A double-blockchain architecture for secure storage and transaction on the Internet of Things networks

Khalid Aldriwish

Department of Computer Science,
College of Science and Humanities of Al-Ghat,
Majmaah University,
Majmaah 11952, Saudi Arabia

Summary
The Internet of Things (IoT) applications are quickly spread in many fields. Blockchain methods (BC), defined as a distributed sharing mechanism, offer excellent support for IoT evolution. The BC provides a secure way for communication between IoT devices. However, the IoT environments are threatened by hacker attacks and malicious intrusions. The IoT applications security are faced with three challenges: intrusions and attacks detection, secure communication, and compressed storage information. This paper proposed a system based on double-blockchain to improve the communication transactions' safety and enhance the information compression method for the stored data. Information security is enhanced by using an Ellipse Curve Cryptography (ECC) considered in a double-blockchain case. The data compression is ensured by the Compressed Sensing (CS) method. The conducted experimentation reveals that the proposed method is more accurate in security and storage performance than previous related works.

Key words:
Internet of Things, Blockchain, Information security, Encryption

1. Introduction

The innovation of technologies and the growth of artificial intelligence algorithms are the main support for developing the Internet of Things environments. The IoT is merged in many fields as smartwatches, smart homes, health-based-IoT, and business-based-IoT [1]–[4]. According to statistics cited in [5], the number of connected IoT devices will be more than 24 billion by the end of 2030. This expectation reveals that the IoT applications achieved the goal of the most monitoring and remote-control systems. However, the massive number of the connected IoT devices imposes to take into account problems related to attacks and intrusions. Attacks could damage the functionality of IoT systems by retrieving data, modifying data read by the sensor, and even lock down the system. Furthermore, traditional attempts based on distributed databases provided to support IoT requests suffer from a lack of security [6]. Therefore, the necessity of a security strategy is required to ensure privacy and the proper functioning of IoT systems. Most existing systems are secured with a username and password when a data or transaction has occurred. However, this kind of security mechanism is insufficient and lets hackers attack IoT systems.

In 2016, Mirai malware-infected many IoT devices. The attack is considered a distributed denial of service (DDoS) attack [7], [8]. The Mirai malware attempted to remote IoT devices to be used as part of a botnet in large-scale network attacks. The Mirai attack succeeded when the virus accomplished access to the computer number control server, the IoT device, and the load server [9]. Upon the IoT device is stolen, the computer number control server will control it, and it will be managed for a coordinated attack. The load server could send the Mirai virus to the IoT device when the default factory username and password are not changed. This malware is invaded because most users of IoT systems have not changed the default authentication, or the username and password are not updated for a long time. This case is discussed to highlight the need for an accurate security mechanism to avoid dangerous attacks. Therefore, providing a security method other than username and password is requested.

Recent studies in information security proposed an architecture composed of four layers, as shown in figure 1: perception layer, transport layer, processing layer, and application layer. The perception layer comprises sensors, gateways, routing, and network technologies such as wireless, Bluetooth, ZigBee, and WiFi [10]. A lightweight security method is adopted for the perception layer because sensor nodes are limited resources and processing capacity. The network infrastructure as the Internet and mobile networks are belonging to the transport layer [11]. Therefore, the security method related to this layer is mainly tied to the security approach of the Internet. The processing layer aimed to ensure data processing through a cloud computing platform or a common processor. The security of the storage data is the primary purpose of this layer. Finally, the application layer security includes various methods like privacy protection and mobile security technology.

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.16

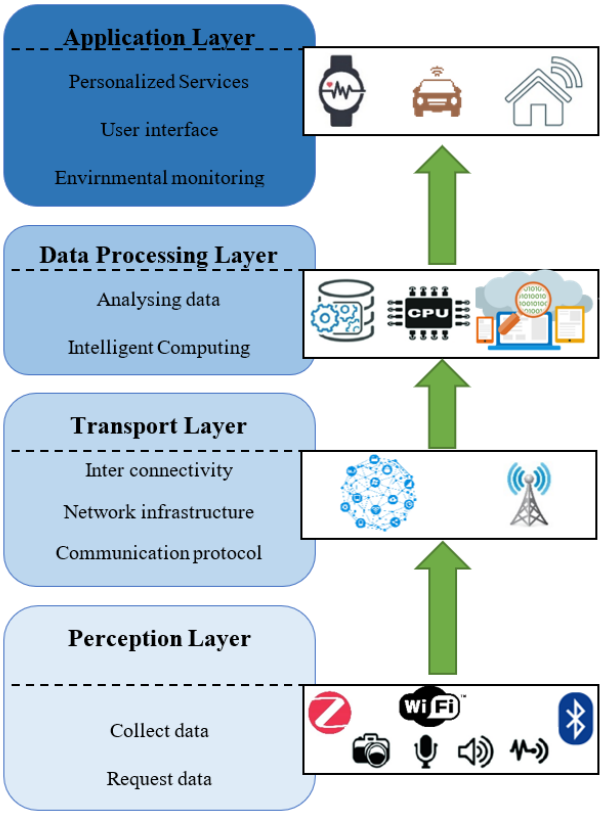

Fig. 1. Information security architecture

Aliyun company conducted a link security product based on Hardware and Software security services [12]. Its low cost characterizes it. A two-way authentication between server and device was the main idea of the Link security method. This security solution is widely implemented in smart house and bicycle applications.

