Computers, Materials & Continua
DOI:10.32604/cmc.2022.020614
Article

Tech Science Press

An IoT Based Secure Patient Health Monitoring System

Kusum Yadav[1], Ali Alharbi[1], Anurag Jain[2,*] and Rabie A. Ramadan[1]

[1]College of Computer Science and Engineering, University of Ha'il, Ha'il, Kingdom of Saudi Arabia
[2]Virtualization Department, School of Computer Science, University of Petroleum and Energy Studies, Dehradun-248007, Uttarakhand, India
[*]Corresponding Author: Anurag Jain. Email: anurag.jain@ddn.upes.ac.in
Received: 31 May 2021; Accepted: 11 July 2021

Abstract: Internet of things **(**IoT) field has emerged due to the rapid growth of artificial intelligence and communication technologies. The use of IoT technology in modern healthcare environments is convenient for doctors and patients as it can be used in real-time monitoring of patients, proper administration of patient information, and healthcare management. However, the usage of IoT in the healthcare domain will become a nightmare if patient information is not securely maintained while transferring over an insecure network or storing at the administrator end. In this manuscript, the authors have developed a secure IoT healthcare monitoring system using the Blockchain-based XOR Elliptic Curve Cryptography (BC-XORECC) technique to avoid various vulnerable attacks. Initially, the work has established an authentication process for patient details by generating tokens, keys, and tags using Length Ceaser Cipher-based Pearson Hashing Algorithm (LCC-PHA), Elliptic Curve Cryptography (ECC), and Fishers Yates Shuffled Based Adelson-Velskii and Landis (FYS-AVL) tree. The authentications prevent unauthorized users from accessing or misuse the data. After that, a secure data transfer is performed using BC-XORECC, which acts faster by maintaining high data privacy and blocking the path for the attackers. Finally, the Linear Spline Kernel-Based Recurrent Neural Network (LSK-RNN) classification monitors the patient's health status. The whole developed framework brings out a secure data transfer without data loss or data breaches and remains efficient for health care monitoring via IoT. Experimental analysis shows that the proposed framework achieves a faster encryption and decryption time, classifies the patient's health status with an accuracy of 89%, and remains robust compared with the existing state-of-the-art method.

Keywords: Internet of things; blockchain-based XOR elliptic curve cryptography; linear spline kernel-based recurrent neural network; health care monitoring; length Ceaser cipher-based Pearson hashing algorithm; elliptic curve cryptography; fishers yates shuffled based Adelson–Velskii and Landis tree

1 Introduction

An emerging trend for every future generation technology is deemed to be IoT [1]. It is the interconnection of exclusively detected smart objects along with devices. For tracking data, IoT is surrounded by disparate sensors that are linked to many objects, which are invisibly attached all over the surroundings [2]. The highest ordinary research application in wearable electronics is Health Monitoring (HM). The union of smart computing and remote HM with IoT is called Smart HM [3].

Through HM, monitoring and caring for patients can be done outside of the traditional clinical boundary (i.e., house, for instance). A particularly designed monitoring device for monitoring and transmitting health data to smart contracts, a smartphone with internet connectivity, along with an HM application, is the main component of an HM system [4]. Wearable devices and IoT play a crucial part in HM and the current push for developing smart cities [5]. Wearable devices gather patient health data, transmitting it to hospitals or medical institutions for facilitating HM, disease diagnosis, and treatment. Thus, a Big Data situation is developed as every patient's data is examined and transmitted [6]. Furthermore, secure data sharing is demanded by such infrastructure for handling patient data with other institutions [7].

One of the most crucial aspects of any system is security. Concerning security, disparate perception is possessed by people, and thus, it is defined in multiple ways [8,9]. Generally, a notion similar to the system's safety as a whole is security. Nowadays, the communication in IoT-centered HM is mainly wireless, which might cause different security threats to these systems [10,11]. Serious issues could be posed by these security problems to the wireless sensor devices [12,13]. Hence, a vital necessity for safe and secure medical and health data management is the execution of data security methods, namely lightweight block encryption techniques for medical IoT resources [14].

Data mining are extensively utilized in medical monitoring, including classification as well as clustering methods [15], neural networks [16], together with other approaches centered on disparate machine learning methods for attaining diagnostic information to envisage the patient's abnormal health changes from the IoT data [17,18]. For offering a safe data transfer and a precise patient monitoring system, a safe patient HM system utilizing BC-XORECC and a patient monitoring system utilizing LSK-RNN is formed by the work that benefits from clouds and IoT technologies. In this, the patient could remotely be monitored via the medical squads for the early diagnosis of their crucial conditions.

This paper is categorized as: Section 2 analyzes the associated studies, Section 3 surveys the proposed work, Section 4 demonstrates the results along with discussion for the proposed method; in addition, Section 5 offers the conclusion with future scope.

2 Literature Review

This section contains the details of security mechanisms proposed by different researchers for IoT-based healthcare systems.

Gope et al. [19] have addressed the limitations in the present IoT-enabled healthcare system. Authors have utilized an authentication technique that is based on a physical unclonable function. In addition, to further strengthen security, the proposed decision-making scheme is fault-tolerant.

Seong-Kyu et al. [20] formed Artificial Intelligence (AI)-centered BlockChain (BC) algorithms for ensuring safe corroboration of data (medical). The approach rendered an information security BC-AI framework; it verified BC systems aimed at accurate extraction, storage, together with

verification of data. Additionally, disparate verification and performance assessment indicators were set to acquire the Translations Per Second (TPS) of data (medical) and for the standardization work execution. As a result, the BC confidentiality, together with the AI sensitivity, was maximized. However, it was susceptible to internal attacks.

Akhbarifar et al. [21] ascertained the patient's health status through envisaging critical situations via data mining. It analyzed all through their data (biological ones) sensed using smart medical IoT devices. For ensuring the security of patients' private data, lightweight, safe block encryption was employed. Next, centered on the K-Star classification, the patient's health status was classified. The K-star classification attainted the best outcomes amongst disparate classifiers; it got 95% accuracy. Thus, the work attained an excellent accuracy; however, the approach lagged to Security Level (SL).

