, identification and objects and standardization | [3, 28] |
| A large number of objects | The multiplicity of various objects and communications and the large amount of data produced and the processing and control of the volume of information and communications | [31, 19] |
| Energy consumption | The development of the Internet of Things will increase the consumption of electrical energy and increase the cost and impact on the environment | [15, 26] |
| Big data | Concerns in the collection, storage and control of data processing due to the increase in the volume of data and their transfer strategies and the creation of big data. | [1, 22] |
| The ability of devices and objects to work with each other | The establishment of communication and maximum productivity of the Internet of Things has affected the ability to work with various objects | [24, 8] |
| Save | Storage concerns in the volume of data generated due to the increase in data volume | [30, 5] |
| Heterogeneity of things | Increasing the number of heterogeneities and the need to establish communication and different types of data created and manage and process them | [27, 17] |

## 3 Presented Non-Linear Model for Smart Home

To create a new model in the Cisco Packet Tracer software environment, a new project must be created and the required objects such as washing machines, lights, etc. must be placed on this page. Then all objects are connected to a switch to connect to the control device. The control device can be a mobile phone or a laptop and is connected through a wireless network. The design of the created components is according to Figures.

After adding these objects to the simulator environment, all these objects should be addressed like in the real environment and given a unique number so that they can be placed in the network and can be accessed from different ways such as mobile phones or tablets, and with Enter the username and password and after authentication, control the relevant device. To access the data, just go to the desired object and double click on it. For scripting in the software, you must enter the settings of each object, then select the advanced option and select the programming tab. You can write scripts in this section. In the simulation, a number of sensors used in a smart home are used. Each of these sensors is called an object. The implementation of the model is checked in the simulator with the arrangement of different states and different conditions.
The modes considered in this article are as follows:

**First mode**: a smart house including a refrigerator, gas stove, TV, heating cooling system, lighting system, fire extinguishing system, temperature sensor, entrance door lock, window lock and including 8 cameras, i.e. to the rooms, kitchen, roof and It is the yard.The design of the created components is according to Figure 1. . **The second mode**: a three-story smart house, where each floor has smart things like a refrigerator, gas stove, TV, heating cooling system, lighting system, and each floor has 5 cameras and 5 cameras for the stairs of the floors, and also has a smart lock on the entrance door. Each floor is the building's parking lock, and each person has access to their smart objects on each floor and to the common cameras of the staircases and entrance doors and the building's parking lot. The design of the created components is according to Figure 2.

**The third mode**: It is a two-story residential office building, where the first office floor includes heating cooling system, lighting system, fire extinguishing system, audio system and indoor cameras. The second floor includes heating cooling system, lighting system, fire extinguishing system, refrigerator and gas stove and 5 cameras. Each floor has

Table 2: Challenges of IoT in the field of smart home

| No | Threat title | Ref. |
|---|---|---|
| 1 | Tampering | [21, 27] |
| 2 | Impersonation | [9, 23] |
| 3 | Eavesdropping | [4, 1] |
| 4 | Block Channel and Jamming | [12, 19] |
| 5 | Traffic Analyzing | [2, 19] |
| 6 | Denial of service | [18, 1] |
| 7 | Ransom Ware | [23, 1] |
| 8 | Fake phone control programs | [11, 27] |
| 9 | Man in the middle | [23, 19] |
| 10 | Fake | [19, 15] |
| 11 | Reconnaissance | [19, 26] |
| 12 | Malicious Codec | [19, 1] |
| 13 | Replay | [22, 27] |
| 14 | Fragmentation | [30, 27] |
| 15 | Replication | [5, 27] |

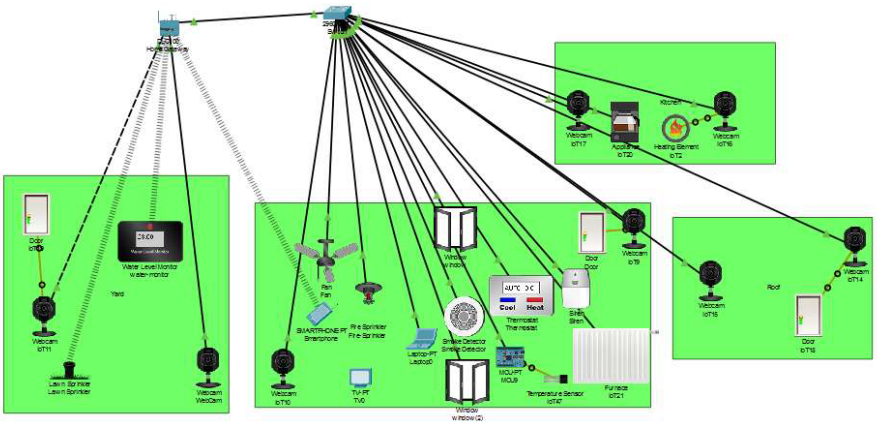

Figure 1: Presented Model

a separate smart door and a common parking door and 5 common cameras outside the building. The design of the created components is according to Figure 3.