Huawei company provided a protection solution at the Hardware level [13]. A Hardware security model is added to sensors chips and network gateways.

Blockchains [14], [15] are defined through a distributed mechanism. The BC is based on a computing paradigm for the asymmetric encryption algorithm. This approach is proposed for the security of electronic cash systems like Bitcoin. This concept aimed to ensure the safety of the transaction process with lower risks and costs. Unfortunately, few studies provide security architecture based on the blockchain approach.

This paper attempts to provide an accurate security architecture by combining the peer-to-peer model of the blockchain approach and an encryption mechanism of storage and communication. The proposed contributions could be summarized as follow: (1) Design a structure based on double-blockchain, (2) Propose a compressed sensing method for information compression and reconstruction, and (3) Perform the Ellipse Curve Cryptography algorithm to ensure asymmetric image encryption.

The rest of the paper is organized as follows: the related works are presented in section 2. The proposed security architecture is detailed in section 3. Then, the experimental results are described and discussed in section 4. Finally, the paper is concluded in section 5.

2. Related Works

This section outlines previous related works dealing with security models for IoT systems based on the BlockChain concept.

Zyskind et al., [16] introduced an Enigma computational model composed of multi-party computation. The proposed model used a modified distributed hashtable method for storage. An external blockchain ensures the security part, including controlling the network and managing access. The Enigma model provided by the authors was similar to the security model used for Bitcoin.

Zhang et al., [17] presented a new E-business platform based on the IoT environment. The authors designed the proposed E-business model according to traditional business model requirements. The blockchain and the smart contract are used to perform P2P transactions.

Bahga et al., [18] proposed an IoT model for the industrial system to support manufacturing services. The model is designed using a cloud-based manufacturing concept. The authors announced the BPIIoT platform according to peer-to-peer strategy and using blockchain technology. The interaction ensured in the BPIIoT platform is supported by the blockchain that did not request a trusted intermediary.

Christidis et al., [19] attempted to study the benefits of blockchain and IoT technology aggregation. The authors prove that blockchains supported a distributed peer-to-peer network for non-trusted users. Furthermore, blockchains provide an automated cryptographically with an easy method for sharing services and resources. The conducted experiments revealed that blockchain-IoT was a powerful, secure technology.

Islam et al., [20] introduced a healthcare system based-blockchain. The proposed model collected health data through Unmanned Aerial Vehicle (UAV) to enable low-power secure communication. Then, the UAV based on two-way authentication, decrypted the health data. After that, the data is stored securely in the blockchain. The authors conducted a deep discussion around the feasibility of the proposed model. Simulation results and implementation tests prove that the system achieved high performance and security.

Biswas et al., [21] designed a framework called GlobeChain based on the blockchain-IoT model. The framework aimed to manage vaccination data and other

medical services. In addition, the proposed attempted to overcome the problem of outbreak records presented in a traditional centralized framework.

Ren et al., [22] established a framework based on a double-blockchain-IoT solution called InterPlanetary File System (IPFS) designed for agricultural applications. The IPFS purposed to store securely sampled data into designed consortium blockchain blocks called Agricultural Sample Data Chain (ASDC). In malicious attacks, a public record is kept using a generated blockchain uploaded on the main chain of Ethereum. Experimentations proved that the proposed model requested a low cost-time than cloud storage and blockchain only.

Banotra et al., [23] summarized the use of the blockchain-IoT methods for business applications. Such platforms aimed to group enterprises to employ one secure and trust platform.

Harish et al., [24] introduced a platform based on the Internet of Things, blockchains, and a cyber-physical system called Log-Flock to support logistic companies. The proposed scheme helped digital asset generation, and the core is designed according to the tokens and smart contracts. However, the authors verified their model using a simulation model.

To sum up, related works need to improve the security level for transactions and storage, reduce the computation complexity, and speed up the encryption phase. Consequently, this paper represents an attempt to solve these issues by proposing an IoT platform using double-blockchain to provide a full service and secure transactions and storage.

