EASR

Engineering and Applied Science Research

https://www.tci-thaijo.org/index.php/easr/index

Published by the Faculty of Engineering, Khon Kaen University, Thailand

Security enhancement of decentralized healthcare system by transformer blockchain mechanism

Akanksha Goel* and Subbu Neduncheliyan

Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu - 600073, India

Received 23 May 2024
Revised 15 November 2024
Accepted 21 November 2024

Abstract

Medical data plays an essential role in diagnosing diseases and planning therapeutic. However, securing these data is a very critical function in the healthcare system. Some of the traditional Encryption and decryption mechanisms have resulted in a loss of sensitive medical information. In addition, maintaining the confidential score of the medical information is a much more needed and essential task. Considering these cases, the healthcare application was adopted in this present study. Therefore, to enhance security, a novel Transformer Neural Data Encryption Blockchain (TNDEB) has been proposed in this research. The IoMT database was initially collected and trained to detect and eliminate malicious events. Further, the hashing and encryption process has been carried out to secure the data. Moreover, to check the data similarity, the homomorphism function was performed at the verification module, and the verified data was decrypted using the shared private key. The chief contribution of this study is to keep medical information confidential with the support of the holomorphic concept. Additionally, the cryptanalysis was carried out by launching the brute force attack to compute the performance efficiency of the TNDEB model. Subsequently, the validated performance results are compared with existing models. The decrypt and encrypt time achieved by the TNDEB model is 1.260ms and 1.010ms, respectively. In addition, the gained confidential score is 98.8%. Hence, the proposed model is highly suitable for the IMoT application to secure the information at a high confidential rate.

Keywords: Blockchain, Transformer neural system, Medical cloud data, Data encryption standard, Brute force attack

1. Introduction

In the past decades, the technologies of Medicare have extended fundamental functions in day-to-day life, including the healthcare systems [1]. The primary aim of intelligence in the healthcare systems is to offer the best interfacing ability among patients and caretakers to enhance the effectiveness and access to health advice and devices [2]. In recent times, the Internet of Medical Things (IoMT) and Artificial Intelligence (AI) have played the necessary tasks in the remote health care monitoring (RHM) process [3]. The IoMT was used to gather the patient's remote data via wearable sensors or devices and was stored in the cloud databases [4]. The IoMT comprises three stages: the device layer, the fog layer, and the cloud service layer. The RHM was the continuously monitored process of the medical data. The data includes heart rate, physical activity, medication tracking, behavior monitoring, temperature, blood pressure, and diet monitoring [5, 6]. These medical data were transmitted to the users via the cloud [7]. The IoMT supported the quick and secure diagnosis of various disease types and improved decision-making [8]. Leveraging AI systems provides many benefits in healthcare, such as convenience, reduced medical costs, enhanced patient safety, improved diagnosis, and avoiding repeating tests [9].

Monitoring the vital signs is a critical task in Medicare, and these signs help to identify abnormal conditions in the human body [10]. Even in the hospital, based on several conditions, caretakers were allocated to monitor the improvement in health conditions [11]. The monitoring parameters are temperature, pressure, pulse, and breathing rate [12]. Monitoring systems provide alerts about the patient's abnormality and help them get timely aid to escape death [13]. The system prioritizes the patients based on their critical health condition. Subsequently, it collects the patients' medical records and stores them in the cloud for evaluation by the physician [14]. E-healthcare is a suitable way to cheaply offer remedies to people in remote and isolated regions [15]. According to the pulse and temperature level measure, the health data was recorded and preserved in the cloud to visualize in real-time and send patient details. This would help to reduce the gap between rural area patients and the physician [16].

Privacy and data security were the primary concerns for health monitoring systems worldwide. The mHealth allowed the collection of extensive patient data, including the vital symptoms of the disease [17]. The interoperability problem produces interference in the practical information-sharing process [18]. The fraud medical reasoning detection was significant, and the drugs were complex to differentiate from the authorized party. The monitoring process takes more computational time. For instance, a large amount of money was charged for hospitalized patients [19].

Meanwhile, patients staying in remote areas had difficulty accessing the hospital. So, the health monitoring process was done using the IoMT application. The encryption process could be used for data transfer to prevent unauthorized users from accessing the data

*Corresponding author.
Email address: akanksha.rkgit@gmail.com
doi: 10.14456/easr.2024.73

[20]. To overcome these problems, an efficient, optimized technique was used for health monitoring and the diagnostic ecosystem of the patient's vital signs.

