TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 20, No. 4, August 2022, pp. 772~779
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v20i4.23765

A security services for internet of thing smart health care solutions based blockchain technology

Ahmed Hashim Mohammed[1], Rawaa Mohammed Abdul Hussein[2]
[1]Department of Computer Science, College of Education, Mustansiriyah University, Baghdad, Iraq
[2]Computer Engineering Department, Faculty of Engineering, Mustansiriyah University, Baghdad, Iraq

Article Info

Article history:

Received Jul 13, 2021
Revised Apr 11, 2022
Accepted Apr 24, 2022

Keywords:

AES-CBC
Electronic health
Internet of thing blockchain
Security services

ABSTRACT

Pervasive and ubiquitous computing has enabled people better integrate physical things into the digital world. The internet of things (IoT) has been considerably more widely used in business and everyday life in the last decade. Innovative healthcare information and communication technologies are a vast field of research and applications that need IoT benefits, including speed, security, and low cost. The proposed modified advanced encryption standard (AES)-cipher block chaining (CBC)-based blockchain technology offers a shared key to devices that need to communicate directly with or with entities outside the smart healthcare network to give users greater control over transactions. The experiments are carried out using a Raspberry Pi 3, whereas two different sensors are employed in this case. Blockchain technology encrypts data between doctor and patient with varied user numbers. The results from experiments revealed that the proposed modified AES-CBC based blockchain technology could provide the IoT application with security services (confidentiality, integrity, and access control) with efficient execution time.

Corresponding Author:

Ahmed Hashim Mohammed
Department of Computer Science, College of Education, Mustansiriyah University
9C83+WC8, Baghdad, Iraq
Email: dr.ahmedh@uomustansiriyah.edu.iq

1. INTRODUCTION

The internet of things (IoT) is a new term that refers to how things, such as sensors, devices, radio-frequency identification (RFID) tags, and physical objects, are networked with the internet in real-time. The IoT can be used for many things, like healthcare, home automation, smart cities, agriculture, industry, and more [1]. According to current estimates, 50 billion such devices will be in use by 2025 [2]. The objects connected to the internet make it possible for the user to monitor and act quickly in the environment, no matter where they are in the world. Things could send information about a person or a place when they talk to each other from anywhere at any time. The development of new IoT technologies without considering security would put a lot of security threats in the IoT environment and the privacy of data at risk [3], [4].

Sensors and devices in the IoT communicate data like mobile phones and wireless networks. They are thus vulnerable to the same security dangers and assaults that need the three things confidentiality, integrity, and availability (CIA) [5]. Data security is regarded as one of the most significant challenges; it is necessary, particularly for activities and transactions reliant on data collection and manipulation. In reality, data encryption is essential before any data can be transmitted across a network connection [6].

Cryptographic systems are well-known for their effectiveness in ensuring the confidentiality, secrecy, and validity of data. The communications between IoT devices should be encrypted in order to protect their security, but unfortunately, developing solutions based on traditional encryption methods is a difficult task because of the restricted resources available to the IoT devices component including, battery-powered, limited processing and storage capacity. on the other hand, conventional cryptographic methods are sophisticated and need a lot of processing power, making them unsuitable for IoT devices [7]. As a result, they need a security solution that costs a lot less than other devices for IoT environments with limited resources. The current research demonstrated that the IoT has resulted in the emergence of new security threats and that sensors and devices utilized in the IoT network may be targeted by malware and subjected to various attacks [8].

