BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

REVIEW

The Internet of Things Security and Privacy: Current Schemes, Challenges and Future Prospects

Peter Sungu Nyakomitta* **Solomon Ogara** **Paul Abounji**

Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya

ARTICLE INFO

Article history
Received: 26 July 2022
Revised: 2 September 2022
Accepted: 5 September 2022
Published Online: 13 September 2022

Keywords:
IoT
Security
Privacy
Attacks
Performance

ABSTRACT

The Internet of Things devices and users exchange massive amount of data. Some of these exchanged messages are highly sensitive as they involve organizational, military or patient personally identifiable information. Therefore, many schemes and protocols have been put forward to protect the transmitted messages. The techniques deployed in these schemes may include blockchain, public key infrastructure, elliptic curve cryptography, physically unclonable function and radio frequency identification. In this paper, a review is provided of these schemes including their strengths and weaknesses. Based on the obtained results, it is clear that majority of these protocols have numerous security, performance and privacy issues.

1. Introduction

The Internet of Things (IoT) facilitates data sharing among numerous devices and people through a variety of wireless sensors and mobile computing devices [1-3], as shown in Figure 1. As shown here, the IoT building blocks include the smart things, gateways, middleware and applications. Over the recent past, IoT has acted as an enabling technology in a number of application domains such as healthcare, smart homes, military, weather forecasting, smart cities, fire monitoring and intelligent transport systems. As explained by Mamdouh et al. [4], IoT plays a crucial role in the healthcare where it has helped enhance the quality of life. For instance, Internet of Health Things (IoHT) sensors can perceive biomedical data such as blood pressures and heart [5].

An intruder can attack these sensors and cause the death of a patient. In an IoT environment, privacy and security are major issues that need to be upheld during the communication process. As pointed out by Hassan [6],

*Corresponding Author:
Peter Sungu Nyakomitta,
Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya;
Email: pnyakomitta@yahoo.com

DOI: https://doi.org/10.30564/jcsr.v4i3.4925

numerous security gaps lurk that can permit malicious devices and users to gain access to the IoT resources. In addition, this breach can lead to privacy violations as well as economic losses [7]. This can further enable the adversary to use the hijacked devices as vectors to invade the entire network [8]. These security challenges are attributed to vulnerabilities in the authentication procedures [9,10]. According to Wang et al. [11], the susceptibilities in IoHT can threaten the lives of the patients. For instance, eavesdropping, Sybil, man-in-the-middle (MitM), Distributed Denial of Service (DDoS) and spoofing are serious threats in IoT [12]. There is therefore need to uphold high security in terms of availability, confidentiality and integrity for the sensitive data that is being exchanged. Unfortunately, most of the IoT devices are resource constrained in terms of memory, energy, storage, computation, processing capacity and communication capabilities [13,14]. As such, only lightweight security solutions are feasible in an IoT environment [15]. In this paper, an extensive review of the state of the art schemes that have been developed to address security and privacy issues in IoT are investigated.

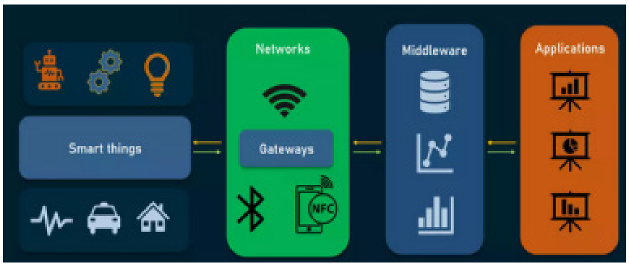

Figure 1. IoT communication architecture

2. Related Work

There have been numerous security solutions developed for an IoT environment, based on techniques such as Physically Unclonable Function (PUF), blockchain, Public Key Infrastructure (PKI), radio frequency identification (RFID) tags among others. For instance lightweight PUF-based identity verification schemes have been presented by Zhao et al. [16], Braeken [17], and Xu et al. [18]. Some of these schemes have been shown to be resilient against replay, cloning and de-synchronization attacks [18]. However, PUF-based schemes have stability issues [19]. On the other hand, blockchain based protocols has been deployed to enhance privacy and identity management in IoT [20-23]. These schemes protect IoT devices against attacks such as cache misappropriation and data modifications [21]. In addition, they offer transparency, time immutability, decentralization and high security for shared data. However, blockchain technology has high computation and storage overheads [24]. Although the RFID-based schemes can secure the IoT communication, they are vulnerable to jamming and cloning attacks [25,26].

