ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8

International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

A Blockchain Architecture for Cloud Gateway Environment and IoT

Hanaa Mohammad Saied[1,2*], Mona Gaber A. Abdel Hafez[3,4]

[1]*Department of Business Management/ Information system, College of Science and Humanities in Al-Ghat, Majmaah University, SAUDI ARABIA.*

[2] *Faculty of Computing Science & IT, Cairo, Egypt, Ahram Canadian University Cairo, EGYPT.*

[3] *Department of English, College of Science and Hummanites Majmaah University, Al-Majmaah 11952, SAUDI ARABIA*

[4] *Al Azhar university,Faculty of Islamic and Arabic Studies , Sohag, EGYPT.*

**Corresponding Author (Email hanaa.e@mu.edu.sa hanaamoh@hotmail.com, m.abdelhafez@mu.edu.sa),*

Paper ID: 12A12P

Volume 12 Issue 12

Received 08 July 2021
Received in revised form 7 September 2021
Accepted 15 September 2021
Available online 24 September 2021

Keywords:
Blockchain Architecture; Cloud gateway; Internet of Things (IoT); Information and communication technology (ICT); Network; Blockchain-based cloud-enabled architecture; Blockchain development stack; Cloud security; Device layer; Gateway layer; Cloud layer; Data management; DDoS.

Abstract

The main aim of this paper is to provide a theoretically and empirically grounded discussion on big data and to propose a conceptual framework for big data based on a temporal dimension. This study adopts two research methods. The first research method is a critical assessment of the literature that aims to identify the concept of big data in a cloud gateway. This method is composed of a search for source materials, the selection of the source materials, and their analysis and synthesis. It has been used to develop a conceptual framework for assessing a cloud gateway's readiness to adopt big data. The purpose of the second research method is to provide an initial verification of the developed framework. We built the suggested network using Ethereum blockchain technology and tested it against industry standards for security, Such as precision and security response time. The results show that the proposed security solutions achieve better results than the current solutions, and this architecture provides the following solutions to reduce the authentication, integrity, and confidentiality issues of the heterogeneous IoT and the central gates that make up the cloud gate. The results of our analysis show that, within appropriate E-business paradigms, BC technology can play an efficient role in facilitating active tasks for all activities over the architecture of IoT in many domains. We also experiment with our design and make a comprehensive discussion

Disciplinary: Information Technology & Computer Systems.

Cite This Article:

Saied, H. M., Hafez, M. G. A. (2021). A Blockchain Architecture for Cloud Gateway Environment and IoT. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 12*(12), 12A12P, 1-10. http://TUENGR.COM/V12/12A12P.pdf DOI: 10.14456/ITJEMAST.2021.247

1 Introduction

There is no doubt that the Internet of Things (IoT) is making extensive use of big data to achieve effective resource management and pervasive sensing, as a result of advances in information and communication technology (ICT) and expansion of sensor technologies. Various IoT devices are connected to big data, and these relationships are based on gates. The importance of gates in big data is undeniable; however, their centralized structure exposes them to a variety of security risks, including availability, integrity, and security. The problem of developing a framework for evaluating cloud gateway readiness to adopt big data based on the time dimension has received insufficient attention. the research is fragmented and dispersed. In this regard, there is a lack of a comprehensive framework as well as examples on how to build and use such a framework in a cloud gateway. Furthermore, [21] present primarily technical frameworks. No maturity approach covers both big data usage and its implications for cloud gateway long-term development. Existing maturity models, such as sustainability maturity models and stakeholder relationship maturity models, on the other hand, do not adequately handle advanced analytics challenges. As a result, a comprehensive maturity framework that integrates these two viewpoints is required.

2 Related work

Blockchain technology has recently been implemented in a variety of areas, including finance, distribution, health care, and energy. At the 2016 World Economic Forum, blockchain was named as one of the key strategies that will lead the era of the Fourth Industrial Revolution. Blockchain was also named one of the technology trends of 2017 by global market research agencies Gartner and Deloitte [11]. the distributed ledger blockchain technology is well known. It can overcome the limitations of indirect and indirect trust guarantees of typical centralized systems by implementing a decentralized system. Lee et al. [9] provides users with a direct and active trust connection. The integrity of the block ensures data integrity [12], and the blockchain can simply be deployed and integrated with a variety of sectors. A blockchain is a digital ledger that records and shares transaction information among network participants [13]. Each member of the network receives a copy of the Ledger.