The necessity for the right cryptographic solution is growing in an IoT world. However, the usage of cryptography on edge devices is constrained by their short battery lives, low power computing, little memory, insufficient power supply, and small size [9]. These low-powered edge devices may not handle standard cryptographic primitives. An RFID tag, for example, cannot use a 1204-bit Rivest, Shamir, and Adleman (RSA) method since it does not have the resources. Today smart industries now require cryptographic solutions for ubiquitous computing and only the most resource-constrained edge devices [10]. Alshammari *et al.* [11] have suggested a method that relied heavily on the advanced encryption standard (AES) and a novel chaotic substitution box (S-box) because AES has been widely employed in embedded systems since the IEEE 802.15.4 standard adopted it. Sruthi and Rajasekaran [12] proposed performing both signature and encryption in the same round. They encrypted the data using AES-cipher block chaining (CBC), a lightweight block cipher, and the session key with the elliptic curve cryptography (ECC) method. Xie and Chen [13] has developed a better way to do IoT decentralized data aggregation (DDA) by using secret sharing to make smart contracts more efficient and run the computers. Full-fledged systems also allow data sharing, such as allowing a leader to look at other people's devices' data. This is done using local differential privacy and cryptographic primitives like token-based encryption. Ayachi *et al.* [14] have proposed a method to encrypt data on a network-on-chip (NoC) based on the light encryption device (LED) algorithm to cut down on the amount of space it takes up and achieve high speed and low power consumption at the same time. Ali *et al.* [15] have suggested a light privacy-conscious IoT-based metering that delivers message integrity and confidentiality to an industrial environment that ensures the privacy of smart gadgets and customers. The original power usage data is encrypted and disseminated safely, so only the smart meter can reconstruct the original value. The suggested approach does not need extra demanding encryption and decryption operations.

Lee and Sim [16] have changed the secret key and initialization vector (IV) of the AES-CBC algorithm every few times that, makes it more secure. Also, they simplified directed acyclic graph (DAG) by sending overlap packets to three blocks at a time. Guan *et al.* [17] have come up with a new ciphertext policy attribute-based encryption (CP-ABE) scheme that keeps the length of the ciphertext the same and does not have much extra work in the encryption and decryption stages. It has also been proven that their scheme is adaptable to be safe under the standard model.

Karbasi and Shahpasand [18] suggested a lightweight security mechanism based on cryptographic ratchets to safeguard IoT items and sensors. Khan *et al.* [19] suggested a novel blockchain model with resource-constrained IoT sensor nodes. A lightweight authenticated encryption (AE) technique is AES-CBC ed for proof-of-authentication. Sensor nodes produce tags based on sensor data and broadcast them to the network. After the cluster head node, the block is hashed and uploaded to the blockchain. Sun *et al.* [20] suggested employing neural cryptosystems and latent binary space for IoT device authentication, encryption, and key distribution. The neural cryptosystems used symmetric, public-key, and no-key encryption techniques.

Sowjanya *et al.* [21] used ECC to make a simple key management system for the CP-ABE scheme. The unique thing about this scheme is that even though the semi-trusted authority (an honest person who wants to know the secret information) makes a secret key, it cannot decrypt a message with these keys unless it also has the private key of the receiver. Dwivedi [22] proposed encrypting data that uses dynamism and two separate cipher parts. The number of rounds that can be played in a session may also change from session to session. Only one type of encryption is used at a time, and the attacker does not know which type of encryption is being used in this case.

Shi *et al.* [23] suggests that access control authorization of data from devices is redefined and that the data be stored on the blockchain. They develop procedures for authorization, permission revocation, access control, and auditing the authorization and access control. They use a lightweight symmetric encryption technique (SEA) to ensure that the privacy of the IoT system is not compromised. Sleem and Couturier [24] have suggested Speck-R, ultra-lightweight Speck-based encryption. It is a hybrid cipher that combines addition/rotation/XOR (ARX) with a layer of dynamic substitution. They proposed the addition of a key-dynamic replacement layer that changes in response to the presence of a dynamic key.

Ragab *et al.* [25] increased the security of the original corrected block tiny encryption algorithm (CBTEA) block cipher by using an upgraded S-box. The modified TEA (M-TEA) also has a chaotic key generating technology, giving the one-time pad concept extra security. When encrypting plaintext, the cipher keys change for each block. It is, therefore, more secure than the TEA and AES algorithm. The M-TEA can boost data security with various text blocks and key sizes. Li *et al.* [26] used homomorphic encryption to keep people's data safe. They looked at how the data owners, untrustworthy third-party cloud servers, and the people who use the data all had to work together to keep their privacy safe. Meanwhile, efficient homomorphic algorithms are proposed to protect the privacy of the people who use the data.

