Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.016950
Article

Tech Science Press

Internet of Things: Protection of Medical Data through Decentralized Ledgers

Abdalla Alameen[*]

Department of Computer Science, College of Arts and Sciences, Prince Sattam Bin Abdulaziz University, Wadi Ad Dawaser, Saudi Arabia
[*]Corresponding Author: Abdalla Alameen. Email: a.alameen@psau.edu.sa

Received: 16 January 2021; Accepted: 17 February 2021

Abstract: It is forecasted that billions of Internet of Things (IoT) and sensor devices will be installed worldwide by 2020. These devices can provide infrastructure-based services for various applications such as in smart hospitals, smart industry, smart grids, and smart industrial towns. Among them, the hospital service system needs to authenticate devices, and medical data are recorded for diagnostic purposes. In general, digital signatures are employed, but the computational power and their huge numbers pose many challenges to the digital signature system. To solve such problems, we developed a ledger system for authenticating IoT medical devices. It is a centralized ledger system architecture for particular authentication purposes only. It uses a very lightweight computational mechanism to authenticate IoT devices and helps secure medical data. We used two phases to analyze the proposed security system. First, we utilized a mathematical model to test its performance. In this phase, we proved that our proposed system cannot generate valid requests and responses for IoT devices without authentication. Second, we utilized a hyperledger to run our proposed system within our test environment to record various performance metrics, particularly the latency required for the security key operation, and message code updates. The analysis shows that our proposed system is secure and highly efficient when dealing with medical data through IoT devices using a centralized ledger system.

Keywords: Internet of things; security; authentication; medical data; blockchain

1 Introduction

Internet of Things (IoT) can be defined as an object that communicates with other objects with the help of the Internet [1]. IoT-based objects such as sensors, smartphones, and wearable devices are connected together for the purpose of delivering a message or involved in the processing of mission-critical data. Currently, there are billions of IoT devices serving socioeconomic factors in a manner that brings about satisfactory outcomes. IoT devices offer services efficiently, resulting in less time and cost when compared with traditional services [2]. However, there are several areas wherein improvements are expected from the research community [3], particularly security, because data should be protected by delivering messages or data between IoT devices, intermediator devices, or to the cloud server. There is considerable research on the use of blockchain [4], cryptographic methods [5], and security key-based solutions [6]. However, these solutions for IoT-based architectures are unable to serve owing to their features such as heterogeneity [7], connectivity, complexity, and dynamicity [8], which are compromised. Thus, providing a solution for application-based services is suitable [9]. Therefore, our proposal is to protect medical data during communication through decentralized ledgers.

Despite the plethora of resources [1–9], only a handful of these studies have achieved privacy concerns focused on personal data. From a privacy perspective, various research groups have built different techniques to protect personal data. One such technique is data anonymization [10] that protects personal data and information. K-anonymity, which is a property of anonymized datasets, involves sensitive knowledge of each data record indistinguishable from at least K-1 others record. Second, the cardinality of any query result on the released data should be at least K.

Another technique to maintain data privacy is L diversity [11]. Owing to its ability to handle a variety of data, it is most likely to be weak with skewness. If records are distributed through various IoT having different equivalence classes, then identity disclosure often leads to attributing disclosure. However, the aforementioned techniques prevent identity disclosures, but not attribute disclosures. However, to solve such problems, they require each equivalence class to have at least one value for each attribute, particularly the sensitive attribute. Furthermore, t-closeness needs sensitive attributes of any equivalence class that will have to be close to the distribution of sensitive attributes of the overall table. Other privacy-preserving schemes use encryption methods; they require computational power and mathematical queries over unprotected networks to protect and encrypt medical data. Recently, a new concept called Bitcoin [12] introduced an accountable system that permits end users to securely send currency in the form of Bitcoin without the presence of a centralized administrator, who verifies it using an open ledger.