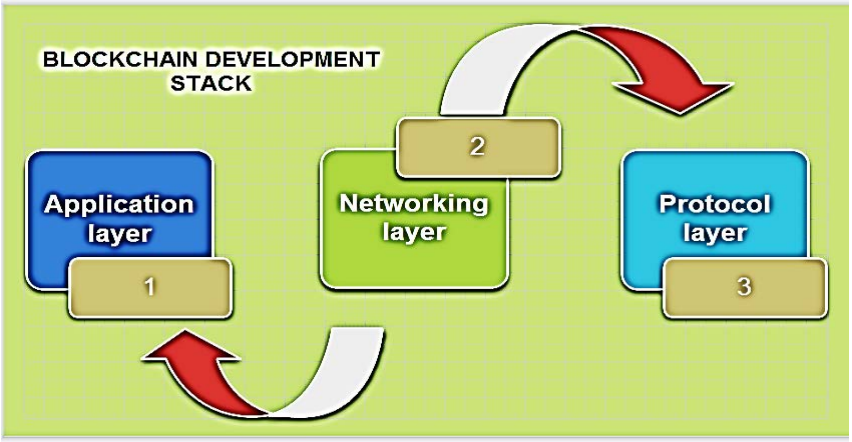

Figure 1: Blockchain development stack.

A new transaction is validated with the consent of all members when it occurs. The Blockchain contains many blocks, each of which includes transaction data. We find it impossible to modify individual data at random because many blocks are linked together to form a blockchain. The blocks match the data owned by the majority of users, with legitimate blocks representing more than 51% of all users. Since the ledger contains the hash value data, if the data of any block is modified or lost, it may simply be restored. It is almost impossible to make changes to the ledger based on a single transaction. Gateway to the cloud As interest in the domestic environment grows as a result of technology advancement, several cloud gateway technologies have sprouted. A residential or living environment outfitted with technologies that can automatically operate equipment and systems is referred to as a cloud gateway [16]. Managing these environments is complicated by several factors, including expenses, resident preferences, and the types of buildings available, all of which are dependent on technology. Residents can be provided with a variety of living settings via a network structure that can automatically modify temperature and security levels, as well as interact efficiently inside and outside cloud gateways [17].

The following ideas are supported by the gateway which is used to create these networks:

- A wide range of network connections for your home.
- Connections to your home network and the internet.
- Home appliance remote control and diagnostics
- Expansion and updating mechanisms that are flexible
- Remote operating approach that is both reliable and secure

In the absence of security standards for cloud gateways and devices, connecting various heterogeneous devices can be difficult. As a result, users will be unable to access a variety of services. The security criteria for gateways in cloud gateways are mentioned below.

- Confidentiality: Cloud gateway networks acquire and store a variety of data, including sensitive data from residents.
- Integrity: When data is transmitted and received among configurations, there must be no falsification during transmission. The hash function decreases the chances of these data being tampered with and enables the tracking and verification of exactly what data is captured.
- Authentication: In cloud gateway network settings, authentication stops an attacker from behaving maliciously inside a normal network from the outside. Blockchain is used to verify that a network member is legitimate, and it can be checked at a certain moment to enable the proper cloud gateway network setup [21].

Sivaraman et al. [22] investigated and assessed security issues in the cloud gateway network layer, and they recommended solutions. Even when connected to the internet, the ISP can be used to monitor and verify certified devices, as well as to control cloud gateway devices. This method, however, is inefficient in providing security to the internal internet environment due to a lack of data to evaluate from users. Composite al. [23] utilized Wireshark to check the flow of the house

and the lack of secret data for devices like fire alarms during the development of cloud gateway devices. Bullet al. [25] proposed a gateway for centralization.

Lee [9] discussed a large number of IoT-enabled gadgets. The suggested gateway is based on a centralized approach, which could lead to a single point of failure. Yin et al. [26] suggested a unique security approach based on human-centric computing by combining the privacy protection scheme with machine learning. However, if there isn't enough training data to create a machine learning model, this strategy is less effective. Panwar et al. [27] explored a variety of security threats as well as cloud gateway solutions.