3. The proposed system structure

In this section, we introduce the proposed system structure. First, a general concept of blockchains is presented. Then, the solution based on double-blockchain with Ellipse Curve Cryptography algorithm is detailed. Finally, the compressed sensing method for storage security is described.

3.1. General concept

The blockchain, defined as a state machine's replica protocol, provides a distributed or decentralized database system [25]. It is characterized by a higher safety and efficient consensus mechanism. No trusted third party is a significant feature of the consensus mechanism. Blockchain systems are typically composed of five layers: (1) application layer, (2) intelligent contract layer, (3) data layer, (4) consensus layer, and (5) network layer. The first layer, which is the higher layer, performs the basic accounting of blockchain systems. The second layer ensures the execution of code to operate input data. The third layer includes the data structure of the blockchain. Each computing node guarantees its own storage. The fourth layer deploys the adequate consensus protocol. The last layer uses the P2P protocol to safeguard the communication between nodes.

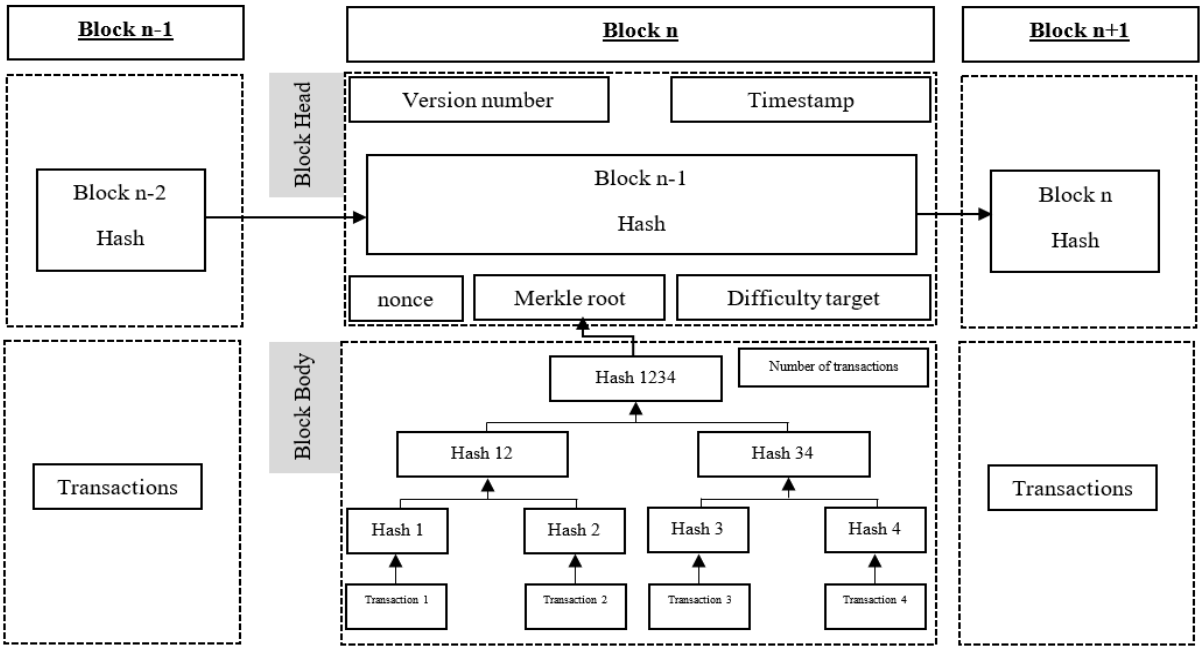

Fig. 2. Blockchain structure

The blockchain divides the data into sequential blocks. A block n is tied to the previous block (n-1) and followed by block (n+1). A block is composed of block head and block body, as shown in figure 2. Every block head includes the hash value of the previous block, and information like current version number, Merkle root, and timestamp. The block body contains the number of transactions and all transaction records.

Blockchains can implement many encryption algorithms as the RSA algorithm, signature algorithm, and the national secret algorithm. The transaction between nodes is performed through these five steps: (1) Perform an asymmetric encryption method using the public and private keys. This step ensures the non-repudiation and authority of blockchains. (2) Verify the validation of the received transaction. The only valid transaction is transmitted to the subsequent node. (3) Collect and package valid transactions on the nodes into a candidate block with a timestamp. (4) Add the block to the respective chain if the block includes a valid transaction, and the hash pointer corresponds to the previous block. (5) Execute the transaction and update the books.