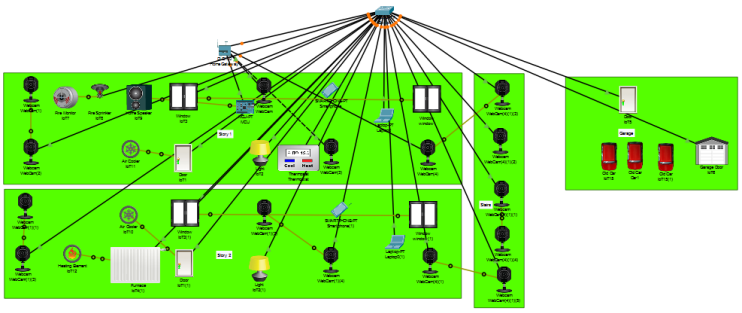

Figure 3: Presented Model

The functions used in the presented model for blockchain and Internet of Things communication are listed in Table 3.

Based on the functions of the above table and its commands, programming was done as follows for the intelligent control of objects on the blockchain platform. The structure of the proposed program is shown in Figure 4.

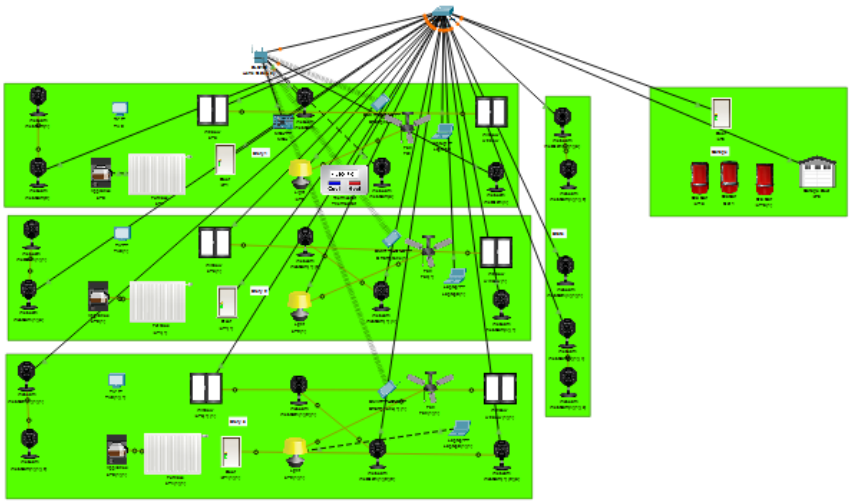

Figure 2: Presented Model

```
1. Add(Webcam)
      CreateSecurity Policy (Webcam)
2.SenSmartContract.Blokchin(Security Policy)
3.function  DynamicAccessControl. Webcam()
 {
          IoEClient.setup(
          {
                    type: " Webcam ",
                    states:
                              {
                                 name: "On",
                                 type: "bool",
                                 controllable: true
                              }
          }

4.        String uri =authReq.getRedirecturiUri();
5.        String AccessCode = getAccessCodeValue();
6.        Request(Smartphone, Webcam)
7.        SmartContract(Webcam, Smartphone, SmartContract)
8.        GrantAccess(Smartphone, Webcam, Tracntesh)
9.        if (GrantAccess(Smartphone, Webcam, Tracntesh)=== 0 )
          {
10.                 Reject(Smartphone, Webcam, Tracntesh )
11.                 Feed(Tracntesh ,Smartphone, Webcam, )
12.                 Update(SmartContract)
          }
             Else
          {
13.                 Add(traconeshtoBlockchin)
14.                 Feed(Tracntesh ,Smartphone, Webcam, )
15.                 Update(SmartContract)
16.                 ExecuteotherAccesscontrol
          }
  }
```

Figure 4: Structure of the proposed program

The description of the code presented in Figure 2, which is part of the original model code, follows.