On the other hand, PKI-based scheme is presented by Jia et al. [27], while an elliptic curve cryptography (ECC) is introduced by Cheng et al. [28]. However, PKI is a centralized authentication approach hence presents a single point of failure. In addition, it has high communication and computation complexities [29], and cannot resist DoS attacks [30,31]. Although the scheme by Cheng et al. [28] is robust against MitM, replay and impersonation attacks, it has high communication costs. A multiparty access authentication mechanism for IoT has been developed by Zhang et al. [32]. However, this protocol is susceptible to modification, replay, MitM and impersonation attacks. The multi-party access mechanism by Zhang et al. [32] also incurs high processing overheads [33] when large numbers of IoT devices are deployed. This problem can be addressed by the protocol developed by Ali et al. [34], which is shown to have less computation overheads and high throughputs. On the other hand, an identity based scheme is presented by Jiang et al. [35] which does not call for certificates storage.

Although the scheme developed by Jesus et al. [36] boosts security and privacy in IoT, it has elongated latencies. Similarly, the technique by Dittmann and Jelitto [37] enhances end-to-end trust between IoT devices but was never evaluated against DDoS [38]. This attack is prevented by the scheme presented by Das et al. [39]. Although the protocol in Al-Jaroodi et al. [40] can offer secure collection and storage of sensitive data, it does not incorporate any form of authentication between the IoHT users and devices. On the other hand, cross-heterogeneous domain authentication protocol is developed by Yuan et al. [41] incurs high computation and communication overheads.

By deploying the key update strategy, a mutual authentication scheme is developed by Naija et al. [42]. However, this approach cannot withstand jamming attacks [43]. To offer better performance and meet security requirements, a radio frequency fingerprint device authentication approach is presented by Tian et al. [44]. However, security and attack analysis of this scheme is lacking. A Certificate Authority (CA) based authentication technique is presented by Yao et al. [45]. However, certificate maintenance in this protocol is complex.

On the other hand, the identity management scheme in Omar and Basir [46] does not present performance evaluation. Similarly, the machine learning based automated identity confirmation algorithm by Poulter et al. [47] has scalability limitations. Although this federated learning based achieves high privacy during the authentication process, it has high energy consumptions [48].

A novel ECC-based pairing free certificateless signature scheme is developed by Shen et al. [49]. Unfortunately, this technique is susceptible to jamming and DoS attacks. To offer enhanced key exchange between IoT devices, an authentication protocol is presented by Alzahrani et al. [50], which is devoid of third-party involvement [51]. On the other hand, an IoHT device authentication approach is developed by Rathee [52] while an IoT node roaming-based authentication model is presented by Wan et al. [53]. Although this protocol prevents replay and malicious nodes attacks, it has high authentication delays when the number of IoT devices increase.

3. Results

The review of the current security solutions has revealed a number of challenges associated with the current schemes. Table 1 presents the summary of these challenges. Based on the information in Table 1, it is clear that the assurance of perfect security and privacy at optimum performance is still challenging.