2. INTERNET OF THING AND BLOCKCHAIN

The internet of objects is a network of things in the physical world that has arisen as a collection of technologies ranging from wireless sensor networks (WSN) to radio frequency identification [27]. Furthermore, to enable a wide variety of new services, the growth in IoT technology also poses issues in protecting the enormous amounts of data collected and preserving individual privacy. Access control may be used to guarantee that data is only accessible by those who have the appropriate permissions [28], [29]. The IoT has generated a tremendous quantity of data, including sensitive personal information about individuals. The IoT security must ensure that all portions of the system are secure, which is a difficult task for developers to overcome. It is necessary to determine how and where the IoTs interaction will be the key to IoT data safety; researchers are combining blockchain with access control, which they believe can remove the need for a central middleman while still allowing real-time, trustful data flow [30]. Participants may uniquely identify each device by making digital replicas of real things on a blockchain-based network. At the same time, the data they supply is permanently saved and cannot be changed.

In 2008, an unknown individual or group by the name of for the first time, Satoshi Nakamoto, introduced blockchain technology, which serves as the foundation of the cryptocurrency Bitcoin, to the rest of the world [31]. Combining blockchain technology with IoTs platforms would result in a dependable solution. In the decentralized and trustless blockchain environment, distributed ledger technology is used to aid decentralized and distributed computing. Blockchain is a shared public database of all conducted digital activities that stores time-stamped transactions in the form of blocks. Each block header retains the previous block's hash. Because of this block structure, the records of blockchain are immutable. Even a minor alteration in a single transaction would result in a new hash, resulting in a mismatch between the hash of that transaction and the hash of the nearby block. Blockchain technology allows businesses that do not trust one another to exchange transactions and information without the involvement of a third party [32]. Blockchain technology is distinguished by characteristics such as decentralization, security, transparency, redundancy, and reputation, as well as traceability, all of which provide value to any industry that adopts blockchain technology [33].

There are three sorts of blockchains: public, private, and hybrid. Public blockchain means that anybody can join ad participate. Private blockchains are the most appropriate form of connecting with IoT and adding value since they are not available to the general public. Hybrid blockchains combine the best features of both private and public blockchains in one system [34]. The IoT would benefit significantly from blockchain technology, mainly when implemented smart contracts. It removes the need for central servers and enhances fault tolerance and scalability, and makes peer-to-peer messaging far quicker than it would be with the current centralized architecture. Smart contracts may be used to automatically update devices' firmware to cope with vulnerabilities and improve the overall security of the underlying IoT system, which is beneficial to both parties [35], [36]. When individuals trade money, property, shares, or anything else of value without the need for a third party to intervene, they are referred to as smart contracts. In the blockchain network, smart contracts are computer programs or written scripts that have unique addresses integrated into the network. The blockchain consensus mechanism, which enables the system to enforce the conditions of a contract, is responsible for ensuring that the contract is carried out as agreed [37].

3. PROPOSED ENCRYPTION ALGORITHM

The IoT is a potential future technology that will link billions of things. It is projected that increasing communication would result in data posing a security risk. Depending on how many critical factors must be considered to achieve full performance. These challenges, scalability and resource efficiency, impact other issues like security and energy efficiency. Healthcare systems based on IoT may regulate hospital equipment such as patient temperature, pulse rate, and pressure via a web interface or smartphone application. Numerous technologies, such as standalone lightweight IoT security and protocols for data transmission, are being developed to support this approach. A flowchart of the safe healthcare system can be shown in Figure 1 to provide the security services for IoT-based applications in healthcare devices.

The classical encryption techniques are computationally costly owing to their complexity and necessity for several encryption rounds. The encryption algorithm based blockchain is proposed to identify any changes in the content of transactions while they are being sent. Transactions are linked together as an immutable ledger in the local private blockchain, which is not accessible to the public. A miner is a device that manages the processing of incoming and outgoing transactions to and from a smart healthcare system. The miner might be integrated with the hospital internet gateway in some instances.

In contrast, it could be an independent device in others, such as a computer. Each device inside the hospital may request data from another device to provide certain services. In order to provide users with more control over transactions, the miners should create a shared key for devices that communicate with each other directly or with entities outside of smart healthcare. The miner receives the data and the request from the device to save data on the cloud storage service. After verifying that the device has been approved, the miner takes the most recent block number and hash from the local blockchain and transfers it to a storage device, together with the data, as shown in Figure 2.

Because data security is vital in IoT applications, it is important to consider which paradigm to use to exchange keys. In this research, the data is encrypted using a modified AES-CBC asymmetric encryption-based blockchain approach, as seen in Figure 3. The input plaintext (P1, P2, and Pn) has been encrypted using three blocks in this chain, namely BC0, BC1, and BC2, in the order of appearance with intial value. The result of the encryption method is a series of blocks of ciphertext (C1, C2, and Cn).