They provide a complete review of cloud gateway security, including statistics on various assaults. Poh et al. [28] presented PrivHome, a privacy-preserving technique. For cloud gateway systems, it allows authentication, safe data storage, and query. To support data authentication and confidentiality, it learns and alters the data transferred between the user, gateway, service provider, and device. Sharan et al. [29] presented the impact of several security threats on cloud gateways and categorized them as low, moderate, or high to find appropriate mitigation methods. Other security measures rely on IoT and cyber-physical system security, in which various emergencies are addressed

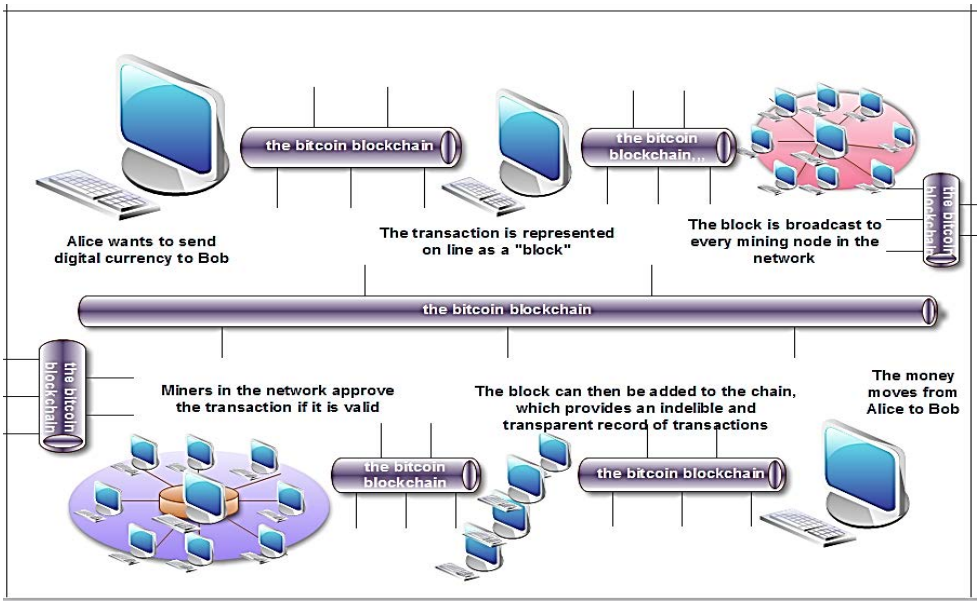

Figure 2: blockchain works.

Cloud gateway network based on blockchain Network configuration that has been proposed The use of blockchain in cloud gateway gateways is an important aspect of ensuring data transfer integrity and confidentiality between devices and other media. Although each Cloud gateway has a centralized network form, by employing blockchain at the cloud layer, it was transformed from a centralized to a distributed network. Figures 1 and 2 show how this can be expressed.

3 Proposed Model

The three layers of a cloud gateway based on the proposed blockchain are the device layer, gateway layer, and cloud layer. The device layer is made up of sensors and devices that gather and

monitor data in the cloud gateway network environment via multiple heterogeneous IoTs. After the Device Layer, the Gateway Layer stores the data created by the Device Layer and makes it available to users as needed. The cloud layer of the blockchain registers the gateway's ID as well as the data processed by each gateway.