1. First, the camera object is created and then the security policy rules are created for it.
2. A function is defined to publish the smart contract in the blockchain network.
3. The camera access function defines the required variables.

Table 3: Functions used in the presented model

| No. | Code | Explanation | Description | Command |
|---|---|---|---|---|
| 1 | A | Applicant | How does user want to access the resources? | |
| 2 | B | Source with purpose | Objects that are desired | |
| 3 | A, B | Request | Requester A sends an access request to target or object B | Req (A, B) |
| 4 | B, A, S | Forwarding Smart contract | Target B forwards topic A to smart contract S | SmartContract (B, A, S) |
| 5 | A, B, T | Allow access | It completes the remaining steps for access and then allows A to access B. It also creates a transaction T. | GrantAccess (A, B, T) |
| 6 | T | Adding | Transaction T is added to the blockchain | AddBC(T) |
| 7 | A, B, T | Feedback | Send feedback information of transaction T to A and B | feed (A, B, T) |
| 8 | B | Updating | Update the information | update (B) |
| 9 | A, B, R | Reject | Denying access from A to B means that it will reject R's request from now on | Reject (A, B, R) |

4. The information that is to be exchanged between two users must first be converted into a string, and for this reason a function is defined to convert the information of the object that is to be accessed into a string.
5. Function definition with the purpose of sending the information in the form of a message to the operation.
6. An access request is sent to the camera from a smartphone.
7. The camera directs the smartphone request to the smart contract to check the access permission.
8. Blockchain implements the smart contract and checks its validity. If the object has access rights according to the security policy defined in the blockchain, this blockchain is added to the sent transaction and the authentication process continues. If the object is not allowed to be used according to the security policy, the request is canceled and this feedback is sent to both the requested object (camera) and the target (smartphone).
9. The transaction requesting access to the smart object is checked. If the access request to this object has already been canceled, access is not possible and the entire request is canceled.
10. This access request is cancelled.
11. The feedback of this result is sent to the object and target.
12. The smart contract is updated again with new information.
13. If access to this object is valid, the transaction will be added to the requested blockchain.
14. The feedback of the permission of this access is sent to the object and target.
15. The smart contract is updated with the new information of this transaction
16. If the smart contract is valid, a function is executed that performs other conditions of access to the object, such as checking the password ID, etc.

The steps of considering the blockchain for the above smart home are mentioned in the form of a flowchart in Figure 5.

Finally, the proposed model was compared with the research of other researchers, which is shown in Table 4.