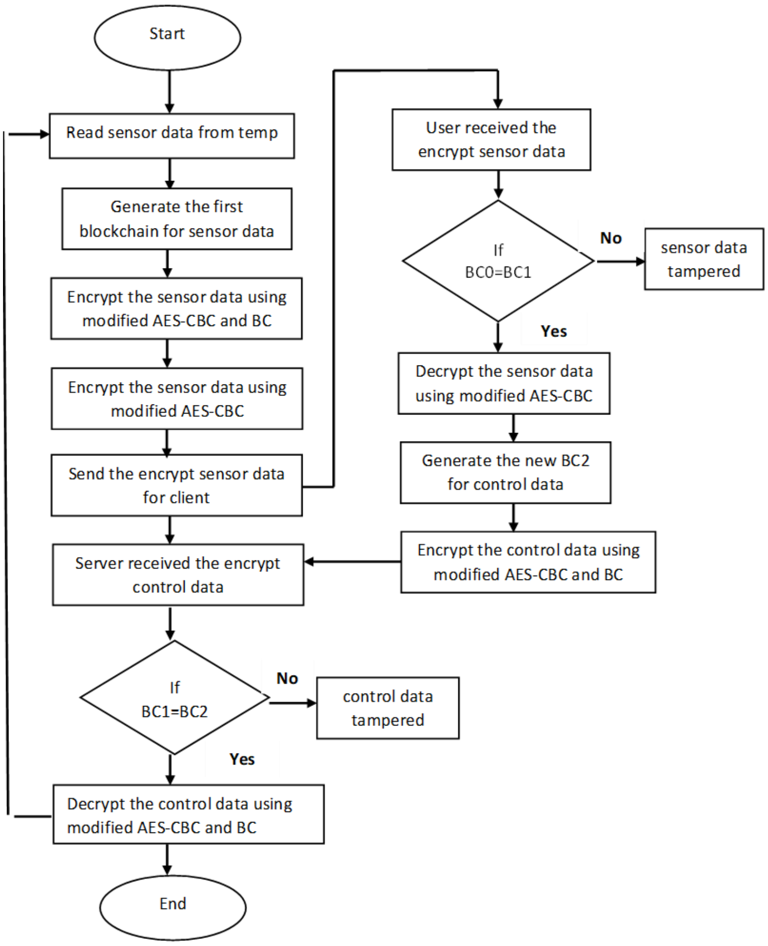
Start
Read sensor data from temp
Generate the first blockchain for sensor data
Encrypt the sensor data using modified AES-CBC and BC
Encrypt the sensor data using modified AES-CBC
Send the encrypt sensor data for client
Server received the encrypt control data
If BC1=BC2
No
control data tampered
Yes
Decrypt the control data using modified AES-CBC and BC
End
User received the encrypt sensor data
If BC0=BC1
No
sensor data tampered
Yes
Decrypt the sensor data using modified AES-CBC
Generate the new BC2 for control data
Encrypt the control data using modified AES-CBC and BC