Intelligent models like machine learning and deep learning have recently been introduced to secure medical records. Hence, the convolutional neural model with recurrent system [21], sequence network [22], decision-based machine learning [23], AI-based regression model [24], etc., acted as the securing mechanism to store the medical records with the blockchain facilities. However, those models failed to perform the data integrity analysis. Even though intelligent features were incorporated into the blockchain mechanism, the data records' confidential score was average. These issues motivated this study to create an intelligent crypto strategy in the healthcare system. So, the present work has proposed an intelligent encryption system and the holomorphic concept to offer data integrity.

IoMT-based intelligent healthcare devices have made health service an immense requirement by integrating better mobile services, user-friendly interfaces, and computing applications. In contrast, patients can identify and analyze healthcare data. The existing works of health monitoring systems presented limitations, including maximum medical cost. However, IoMT applications produce a massive amount of data that is too complex to analyze and generate immediate reports of the patients. Recent innovative technology could not provide real-time monitoring and diagnostics of a patient's essential signs. These problems were motivated by an efficient, optimized approach to developing the data-driven health monitoring system. The main scope of this study is to develop an intelligent blockchain system for healthcare applications to secure medical records from malicious events. The critical contribution of this research study is detailed as follows,

- The IoMT decentralized database was primarily considered and trained in the Python environment.
- Then, a unique blockchain mechanism, TNDEB, was designed for a decentralized environment.
- Consequently, the database is monitored for any malicious event. If there is any malicious event, then it is predicted and neglected.
- Hereafter, the database was hashed and encrypted using the TNDEB encryption function.
- Furthermore, the crypt analysis is carried out by launching a brute-force attack on the hidden data.
- Finally, the chief parameters, such as Decryption and Encryption time, confidential rate, error rate, and execution time, were measured and validated using existing studies.

The executed blockchain-based security system work is arranged in the following order. A few recent works of literature are explained with advantages and limitations in section 2. The problems from past studies of the survey are discussed in section 3. The presented security solution is elaborated on in section 4. The framework results with comparison are detailed in section 5, and the research conclusion is explained in section 6.

2. Related work

Several recent works carried out for the health monitoring system were described as follows:

Jamil et al. [25] proposed a Healthcare IoT blockchain model to investigate the patients' symptoms. This technique used the hyper ledger composer to design intelligent contracts to monitor patients' vital signs securely. Here, the critical movement was stored successfully after selecting the patient from the set of patients, and the doctor assigned the healthcare device to get vital sign information. Finally, sensors were used to monitor the patient's vital signs, and communication was done through the constrained application protocol (CoAP). This scheme obtains an increase in throughput and latency for monitoring.

The sharing of medical data from the cloud is vulnerable to cyber-attacks. Therefore, to preserve the data in encryption format, Mamta et al. [26] introduced an Attribute Search Encryption (ASE) Scheme. The simulation of this process is done with the data collected from the resource-strained devices. The computation cost of the encryption process is reduced by incorporating the decentralized blockchain strategy. It is load-balanced and prevents system failure. However, this system needs to add extra features for search result verification. Saidi et al. [27] modeled identity-based blockchain architecture to enhance medical information security. It gives exclusive access to the patients to control their medical records. It is structured with the decentralized providers and credential verification phase for the emergency. This system satisfied privacy factors such as sustainability, scalability, emergency case access, etc. The hybrid algorithm provides better protection for data and user privacy.

Khan et al. [28] proposed a hybrid machine learning technique that aimed to monitor the patient's vital signs, and the outliers were neglected from the collected data. The allocation of the channel state information avoids the fluctuation in the Wifi. The patient's respiration rate in sleep was monitored with minimum hardware-related cost. Consequently, the hybrid model is made for the feature selection and prediction of the patient's health condition from the noise-eliminated and balanced data. This system transmits large amounts of redundant and inconsistent data. Aujla and Jindal [29] designed a decoupled blockchain-based system for privacy in medical procedures. Specific devices perform this scheme to decouple the blocks of the blockchain architecture that export medical data from the sensors to the incorporated edge devices. Then, the incremental tensor-based approach was used to transmit and save the data in the cloud. This system aimed to minimize the duplication process of the bulk data transferred to the IoT network. Hence, the need for sample cloud storage space is reduced.

Khan et al. [30] have developed a unique approach using fuzzy logic and generative adversarial networks (FLGAN) for multimedia streaming data compression and encoding techniques. This cooperative framework minimizes lossless video files, removes adversarial loss, and guarantees safe data compression. The experiment outcomes demonstrate better compression ratios but have limitations in the GAN model overfitting certain data distributions. Khan et al. [31] have discussed serverless consortium networks and blockchain hyperledger's application to fog and edge computing. It suggests a serverless edge-based distributed outsourced compute architecture supported by blockchain and Hyperledger Sawtooth (BHLS), providing strong data security, provenance, transparency, and privacy protection. However, using blockchain technology results in higher communication and processing expenses. Khan et al. [32] have suggested a cooperative method for fog node management that uses the blockchain hyperledger architecture and the B-Drone evolutionary algorithm (BHLBE). This allows for the gathering, scheduling, processing, administration, optimizing, and preserving of data using drones in a secure node. The results demonstrate storage increased by 73.11% while computation costs decreased by 12.03% but faced challenges in handling large-scale images.