Sarmah et al. [22] recommended a method, which encompassed '3' steps: a) Authentication, b) Encryption c) Classification. Initially, SHA-512 was employed as an authentication method. Next, the wearable IoT device transferred the sensor data concurrently to the cloud. These devices were installed on the patient's body. Centered upon Patient and Doctor Id, along with Hospital Id-Advanced Encryptions Standard (PDH-AES), the sensor data was encrypted as well as transmitted securely to the cloud. Next, the encrypted data was decrypted, and also Deep Learning Modified Neural Network performed the classification. The PDH-AES brought about 95.87% securities; however, it encompassed computational intricacy for generating keys.

Mohame et al. [23] posited Deep-Q-Networks that lessened malware attacks when transmitting medical data. As per the Q-learning conception, the technique scrutinized the medical details in disparate layers that minimized intermediary attacks with lesser intricacy. The system's efficiency was assessed concerning experimental outcomes as well as discussions. As a result, the Deep-Q-Network lessened the intermediary attacks; however, the data loss was higher.

Ramesh et al. [24] ameliorated a Role-centered Access Control with a '2' fish algorithm for protecting IoT health data on HC systems as a public cloud storage perception. It significantly helped in the effectual storage of data (medical) on IoT applications and rendered safe storage of data (medical) on the cloud on account of the role-centered access policies. Additionally, to diminish the waiting time for retrieving pertinent medical data, a clustering scheme was implemented. However, the access process was complicated to utilize.

Kesavan et al. [25] posited a method that utilized '4' disparate phases for transmitting the data. Those are Data Acquisition (DA), Fog to Cloud (FC), Decision-Making (DM), together with execution. The DA encompassed data storage as well as collection. Together with the cloud layer, the fog layer is the '2' disparate layers of the FC; it also described the safe integration of FC. The DM involved feature extraction along with classification. For attaining the best optimum solution, Adaptive Deep Convolution Neural Networks with the Levy Flight centered Grey Wolf Optimization was utilized in the classification. Unfortunately, the developed technique had lagged because of data breaches.

Khan et al. [26] have proposed a two-step security mechanism for IoT-based healthcare systems. The first level of security is achieved through a combination of user names and passwords with biometric credentials. The integrity of the authentication system is ensured by SHA-512 algorithm. At the second level, improved elliptical curve algorithm and substitution Ceaser cipher algorithms are used to ensure the confidentiality of messages during transmission.

Though different researchers have proposed different methodologies to make a secure IoT-based healthcare system, limitations in the existing system have motivated authors to propose a new security framework to make an IoT-based secure health monitoring system.

3 Proposed IoT Based Secure Patient Health Monitoring System

IoT-based patient monitoring system helps patients enjoy healthcare-related services sitting at a remote location in their homes. Patient's privacy, safety, and security, in this case, are very much essential. Therefore, a secured IoT-based health monitoring system is a crucial scheme to provide all kinds of shields against possible vulnerabilities. Various healthcare secure data monitoring has been developed. However, still, the method fails to protect the data which is vulnerable to some of the attacks, such as the denial-of-service attack, replay attack, man-in-the-middle attack, offline password guessing attack, a smart card is stolen attack, forward secrecy attack, user anonymity attack, mutual authentication attack, etc. The work has developed a secure Blockchain-based healthcare monitoring system in IoT by addressing the vulnerability attacks, as illustrated in Fig. 1.

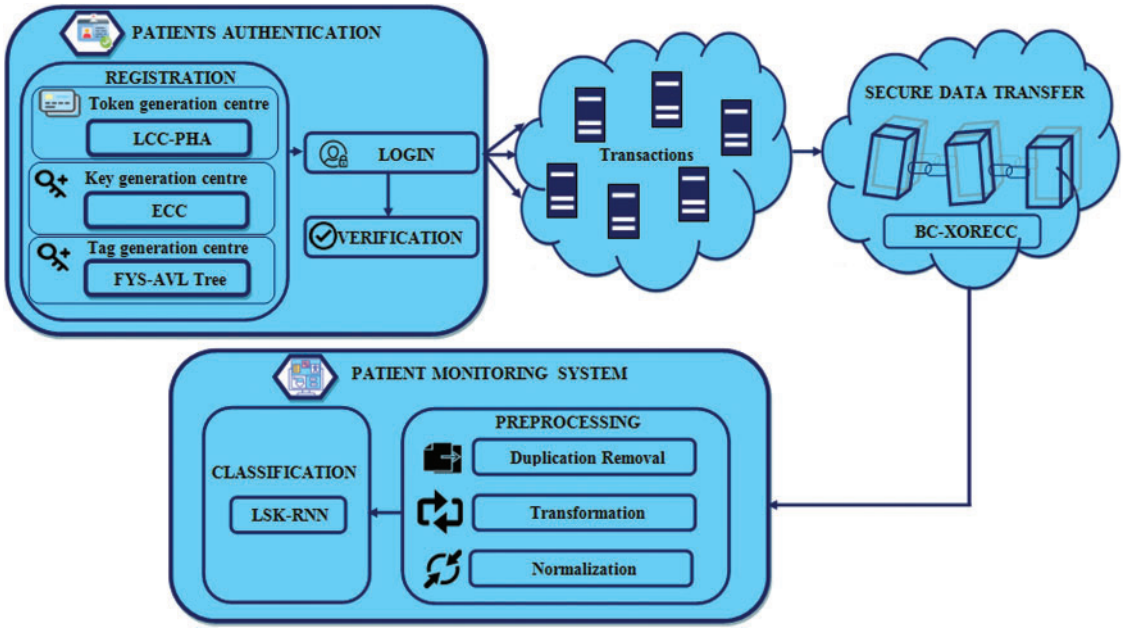


Figure 1: Proposed framework for IoT based secure patient health monitoring system

3.1 Authentication

Authentication provides to get authenticated by its own identity before transferring data. The authentication is provided to access the records or patients' data to those permitted as authenticated users. It conquers the internal attacks as well as the attacks during transit. The authentication phase comprises three subphases:

1) Registration Phase
2) Login Phase
3) Verification Phase.