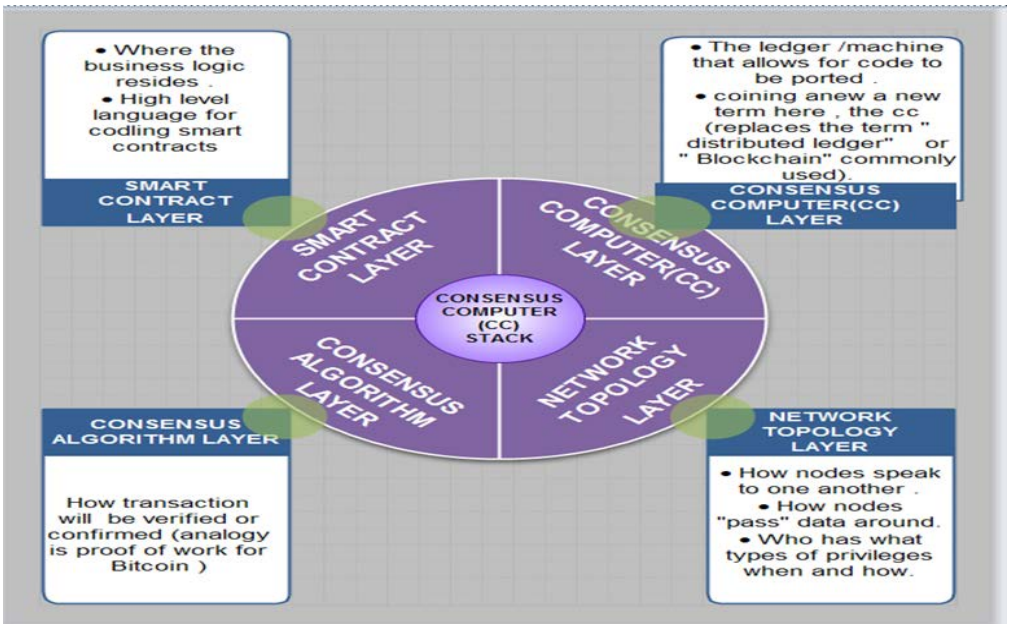

Figure 3: Blockchain application stack.

The blocks are shared so that users can get information at any time and from any location. Figure 3 depicts the blockchain application stack, which enables data from end devices to be collected, registered on the blockchain, and suitably presented to users.

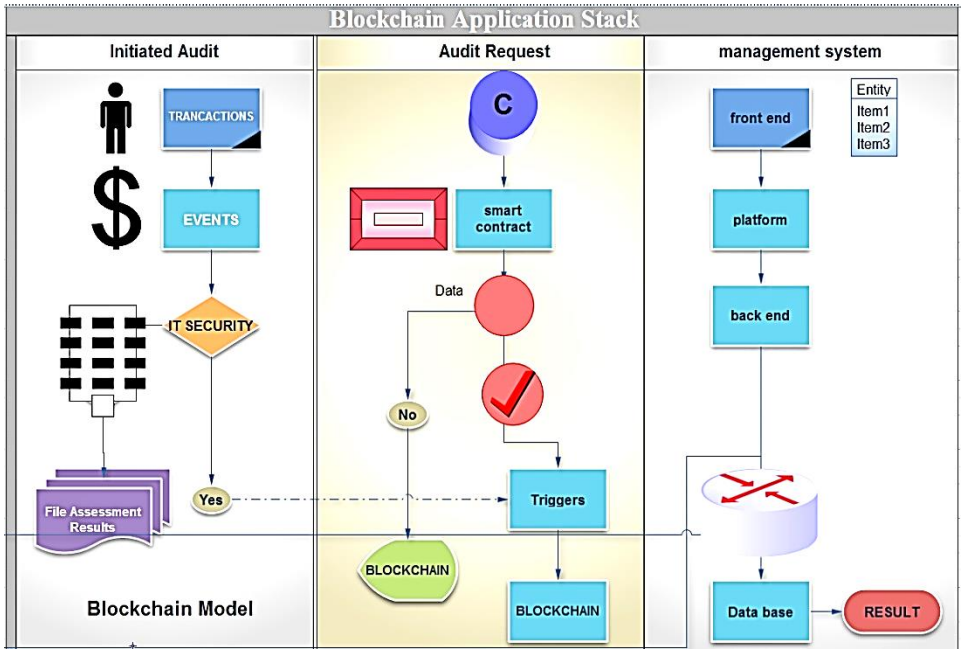

Figure 4: blockchain application stack

The acquired data undergoes hash value processing and formatting, builds blocks, and validates them periodically to ensure integrity even if data falsification happens for the data to be collected and supplied to the user. To offer consumers only the information they need, data analysis and quality maintenance should be done regularly as shown in Figure 4 . Identifying and

collecting data from gateway devices IoT devices configured in cloud gateways are connected to a single gateway, with an ID provided to each device. These gateways and devices have fixed IDs and the processing power to run PKI, encryption, and decoding methods.