3.2. System Structure

The system structure is composed of three network layers associated with the different phases of data processing, as shown in figure 3. The first layer is based on Ellipse Curve Cryptography (ECC) [26]. At this stage, sensors transmit the sampled data to be stored. As a data center, this layer needs to understand, process, and store the data. The ECC ensures information security via encryption. It is based on the public key cryptography algorithm and the elliptic curve discrete problem. This solution attempts to replace finite cycle groups by using finite point groups of elliptic curves. The ECC algorithm is characterized by less storage size, fewer computations, higher security, and lower bandwidth. The elliptic curve method is defined based on Weiestrass equation (1).

$$y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

Where a_i is associated with a number field as a real number, a complex number, a rational number, or a linear number. A unique number in the network defines each sensor. Once the sensor collects the real-time sampled data, it is refined and transmitted to the double blockchain system. The ECC network layer provides a level of security based on content-based retrieval. When the hash is verified, this process guarantees a communication without providing identity details. Stored data in the ECC network are accessible by content hash in the fetch step.

When the connected IoT device is considered as a physical node, the system would include thousands of nodes. Therefore, a large amount of heterogeneous data is generated by sensors, and the needed space storage by one day will achieve 1 TB. Cloud storage provides a structured data storage service, block storage service, and file-level storage service. In our case, the data transmission is guaranteed by the compressing sensing algorithm described in the next section.

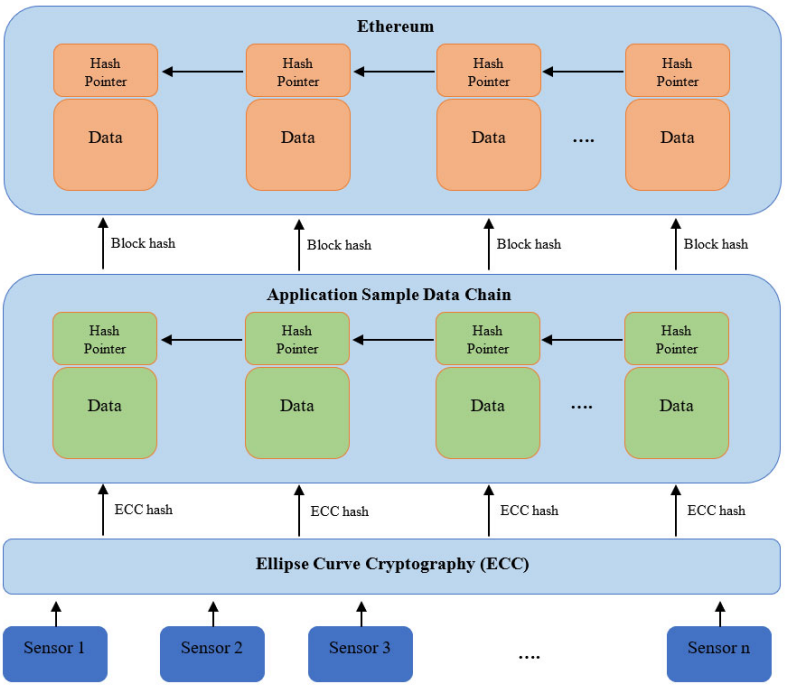

Fig. 3. System structure based on double-blockchain

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.16

Then, the hash values provided by the ECC method (ECC hash) will be uploaded to the second layer corresponding to the Application Sample Data Chain (ASDC). Blocks, in that level, store ECC hash values then each block is computed in the ASDC chain to obtain block hash values. Thus, the ECC hash is stored without data benefits from less storage required, fewer computations, and more safety.

In the end, the block hash is uploaded by the ASDC chain to Ethereum [27]. The third layer aims to ensure backup and public queries. It allocates a specific memory to keep object account and hash records publicly for tracking and searching activities.

The benefits of the proposed system structure based on double-blockchain approach can be summarized as follow: (1) The real-time Ethereum protects sampled data and two hash functions, (2) The traceability of the data it can be performed on Ethereum and ECC layer, (3) The sampling behaviors and data are protected from malicious risks and tampering.

Figure 4 describes the logical flow of the proposed double-blockchain. The sensor performs two actions: (1) uploads sampled data to ECC, (2) computes the hash function and transmits it to the ASDC layer. The data hash is stored in the account domain. Then, the ASDC system transmits the block hash to Ethereum to be saved.

A consensus algorithm called Proof of Works is used in the ASDC layer to provide data protection. Attacks are reduced due to the absence of the trading function in the proposed blockchain. Finally, the block hash is uploaded to the principal chain (Ethereum). The communication mechanism between two blockchains is supported by the Polkadot technique [28]. This technique permits to decrease system redundancy. The Polkadot technique uploads and saves the block height and the hash value into Ethereum once the hash value is authenticated. A feedback protocol containing the block address is sent to the smart contract. If the system detects a variation of the hash value, it proceeds to a block rejection method. Therefore, the used Polkadot method reduces malicious intrusions.