Figure 1. Flowchart of the proposed algorithm

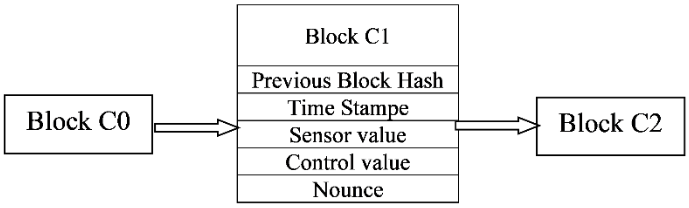

Figure 2. Blockchain structure

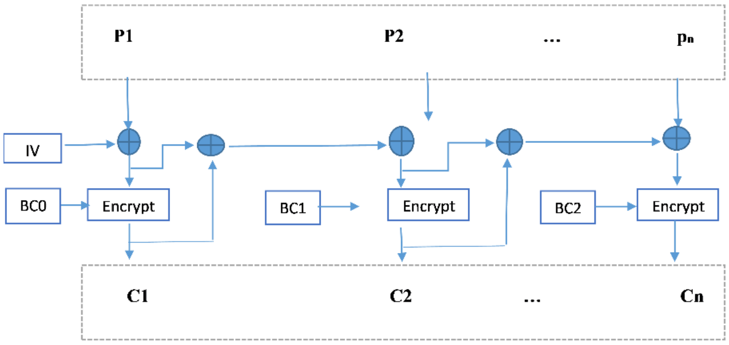

Figure 3. Modified AES-CBC algorithm based blockchain

This kind of encryption has the benefit of having a minimal execution time, which makes it suitable for use in high-speed related to smart tasks that need limited processing resources. Both the sender and the receiver know a standard secret key. The proposed encryption algorithm process can be summarized in the following steps.

```
Algorithm 1. Encryption algorithm
Input: Plaintext
Output: Ciphertext
Steps:
Step 1: Read data from the sensor
Step 2: Generate the first blockchain for sensor data
Step 3: Encrypt the sensor data using the first blockchain key
Step 4: XOR (state, IV)
Step 5: Add round key (state, BC0)
Step 6: XOR (state, IV)
Step 7: Send the encrypted sensor data to the client
Step 8: End
```

Decryption is the process of reversing the encryption process. It refers to the process of converting encrypted text into the plain text as shown below.

```
Algorithm 2. Decryption algorithm
Input: Ciphertext
Output: Plaintext
Steps:
Step 1: User received the encrypted sensor data
Step 2: If first blockchain = second blockchain then decrypt the sensor data using the first blockchain else
sensor data has tampered
Step 3: Generate the new blockchain for control data
Step 4: Encrypt the control data using new blockchain
Step 5: XOR (state, IV)
Step 6: Add round key (state, Ki)
Step 7: XOR (state, IV)
Step 8: Send the encrypted control data to the server
Step 9: End
```

4. RESULTS AND DISCUSSIONS

The experiments are carried out using a Raspberry Pi 3, whereas two different sensors are employed in this case. The first is a temperature sensor, while the second is a pulse sensor. The infrared sensor thermometer may be used for non-contact temperature detection. After installing the library, identify the general-purpose input/output (GPIO) data pins for taking a patient’s temperature every few seconds using node js and express environment. The second pulse amped is a heart-rate sensor compatible with Arduino and the Raspberry Pi. Its primary optical heart rate sensor, amplification, and noise reduction technology provides rapid and straightforward pulse readings.

Moreover, it uses less power, using just 4 mA at 5 V, making it particularly well suited for IoT applications. It is possible to use sensors to detect when a patient's finger is placed into a linked line connected to the Raspberry Pi 3. Confidentiality, integrity, and availability are the three essential security criteria that any IoT application security must handle. Confidentiality ensures that only the intended receiver of the communication has access to it. Integrity no tampering with the message should be allowed; availability ensures the service or data must be accessible to the user at all times.

Security services' confidentiality integrity and availability have been accomplished via modified AES-CBC symmetric encryption and blockchain technology. A shared key is created between the devices. The execution time of an algorithm in an IoT environment was an important metric to consider while assessing the method. This method must be fast and efficient while also delivering a high degree of security. An evaluation of the suggested encryption method (modified AES-CBC algorithm) in comparison to the AES-CBC algorithm is performed in this system. We compute the time it takes to encrypt and decode particular data received from the sensors. Table 1 illustrates the system execution time in milliseconds for both the AES-CBC without blockchain and modified AES-CBC with blockchain algorithms using 100 bytes file stored on the Raspberry Pi. The modified AES-CBC algorithm using blockchain was executed faster than the original AES-CBC method. Consequently, the suggested method is well-suited for the system under consideration.

The execution time of any algorithm used in the IoT environment was very important for the evaluation of that algorithm; therefore, another evaluation of the average encryption time of using the modified AES-CBC encryption algorithm based on blockchain technology is listed in Table 2 among different numbers of users (1–100). The modified AES-CBC algorithm based blockchain is implemented with key lengths of 128 bits and two separate data sensors, which are both used in the implementation. A calculation has been made to determine the amount of time required for the encryption and decryption of data received from sensors, as well as for each control instruction to modify the state of a device. Increasing the number of users connecting to the IoT healthcare solution has a direct impact on the length of time it takes the server to decode a set message size.