1. Devices that are certified to a gateway must be checked regularly. The device layer tries to register with the gateway directly or connects to it automatically. The gateway either requests an ID from the connected device or seeks information about the connected device.
2. To encrypt the gateway information to the device and send the message, the device's gateway uses a cryptographic method. Encrypted messages are decoded by devices using pre-shared keys.
3. Gateway information is decrypted from encrypted messages. When they are received, they are requested to the unregistered or unencryptable gateway. Flow diagram of a blockchain-based cloud-enabled architecture for a cloud gateway.
4. We encrypt the device ID and SHA2 key to send messages to the gateway to share the SHA2 encryption method key for ongoing communication between devices and routers.

5-6. The gateway decodes the messages sent to ensure that they are registered as normal devices.

7. Once the gateway and device have successfully identified each other, we store the device ID registered on the gateway in the cloud. To keep the device ID list up to date, the gateway talks with the cloud over time.
8. The gateway creates a request message to gather data generated by the device.
9. The key of the SHA2 password algorithm that was validated in the previous procedure is used to encrypt data request messages.

10-11. When transmitting raw data, the device is prompted to provide a key to an encrypted message decoding and encryption gateway.

12. The gateway saves the incoming raw data by decoding gateway data management using a blockchain network made up of block chains that ensure the data transmission process and records are accurate. The SHA-3 hash algorithm based on information created can be used to save data generated from end nodes participating in the network or kept in the database.

These blocks are compared in real-time on a cloud-based blockchain network. They authenticate data by identifying if a blockchain is fabricated. The accompanying Fig. 4 depicts the blockchain registration and monitoring process for these gateway data. Inside the gateway, data is preprocessed. The data generated by heterogeneous IoT devices in the cloud gateway is sent to the cloud gateway in various sizes and formats. The suggested architecture's cloud gateway must accurately control IoT and process data in response to user requests. Figure 5 depicts the data transmission process from IoT to cloud gateway, with three kinds of data processing: collecting, preprocessing, and hashing.

• Stage 1: Data collection: The device sends data to the router for a set period. Data is requested from the device when new data is required at the gateway or when an event occurs. The raw data is then sent and saved in the gateway's storage device.

• Preprocessing: Inside the gateway, raw data transmitted from the device is preprocessed. It filters and stores only the data needed by the router based on device ID and is saved using the standardization and categorization procedure to save storage space.

• Stage 3: Hashing: Data created in the cloud gateway contains sensitive user information that can be handled by encryption. The hash function is used to store the device's common data, and the SHA256 method is used to apply it based on the user's password.