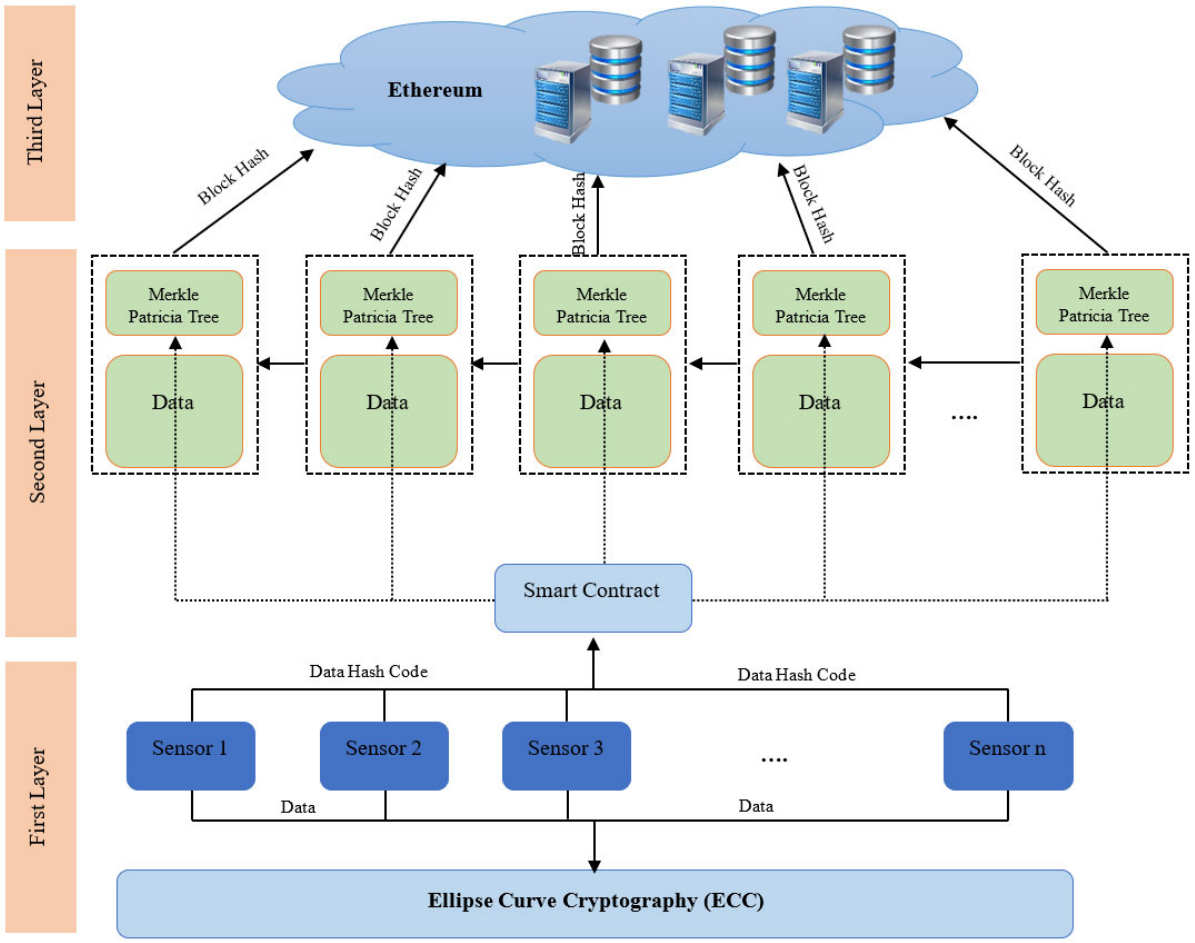

Fig. 4. Logical flow of the proposed double-blockchain

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.16

3.3. Compressed sensing

The proposed model uses the compressed sensing method to compress stored data [29]. In this section, a profound description of the method is presented.
The compressive sensing is characterized by an accurate recovering of the compressed signal with a high compression rate. Therefore, the algorithm has to be completed before storage.
Consider x as a non-sparse real signal. It is presented linearly on orthogonal bases; see equation 2.

$$\begin{cases} x = \sum_{i=1}^{N} s_i V_i \\ x \in R^N \\ s_i = V_i^T x \end{cases} \quad (2)$$

Where S_i is the sparse coefficient, the V is the domain.
Then $\delta_{M\times N}$ as an observation matrix is performed without any relation with the orthogonal basis matrix V. The achieved observation is defined in equation 3 by y.

$$\begin{cases} y = \delta V x = Cx \\ y \in R^M \end{cases} \quad (3)$$

Where C defines the sensing matrix.
The compressed sensing theory requests to reconstruct the signal because the current observation equation is inferior to the unknown quantity. This problem could be solved using an ill-conditioned inversion solution. The reconstruction signal can be minimally expressed by equation 4.

$$\begin{cases} \hat{x} = argmin\|x\| \\ y = \delta x \end{cases} \quad (4)$$

Equation 3 represents a non-convex combinatorial optimization problem. Therefore, it is considered a non-deterministic polynomial (NP) problem. Equation 3 is considered for the level 1 problem to minimize the vector's norm and solve the problem easily.