3.1.1 Registration Phase

The registration phase provides with collecting the patient's details, which consists of the patient's name, patient's ID (P_{ID}), username $\left(UN_i^N\right)$, password generation $\left(PW_i^N\right)$, etc., that are enrolled into the records of the hospitals. This phase is necessary to provide the patient with hospital services and to monitor the various services that each patient receives. But storing patient details may get attacked if it is stored without any security. Hence, to provide proper data security, the work has been enhanced with token, key, and tag generation with its respective centers. Details of the three processes are given below:

Token Generation Centre

Token generation center allows the user to verify their identity, and in return, they receive a token to access the data. The user retains access as long as the token remains valid. Once the user logs out or quits an app, the token is invalidated.

In a token generation, initially, the Server (S_i^N) ask for access of the user to the protected data by providing the username and password $Z_i^n = \left(UN_i^N + PW_i^N\right)$ details obtained during registration as shown in (Eq. (1)).

$$UN_i^N + PW_i^N \rightarrow S_i^N \tag{1}$$

The center verifies the username and password i.e., $S_i^N \xrightarrow{Checks} Z_i^n = P_{ID}$ and generates the token after verification as shown in (Eq. (2)).

$$S_i^N \underset{Z_i^n = P_{ID}}{\overset{Verified}{\longrightarrow}} T_i^N \tag{2}$$

Finally, the token, username, and password are stored using the Length Ceaser cipher Pearson hashing algorithm to secure the details confidentially and stored within the user browser while the work continues. Initially, the Length Ceaser Cipher first transfers the letters into numbers. Encryption of a letter can be described mathematically as shown in (Eqs. (3)–(5)):

$$E_{CP}\left(U_I^N\right) = \left(U_I^N + n\right) \text{mod} 26 \tag{3}$$

$$D_{CP}\left(U_I^N\right) = \left(U_I^N - n\right) \text{mod} 26 \tag{4}$$

$$n = len\left(P_{ID}^N\right), \quad i = 1, 2, 3 \ldots . n \tag{5}$$

where, E_{CP} denotes the encryption of attributes U_I^N is the input attributes n is the shifting value, which depends upon the length of each attribute, D_{CP} is the decryption of attribute.

The L-Caesar Cipher algorithm encryption helps us secure the data by varying the shifting value based on the length of the attribute. Now, the converted ciphertext (CP_i^N) is converted into hash code using the Pearson hashing algorithm. The PHA provides an output in which a single byte of data is strongly dependent on every byte of the input. The algorithm computes the hash code (λ) for the (CP_i^N). Initially, the hash variable is initialized that is $(\lambda: = 0)$, now, based on the length of the ciphertext, the loop is continued until the ciphertext ends as given in (Eqs. (6)–(8)):

$$\lambda: = \hbar[\lambda \, XOR \, c] \tag{6}$$

$$c = len\left(CP_i^N\right) \tag{7}$$

$$\hbar[i] = 255 - i \tag{8}$$

Finally, the hash value is obtained for the converted ciphertext, and any small changes in the value make the developed algorithm generate a different hash algorithm.

Key Generation Centre

Key generation is an essential factor that generates the key, i.e., both the public and the private keys that are used to encrypt and decrypt IoT sensing data. ECC is an asymmetric public key-based encryption algorithm that provides high security even with small-length keys [27]. It is based on the elliptic curves. For developing the key, the work has adopted an ECC algorithm that allows the key size to remain shorter but provides a higher security level. Initially, the ECC generates the ciphertext private key $\left(\Re_{PRI}^{CP}\right)$ randomly using (Eq. (9)); after that, calculate the ciphertext public key $\left(\Re_{PUB}^{CP}\right)$ using (Eq. (10)). Finally, the shared secret key $(\Im_s)$is calculated using (Eq. (11)).

$$\Re_{PRI}^{CP} = rand\left(\mathrm{K}_{PRI}\right) \tag{9}$$

$$\Re_{PUB}^{CP} = \Re_{PRI}^{CP} * G \tag{10}$$

$$\Im_s = \Re_{PRI}^{CP} * \mathrm{K}_{PUK} \tag{11}$$

G is the random number ranging between (1 to $n-$ 1), K_{PUK} denotes the public key, and K_{PRI} is the private key.

Tag Generation Centre

Tag is generated for the patient details to make it more secure. The tag generation is performed using the Fisher–Yates shuffled AVL–Tree algorithm. The developed tag generation provides the self-balancing binary tree for the patient details. For each node of the tree, the height difference of its sub-trees is at most 1; therefore, it is also height-balanced. The tree formation is based upon the shuffling provided by the fisher Yates. The fisher Yates provides the shuffling of the entire data of individual patients until it gets finished. The AVL tag generation is illustrated in Fig. 2.

Fig. 2 states the AVL tree generation for the details such as Patient ID (P001), Hospital ID (H001), Patient Name (Alex), Hospital Name (Miot), Age (39), and Sex (male). According to the developed Fisher-Yates shuffled AVL–Tree algorithm, the details are initially shuffled, such as "mioth00139p001malealex", and based on each character, the tree is constructed. Then, based on the tree formation, the tag is generated.

3.1.2 Login

The user is logged in by inputting there U_i^{ID} $\mathrm{P}w_i^v$ and T_i^N to R_i. After entering the details, the R_i computes $L_i^* = f\left(U_i^{ID} \| \mathrm{P}w_i^v \| \mathrm{T}_i^N\right)$ and checks if L_i^* equals U_i. If the information entered by the user is right, this request is preceded.