The randomness features of cryptographic algorithms may be evaluated using various statistical techniques. After running two algorithms for a certain amount of time on a text file, this article gathered 100 bits. National Institute of Standards and Technology (NIST) statistical testing indicated that the suggested method worked tremendously and passed all the statistical randomness tests, as shown in Table 3.

Table 1. Execution time

Algorithm	Average encryption time
AES-CBC	0.1841
Modified AES-CBC	0.0741

Table 2. The average execution times

No of users	AES-CBC	Modified AES-CBC
1	0.4934	0.3729
10	2.1922	1.9221
20	2.5941	2.1551
30	3.2131	2.5691
40	4.1931	3.4690
50	6.5540	4.3240
100	7.9021	5.8951

Table 3. NIST test

NIST tests	Modified AES-CBC
Frequency test	Pass
Frequency test within a block	Pass
Longest-run-of-ones in a block	Pass
Binary matrix rank test	Pass
Discrete fourier transform (spectral) test	Pass
Non-overlapping template matching test	Pass
Overlapping template matching test	Pass
Maurer's "Universal Statistical" test	Pass
Linear complexity test	Pass
Serial test	Pass
Approximate entropy test	Pass
Cumulative sums test	Pass
Random excursions test	Pass
Random excursions variant test	Pass

5. CONCLUSION

People have better integrated physical objects into the digital realm due to pervasive and ubiquitous computing. IoT has been extensively utilized in business and daily life in the previous decade. This trend is expected to continue. Using information and communication technologies in e-health is a massive field of study and applications that require the IoT to provide security and cost-effectiveness. This article described the development of an IoT system for remote patient monitoring at a hospital (using any computer or mobile device to control and switch on/off the devices). In order to give users greater control over transactions, the proposed modified AES-CBC based blockchain technology provides a shared key to devices that need to communicate directly with one another or with entities outside of the smart healthcare network. The test of the proposed system was carried out using a Raspberry Pi 3 computer, with two distinct types of sensors being used in this instance. Blockchain technology is being used to encrypt data between a doctor and a patient, with various users participating. The results demonstrated that the suggested modified AES-CBC-based blockchain technology might be used to deliver security services (confidentiality, integrity, and access control) to IoT applications while ensuring that the execution time is as short as possible.

REFERENCES

[1] F. G. Abdulkadhim, Z. Yi, C. Tang, M. Khalid, and S. A. Waheeb, “A Survey on the applications of IoT: an investigation into existing environments, present challenges and future opportunities,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 3, pp. 1447–1458, Jun. 2020, doi: 10.12928/telkomnika.v18i3.15604.

[2] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, “A privacy preserving communication protocol for IoT applications in smart homes,” *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844–1852, Dec. 2017, doi: 10.1109/JIOT.2017.2707489.

[3] F. Siddiqui, J. Beley, S. Zeadally, and G. Braught, “Secure and lightweight communication in heterogeneous IoT environments,” *Internet of Things*, vol. 14, p. 100093, Jun. 2021, doi: 10.1016/j.iot.2019.100093.

[4] A. H. Mohammed and A. M. Mahdi, “A security services of proposed social web of things,” *UPB Scientific Bulletin, Series C: Electrical Engineering and Computer Science*, vol. 83, no. 4, pp. 283–292, 2021. [Online]. Available: https://www.scientificbulletin.upb.ro/rev_docs_arhiva/rez64d_526806.pdf

[5] D. A. N. Gookyi, G. Kanda, and K. Ryoo, “NIST lightweight cryptography standardization process: classification of second round candidates, open challenges, and recommendations,” *Journal of Information Processing Systems*, vol. 17, no. 2, pp. 253–270, 2021, doi: 10.3745/JIPS.03.0156.

[6] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, “Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities,” *IEEE Access*, vol. 9, pp. 28177–28193, 2021, doi: 10.1109/ACCESS.2021.3052867.

[7] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, “Internet of things applications: A systematic review,” *Computer Networks*, vol. 148, pp. 241–261, Jan. 2019, doi: 10.1016/j.comnet.2018.12.008.

[8] R. M. Abdul-Hussein, R. S. Mohammed, and A. H. Mohammed, “Review: Security challenges and cyber-attacks for internet of things,” in *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*, Apr. 2021, pp. 81–85, doi: 10.1109/BICITS51482.2021.9509899.