Table 1. Summary of challenges of current schemes

Scheme	Challenges
Zhao et al. [16] Braeken [17] Xu et al. [18]	PUF-based schemes have stability issues
Ding et al. [20] Yang et al. [21] Singh [22] Jabbar et al. [23]	Blockchain technology has high computation and storage overheads
Jia et al. [27]	Presents a single point of failure; it has high communication and computation complexities; cannot resist DoS attacks
Cheng et al. [28]	Has high communication costs
Zhang et al. [32]	Is susceptible to modification, replay, MitM and impersonation attacks; incurs high processing overheads
Jesus et al. [36]	Has long latencies
Dittmann and Jelitto [37]	Is never evaluated against DDoS
Al-Jaroodi et al. [40]	Does not incorporate any form of authentication between the IoHT users and devices
Yuan et al. [41]	Incurs high computation and communication overheads
Naija et al. [42]	Cannot withstand jamming attacks
Tian et al. [44]	Lacks security and attack analysis
Yao et al. [45]	Certificate maintenance in this protocol is complex
Omar and Basir [46]	Does not present performance evaluation
Poulter et al. [47]	Has scalability limitations
Shen et al. [49]	Is susceptible to jamming and DoS attacks
Wan et al. [53]	It has high authentication delays when the number of IoT devices increase

Some of the identified issues revolve around certificate management, output stability, single point of failure, DoS, DDoS, modification, jamming, replay, MitM, lack of authentication, long latencies, impersonation, and high complexities in terms of computation, storage overheads and communication overheads. It is also evident that some of these schemes also lack security and attack analysis. Table 2 presents the layered approach of these security, performance and privacy setbacks. It is evident from Table 2 that each and every entity in the IoT infrastructure has some issues that need to be solved.

Table 2. Layered IoT Challenges

Category	Challenges
IoT devices	Authorization, authentication, performance
Application	Authentication, trust, performance, authorization
Data	Trust, privacy
Network	Eavesropping, interception, availability

To address some of these performance, security and privacy shortcomings, the recommendations in the sub-section that follows are deemed necessary.

4. Recommendations

In light of the above IoT security, performance and privacy challenges, the following technologies and procedures are recommended as possible solutions.

Machine learning: In an IoT environment, machine learning (ML) algorithms can be deployed for the detection and prediction of attacks. This can be achieved by monitoring the encryption key size as well as the utilized protocols. This can potentially prevent zero-day attacks, misuse as well as abnormal patients' behavior using their profiles. These profiles can then be stored as signatures in databases to be deployed by security solutions such as next generation firewalls. When utilized at the perception layer, these ML algorithms can perform device authentication to thwart the transmission of false information such as malicious identities.

Separation of access privileges: In this approach, the IoT administrators have distinct privileges to the devices and sensors. This is achieved by having passwords that are quite different from those of the IoT devices. Since recalling all these passwords is challenging, Single Sign On (SSO) technique is used to identify these administrators. This allows for the migration of these passwords with device passwords, facilitating different permissions and policies to offer diverse levels of privileges to access IoT devices. It therefore becomes possible to utilize one unique identity to access multiple services from these IoT devices.

Digital signature: In an IoT environment, a digital signature will help the system administrator to utilize their private keys to authenticate and validate the devices. Essentially, hash functions are deployed during the signing operations and enciphers the exchanged data using private keys. On the other hand, the verification process involves the usage of hash function while the deciphering procedures involve the public keys. In essence, when the output of the hash function and the data decryption are identical, then the implication is that the digital signature is valid. Otherwise, this particular digital signature is invalid.

Cloud computing: In an IoT environment, a massive amount of data is exchanged across the network. Therefore, the cloud can offer services such as the data storage as well as data analysis. In this regard, IoT benefits from the high processing capabilities of cloud computing and hence artificial intelligence, deep learning and machine learning techniques can be deployed for the prediction of the critical cases of threats and attacks in this environment. In addition, artificial intelligence and machine learning algorithms benefit from the scalability of cloud computing which can enable them to develop reliable and efficient authentication techniques. This enables the IoT environment to prevent malicious entities from invading the network.

Fog edge computing: the fog computing layer is lies between the cloud and the IoT devices. Here, it is utilized to enhance the performance of cloud computing. In so doing, it reduces the communication latency as well as offering availability, scalability and security through the sharing of the data on the cloud.

Identity authentication: To uphold security among the numerous heterogeneous IoT devices and sensors using diverse protocols, standards and scenarios, device fingerprints are deployed. This ensures that the devices can be securely identified so as to protect the sensitive data.