An IoT network architecture and its security requirements are derived from the nature of the job it serves; in fact, security directly depends on the application and its environment. First, authentication is considered as a basic and crucial requirement of the application. If a single unprotected IoT device can be a gateway to malicious users, it can eventually cause a complete collapse of the application. Hence, the aforementioned privacy-preserving method cannot be utilized to secure IoT devices as these privacy-preserving algorithms require high processing power to produce crypto output to produce results to proceed to the next course of action with the aim of protecting data. Therefore, lightweight authentication schemes are built in the context of IoT device communication [13]. It is well known that IoT devices have limited energy and computation power. Therefore, the proposed decentralized IoT features enable the immutability of ledgers to secure IoT data. It is already proved that possession of the secret keys will not tamper with the IoT data. These features enable power and computational-constrained IoT devices to minimize the burden on them. In this article, we provide a security analysis of the cryptographic methods and present the implementation and configuration details.

2 Literature Review

IoT devices are widely used owing to the availability of hardware and computational power. However, their security is of immense concern with the aim of securing their data and IoT networks. Medical data are transmitted using IoT devices, but not widely implemented; by using cryptographic methods, privacy can be preserved [14]. Several research papers on IoT are focused on security and privacy. We can conclude from this research contribution that the application of security with respect to IoT is completely different from the fact that IoT never uses conventional network security methods. The IoT network is built using the heterogeneity of the underlying IoT devices and protocols and considering the most dynamic features such as network scalability. There are several challenges that exist in IoT with respect to security. Challenges include heterogeneity, resources, privacy, large scale, and reliability. Many research papers reported [15–18] that IoT is under threat owing to the layers and their countermeasures. However, very few researchers have suggested and addressed key management, privacy, confidentiality, and communication schemes. They have suggested using cryptographic methods, software-defined technologies, and blockchain for solving the security issues of IoT communication. Network simulation has played a key role in the fast implementation and testing of IoT security. Many simulators have been used in this research area [19]. However, the rapid research in IoT has led to increased demand for security-based protocol evaluators. One such protocol evaluator is the automated validation of Internet security protocols and applications. To preserve the privacy and confidentiality of data, IoT can only be had by applying security. These security patches are applied according to the threat vector. A more recent survey paper concluded that the authentication method is widely used. However, it is observed that lightweight and low-cost cryptographic methods are also deployed without any problems, knowing that IoT devices run under low computational power and battery issues.

Authentication is usually used to identify a user and IoT devices in a specified network and grants access to the secured area of devices to data. However, it can also initiate attacks on IoT devices, such as reply attacks, man-in-the-middle attacks, Sybil attacks, and impersonation attacks. Secured socket layer and transport layer security are used to secure communication between IoT devices. For IoT devices, various combinations of a pre-shared key are available to perform authentication using RSA and DH public key and cryptographic methods. These schemes enable authentication between IoT devices provided they prove their legitimacy by means of pre-shared key protocols. Hence, the asymmetric key is being used in these schemes; it is the most suitable authentication method for IoT devices, particularly sensor networks.

Two-way communication is possible in an IoT environment with respect to users and devices. The devices usually send and receive data to the server in a mutually agreed authentication system to check the validity of both the device and the user. Mutual authentication uses lightweight and encryption methods that have very recently been used to secure security between users and devices [20–24]. In these studies, authors have proved that to secure communication between IoT devices, lightweight authentication can play a vital role in access control. To attain an effective end-to-end communication with IoT device constraints, light encryption on the network layer is the only solution.

However, the encryption of IoT architecture is still in the early stages and does not prevent malicious attacks. Most devices have a hardcoded authentication system that can easily bypass the authentication system. Therefore, most recent papers focus on improving the security system of devices and keeping the privacy of the data.