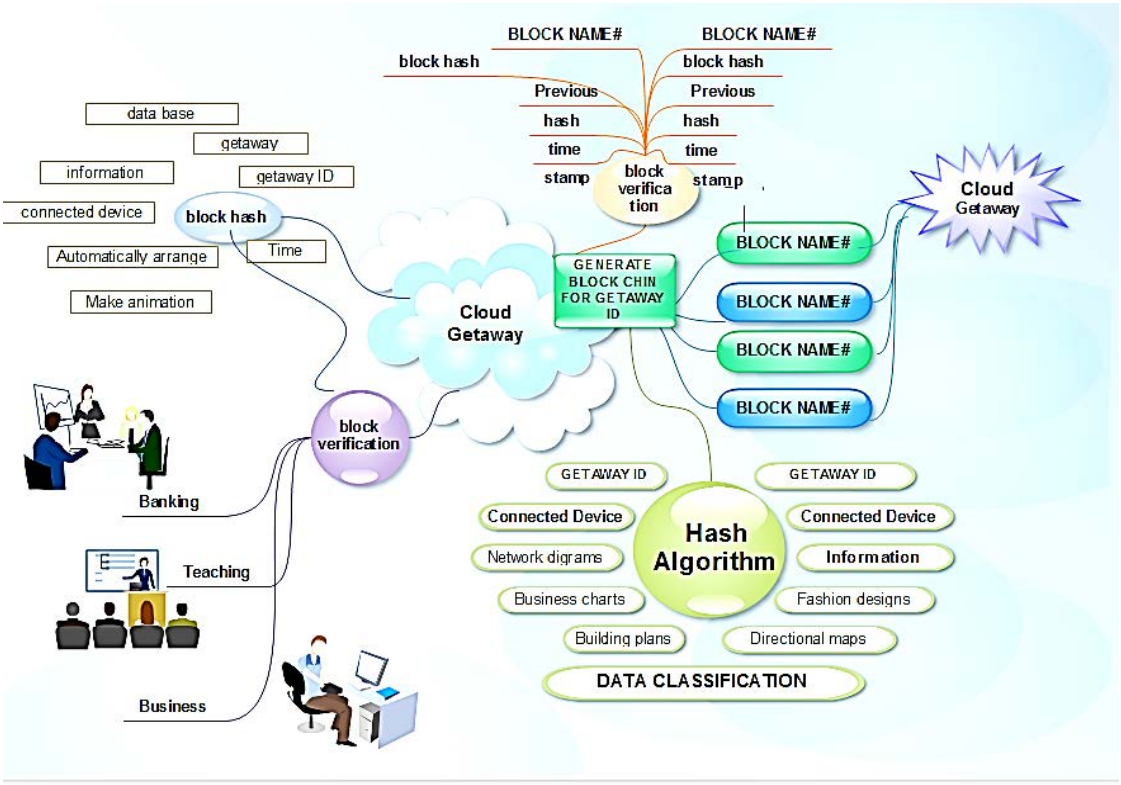

Figure 5: Blockchain-based gateway data management.

Information that is required has been created. These blocks are compared in real-time on a cloud-based blockchain network. They authenticate data by identifying if a blockchain is fabricated. The accompanying Figure 4 depicts the blockchain registration and monitoring process for these gateway data. Inside the gateway, data is preprocessed. The data created by the smart home's heterogeneous IoT devices is sent to the smart home gateway in various sizes and data formats. The suggested architecture's smart home gateway must accurately control IoT and process data following the proposed design. in response to the user's request Figure 5 depicts the data transfer process from IoT to the smart home gateway, which is divided into three categories: collection, processing, and storage.

4 Preprocessing and Hashing

• Stage 1: Data collection: The device sends data to the router for a set period. Data is requested from the device when new data is required at the gateway or when an event occurs. The raw data is then sent and saved in the gateway's storage device.

• Preprocessing (Stage 2): The gateway preprocesses the raw data sent from the device. It filters and stores only the data needed by the router based on device ID for storage efficiency, and it uses the standardization and categorization process to store it.

• Hashing (Stage 3): Data created in the smart home contains sensitive user information that must be handled by encryption. The hash function is used to save the Device's common data, and the SHA256 method is used to apply it based on the password given by the user.

Assaults 51% on the blockchain are hacking efforts to profit by changing transaction information after acquiring more than half of the hash nodes across the whole blockchain [38]. In other words, a 51 percent attack means a hostile attacker controls more than half of the network's hash computing power. So that other nodes can store falsified data, the attacker can produce new blocks and add them to the blockchain network faster than other honest nodes. Other blocks are forced to accept a blockchain that contains fabricated data as a result of the assault.

However, in the proposed blockchain-based architecture, the hash power of all nodes participating in the blockchain network must be larger than the sum of the hash computation power for the 51% attack to succeed. Furthermore, as the number of nodes participating in the design grows, the architecture becomes more effective in defending against attacks. As a result, the proposed blockchain-based architecture is immune to the blockchain 51% assault. DDoS (Distributed Denial of Service): A distributed denial of service (DDoS) attack causes a server's services to be disrupted by flooding it with traffic from infected devices [39,40].

Authentication and integrity services are disabled if an attack is detected on an existing centralized smart home gateway network. By avoiding using loops like If/While/for in simple IoT request scripts, the suggested design eliminates DDoS traffic during data processing. Using the blockchain's resource consumption restriction, the attacker will be unable to continue indefinitely. DDoS assaults on the entire blockchain network are also unachievable on all nodes at the same time. The environment in which the nodes are distributed determines this. Finally, to validate the significance of our research, we compared our proposed work to previous work in terms of security architecture, methodology, research gap, and recommended approach.