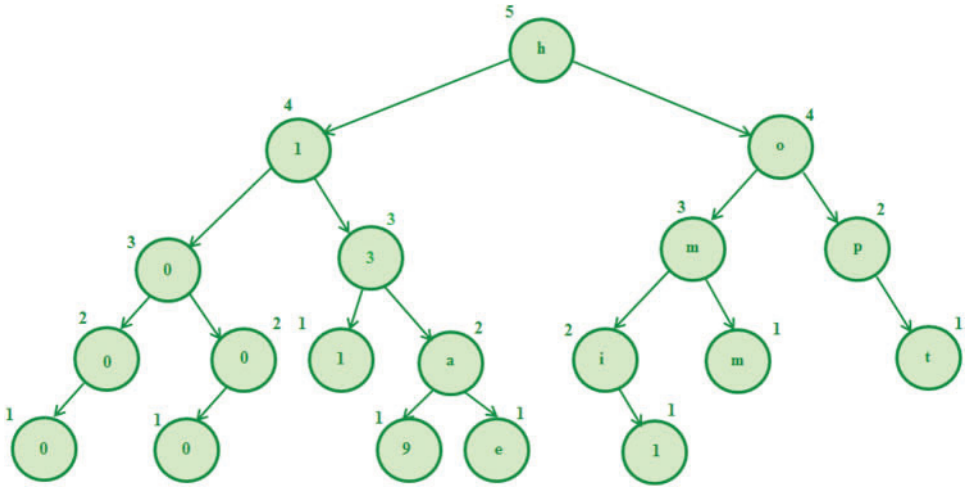


Figure 2: Fisher–Yates shuffled AVL–tree algorithm

3.1.3 Verification

This phase checks whether the login user is registered or not, and after that, communicates with the cloud environment, i.e., initially, the validity of the L_i^* is verified, and if the verification output ($V_\Theta = 1$) is then the process continues by communicating with the cloud, or else change of password is suggested for the user. Hence, all the authentication phase information is stored in a blockchain (BC_i^n) to provide a secure data transfer.

3.2 Secure Data Transfer

Secure data transfer is the most crucial task, which provides the hackers with a comfort zone to steal the data. Therefore, the data transfer has to be more robust to avoid malicious attacks. The work has used a Blockchain mechanism to transfer the data, but it comprises data storage (i.e.,) issue, storing big IoT data over the blockchain is not possible. Therefore, we use cloud servers to store encrypted data blocks, which is performed by XORECC algorithm.

Initially, the blockchains perform various steps to process the patient health care details from IoT. First, the user requests for a transaction in the blockchain as shown in (Eq. (12)):

$$U_i \overset{request}{\longrightarrow} BC_i^N \tag{12}$$

After that, the new transactions (U_i) are passed over to the individual peer network, including the PC nodes. After the individual's verification, a hash code is generated using SHA256. The algorithm generates a unique hash code as shown in (Eqs. (13)) and ((14)):

$$BC_i^N(U_i) = BC_1^N(U_i) + BC_2^N(U_i) + \ldots . BC_n^N(U_i) \tag{13}$$

$$BC_i^N \overset{verifies}{\longrightarrow} U_i \tag{14}$$

where BC_i^n denotes the blockchain of i users that consists of n details of the individual users. Now, the hash code is generated by the SHA 256, which undergoes a message block schedule and compression function. Initially, the N-Bit user details get looped until it satisfies the (Eq. (15)):

$$U_i + 1 + k = 448 \bmod 512 \tag{15}$$

where k, denotes the number of zero bit that is to get added up. The user details are converted into 64 bits binary values and further added with 448-bit to obtain the 512-bit message block. The block is further divided into sixteen 32-bit blocks, which are processed by compression to finally form the hash values as shown in (Eq. (16)).

$$H_i\left(U_i^N\right) = H_0H_1H_2H_3H_4H_5H_6H_7 \tag{16}$$

Every generated hash code is linked with the previous hash code in the block, which makes the blockchain mechanism an unbreakable network for transferring data. If someone tries to attach a transaction, the network node or a smart agreement will validate it. Therefore, this unchanging ledger cannot be modified. This process creates a decentralized system with secure and reliable data transfer. Finally, it checks if the user is genuine with an algorithm. After verifying a transaction, a new block in the network is added to the ledger. The block has an index structure, timestamp, data, previous hash block, and current hash block. A new block is then added to the blockchain, which remains to be unchanged and secure.

To avoid storage issues, each block is again encrypted using the developed XORECC cryptographic algorithm, which uses the key generated by KGC to encrypt and decrypt the block and performs the XOR of the hash code with the encryption and decryption key generated in TGC. Thus, the encryption and decryption of the blocks are computed as:

(a) Encryption

The encryption of the (BC_i^n) is carried out by randomly selecting Γ from [1 to $n-$ 1]. The encryption is performed under two ciphertexts, $\hbar_1$ and $\hbar_2$ is shown in (Eq. (17)) and (Eq. (18)):

$$\hbar_1 = \Gamma \times \mathrm{P} \tag{17}$$

$$\hbar_2 = BC_i^n + \Gamma \times \mathrm{K}_{PUK} + \bar{\lambda} \tag{18}$$

where, $\bar{\lambda}$ is the hash code generated by KGC. Thereafter, $\hbar_1$ and $\hbar_2$ will be sent further for decryption.

(b) Decryption

We have to get back the message that was sent to us. Its formula is shown in (Eq. (19)):

$$BC_i^n = \hbar_2 - \frac{\mathrm{K}_{PRI} \times \mathrm{K}_{PUK}}{\gamma_{GK} \times \mathrm{E}_{CP}} + \bar{\lambda} \tag{19}$$

Thus, BC_i^n is the original message decrypted using the distributed key. Thus, the secure data transfer outline is illustrated in the form of pseudo-code stated in Fig. 3.

3.3 Patient Monitoring System

The secured data is now processed under health care monitoring to get the status of patient health. However, before getting the patient's health status, the collected IoT secure data is preprocessed to improve the data quality.

3.3.1 Preprocessing

Preprocessing provides healthier data to avoid the chance of error. Preprocessing helps the model to obtain better accuracy.