4. Experimentations

This section details the framework design and discusses the achieved verification results based on co-simulation approach [30]. The evaluation of the proposed model is implemented in the experimental environment shown in table 1. The experiment considers 200 storage nodes, each node allocates 2 TB in maximum, and the network speed, including data storage and the information channel, is set to 1Gigabits/s. The target storage needs 10 TB.

Table 1: Experimental environment

Characteristic	Feature
CPU model	Intel Core i7-8565U
CPU frequency	1.8 Ghz
Random Access Memory	16 GB
Operating system	Windows 10
Software tool	Matlab R2016a

The evaluation of the proposed system is conducted based on storage load balancing and storage capacity criteria.
To understand more the performance of the proposed storing method based on compressed sensing, a comparison with the traditional method as HDFS storage method and distributed storage is drawn in figure 5. The standard deviation curve of the HDFS storage method is the largest. It indicates that the HDFS method achieves the most insufficient load balancing performance. On the other hand, the standard deviation curve of the proposed compressed sensing method is the smoothest one. Therefore, drawn curves in figure 5 prove that the proposed reaches the best load balancing performance, and the rising trend is slower.

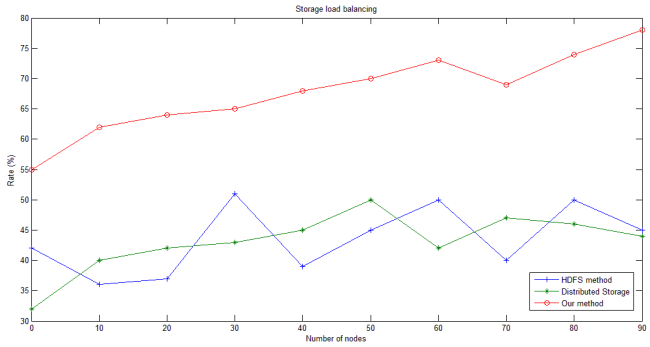

Fig. 5. Comparison results of Storage Load balancing

The storage capacity is computed to highlight the efficacity of our method. Figure 6 shows the required storage space in correspondence with the amount of data transmitted by the network. The three ways support a similar storage capacity when the amount of information inferior to 600. However, our proposed method achieves a high storage capacity than HDFS storage and distributed storage methods. Results drawn in figure 6 indicate that our approach has not lost information and supports storage for large-scale data.

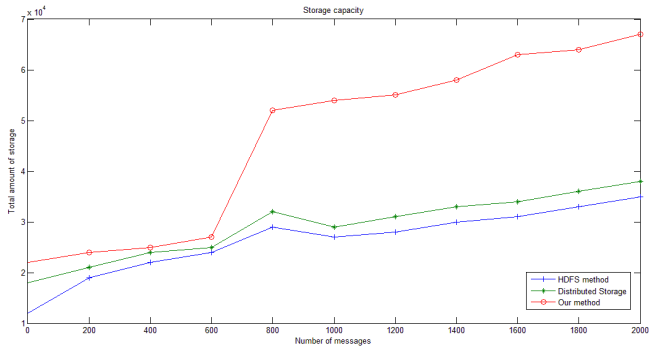

Fig. 6. Comparison of the storage capacity

To evaluate the performance of the used ECC algorithm, a comparison between the DSA encryption, the RSA

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.16

encryption algorithm is presented. The evaluation is based on security level and encryption speed. Three-level of security are considered in our experimentation: lower, medium, and higher.

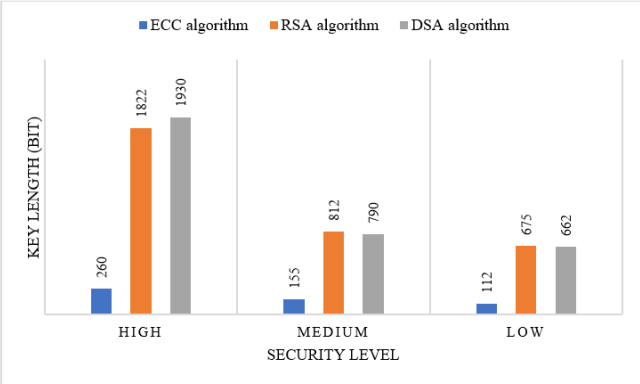

Fig. 7. Comparative security level depending on key length

Figure 7 presents the requested key length according to the security level. For the same level of security, the RSA algorithm and the DSA algorithm need a long key compared with the ECC algorithm. For example, the RSA and DSA algorithm request more than 1800 bit to guarantee a high level of security. Therefore, the ECC algorithm ensures a high level of security using only a little key length (about 300 bit).