5 Conclusion

For the existing cloud gateway environment and IoT, we proposed a blockchain-based data tamper-proofing gateway architecture in this article. The following solutions are provided by this architecture to decrease the cloud gateway's heterogeneous IoT and centralized gateways' confidentiality, integrity, and authentication concerns. In cloud gateways and heterogeneous IoT, the SHA2 encryption technique is used to tackle secrecy and authentication issues. In addition, blockchain technology is employed to ensure that data kept in the gateway is secure. By efficiently molding raw data, the data transformation method is applied in the architecture. Three considerations and scenarios are offered to compare the proposed design to existing research, demonstrating the proposed architecture's effectiveness in comparison to past studies. However, because of the added processing complexity imposed by blockchain operations, our suggested

network design has some limitations in teams. The presented work can be improved by offloading the computation using the concept of mobile edge computing.

6 Availability of Data and Material

Data can be made available by contacting the corresponding author.

7 Acknowledgement

The authors extend their appreciation to the deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number (R-2021-291).

8 References

[1] Ahram T, Sargolzaei A, Sargolzaei S, Daniels J, Amaba B. Blockchain technology innovations. In: 2017 IEEEtechnology & engineering management conference (TEMSCON), 2017.

[2] Bull P, Austin R, Popov E, Sharma M, Watson R. Flow-based security for IoT devices using an SDN gateway. In: 2016 IEEE 4th international conference on the future internet of things and cloud (FiCloud). 2016.

[3] Chandramohan J, Nagarajan R, Satheeshkumar K, Ajithkumar N, Gopinath PA, Ranjithkumar S (2017) Intelligentcloud gateway automation and security system using Arduino and Wi-fi. Int J Eng Comput Sci. 6: 20694-20698.

[4] Chen M, Yang J, Zhu X, Wang X, Liu M, Song J. Cloud gateway 2.0: innovative cloud gateway system powered by botanical IoT and emotion detection. Mob Netw Appl. 2017; 22:1159-1169.

[5] Copos B, Levitt K, Bishop M, Rowe J. Is anybody home? Inferring activity from cloud gateway network traffic. In: 2016 IEEE security and privacy workshops (SPW), 2016.

[6] Gartner. Gartner: blockchain and connected home are almost at the peak of the hype cycle. 2016. https ://prwire.com.au/pr/62010/gardener-blockchain-and-connected-home-are-almost-at-the-peak-of-the-hype-cycle . Accessed Dec 2019.

[7] Gu K, Yang L, Yin B Location data record privacy protection based on differential privacy mechanism. InfTechnol Control. 2018; 47(4):639-654.

[8] He S, Zeng W, Xie K, Yang H, Lai M, Su X. PPNC: privacy Preserving Scheme for Random Linear Network Coding Smart Grid. KSII Transact Internet Inf Sys. 2017; 11(3):1-10.

[9] Lee B, Malik S, Wi S, Lee JH. Firmware verification of embedded devices based on a blockchain. In: international conference on heterogeneous networking for quality, reliability, security and robustness, 2016.

[10] Lin H, Bergmann N. IoT privacy and security challenges for cloud gateway environments. Information. 2016; 7:1-1.

[11] Mittal Y, Toshniwal P, Sharma S, Singhal D, Gupta R, Mittal VK. A voice-controlled multi-functional cloud gateway automation system. In: 2015 Annual IEEE India conference (INDICON), 2015.

[12] Panwar N, Sharma S, Mehrotra S, Krzywiecki L, Venkatasubramanian N. Cloud gateway survey on security andprivacy. 2019. arXiv preprint. arXiv:1904.05476.

[13] Park JH, Salim MM, Jo JH, Sicato JC, Rathore S, Park JH. CIoT-Net: a scalable cognitive IoT based smart city network architecture. Human-centric Computing and Information Sciences. 2019; 9(1):1-20.

[14] Poh GS, Gope P, Ning J. Privhome: privacy-preserving authenticated communication in cloud gateway environment. IEEE Trans Depend Secure Comput. 2019. DOI: 10.1109/TDSC.2019.29149 11.

[15] Pongle P, Chavan G (2015) A survey: attacks on RPL and 6LoWPAN in IoT. In: 2015 international conference on pervasive computing (ICPC), 2015.