Input: Patients detail
Output: Secure data transfer

Begin
Initialize the Block chain (BC_i^n), Hash code (H_i)
For i=1 to N
Request given to the Block chain
$U_i \xrightarrow{request} BC_i^N$
If $\left(BC_i^N \xrightarrow{verifies} U_i = 1\right)$
Generate Hash code
For $(i = len(U_i))$
Performs hashing of the details
$U_i + 1 + k = 448 \bmod 512$
End for
Else
User is unauthorized or malicious user
End if
If $\left(len(BC_i^n) > 250GB\right)$
Store the block in cloud storage
Encrypt the block using,
$\hbar_1 = \Gamma \times \mathrm{P}$
$\hbar_2 = BC_i^n + \Gamma \times \mathrm{K}_{PUK} + \lambda$
Perform secure data transfer
Else
Store it in block chain and perform secure data transfer
End if
End for
End begin

Figure 3: Pseudo code for BC-XORECC

(a) Duplication Removal

It removes the entire repeated context from the database (λ_{text}) that may not bring that much change while training a model. The repeated data occupies the database space and also may lead to more processing time. The repetition function ($\mathrm{H}_{\mathrm{P}}^{Rep}$) is given by (Eq. (20)):

$$\mathrm{H}_{\mathrm{Re}p} = \mathrm{H}_{\mathrm{P}}^{\mathrm{Re}p}[\lambda_{text}] \tag{20}$$

(b) Transformation

Transformation ($\mathrm{H}_{\mathrm{P}}^{T}$) provides converting of the characters into numeric values. It helps to make the data more understandable and improve the precision of monitoring the patient's status. It is given in (Eq. (21)):

$$\mathrm{H}_{MVT} = \mathrm{H}_{\mathrm{P}}^{T}[\lambda_{text}] \tag{21}$$

(c) Normalization

Normalization (H_{nor}) contributes towards scaling the data between 0 and 1. Normalization provides the same units and helps to reduce the upcoming errors. Normalization is given by (Eq. (22)):

$$\mathrm{H}_{nor} = \frac{\lambda - \lambda_{\min}}{\lambda_{\max} - \lambda_{\min}} \tag{22}$$

Thus, overall it obtains a clean text which is then preceded into the training process. The preprocessed text is given by (Eq. (23)):

$$H_{Pre} = [\lambda_1, \lambda_2, \lambda_3, \lambda_4, \ldots\ldots \lambda_n] \tag{23}$$

3.3.2 Classification

Classification provides the health status of the patient based on the preprocessed IoT Data. Classification gets trained over the data. Let's consider the liver dataset of the patients. Based on the dataset, the classification gets trained, and the testing is done to analyze the patient's health status. The work has developed a linear spine kernel-based recurrent neural network (LSK-RNN), which addresses vanishing gradient problems and the computational complexity during the training of the data. The LSK-RNN is performed on the input data $H_{Pre} = [\lambda_1, \lambda_2, \lambda_3, \lambda_4, \ldots, \lambda_t]$ that consists of a hidden vector sequence $\aleph_{hidden} = [\aleph_1, \aleph_2, \aleph_3, \aleph_4, \ldots, \aleph_t]$ and output vector sequence $\Theta = [\Theta_1, \Theta_2, \Theta_3, \Theta_4, \ldots, \Theta_n])$ by iterating the following sequence from $t = 1$ *to* T is given by (Eqs. (24)–(26)):

$$\aleph_t = \Phi_{act}\left[w_{\lambda\aleph}\lambda_t + w_{\aleph\aleph}\aleph_{t-1} + b\right] \tag{24}$$

$$\Theta_t = \sigma\left[w_{\lambda\Theta}\aleph_t + b\right] \tag{25}$$

$$\lambda = w_{\lambda\Theta}\aleph_t + b \tag{26}$$

where the w_i terms denote weight matrices (e.g., $w_{\lambda\aleph}$ is the input-hidden weight matrix), the b terms denote bias vectors and Φ_{act} is the hidden layer activation function, which is computed using line spine kernel function computed as (Eq. (27)):

$$\Phi_{act}(\lambda, \Theta) = 1 + \lambda\Theta + \lambda\Theta \min(\lambda, \Theta) - \frac{\lambda + \Theta}{2}\min(\lambda, \Theta)^2 + \frac{1}{3}\min(\lambda, \Theta) \tag{27}$$

For output layer sigmoid activation (σ) function is used, which is computed as given in (Eq. (28)):

$$\sigma(\lambda) = \frac{1}{1 + e^{-\lambda}} \tag{28}$$

Hence, based on the predicted output, loss value is evaluated as shown in (Eq. (29)):

$$L = \left(\lambda - \hat{\lambda}\right)^2 \tag{29}$$

where, λ and $\hat{\lambda}$ denotes the actual value and predicted value for the liver dataset. Now, if L=0 then the model gives the exact true value, but if $L \neq 0$, then backpropagation is performed by updating the weights. Thus, the proposed framework provides a secure data transmission by avoiding data loss and data breaches and able to classify the patient's health status based on the IoT data.

4 Result & Discussion

In this section, the proposed secured IoT-based health care monitoring framework is assessed with various performance metrics and compared with the existing methodologies to analyze or observe the proposed work efficiency. The results are evaluated based on the number of data ranging from 100 to 500. The system is implemented in the working platform of JAVA with the system configuration be Intel Core i7 processor, 3.20 GHz CPU speed, and 4GB RAM. The work was carried out on publically available datasets.

4.1 Performance Analysis

This section analyses the performance of the proposed method with existing methods. The proposed LCC-PHA, BC-XORECC, and LSK-RNN for Hash code generation, secure data transfer, and patient status classification are compared with the existing techniques regarding some performance metrics.

4.1.1 Performance Evaluation of Proposed LCC-PHA for Hash Code Generation Based on Hash Generation Time

Here, the analysis of time taken for generating the hash code for the data by the proposed LCC-PHA method is contrasted with the existing RIPEMD, MD5, Spooky Hash, FNV method and is illustrated in Tab. 1.