[9] X. Luo *et al.*, “A lightweight privacy-preserving communication protocol for heterogeneous IoT environment,” *IEEE Access*, vol. 8, pp. 67192–67204, 2020, doi: 10.1109/ACCESS.2020.2978525.

[10] I. R. Chiadighikaobi and N. Katuk, “A scoping study on lightweight cryptography reviews in IoT,” *Baghdad Science Journal*, vol. 18, no. 2, pp. 989–1000, Jun. 2021, doi: 10.21123/bsj.2021.18.2(Suppl.).0989.

[11] B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, and A. Alzamil, “Implementing a symmetric lightweight cryptosystem in highly constrained iot devices by using a chaotic s-box,” *Symmetry*, vol. 13, no. 1, pp. 1–20, Jan. 2021, doi: 10.3390/sym13010129.

[12] M. Sruthi and R. Rajasekaran, “Hybrid lightweight signcryption scheme for IoT,” *Open Computer Science*, vol. 11, no. 1, pp. 391–398, 2021, doi: 10.1515/comp-2020-0105.

[13] X. Xie and Y. -C. Chen, “Decentralized data aggregation: a new secure framework based on lightweight cryptographic algorithms,” *Wireless Communications and Mobile Computing*, vol. 2021, no. 3, pp. 1–12, Apr. 2021, doi: 10.1155/2021/5565663.

[14] R. Ayachi, A. Mhaouch, and A. Ben Abdelali, “Lightweight cryptography for network-on-chip data encryption,” *Security and Communication Networks*, vol. 2021, pp. 1–10, May 2021, doi: 10.1155/2021/9943713.

[15] W. Ali, I. U. Din, A. Almogren, M. Guizani, and M. Zuair, “A lightweight privacy-aware IoT-based metering scheme for smart industrial ecosystems,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, pp. 6134–6143, Sep. 2021, doi: 10.1109/TII.2020.2984366.

[16] S. -W. Lee and K. -B. Sim, “Design and hardware implementation of a simplified dag-based blockchain and new aes-cbc algorithm for iot security,” *Electronics*, vol. 10, no. 9, p. 1127, May 2021, doi: 10.3390/electronics10091127.

[17] Z. Guan, W. Yang, L. Zhu, L. Wu, and R. Wang, “Achieving adaptively secure data access control with privacy protection for lightweight IoT devices,” *Science China Information Sciences*, vol. 64, no. 6, pp. 1–14, Jun. 2021, doi: 10.1007/s11432-020-2957-5.

[18] A. H. Karbasi and S. Shahpasand, “SINGLETON: A lightweight and secure end-to-end encryption protocol for the sensor networks in the Internet of Things based on cryptographic ratchets,” *The Journal of Supercomputing*, vol. 77, pp. 3516–3554, 2021, doi: 10.1007/s11227-020-03411-x.

[19] S. Khan, W. -K. Lee, and S. O. Hwang, “AEchain: A lightweight blockchain for IoT applications,” *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 64–76, Mar. 2022, doi: 10.1109/MCE.2021.3060373.

[20] Y. Sun, F. P.-W. Lo, and B. Lo, “Light-weight internet-of-things device authentication, encryption and key distribution using end-to-end neural cryptosystems,” *IEEE Internet of Things Journal*, vol. 14, no. 8, pp. 1–10, 2021, doi: 10.1109/JIOT.2021.3067036.

[21] K. Sowjanya, M. Dasgupta, and S. Ray, “A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IoT healthcare systems,” *Journal of Systems Architecture*, vol. 117, p. 102108, Aug. 2021, doi: 10.1016/j.sysarc.2021.102108.

[22] A. D. Dwivedi, “Brisk: Dynamic encryption-based cipher for long term security,” *Sensors*, vol. 21, no. 17, p. 5744, Aug. 2021,

doi: 10.3390/s21175744.

[23] N. Shi *et al.*, “BacS: A blockchain-based access control scheme in distributed internet of things,” *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2585–2599, Sep. 2021, doi: 10.1007/s12083-020-00930-5.

[24] L. Sleem and R. Couturier, “Speck-R: An ultra light-weight cryptographic scheme for internet of things,” *Multimedia Tools and Applications*, vol. 80, pp. 17067–17102, May 2021, doi: 10.1007/s11042-020-09625-8.