5G networks: Conventionally, the IoT devices and sensors transmit data at low data rates over the cloud. Since numerous devices and sensors are involved, identity and access management can be transmitted at the same time slot. Fortunately, 5G networks can achieve high levels of security and performance and hence can be deployed as the backbone infrastructure to offer high flexibility, fast response times, high data rates, low latencies and high scalability. In addition, 5G can be deployed during the process of authenticating IoT users and devices. Moreover, 5G can help in boosting security in terms of access control, user authentication, key management, device authentication, intrusion detection as well as protection.

Figure 2 illustrates the six concepts that can be deployed to protect the IoT environment from attacks. As shown in Figure 2, these principles include device intelligence using ML algorithms; edge fog processing; device initiated connections; message control, identification, authentication and encryption; and remote control and update of devices.

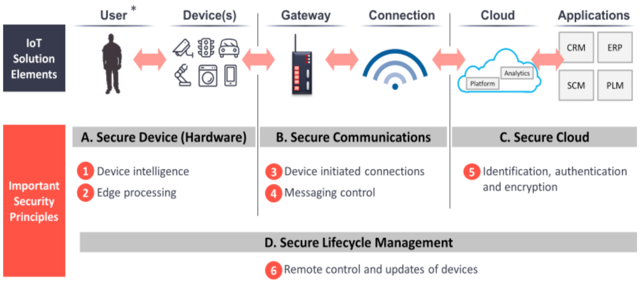
User *
Device(s)
Gateway
Connection
Cloud
Applications
IoT Solution Elements
CRM
ERP
SCM
PLM
Analytics
Platform
Important Security Principles
A. Secure Device (Hardware)
B. Secure Communications
C. Secure Cloud
1 Device intelligence
2 Edge processing
3 Device initiated connections
4 Messaging control
5 Identification, authentication and encryption
D. Secure Lifecycle Management
6 Remote control and updates of devices

Figure 2. Secure IoT communication architecture

On the other hand, the basic components that are required to secure the IoT environment may include users, devices, gateways, connections, cloud and applications. For instance, user training and awareness, proper device disposal, installation of next generation firewalls at the gateways, and the incorporation of strong authentication protocols during connection establishments can potentially boost security. In addition, the incorporation of security during each step of the application development lifecycle can also go a long towards boosting security.

5. Conclusions

The IoT devices have been widely deployed in numerous application domains. However, privacy, performance and security remain key challenges in this IoT environment. As such, there has been active research on the novel security schemes that can help address these issues. In this paper, an extensive review of these techniques is provided. Based on the findings, it is clear that in as much as some progress has been made in IoT security, a number of challenges still lurk. Consequently, a number of recommendations are provided towards the end of this paper. Future work lies in the actual incorporation of these recommendations in the security solutions so that their effects on security, performance and privacy can be determined.

Conflict of Interest

There is no conflict of interest.

References

[1] Mbarek, B., Ge, M., Pitner, T., 2020. An efficient mutual authentication scheme for internet of things. Internet of things. 9, 100160.

[2] Luo, H., Wen, G., Su, J., et al., 2018. SLAP: Succinct and Lightweight Authentication Protocol for low-cost RFID system. Wireless Networks. 24(1), 69-78.

[3] Nyangaresi, V.O., 2022. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 3(5), 1-16.

[4] Mamdouh, M., Awad, A.I., Khalaf, A.A., et al., 2021. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. Computers & Security. 111, 102491.

[5] Rodrigues, J.J., Segundo, D.B.D.R., Junqueira, H.A., et al., 2018. Enabling technologies for the internet of health things. IEEE Access. 6, 13129-13141.

[6] Hassan, W.H., 2019. Current research on Internet of Things (IoT) security: A survey. Computer networks. 148, 283-294.

[7] Lee, I., 2019. The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. Internet of Things. 7, 100078.

[8] Li, M., Sun, Y., Lu, H., et al., 2019. Deep reinforcement learning for partially observable data poisoning attack in crowdsensing systems. IEEE Internet of Things Journal. 7(7), 6266-6278.