Table 1: Evaluation of the proposed LCC-PHA based on hash code generation

No of data/Techniques	100	200	300	400	500
RIPEMD	15.641	16.455	18.546	19.661	21.314
MD5	10.456	11.874	13.564	15.648	20.158
Spooky hash	10.254	13.569	17.889	18.654	19.854
FNV	9.879	11.247	13.568	14.587	15.649
Proposed LCC-PHA	2.789	3.879	4.895	5.798	6.667

Tab. 1 indicates the Hash code generation time for the existing and proposed system. The table illustrates that the proposed method tends to achieve a hash code generation time ranging between 2.789–6.667 s for the data ranging from 100–500. But the existing methodologies achieve a hash generation time varying between 9.879–19.661 s, which is relatively high compared to the proposed method. Therefore, for a hashing algorithm to be robust, it must constrain a low hash generation time and increased security. Nevertheless, the proposed method remains faster and highly secured due to the improvisation done using the Length Ceaser cipher in the Pearson hashing algorithm that leads the existing methodologies.

Fig. 4 shows the Hash code generation time for the existing and proposed system. The graphical analysis states that the proposed method performs a faster generation of hash code than the current methodologies and avoids attacks by performing a highly secured hash code.

4.1.2 Performance Evaluation of Proposed BC-XORECC For Secure Data Transfer Based on Encryption Time, Decryption Time, and Security Level

Here, the analysis of the time taken for the encryption and decryption of the data by the proposed BC-XORECC method is contrasted with the existing Blowfish, DES, RC4, and AES. The evaluation of the metrics is illustrated in Tab. 2.

Tab. 2 illustrates the evaluation of the encryption time and decryption time for the proposed method along with the existing methods. To differentiate one encryption algorithm from another, it should have the ability to secure the data against attackers and its speed and efficiency in doing so. According to that, the proposed BC-XORECC can secure the data and maintain the speed by performing faster encryption and decryption. The proposed method tends to achieve a low encryption time ranging between 1.203–3.784 s for the data ranging from 100–500 and at the same time maintaining a faster decryption time ranging between 1.201–4.124 s. But the existing methods

tend to achieve an encryption time ranging between 3.456–14.897 s and decryption time ranging between 2.489–16.457 s for the data ranging from 100–500. Thus, the proposed method remains to be efficient in securing the data and the speed of the execution. The graphical analysis of the proposed method is illustrated in Fig. 5.

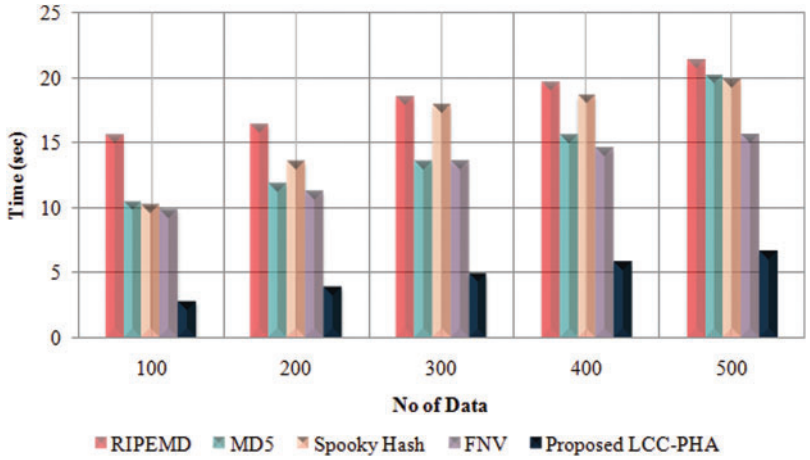
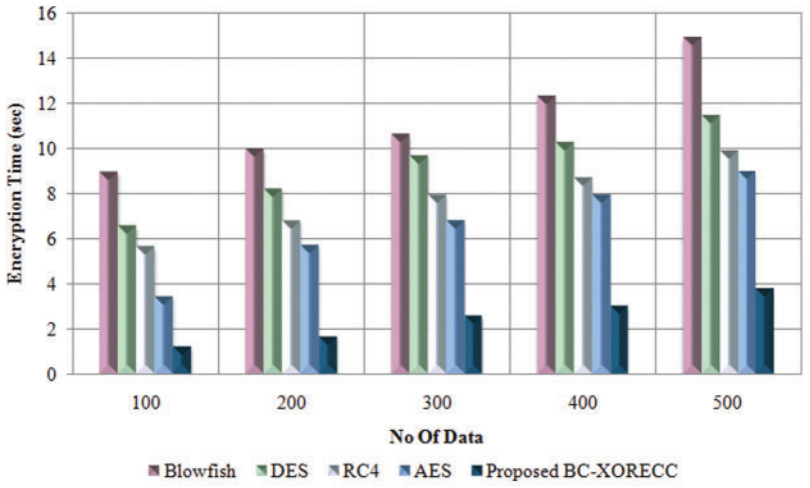


Figure 4: Graphical representation of LCC-PHA based on hash code generation time

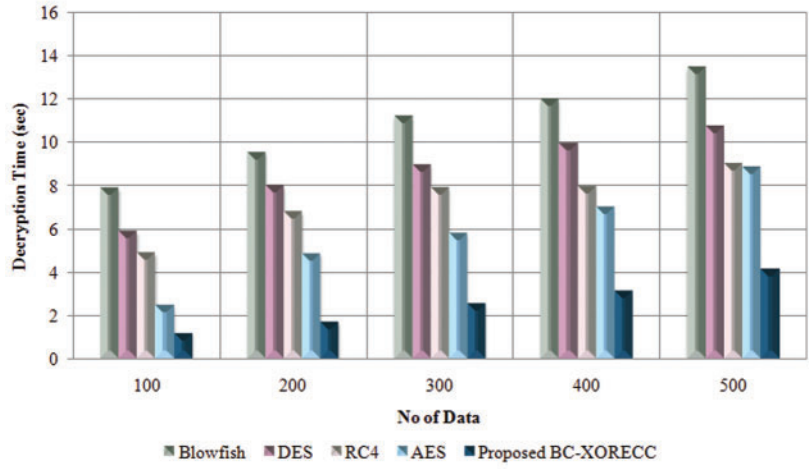
Table 2: Evaluation of the proposed BC-XORECC with the existing methods in terms of encryption and decryption time (s)