3 Proposed Method

We used permissioned ledgers because they remove the unnecessary CPU intense calculation required to reach consensus on the network and improve the overall performance. However, they have their own predefined computer nodes for validating medical data transactions. In other words, nodes contributing to ledger/bookkeeping know each node's messages by verifying digital data along with security parameters such as a public key. Second, permissioned ledgers have proper governance procedures. This approach enables administrators to consume very little time to run queries with respect to the rules over the network. Unlike a public ledger that has the requirement of consensus once the new update implementation arrives, in our approach, we have three entities, as shown in Fig. 1. End-user systems are usually IoT devices, ledgers, and cloud edge servers. IoT devices are placed at the medical departments or any medical device that can be an IoT-enabled device, and clients are prepared with public and private keys. Their public keys are certified by the Certificate Authority (CA). These approaches are available in the form of hardware and software technologies. These security services are possible because of the transport layer security, which is developed after a secure socket layer protocol along with a certificate issued by the X.509 authority. Hence, the predefined protocol helps secure medical data and patients' personal information. The collection of IoT devices is scheduled to work together to manage the ledgers used in our framework, providing data authenticity protection apart from medical-related data transmission. It is proved that a single IoT device can be compromised. However, it is not possible for the adversary to control all nodes because the consensus technique guarantees that all decentralized ledger systems are completely trusted and retains the reservation of feature execution.

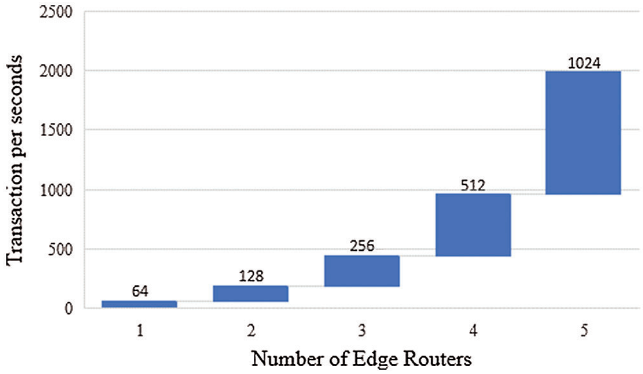

Figure 1: Performance of transaction submission of the proposed system

The data generated by IoT devices is considerable, and such huge data are computed through cloud and edge servers, which are very powerful devices. Hence, adversaries may alter data through IoT devices and might reach cloud and edge servers. Therefore, it is necessary for the framework to detect such attacks on data. The present IoT devices have the ability to interoperability, information transformation, and technical assistance, and decentralized decisions, but efficiency in computation, security, and IoT management are also important objectives for any IoT-based architecture. Hence, in the next section, we present these features.

3.1 Connection

There are numerous medical devices divided into different groups depending on the nature of service they render to hospitals and their various departments. These different groups of various IoTs are managed by the edge server, and they also manage edge ledgers, and these edge ledgers are handled by the cloud global servers. Each edge ledger is connected directly to the cloud server. Each of the hospitals hosting IoT medical devices are denoted by $\mathcal{H}_i$, and these hospital IoT devices are served by the edge ledger $\mathcal{L}_{ei}$, which is reliant on edge servers E_{is}. Each IoT device is in close proximity to the edge ledger. Each of these ledgers is connected to a server called a global ledger G_L. However, IoT devices are connected to each other, but $\mathcal{L}_{ei}$ are not connected to each other for reducing computational complexity []. In edge computing, some of the IoT devices within $\mathcal{H}_i$ may be unreliable and might not discover at any moment. This situation brings the complete system into disjoint parts; eventually, reliability is lost. However, IoT devices can overcome this condition by indulging in a technique for IoT device failure when new IoT nodes join $\mathcal{H}_i$ at the IoT node discovery phase. Therefore, by default, each IoT stores extra neighbor nodes that do not happen to be neighbors in tier in their close proximity, this setting maintains the connectivity in case the neighbor fails. Moreover, both edge and global ledgers are connected to each hospital, and $\mathcal{H}_i$ can also share node information.

3.2 Certification

Each hospital edge ledger detects a request from an IoT device within hospital proximity. The request carries information regarding its detailed device, signature by the device private key, and certificate chain containing the model certificate and owner or manufacturer certificate attached. In the decentralized architecture, the edge ledger has no connection with the device, and it does not carry root CA certificate. The edge ledger $\mathcal{L}_{ei}$ connects to the blockchain, looks for the IoT device model, and checks IoT device certificate, test device compliance, and interoperability. If the edge ledger $\mathcal{L}_{ei}$ obtains the certificate and policies are matched, then the connection request and a secured communication channel is opened for the device. Each IoT device $\mathcal{H}_i$ has its own certificate in our proposed decentralized ledger communication. In our approach, certificates of IoT devices are stored in an $\mathcal{H}_i$ edge ledger. The revocation of certificates is decided by the ledger. The revocation of the IoT device within the hospital is handled by the immediate edge, and the broadcast of the ledger node certificate for the whole system. On the contrary, when a device is unable to provide a certificate, it will be known to edge ledger via a global ledger. This will not be a revocation of certificate; however, it lowers the trust associated with the device.