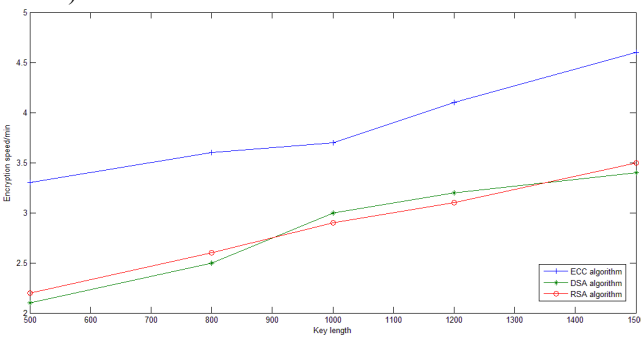

Fig. 8. Comparison results of speed encryption

The speed of encryption results is presented in figure 8. The encryption speed increases when the key length growing. In conclusion, the ECC encryption algorithm is the fastest method compared with the DSA algorithm and RSA algorithm.

The security data storage methods are verified using a typical operating system attack tool. Three kinds of attacks are considered in our case: (1) shared memory attack, (2) Virtual machine attack, and (3) DoS attack. Achieved results prove that the RSA algorithm and the DSA algorithm failed to prevent access. However, the ECC algorithm succeeded in blocking all kinds of attacks.

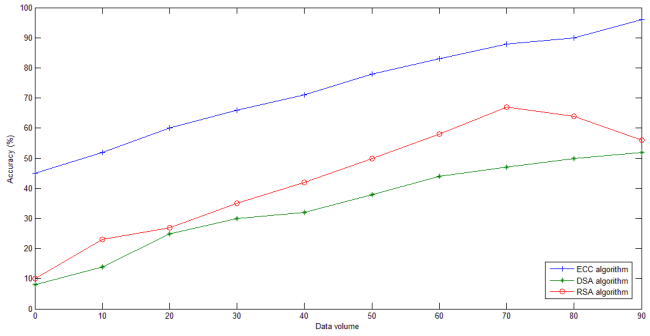

Fig. 9. Comparison results of the accuracy

Figure 9 shows the accuracy results to evaluate the effectiveness and the feasibility of the proposed encryption method based on the ECC algorithm. Achieved results indicate that the DSA algorithm reached an accuracy of about 52%. The RSA algorithm obtained an accuracy of about 56%, but the accuracy is reduced when the data volume increases. Figure 9 proved that the proposed encryption method based on the ECC algorithm reached the best accuracy with 96%. It can be concluded that using the ECC algorithm provides more security.

5. Conclusion

The growth of the Internet of Things applications worldwide and the increasing number of IoT devices connected to the network have become a great challenge. Unfortunately, traditional distributed systems suffer from the weaknesses of the security level caused by using a username and password methods. The present paper attempts to overcome the following shortcomings: low security, massive computation, and low-speed encryption. During this paper, a system based on a double-blockchain is used. The Ellipse Curve Cryptography algorithm ensures information security, and the data compression is performed by the Compressed Sensing method.
The experimental results prove the effectiveness of the proposed system in terms of storage load balancing, storage capacity, and the speed of encryption. Furthermore, the accuracy reached 96%, which is better than the RSA algorithm and the DSA algorithm.

Acknowledgments

The author would like to express thankful for Deanship of Scientific Research at Majmaah University for funding this project.

References

[1] I. Yaqoob et al., "Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges," IEEE Wirel. Commun., vol. 24, no. 3, pp. 10–16, 2017.

[2] P. P. Ray, "A survey on Internet of Things architectures," J. King Saud Univ. Inf. Sci., vol. 30, no. 3, pp. 291–319, 2018.

[3] S. K. Singh, S. Rathore, and J. H. Park, "Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," Futur. Gener. Comput. Syst., vol. 110, pp. 721–743, 2020.

[4] M. Ben Ayed, A. Massaoudi, and S. A. Alshaya, "Smart Recognition COVID-19 System to Predict Suspicious Persons Based on Face Features," J. Electr. Eng. Technol., pp. 1–6, 2021.

[5] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K.-K. R. Choo, "Consumer, commercial and industrial iot (in) security: attack taxonomy and case studies," IEEE Internet Things J., 2021.