	File size (MB)	Blowfish	DES	RC4	AES	Proposed BC-XORECC
Encryption	100	8.978	6.554	5.647	3.456	1.203
	200	9.987	8.201	6.788	5.689	1.658
	300	10.625	9.689	7.924	6.789	2.546
	400	12.345	10.247	8.678	7.945	2.987
	500	14.897	11.457	9.897	8.976	3.784
Decryption	100	7.897	5.902	4.897	2.489	1.201
	200	9.563	7.998	6.788	4.887	1.699
	300	11.203	8.958	7.896	5.789	2.568
	400	11.989	9.978	7.982	6.996	3.106
	500	16.457	10.733	9.012	8.841	4.124

In Figs. 5a & 5b, the time taken for encrypting and decrypting the varied data sizes is shown. Thus, it shows that encryption and decryption of any large size of files will only take significantly less time for the proposed system when compared with the existing Blowfish, DES, RC4, and AES methods and provides a high level of security. Security level elaborates the strength of the cryptographic primitives, such as cipher or hash function. Based on the security level, the proposed method is analyzed graphically in Fig. 6.



(a)



(b)

Figure 5: Graphical representation of BC-XORECC based on (a) Encryption time (b) Decryption time

The security level is the most important metric that illustrates the framework's efficiency by bringing the users' trust. Therefore, a high percentage of security level indicates a better framework for transferring data. The proposed method tends to achieve a security level of 93.56%, as shown in Fig. 6. In contrast, the existing Blowfish, DES, RC4, and AES methods tend to achieve a security level of 87.96%, 91.54%, 90.89%, and 91.84%, respectively comparatively lower than the proposed method. Thus, the proposed BC-XORECC tends to be more secure for transferring user details or medical details by avoiding malicious attacks.

4.2 Performance Evaluation of Proposed LSK-RNN for Patient Monitoring System Based on Metrics

The proposed LSK-RNN patient monitoring system is analyzed based on the liver dataset, which is publically available. The proposed method is evaluated based on the metrics, such as Accuracy, Specificity, False positive rate (FPR), and False negative rate (FNR), along with the

existing methodologies, such as Deep neural network (DNN), Ensemble method, Support vector machine (SVM), and Recurrent neural network (RNN).

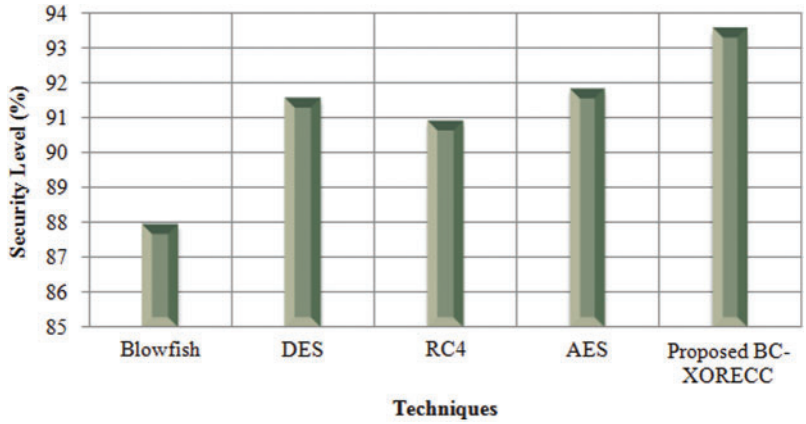


Figure 6: Graphical representation of BC-XORECC based on the security level

Fig. 7 illustrates the IoT data-based patient health monitoring system. The performance evaluation helps to know the efficiency of the proposed techniques. From the tabulation, it is known that the proposed LSK-RNN achieves an accuracy of 89.96% and specificity of 89.99%. In contrast, the existing methods achieve the metric value ranging between 75.68%–83.54%, which is relatively low compared to the proposed technique. In addition to that, the proposed method avoids misclassification by achieving lower FPR and FNR values of 14.52% and 12.53%, respectively. Nevertheless, it remains to be robust as compared to the existing methodologies.

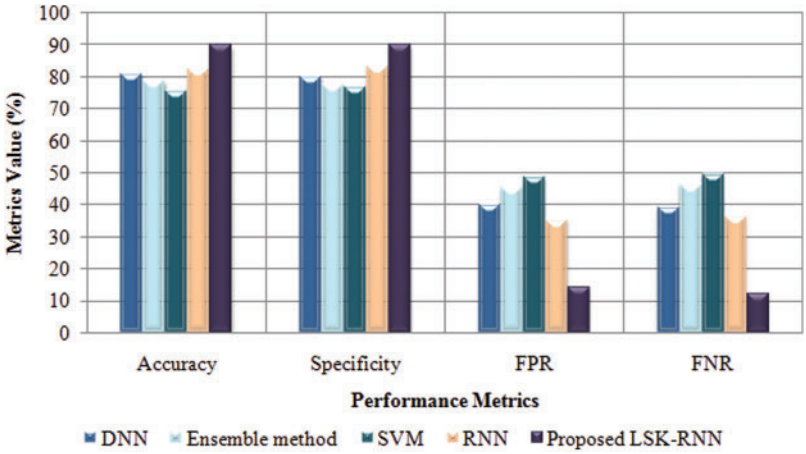


Figure 7: Graphical representation of LSK-RNN based on accuracy, specificity, FPR, and FNR

5 Conclusion & Future Scope

Secure data transmission is a vital task in the IoT environment. As there is a lot of chances to steal the data within the IoT platform because IoT devices are generally accessed through an untrusted network, so there is a need to protect the privacy of healthcare data while it travels over

an untrusted network. In this paper, the authors have developed a BC-XORECC based Secure IoT healthcare monitoring system to avoid various vulnerable attacks. First, the work allows the authorized user to access the data by implementing a strong authentication process using LCC-PHA, ECC, and FYS-AVL tree. The authentications prevent internal attacks. Secondly, the data is transferred securely by maintaining the confidentiality, integrity, and availability of the data by avoiding the interference of the attackers using BC-XORECC. Finally, secured data is trained under LSK-RNN classification to monitor the patient's health status. Experimental analysis has shown that the proposed framework has achieved a Hash code generation time of an average of 4.8056 s with a faster encryption time of 3.784 s and decryption time of 4.124 s. It has also classified the patient's health status with an accuracy of 89.96% and remains to be robust compared with the existing state-of-the-art method.