3.3 Device Authentication

Device authentication is the fundamental step to secure IoT devices, and the security process starts from the verification of the IoT device to access control. Identity attacks have been spoofing devices to deny services. Hence, traditional security shields for IoT devices have been constantly challenged for their inefficiency in providing security. Therefore, communication between IoT devices and global devices is covered with highly sophisticated hardware protocols. In our proposal, we propose a two-step authentication method. In Step one, the $\mathcal{H}_i$ device stores its digital signature in the edge ledger; $\mathcal{L}_{ei}$ hence, nodes of the edge ledger $\mathcal{L}_{ei}$ can be verified for further processing. Second, the $\mathcal{H}_i$ device can change its place and a new edge can access its certificate from a global edge. The information exchange between them is the RSA-based accumulator. An accumulator collects a large set of input data into a small set of accumulators. Hence, computational efficiency is witnessed for the input data and accumulator [25]. The following steps are applied for device authentication as shown in the Tab. 1.

Table 1: Steps for device authentications

Steps	Process Description
Setup	When both edge ledger communicate for the accumulator value is considered as transaction. 1. Yield two prime numbers, p and q, perform N = pq. 2. Pick a value u from quadratic residue, QR and $u \neq 1$ A public parameter is (N, u)
Accumulation	Update the global ledge by performing following steps 1. For each transaction on public parameter, update global ledger via edge ledger 2. Output accumulator value by using public parameter (N, u) and prime numbers R = $r_1, r_2, r_3 \ldots\ r_n$ to generate accumulator $A = u^{r_1, r_2, r_3 \cdots\ r_n}\ mod\ N$. Edge ledger sends accumulator value to the global ledger. To reach the consensus on the accumulator value, a pair is created by device id and accumulator ($\mathcal{L}_{ei},\ A$) only when it succeeds.
Witness checking	Edge ledger checks the Accumulator value 1. Edge ledger receives latest accumulator from the global communicator ledger. 2. Receiver edge requires proof for the received accumulator value Proof is generated using public parameter $w = (N, u, R)$
Verify	To verify the received data, the following steps are concluded If $\boldsymbol{w^r} = \boldsymbol{A\ mod\ N}$; outputs 1 when it is successful, then only receives and stores the transaction data.

3.4 Device Data Authentication

Robust device authentication will satisfy IoT-intended communication and trusted they purported to be. Whenever IoT devices initiate communication with other devices through a ledger or global ledger, it must be authenticated. If they are unable to behave in a controlled manner, then IoT network administrators can revoke their privileges. This section comprise an introduction to the primitives of our proposed cryptosystem.

3.4.1 Bilinear Maps

By using bilinear maps, one can construct a pairing-based crypto system and establish a relation between cryptographic groups. Let *G1*, *G2*, and *GT* be the cyclic order of multiplicative group of order *p*. Let *g1* and *g2* be the generators of *G1* and *G2*, respectively. A bilinear map is defined as follows.

$$e : G_1 \times G_2 \longrightarrow G_T \tag{1}$$

Such that $\boldsymbol{u \in G_1, v \in G_2}$ and $\boldsymbol{a, b \in Z_p, e(u^a, v^b) = e(u,v)^{ab}}$ Hence it implies that $\boldsymbol{u_1}$ and $\boldsymbol{u_2} \in \boldsymbol{G_1}$ and v ϵ $\boldsymbol{G_2}$.

Non-Degeneracy:- e(g_1, g_2) ≠1.

Computability:- ***e*** is efficiently computable.