[25] A. A. M. Ragab, A. Madani, A. M. Wahdan, and G. M. I. Selim, “Design, analysis, and implementation of a new lightweight block cipher for protecting IoT smart devices,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, Jan. 2021, doi: 10.1007/s12652-020-02782-6.

[26] S. Li, S. Zhao, G. Min, L. Qi, and G. Liu, “Lightweight privacy-preserving scheme using homomorphic encryption in industrial internet of things,” *IEEE Internet of Things Journal*, 2021, doi: 10.1109/JIOT.2021.3066427.

[27] A. Aborujilah, M. N. M. Yatim, and A. Al-Othmani, “Blockchain-based adoption framework for authentic land registry system in Malaysia,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, no. 6, pp. 2038–2049, Dec. 2021, doi: 10.12928/telkomnika.v19i6.19276.

[28] W. Xiang and Z. Yuanyuan, “Scalable access control scheme of internet of things based on blockchain based on blockchain,” *Procedia Computer Science*, vol. 198, pp. 448–453, 2022, doi: 10.1016/j.procs.2021.12.268.

[29] J. Gong and N. J. Navimipour, “An in-depth and systematic literature review on the blockchain-based approaches for cloud computing,” *Cluster Computing*, vol. 25, pp. 383–400, 2022, doi: 10.1007/s10586-021-03412-2.

[30] S. Villamil, C. Hernández, and G. Tarazona, “An overview of internet of things,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 5, pp. 2320–2327, Oct. 2020, doi: 10.12928/telkomnika.v18i5.15911.

[31] M. M. Khubrani and S. Alam, “A detailed review of blockchain-based applications for protection against pandemic like COVID-19,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, no. 4, pp. 1185–1196, Aug. 2021, doi: 10.12928/telkomnika.v19i4.18465.

[32] K. M. Khan, J. Arshad, W. Iqbal, S. Abdullah, and H. Zaib, “Blockchain-enabled real-time SLA monitoring for cloud-hosted services,” *Cluster Computing*, vol. 25, no. 1, pp. 537–559, 2022, doi: 10.1007/s10586-021-03416-y.

[33] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities,” *Future Generation Computer Systems*, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/j.future.2018.05.046.

[34] S. Auer, S. Nagler, S. Mazumdar, and R. R. Mukkamala, “Towards blockchain-IoT based shared mobility: Car-sharing and leasing as a case study,” *Journal of Network and Computer Applications*, vol. 200, p. 103316, Apr. 2022, doi: 10.1016/j.jnca.2021.103316.

[35] A. A. Sadawi, M. S. Hassan, and M. Ndiaye, “A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges,” *IEEE Access*, vol. 9, pp. 54478–54497, 2021, doi: 10.1109/ACCESS.2021.3070555.

[36] J. J. Hunhevicz, M. Motie, and D. M. Hall, “Digital building twins and blockchain for performance-based (smart) contracts,” *Automation in Construction*, vol. 133, p. 103981, Jan. 2022, doi: 10.1016/j.autcon.2021.103981.

[37] B. Assiri and W. Z. Khan, “Fair and trustworthy: Lock-free enhanced tendermint blockchain algorithm,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 4, pp. 2224–2234, Aug. 2020, doi: 10.12928/telkomnika.v18i4.15701.

BIOGRAPHIES OF AUTHORS

Ahmed Hashim Mohammed received a Computer Science degree from Al-Rafidain University, Baghdad, Iraq, in 2003, and M.Sc. degree in computer science from Informatics Institute for Postgraduate Studies, Baghdad, Iraq, in 2006, and a PhD degree in computer science from the University of Technology, Baghdad, Iraq in 2015. He is Currently Assist Prof. lecturer at Al- Mustansiriyah University. His research interests include internet of things, cloud computing, cyber security, network security and cryptanalysis. He can be contacted at email: dr.ahmedh@uomustansiriyah.edu.iq.

Rawaa Mohammed Abdul Hussein works as a Lecturer in the computer engineering department -faculty of engineering / University of Mustansiriyah. From 2001-to 2005, she got a Bachelor’s degree in “computer and software engineering” from the university of Mustansiriyah. From 2006-to 2008, she received a Master’s degree in “information technology” from the University of Technology. Her research interests are cloud computing, software engineering, intelligent algorithm, logic design, and web application security. She can be contacted at email: mscrawaahm@uomustansiriyah.edu.iq.