In the future, authors have planned to enhance this work by integrating the work with an android based app so that the proposed model can also be used on mobile. It can be implemented by the use of some lighter deep learning models.

Funding Statement: This project has been funded by the Scientific Research Deanship at the University of Ha'il–Saudi Arabia through project number BA-2105.

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

References

[1] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson *et al.,* "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 7, pp. 1–7, 2018.

[2] G. Rathee, A. Sharma, H. Saini, R. Kumar and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," *Multimedia Tools and Applications*, vol. 79, no. 12, pp. 1–23, 2019.

[3] R. J. Oskouei, Z. MousaviLou, Z. Bakhtiari and K. B. Jalbani, "IoT-based healthcare support system for alzheimer's patients," *Wireless Communications and Mobile Computing*, vol. 2020, no. 3, pp. 1–15, 2020.

[4] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, 2015.

[5] P. Verma, S. K. Sood and S. Kalra, "Cloud-centric IoT based student healthcare monitoring framework," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 5, pp. 1293–1309, 2018.

[6] H. A. El Zouka and M. M. Hosni, "Secure IoT communications for smart healthcare monitoring system," *Internet of Things*, vol. 13, pp. 1–14, 2019.

[7] S. S. Ambarkar and N. Shekokar, "Toward smart and secure IoT based healthcare system," in *Internet of Things, Smart Computing and Technology: A Roadmap Ahead*. Vol. 2020. Cham: Springer, pp. 283–303, 2020.

[8] S. R. Moosavi, T. N. Gia, A. M. Rahmani, E. Nigussie, S. Virtanen *et al.,* "SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," *Procedia Computer Science*, vol. 52, pp. 452–459, 2015.

[9] G. S. Aujla and A. Jindal, "A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 1–9, 2020.

[10] P. K. Dhillon and S. Kalra, "Multi-factor user authentication scheme for IoT-based healthcare services," *Journal of Reliable Intelligent Environments*, vol. 4, no. 3, pp. 141–160, 2018.

[11] X. Wang and S. Cai, "Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud," *Future Generation Computer Systems*, vol. 112, no. 1, pp. 320–329, 2020.

[12] D. S. Rajput and R. Gour, "An IoT framework for healthcare monitoring systems," *International Journal of Computer Science and Information Security*, vol. 14, no. 5, pp. 451–455, 2016.

[13] B. K. Bhoomika and K. N. Muralidhara, "Secured smart healthcare monitoring system based on Iot," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 3, no. 7, pp. 4958–4961, 2015.

[14] G. Sharma and S. Kalra, "A lightweight user authentication scheme for cloud-IoT based healthcare services," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, no. 1, pp. 619–636, 2019.

[15] A. Abuelkhail, U. Baroudi, M. Raad and T. Sheltami, "Internet of things for healthcare monitoring applications based on RFID clustering scheme," *Wireless Networks*, vol. 27, no. 1, pp. 747–763, 2021.

[16] P. M. Kumar, S. Lokesh, R. Varatharajan, G. C. Babu and P. Parthasarathy, "Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier," *Future Generation Computer Systems*, vol. 86, no. 3, pp. 527–534, 2018.

[17] A. Gondalia, D. Dixit, S. Parashar, V. Raghava, A. Sengupta *et al.,* "IoT-based healthcare monitoring system for war soldiers using machine learning," *Procedia Computer Science*, vol. 133, no. 3, pp. 1005–1013, 2018.

[18] A. Souri, M. Y. Ghafour, A. M. Ahmed, F. Safara, A. Yamini *et al.,* "A new machine learning-based healthcare monitoring model for student's condition diagnosis in Internet of Things environment," *Soft Computing*, vol. 24, no. 9, pp. 17111–17121, 2020.

[19] P. Gope, Y. Gheraibia, S. Kabir and B. Sikdar, "A secure IoT-based modern healthcare system with fault-tolerant decision making process," *IEEE Journal of Biomedical and Health Informatics*, vol. 25, no. 3, pp. 1–13, 2020.

[20] K. Seong-Kyu and H. Jun-Ho, "Artificial neural network blockchain techniques for healthcare system: focusing on the personal health records," *Electronics*, vol. 9, no. 5, pp. 763, 2020.

[21] S. Akhbarifar, H. S. Javadi, A. M. Rahmani and M. Hosseinzadeh, "A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment," *Personal and Ubiquitous Computing*, vol. 23, no. 5–6, pp. 1–17, 2020.

[22] S. S. Sarmah, "An efficient IoT-based patient monitoring and heart disease prediction system using deep learning modified neural network," *IEEE Access*, vol. 8, pp. 135784–135797, 2020.

[23] P. S. Mohame, S. Baskar, V. R. S. Dhulipala, S. Mishra and M. M. Jaber, "Maintaining security and privacy in health care system using learning based deep-Q-networks," *Journal of Medical Systems*, vol. 42, no. 10, pp. 1–10, 2018.

[24] S. Ramesh, T. Jayasankar, R. M. Bhavadharini, N. R. Nagarajan and G. Mani, "Securing medical data using extended role based access control model and two fish algorithms on cloud platform," *European Journal of Molecular & Clinical Medicine*, vol. 8, no. 1, pp. 1075–1089, 2021.

[25] R. Kesavan and S. Arumugam, "Adaptive deep convolutional neural network-based secure integration of fog to cloud supported internet of things for health monitoring system," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 10, pp. 1–18, 2020.

[26] M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data," *IEEE Access*, vol. 8, pp. 52018–52027, 2020.

[27] N. Koblitz, A. Menezes and S. Vanstone, "The state of elliptic curve cryptography," *Designs Codes and Cryptography*, vol. 19, no. 2, pp. 173–193, 2000.