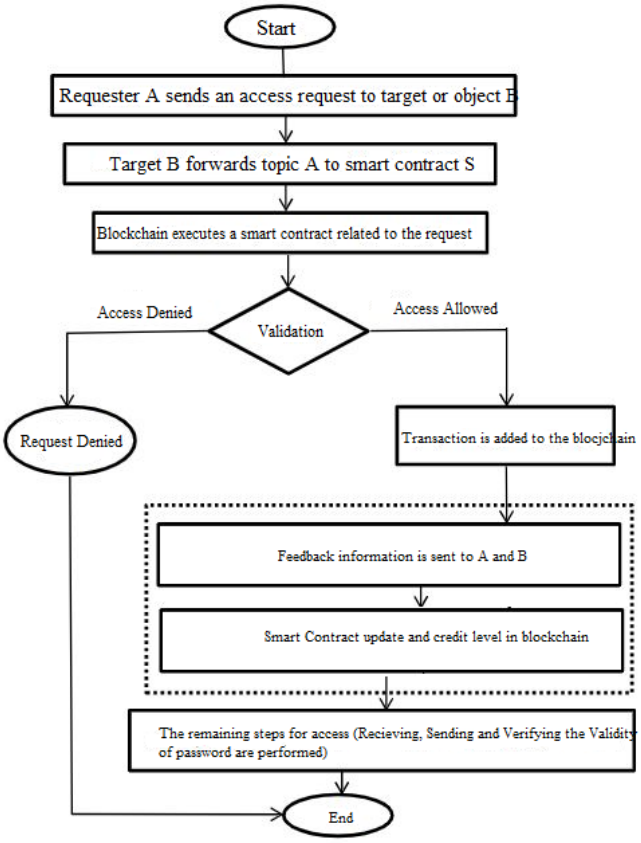


Figure 5: Flowchart of the proposed model

Table 4: Comparison of the proposed model with the research of other researchers

| **Researcher** | **Year** | **Access control model** | **Usability** | **Flexibility** | **Interoperability** | **Distribution** | **Static** |
|---|---|---|---|---|---|---|---|
| E. Braka | 2015 | RBAC | M | M | VH | NO | Yes |
| Y. Zhu | 2014 | ABAC | M | M | M | NO | Yes |
| G. Zhang | 2011 | UCON | L | L | L | NO | Yes |
| S. Gusmeroi | 2013 | CAPBAC | H | H | H | M | Yes |
| J.E. Kim | 2013 | XACML | L | L | L | H | Yes |
| P. Fremantle | 2015 | OAUTH | H | H | VH | VL | Yes |
| V. Varadharajan | 2016 | UMA | H | H | L | VL | Yes |
| E. Sciancaleore | 2017 | OAuth-IoT | H | H | VH | VL | Yes |
| T. Le | 2018 | CapChain | H | L | VH | H | Yes |
| S. K. Pinjala | 2019 | DCACI | H | H | VH | H | Yes |
| D. Gupta | 2020 | GCPAC | VH | VH | VH | H | Yes |
| Presented model | 2023 | Presented model | H | H | VH | H | Yes |

Symbols: VH=Very High: 5; H=High: 4; M=Medium: 3; L=Low: 2; VL=Very Low: 1; No=Null: 0

As shown in Table 4, the presented model was compared with other researchers' models from 2011 to 2020. The comparison of the results showed that the access control mechanism by following the centralized approach reduces the process calculations and shows good interoperability. As a result, it provides easy management policies for access control. A centralized approach to limited smart devices enables costly operations such as evaluating security policies and verifying external entities, thus reducing process computations. The important point is that such approaches cannot store access policies, access control lists, and confidential documents such as keys or certificates. Centralized approaches introduce overhead communication for smart devices that send the access code to an external entity to

make a decision about its approval due to more communication with external entities. Such communication increases the response time to requests, which is not suitable for time-sensitive fields.

## 4 Conclusion

In the proposed plan, if there is a problem with the object, by writing and using algorithms in the blockchain, such problems are recorded in the smart contract in the blockchain, and instant access requests are prevented from referring to this object. This approach reduces network communication and silence and increases communication and collaboration in the network.

In the implementation of a plan of a smart house based on the model provided in the Internet of Things simulator software, it was evaluated to check the characteristics of the availability of objects, the duration of access, the response of the object to the requester. The response time of objects, flexibility in relation to other objects, timely response, making changes by the user and other things were investigated. The results showed that features such as distributedness, interoperability, flexibility and changes by the user are in good condition, but things such as responding in time due to checking the validity of the object in the blockchain and updating the feedback are at a lower level. On the other hand, distributed approaches are suitable for performing political functions and authentication decisions for IoT systems and applications because distributed approaches show good scalability.

## References

[1] H. Abdulkarim, *Review on machine learning and deep learning algorithms for IoT security*, Int. J. Nonlinear Anal. Appl. **14** (2023), no. 5, 27–35.

[2] M. Amoozadeh, A. Raghuramu, Ch.-N. Chuah, D. Ghosal, H.M. Zhang, J. Rowe, and K. Levitt, *Security vulnerabilities of connected vehicle streams and their impact on cooperative driving*, IEEE Commun. Mag. **53** (2015), no. 6, 126–132.

[3] A. Baliga, *Understanding blockchain consensus models*, Persistent **4** (2017), no. 1, 14.

[4] A. Banafa, *IoT and blockchain convergence: Benefits and challenges*, IEEE Internet of Things **9** (2017), no. 2017.

[5] V. Beltran, J.A. Martinez, A. Skarmeta, and P. Martinez-Julia, *An arm-compliant IoT platform: Security by design for the smart home*, IEEE 5th Glob. Conf. Consum. Electron., IEEE, 2016, pp. 1–2.

[6] G. Brambilla, M. Amoretti, and F. Zanichelli, *Using blockchain for peer-to-peer proof-of-location*, arXiv preprint arXiv:1607.00174 **20** (2016).

[7] J. Buchmann, *Introduction to Cryptography*, vol. 335, Springer, 2004.

[8] E. Castelló Ferrer, *The blockchain: A new framework for robotic swarm systems*, Proc. Future Technol. Conf. (FTC) 2018, Volume 2, Springer, 2019, pp. 1037–1058.

[9] M.L. Das, *Privacy and security challenges in Internet of Things*, Distrib. Comput. Internet Technol.: 11th Int. Conf., ICDCIT 2015, Bhubaneswar, India, February 5-8, 2015. Proceedings 11, Springer, 2015, pp. 33–48.