For the proposed scheme, we used ring signatures to cover the identity of the IoT devices; therefore, all information carried by each device of the hospital is not disclosed to the edge ledger. Traditional ring signatures are used without block-less verification; therefore, we have modified traditional ring signatures [4,5], to support block-less verification. Without block-less verification, the edge ledger has to download the whole private information to check for correctness of the shared data; hence, it will consume more time for huge data. In the proposed scheme, we have only three algorithms: KeyGen, RingSign, and ChekRing. In KeyGen, devices generate private and public keys. In RingSign, devices under the hospital are eligible to sign data with their private keys and all IoT public keys. Edge ledger has the advantage of checking the correctness of the sign. A hospital wishing to join a global ledger has to generate public and private keys with the help of a random key $\boldsymbol{x_i \epsilon\ Z_p}$ as well as compute the private and public keys. $w_i = g_2^{x_i}$ is the public key, and the private key is $\boldsymbol{Sk_i} = \boldsymbol{x_i}$. Edge ledger signs the password by looking at its database for the requested user. Hence, it uses its private key and the user's public key to sign on the password. For the WLAN user ***L***, a password denoted as ***m***, as $\boldsymbol{m \in Z_p}$ and private key of the registrar is $\boldsymbol{Sk_s}$. edge ledger randomly chooses $\boldsymbol{a_i \in Z_p}$ for i ≠ s, and $\sigma_i = \boldsymbol{g_1}^{\boldsymbol{ai}}$ then computes the following.

$$\beta = H_1 g^m \ \epsilon G_1 \tag{2}$$

The edge ledger of the hospital has the ability to sign a password with its private key and all the group members' public keys. Hence, the following equation is the group signature for the password ***m*** is $\boldsymbol{\sigma} = \{\sigma_1, \sigma_2 \ldots \sigma_d\}$ and belongs to G_1^d the group of WLAN users.

$$\sigma_s = \left(\frac{\beta}{\psi\left(\pi_{i \neq s} w^a\right)}\right)^{\dfrac{1}{x_s}} \tag{3}$$

Group signature on the user's password is $\sigma_s \ \epsilon G_1^d$

Edge ledger first computes Eq. (1) $\boldsymbol{\beta}$ for the WLAN ***L*** user with its public key $\boldsymbol{pk_1}$, password, and then checks the sign of user ***L***.

$$(\beta, g_2) = \prod_{i=1}^{d} e(\sigma_i, w_i) \tag{4}$$

If Eq. (4) holds, then user $\boldsymbol{L}$ is authenticated and is otherwise rejected. Our proposed scheme used for device data authentication is the storage of signatures. According to the generation of signatures in Homomorphic Authenticable Ring Structures (HARS), to audit an m-sized block of data, which has a huge number of ring signatures; therefore, it needs a large number space for storing signatures. Furthermore, HARS will consume more space owing to its underlying design of the ring signature, and the cloud service provider will also charge more on the storage space occupied by the HARS client. Therefore, we need to send a block of data from all devices so that we can reduce the computational complexity.

3.4.2 Support for Batch Data Transmission

We have used batch data transmission using a privacy-preserving technique; the IoT may concurrently send and receive data to the global edge via an edge ledger. Individual data transmission can be a burden on the edge ledger and is very inefficient. There exist many IoTs, and it is more useful for our proposed method to schedule these data transfer batch-wise at a time. During the setup phase, each IoT independently executes the setup phase. Suppose we have N number of IoTs, and each IoT has data to transfer to the edge ledger.

$D_{IoT} = \left\{m_{k,1}, m_{k,2}, m_{k,3}, \ldots\ m_{k,n}\right\}$, each data file has the same size. Further, each IoT has its own secret key and a public key, and it generates a data tag using data and sign (public and private key) and computes a file tag. The following steps are executed to achieve batch-based data transmission.