[9] Bangui, H., Ge, M., Buhnova, B., 2018. Exploring Big Data Clustering Algorithms for Internet of Things Applications. IoTBDS, Springer. pp. 269-276.

[10] Nyangaresi, V.O., Alsamhi, S.H., 2021. Towards secure traffic signaling in smart grids. 2021 3rd Global Power, Energy and Communication Conference (GPECOM) (pp. 196-201). IEEE.

[11] Wang, L., Ali, Y., Nazir, S., et al., 2020. ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods. IEEE Access. 8, 152316-152332.

[12] Zou, S., Xi, J., Wang, S., et al., 2019. Reportcoin: A novel blockchain-based incentive anonymous reporting system. IEEE access. 7, 65544-65559.

[13] El-Hajj, M., Fadlallah, A., Chamoun, M., et al., 2019. A survey of internet of things (IoT) authentication schemes. Sensors. 19(5), 1141.

[14] Kou, L., Shi, Y., Zhang, L., et al., 2019. A lightweight three-factor user authentication protocol for the information perception of IoT. CMC-Computers, Materials & Continua. 58(2), 545-565.

[15] Nyangaresi, V.O., Petrovic, N., 2021. Efficient PUF based authentication protocol for internet of drones. 2021 International Telecommunications Conference (ITC-Egypt) (pp. 1-4). IEEE.

[16] Zhao, B., Zhao, P., Fan, P., 2020. ePUF: A lightweight double identity verification in IoT. Tsinghua Science and Technology. 25(5), 625-635.

[17] Braeken, A., 2018. PUF based authentication protocol for IoT. Symmetry. 10(8), 352.

[18] Xu, H., Ding, J., Li, P., et al., 2018. A lightweight RFID mutual authentication protocol based on physical unclonable function. Sensors. 18(3), 760.

[19] Nyangaresi, V.O., Abd-Elnaby, M., Eid, M.M., et al., 2022. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. pp. e4528.

[20] Ding, S., Cao, J., Li, C., et al., 2019. A novel attribute-based access control scheme using blockchain for IoT. IEEE Access. 7, 38431-38441.

[21] Yang, Q., Lu, R., Rong, C., et al., 2019. Guest editorial the convergence of blockchain and IoT: Opportunities, challenges and solutions. IEEE Internet of Things Journal. 6(3), 4556-4560.

[22] Singh, M., 2020. Blockchain technology for data management in Industry 4.0. Blockchain Technology for Industry 4.0 (pp. 59-72). Springer, Singapore.

[23] Jabbar, R., Kharbeche, M., Al-Khalifa, K., et al., 2020. Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using ethereum. Sensors. 20(14), 3928.

[24] Nyangaresi, V.O., Ogundoyin, S.O., 2021. Certificate Based Authentication Scheme for Smart Homes. 2021 3rd Global Power, Energy and Communication Conference (GPECOM) (pp. 202-207). IEEE.

[25] El Beqqal, M., Azizi, M., 2017. Classification of major security attacks against RFID systems. 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS) (pp. 1-6). IEEE.

[26] Khattab, A., Jeddi, Z., Amini, E., et al., 2017. RFID security threats and basic solutions. RFID Security (pp. 27-41). Springer, Cham.

[27] Jia, X., Hu, N., Su, S., et al., 2020. IRBA: an identity-based cross-domain authentication scheme for the internet of things. Electronics. 9(4), 634.

[28] Cheng, X., Zhang, Z., Chen, F., et al., 2019. Secure identity authentication of community medical internet of things. IEEE Access. 7, 115966-115977.

[29] Nyangaresi, V.O., 2021. Provably Secure Protocol for 5G HetNets. 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) (pp. 17-22). IEEE.

[30] Cao, B., Li, Y., Zhang, L., et al., 2019. When Internet of Things meets blockchain: Challenges in distributed consensus. IEEE Network. 33(6), 133-139.

[31] Hammi, M.T., Hammi, B., Bellot, P., et al., 2018.

Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security. 78, 126-142.