[10] S.K. Datta, Ch. Bonnet, and N. Nikaein, *An IoT gateway centric architecture to provide novel m2m services*, IEEE World Forum on Internet of Things (WF-IoT), IEEE, 2014, pp. 514–519.

[11] M.C. Domingo, *An overview of the internet of underwater things*, J. Network Comput. Appl. **35** (2012), no. 6, 1879–1890.

[12] A. Dorri, S.S. Kanhere, R. Jurdak, and P. Gauravaram, *Blockchain for IoT security and privacy: The case study of a smart home*, IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom workshops), IEEE, 2017, pp. 618–623.

[13] A. Ekblaw, A. Azaria, J.D. Halamka, and A. Lippman, *A case study for blockchain in healthcare: "medrec" prototype for electronic health records and medical research data*, Proc. IEEE Open Big Data Conf., vol. 13, 2016, pp. 13.

[14] H. Gross, M. Hölbl, D. Slamanig, and R. Spreitzer, *Privacy-aware authentication in the internet of things*, Cryptol. Network Secur.: 14th Int. Conf., CANS 2015, Marrakesh, Morocco, December 10-12, 2015, Proceedings 14, Springer, 2015, pp. 32–39.

[15] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, *Smart locks: Lessons for securing commodity Internet of Things devices*, Proc. 11th ACM Asia Conf. Comput. Commun. Secur., 2016, pp. 461–472.

[16] Sunny King, *Primecoin: Cryptocurrency with prime number proof-of-work*, Preprint https://c3.coinlore.com/pdf/primecoin-white-paper.pdf

[17] I. Kotenko, I. Saenko, and A. Branitskiy, *Framework for mobile Internet of Things security monitoring based on big data processing and machine learning*, IEEE Access **6** (2018), 72714–72723.

[18] L. Li, R. Lu, K.-K.R. Choo, A. Datta, and J. Shao, *Privacy-preserving-outsourced association rule mining on vertically partitioned databases*, IEEE Trans. Inf. Forensics Secur.**11** (2016), no. 8, 1847–1861.

[19] A. Mosenia and N.K. Jha, *A comprehensive study of security of internet-of-things*, IEEE Trans. Emerg. Topics Comput. **5** (2016), no. 4, 586–602.

[20] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016.

[21] A. Ouaddah, H. Mousannif, A. Abou Elkalam, and A.A. Ouahman, *Access control in the internet of things: Big challenges and new opportunities*, Comput. Networks **112** (2017), 237–262.

[22] R. Roman, J. Zhou, and J. Lopez, *On the features and challenges of security and privacy in distributed Internet of Things*, Comput. Networks **57** (2013), no. 10, 2266–2279.

[23] S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini, *Security, privacy and trust in Internet of Things: The road ahead*, Comput. Networks **76** (2015), 146–164.

[24] J. Sun, J. Yan, and K.Z.K. Zhang, *Blockchain-based sharing services: What blockchain technology can contribute to smart cities*, Financ. Innov. **2** (2016), no. 1, 1–9.

[25] A Tandulwadikar, *Blockchain in banking: A measured approach, cognizant reports*, Cognizant Reports, 2020, from https://www.cognizant.com/whitepapers/Blockchain-in-Banking-A-MeasuredApproach-codex1809.pdf.

[26] Ch. Wang, Zh. Bi, and L.D. Xu, *Iot and cloud computing in automation of assembly modeling systems*, IEEE Trans. Ind. Inf. **10** (2014), no. 2, 1426–1434.

[27] Y. Wang and Q. Wen, *A privacy enhanced dns scheme for the Internet of Things*, IET Int. Conf. Commun. Technol. Appl., 2011, pp. 699–702.

[28] G. Wood, *Ethereum: A secure decentralised generalised transaction ledger*, Ethereum project yellow paper **151** (2014), no. 2014, 1–32.

[29] Ch. Yang, X. Chen, and Y. Xiang, *Blockchain-based publicly verifiable data deletion scheme for cloud storage*, J. Network Comput. Appl. **103** (2018), 185–193.

[30] K. Zhao and L. Ge, *A survey on the Internet of Things security*, Ninth Int. Conf. Comput. Intell. Secur., IEEE, 2013, pp. 663–667.

[31] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, *The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved*, IEEE Internet Things J. **6** (2018), no. 2, 1606–1616.