- Key generation for each input along with security parameters.
- Out puts a file tag for each key and data block
- Verifying process accepts and rejects the block of data using security parameters, name of the file, and block of data

$$\text{File tag } = B_d \parallel Sign(Security\ paramert) \tag{5}$$

Signing process for each IoT = $H(File \cdot public\ key) \in \mathbb{G}$

Where H is a cryptographic hash function and $\mathbb{G}$ is a multiplicative cyclic group. In any given situation, an IoT device is responsible for generating information about the medical reports. This produced information is signed by the device itself and sent to the edge ledger. After the reception of the information, the edge ledger signs the information to satisfy security requirements and to keep track of information for future operations. Only, it is being circulated among all hospital IoT devices so as to keep them updated. In our proposal, we have a number of IoT devices connected to each hospital and they are mapped to the edge ledger; hence, each ledger contains many IoT devices connected to the decentralized architecture. The edge ledger has limited storage and processing power; hence, each of its connected IoT devices defines the amount of data stored in the hospital ledger, which is also called the edge ledger. There might be a demand for older updates; hence, it can be fed to the external storage in the application process.

4 Evaluation

This section describes the implementation of our proposed method and discusses the experimental results. The implementation details comprise two parts: the IoT device part and the security analysis of the proposed system. Now, we discuss some important properties of our proposed scheme, including the correctness and correctness of the equation. Hence, we need to prove that Eq. 4 is correct.

$$\prod_{i=d}^{d} e(\sigma_s, w_i)\ = e(\sigma_s, w_s). \prod_{i \neq s}^{d} e(\sigma_s, w_i)$$

$$= e\left(\left(\frac{\beta}{\psi\left(\prod_{i\neq s} w_i^{a_i}\right)}\right)^{\frac{1}{x_s}}, g_2^{x_s}\right) \cdot \prod_{1\neq s} e\left(g_1^{q_i}, g_2^{x_i}\right)$$

$$= e\left(\left(\frac{\beta}{\psi\left(\prod_{i\neq s} g_2^{x_i a_i}\right)}\right), g_2\right) \cdot \prod_{1\neq s} e\left(g_1^{a_i x_i}, g_2\right)$$

$$= e\left(\frac{\beta}{\psi\left(\prod_{i\neq s} g_2^{x_i a_i}\right)}, g_2\right) \cdot\ e\left(\prod_{i\neq s} g_1^{a_i x_i}, g_2\right)$$

$$= \mathrm{e}\left(\frac{\beta}{\psi\left(\prod_{i\neq s} g_1^{x_i a_i}\right)} \cdot \prod_{i\neq s} g_1^{a_i x_i}, g_2\right)$$

$$= \mathrm{e}(\beta, g_2)$$

Fig. 1 shows the performance of our proposed method. It also shows that the load on the system by means of various operations does not affect its performance. IoT implementation comprises a digital signature on data protection technique, calculation of hash function for the handling of key functions such as key commitment and key updating, and authentication of data generated by the IoT. A private key and its corresponding public key are used to encrypt and decrypt messages over the network. However, this is not recommended for sensitive data; hence, digitally signing data is a concrete step toward securing the information. For digital signing, we used a one-way hash function for the data and then used a private key to encrypt the hash. We have also used a digital signature to validate data integrity for the data transferred between the edge ledger and IoT data. It comprise a one-way hash function, and data is encrypted using its private key. Hence, to validate data integrity, the recipient edge ledger uses the public key to decrypt the hash. This hash algorithm provides the original hash to create a one-way hash for the same data. Therefore, the edge ledger has the ability to compare the newly created hash against the original hash function. If these two hashes are similar in nature, the data is intact; otherwise, the data is tampered.

To obtain medical data to be verified, it must be a trusted authority. In a hyperledger, the membership service provider (MSP) is the trusted authority. MSP also recognizes each device of any given hospital in a given chain of hospitals. It also defines rules that govern the legal medical data from a trusted party. MSP uses the certification-based service and is implemented using the X.509 certificate as identities and is built using the Public Key Infrastructure model and uses secure communication in any given network. Our proposed hyper ledger uses a three-layer architecture, namely the application layer, API layer, and transaction layer. Once the medical report is generated by the pathology department, it requests to pass it to the consultant peers; these peers can be from a chain of hospitals. Hence, this transaction is endorsed, and it reaches all peers. To construct this transaction, we used a hyperledger fabric to create a chain code function, so that it can be read and written to the ledger when medical data are shared between two clients irrespective of the type of hospital as shown in the Fig. 2.