[6] Z. Ellouze, N. Louati, M. Ben Ayed, S. A. Alshaya, and R. Bouaziz, "Design, Implementation, and Evaluation of a Real-Time Object-Oriented Database System," Int. J. Comput. Sci. Netw. Secur., vol. 19, no. 10, pp. 125–137, 2019.

[7] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer (Long. Beach. Calif)., vol. 50, no. 7, pp. 80–84, 2017.

[8] D. Arivudainambi, V. K. KA, and S. S. Chakkaravarthy, "LION IDS: A meta-heuristics approach to detect DDoS attacks against Software-Defined Networks," Neural Comput. Appl., vol. 31, no. 5, pp. 1491–1501, 2019.

[9] Š. Koprda, Z. Balogh, M. Magdin, J. Reichel, and G. Molnár, "The Possibility of Creating a Low-Cost Laser Engraver CNC Machine Prototype with Platform Arduino," Acta Polytech. Hungarica, vol. 17, no. 9, 2020.

[10] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," IEEE Commun. Mag., vol. 56, no. 9, pp. 162–169, 2018.

[11] Q. Jiang, X. Zhang, and J. You, "SnO2: a wonderful electron transport layer for perovskite solar cells," Small, vol. 14, no. 31, p. 1801154, 2018.

[12] B. Peng, "Research On Detection Of Malicious Software," in 2021 2nd International Conference on E-Commerce and Internet Technology (ECIT), 2021, pp. 400–403.

[13] M. Busch, J. Westphal, and T. Mueller, "Unearthing the TrustedCore: A Critical Review on Huawei's Trusted Execution Environment," in 14th $\{$USENIX$\}$ Workshop on Offensive Technologies ($\{$WOOT$\}$ 20), 2020.

[14] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," Inf. Process. \& Manag., vol. 58, no. 1, p. 102397, 2021.

[15] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," Expert Syst. Appl., vol. 168, p. 114384, 2021.

[16] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," arXiv Prepr. arXiv1506.03471, 2015.

[17] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in 2015 18th international conference on intelligence in next generation networks, 2015, pp. 184–191.

[18] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," J. Softw. Eng. Appl., vol. 9, no. 10, pp. 533–546, 2016.

[19] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," Ieee Access, vol. 4, pp. 2292–2303, 2016.

[20] A. Islam and S. Y. Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," Comput. \& Electr. Eng., vol. 84, p. 106627, 2020.

[21] S. Biswas, F. Li, Z. Latif, K. Sharif, A. K. Bairagi, and S. P. Mohanty, "GlobeChain: An Interoperable Blockchain for Global Sharing of Healthcare Data-A COVID-19 Perspective," IEEE Consum. Electron. Mag., 2021.

[22] W. Ren, X. Wan, and P. Gan, "A double-blockchain solution for agricultural sampled data security in Internet of Things network," Futur. Gener. Comput. Syst., vol. 117, pp. 453–461, 2021.

[23] A. Banotra, S. Gupta, S. K. Gupta, and M. Rashid, "Asset Security in Data of Internet of Things Using Blockchain Technology," in Multimedia Security, Springer, 2021, pp. 269–281.

[24] A. R. Harish, X. L. Liu, R. Y. Zhong, and G. Q. Huang, "Log-flock: A blockchain-enabled platform for digital asset valuation and risk assessment in E-commerce logistics financing," Comput. \& Ind. Eng., vol. 151, p. 107001, 2021.

[25] J. Kolb, M. AbdelBaky, R. H. Katz, and D. E. Culler, "Core concepts, challenges, and future directions in blockchain: a centralized tutorial," ACM Comput. Surv., vol. 53, no. 1, pp. 1–39, 2020.

[26] Y. El Housni, "Introduction to the Mathematical Foundations of Elliptic Curve Cryptography," 2018.

[27] N. Grech, M. Kong, A. Jurisevic, L. Brent, B. Scholz, and Y. Smaragdakis, "Madmax: Surviving out-of-gas conditions in ethereum smart contracts," Proc. ACM Program. Lang., vol. 2, no. OOPSLA, pp. 1–27, 2018.

[28] I. Scott, M. de Castro Neto, and F. L. Pinheiro, "Bringing trust and transparency to the opaque world of waste management with blockchain: a Polkadot parathread application," Available SSRN 3825072, 2021.

[29] A. Bora, A. Jalal, E. Price, and A. G. Dimakis, "Compressed sensing using generative models," in International Conference on Machine Learning, 2017, pp. 537–546.

[30] M. Ben Ayed, A. Massaoudi, S. A. Alshaya, and M. Abid, "System-level co-simulation for embedded systems," AIP Adv., vol. 10, no. 3, p. 35113, 2020.