[32] Zhang, Y., Ren, F., Wu, A., et al., 2019. Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks. IEEE Access. 7, 114721-114730.

[33] Nyangaresi, V.O., Ahmad, M., Alkhayyat, A., et al., 2022. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. pp. e13126.

[34] Ali, G., Ahmad, N., Cao, Y., et al., 2020. xDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things. IEEE Access. 8, 58800-58816.

[35] Jiang, X., Liu, M., Yang, C., et al., 2019. A blockchain-based authentication protocol for WLAN mesh security access. Computers Materials & Continua. 58(1), 45-59.

[36] Jesus, E.F., Chicarino, V.R., De Albuquerque, C.V., et al., 2018. A survey of how to use blockchain to secure internet of things and the stalker attack. Security and Communication Networks.

[37] Dittmann, G., Jelitto, J., 2019. A blockchain proxy for lightweight iot devices. 2019 Crypto valley conference on blockchain technology (CVCBT) (pp. 82-85). IEEE.

[38] Nyangaresi, V.O., 2022. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 15, 100210.

[39] Das, A.K., Wazid, M., Yannam, A.R., et al., 2019. Provably secure ECC-based device access control and key agreement protocol for IoT environment. IEEE Access. 7, 55382-55397.

[40] Al-Jaroodi, J., Mohamed, N., Abukhousa, E., 2020. Health 4.0: on the way to realizing the healthcare of the future. IEEE Access. 8, 211189-211210.

[41] Yuan, C., Zhang, W., Wang, X., 2017. EIMAKP: Heterogeneous cross-domain authenticated key agreement protocols in the EIM system. Arabian Journal for Science and Engineering. 42(8), 3275-3287.

[42] Naija, Y., Beroulle, V., Machhout, M., 2018. Security enhancements of a mutual authentication protocol used in a HF full-fledged RFID tag. Journal of Electronic Testing. 34(3), 291-304.

[43] Nyangaresi, V.O., Mohammad, Z., 2023. Session Key Agreement Protocol for Secure D2D Communication. The Fifth International Conference on Safety and Security with IoT (pp. 81-99). Springer, Cham.

[44] Tian, Q., Lin, Y., Guo, X., et al., 2020. An identity authentication method of a MIoT device based on radio frequency (RF) fingerprint technology. Sensors. 20(4), 1213.

[45] Yao, Y., Xingwei, W., Xiaoguang, S., 2011. A cross heterogeneous domain authentication model based on PKI. 2011 Fourth International Symposium on Parallel Architectures, Algorithms and Programming (pp. 325-329). IEEE.

[46] Omar, A.S., Basir, O., 2018. Identity management in IoT networks using blockchain and smart contracts. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 994-1000). IEEE.

[47] Poulter, A.J., Ossont, S.J., Cox, S.J., 2020. Enabling the secure use of Dynamic Identity for the Internet of Things—using the Secure Remote Update Protocol (SRUP). Future Internet. 12(8), 138.

[48] Nyangaresi, V.O., Moundounga, A.R.A., 2021. September. Secure Data Exchange Scheme for Smart Grids. 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) (pp. 312-316). IEEE.

[49] Shen, J., Gui, Z., Ji, S., et al., 2018. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. Journal of Network and Computer Applications. 106, 117-123.

[50] Alzahrani, B.A., Chaudhry, S.A., Barnawi, A., et al., 2020. An anonymous device to device authentication protocol using ECC and self certified public keys usable in Internet of Things based autonomous devices. Electronics. 9(3), 520.

[51] Nyangaresi, V.O., Morsy, M.A., 2021, September. Towards Privacy Preservation in Internet of Drones. 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) (pp. 306-311). IEEE.

[52] Rathee, P., 2020. Introduction to blockchain and IoT. In Advanced Applications of Blockchain Technology (pp. 1-14). Springer, Singapore.

[53] Wan, Z., Xu, Z., Liu, S., et al., 2020. An internet of things roaming authentication protocol based on heterogeneous fusion mechanism. IEEE Access. 8, 17663-17672.