The request is between peers who are consultants of different hospitals. The endorsement policy states that both communicating devices must endorse any transaction; hence, the transaction must proceed to both peers. This transaction is created using a software development kit supplied with the hyperledger; then, the request to invoke a chain code process is processed so that it writes or reads to the central ledger. However, the endorsing consultants must verify the formation of the transaction, the transaction should never have been submitted before, the sign on the transaction should be valid, the sender or consultant should have the privilege to make transactions, and these inputs are wrapped around as arguments to the process of the chain code. Subsequently, the process of chain code is executed, and its resultant outputs are updated in the database. The updated data will also include the response bit, read, and write datasets.

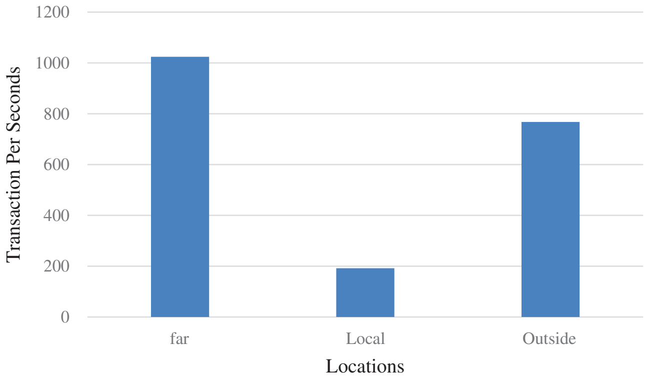

Figure 2: Performance of the proposed system in terms of throughput based on location

5 Conclusion

Our proposed framework checks the endorsing consultant's signature and compares it with the proposed responses. If it is the same, then the process will be executed; otherwise, it will be discarded. If the chain code process queries the ledger, then the proposal checks the query response. In our proposal, the application's resultant value will be updated in the ledger. Before the update, the application will check that the endorsement is initiated by the consultants from any hospital. We performed transactions of the proposed security mechanism and measured latency. This shows that our proposed mechanism is able to perform faster. The performance measure also includes a number of features such as authentication, security key operation, and message authentication code updates. The processing mechanism also includes ledgers who are servicing various consultants within any given hospital governing the idea of IoT transactions. Of course, the performance of the proposal is as direct as the physical location of the edge ledgers and global edge ledgers.

Acknowledgement: The author is thankful to the Deanship of Scientific Research, Prince Sattam Bin Abdulaziz University for providing all the resources and facilities for this research. The author is thankful to all the associated personnel, who contributed to this study by any means.

Funding Statement: The author received no specific funding for this study.

Conflicts of Interest: Author declare that they have no conflicts of interest to report regarding the present study.

References

[1] F. Al-Turjman and J. P. Lemayian, "Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview," *Computers & Electrical Engineering*, vol. 87, no. 1, pp. 1067–1076, 2020.

[2] B. Liao, Y. Ali, S. Nazir, L. He and H. U. Khan, "Security analysis of IoT devices by using mobile computing: A systematic literature review," *IEEE Access*, vol. 8, no. 1, pp. 120331–120350, 2020.

[3] J. Sengupta, S. Ruj and S. D. Bit, "A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, no. 6, pp. 102481, 2020.

[4] M. Alamri, N. Z. Jhanjhi and M. Humayun, "Block chain for Internet of Things (IoT) research issues challenges & future directions: A Review," *International Journal of Computer Science and Network Security*, vol. 19, no. 5, pp. 244–258, 2019.

[5] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah and R. Fotohi, “Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication,” *Journal of Supercomputing*, vol. 76, no. 9, pp. 7081–7106, 2020.

[6] B. Nour, K. Sharif, F. Li and Y. Wang, “Security and privacy challenges in information-centric wireless internet of things networks,” *IEEE Security & Privacy*, vol. 18, no. 2, pp. 35–45, 2020.