[16] Rathore S, Pan Y, Park JH. BlockDeepNet: a Blockchain-based secure deep learning for IoT network. Sustainability. 2019; 11(14):3960-3974.

[17] Rathore S, Park JH. Semi-supervised learning based distributed attack detection framework for IoT. Appl SoftComput. 2018; 72:79-89.

[18] Robles RJ, Kim TH, Cook D, Das S. A review on security in cloud gateway development. Int J Adv Sci Technol. 2010; 15:13-22.

[19] Sanchez I, Satta R, Fovino IN, Baldini G, Steri G, Shaw D, Ciardulli A. Privacy leakages in cloud gateway wireless technologies. In: 2014 international Carnahan conference on security technology (ICCST), 2014.

[20] Schiefer M. Cloud gateway definition and security threats. In: 2015 ninth international conference on IT security incident management & IT forensics, 2015.

[21] Sharma PK, Moon SY, Park JH () Block-VN: a distributed blockchain-based vehicular network architecture in the smart city. JIPS. 2017;13:184-195.

[22] Sharma PK, Rathore S, Park JH. DistArch-SCNet: blockchain-based distributed architecture with li-fi communication for a scalable smart city network. IEEE Consum Electron Mag. 2018; 7(4):55-64.

[23] Shouran Z, Ashari A, Priyambodo T. Internet of things (IoT) of cloud gateway: privacy and security. Int J Comput Appl. 2019; 182:3-8.

[24] Singh S, Sharma PK, Park JH. SH-SecNet: an enhanced secure network architecture for the diagnosis of security threats in a cloud gateway Sustainability. 2017; 9:1-19.

[25] Sivaraman V, Gharakheili HH, Vishwanath A, Boreli R, Mehani O. Network-level security and privacy control for smart-home IoT devices. In: 2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob), 2015.

[26] Sun R, Xi J, Yin C, Wang J, Kim GJ. Location privacy protection research based on querying anonymous region construction for the smart campus. Mobile information systems. 2018.

[27] Wang J, Gao Y, Liu W, Sangaiah AK, Kim HJ. Energy-efficient routing algorithm with mobile sink support for wireless sensor networks. Sensors. 2019; 19(7):1468-1494.

[28] Xie K, Ning X, Wang X, He S, Ning Z, Liu X, Qin Z. An efficient privacy-preserving compressive data gathering scheme in WSNs. Inf Sci. 2017; 390:82-94.

[29] Xiong B, Yang K, Zhao J, Li K. Robust dynamic network traffic partitioning against malicious attacks. J Netw Comput Appl. 2017; 87:20-31.

[30] Yin C, Zhou B, Yin Z, Wang J. Local privacy protection classification based on human-centric computing.Human Comput Inf Sci. 2019; 9(1):33.

Hanaa Mohamed Said is an Assistance Professor at Department of Business Administration, College of Science and Humanities at Alghat, Majmaah University, Kingdom of Saudi Arabia; and Faculty of Computing Science IT, Cairo, Egypt, Ahram Canadian University 6 October, Cairo, Egypt University, Cairo, Egypt. She got a B.SC. in Communications Engineering, Faculty of Engineering, Helwan University. She got a Diploma of Computer Science from Ain Shams University with very good, a Master's degree of Science in Information Systems College of Computing & information Technology with Excellent Grade from Arab Academy for Science, Technology & Maritime Transport. She is a PHD student at Faculty of Computing & Information Science Information Systems Department, Ain Shames University. Her research interests include Software Engineering, E-Business, Stock Market Exchange, Surveillance Systems and Information Security.

Dr Mona Gaber A. Abdel Hafez is an assistance professor at Department of English, College of Science and Humanities at Al Ghat, Majmaah University, Kingdom of Saudi Arabia; and Faculty member at Al Azhar University, Faculty of Islamic and Arabic Studies, Sohag, Egypt. Dr. Hafez got her PHD in the Curricula and methods of teaching English from Minia University, Egypt. Her research interests are Teaching English for Specific Purposes e.g., Computer Science, Engineering, Business Administration, Islamic and Arabic Studies, Law, etc. She also is interested in Content and Language Integrated Learning (CLIL), where English is considered the Medium for Learning different topics such as Physics, Maths, Geography etc.