[7] C. K. Wu, K. F. Tsang, Y. Liu, H. Wang, H. Zhu *et al.,* “An IoT tree health indexing method using heterogeneous neural network,” *IEEE Access*, vol. 7, no. 2, pp. 66176–66184, 2019.

[8] T. Qin, B. Wang, R. Chen, Z. Qin and L. Wang, “IMLADS: Intelligent maintenance and lightweight anomaly detection system for internet of things,” *Sensors*, vol. 19, no. 4, pp. 1–19, 2019.

[9] D. Glaroudis, A. Iossifides and P. Chatzimisios, “Survey, comparison and research challenges of IoT application protocols for smart farming,” *Computer Networks*, vol. 168, no. 1, pp. 1–14, 2019.

[10] B. Alamri, I. T. Javed and T. Margaria, “Preserving patients privacy in medical IoT using blockchain,” in *Int. Conf. on Edge Computing, EDGE 2020. Proc.: Lecture Notes in Computer Science (LNCS 12407)*, New York City, NY, USA, pp. 103–110, 2020.

[11] S. Patil, S. Joshi and D. Patil, “Enhanced privacy preservation using anonymization in IoT-enabled smart homes,” in *Smart Intelligent Computing and Applications, Proc. of the Second Int. Conf. on SCI*, Singapore, pp. 439–454, 2020.

[12] B. Biais, C. Bisiere, M. Bouvard, C. Casamatta and A. J. Menkveld, “Equilibrium bitcoin pricing,” *Social Science Research Network*, vol. 1, no. 1, pp. 1–44, 2020.

[13] M. Wazid, A. K. Das, V. Bhat and A. V. Vasilakos, “LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment,” *Journal of Network and Computer Applications*, vol. 150, no. 1, pp. 102496, 2020.

[14] M. Kolhar, M. M. Abu-Alhaj and S. M. Abd El-atty, “Cloud data auditing techniques with a focus on privacy and security,” *IEEE Security & Privacy*, vol. 15, no. 1, pp. 42–51, 2017.

[15] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, “A survey on security and privacy issues in Internet-of-Things,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[16] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang *et al.,* “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[17] A. R. Sfar, E. Natalizio, Y. Challal and Z. Chtourou, “A roadmap for security challenges in the Internet of Things,” *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.

[18] F. A. Alaba, M. Othman, I. A. T. Hashem and F. Alotaibi, “Internet of Things security: A survey,” *Journal of Network and Computer Applications*, vol. 88, no. 4, pp. 10–28, 2017.

[19] M. Chernyshev, Z. Baig, O. Bello and S. Zeadally, “Internet of things (IoT): Research, simulators, and testbeds,” *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1637–1647, 2018.

[20] J. Srinivas, S. Mukhopadhyay and D. Mishra, “Secure and efficient user authentication scheme for multi-gateway wireless sensor networks,” *Ad Hoc Networks*, vol. 54, no. 2, pp. 147–169, 2017.

[21] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah *et al.,* “A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server,” *Computers & Electrical Engineering*, vol. 63, no. 2, pp. 168–181, 2017.

[22] G. Glissa and A. Meddeb, “6LowPSec: An end-to-end security protocol for 6LoWPAN,” *Ad Hoc Networks*, vol. 82, no. 1, pp. 100–112, 2019.

[23] M. Lavanya and V. Natarajan, “Lightweight key agreement protocol for IoT based on IKEv2,” *Computers and Electrical Engineering*, vol. 64, no. 4, pp. 580–594, 2017.

[24] M. Kolhar, F. Al-Turjman, A. Alameen and M. M. Abualhaj, “A three layered decentralized IoT biometric architecture for city lockdown during COVID-19 outbreak,” *IEEE Access*, vol. 8, no. 1, pp. 163608–163617, 2020.

[25] R. N. A. Kazi, M. Kolhar and F. Rizwan, “Smart CardioWatch system for patients with cardiovascular diseases who live alone,” *Computers, Materials and Continua*, vol. 66, no. 2, pp. 1237–1250, 2021.