Khan et al. [33] have introduced a secure hyper ledger sawtooth-enabled architecture (SHSA), provides pseudo-chain codes and consensus protocols for seamless transactions, and examines the implementation issues of blockchain-enabling industrial Internet of things (IIoT). The multiple proof-of-work examined and replicated the information flow between linked IIoT devices by limiting the use of resources, but it has scalability issues. Khan et al. [34] have developed a Particle Swam Optimisation and Artificial Neural

Networks (PSANN) based machine learning intelligence system for load balancing in telecommunications. The system analyses obstacles to 5G and other next-generation intercommunication technologies while automating transactional load allocation. Automation of transactional load distribution improves reliability. The drawback is strong security measures are required to secure the data from breaches. Khan et al. [35] have optimized data transmission for smart cities through a secure blockchain distributed consortium network using partial swam optimization (DCNPS). It employs NuCypher proxy re-encryption-enabled value encryption for neighborhood encryption, secure transmission, and Artificial Neural Networks (ANNs) to optimize record administration and preservation to tackle smart city data delivery categorization difficulties. A thorough security assessment is required.

Mehmood et al. [36] have investigated permissionless public, private, and consortium chains emphasizing distributed real-time applications using blockchain systems. Using optimization and Byzantine Fault Tolerance, a lightweight Plenum consensus mechanism for consortium blockchain (LPCCB) is introduced. Simulations demonstrate that BLPCA can guarantee node scalability while managing massively distributed traffic, but it has limitations in complexity. Khan et al. [37] have developed a lightweight consensus based on Proof-of-Elapsed Time (LPET) and examined permissioned private chains' advantages. It enhances participant identity, mining privileges, block construction, and transaction verification. System scalability is increased, and the lightweight architecture decreases multi-node efficiency costs. However, large-scale multi-transaction processing still has trouble addressing enormous computing needs.

Table 1 Summary of literature review

References	Method	Merits	Demerits
[25]	CoAP	It has scored a high throughput ratio for data sharing	It has recorded high latency to deliver the message
[26]	ASE	But Encryption and Decryption are processed within a short duration	Here, the data originality is not verified. For the verification process, additional features were required
[27]	identity-based blockchain	Here, the saved data is verified based on the user's credentials	Hence, the decryption process on the other end is not possible
[28]	Hybrid ML with blockchain	It applies to all applications; different data formats are acceptable for this model.	Processing the crypto model is problematic because it accepts redundant and inconsistent data.
[29]	Tensor decouple blockchain	It can reduce the duplicated data. Hence, the cloud space requirement was minimized.	The data integrity verification process is not performed.
[30]	FLGAN	It removes adversarial loss and demonstrates a better compression ratio	Has limitations in overfitting to certain data distribution
[31]	BHLS	This technique addresses multi-execution issues, boosts productivity, and reduces cloud storage usage.	Increases the cost of computing and communication
[32]	BHLBE	Increases the storage by reducing the computation cost	Handling massive picture sizes via a dispersed network is a difficult issue.
[33]	SHSA	An effective use of resources is provided.	It faces limitations in scalability.
[34]	PSANN	Automation of transactional load distribution improves reliability	Requires strong security against intrusions
[35]	DCNPS	It employs secure transmission and handles different data types	It is necessary to thoroughly evaluate the security and privacy assurances on a large scale.
[36]	LPCAB	It can ensure node scalability while handling widely dispersed traffic.	The use of a heterogeneous multithreading approach entails complexity.
[37]	LPET	System scalability is increased, and multi-node efficiency costs are decreased.	Struggle to handle large-scale multi-transaction processing requirements.

In every literature in Table 1, a few limitations were addressed, but still, a few drawbacks were not addressed due to the restrictions of features. Several studies have explained that verification is not done, so the data integrity parameter confidential rate is not measured. The main motive of this study is to introduce homomorphism intelligent blockchain to the healthcare domain.

3. Proposed methodology

A novel Transformer Neural Data Encryption Blockchain (TNDEB) was introduced in this study to safeguard medical records. In addition, the implemented novel blockchain is validated by testing it with the IoMT database. Primarily, the database was trained, and the malicious activities were neglected. Consequently, the blockchain functioning process was activated to secure third-party information. Simultaneously, the originality of the data is checked by performing the homomorphism concept from the encrypted data.

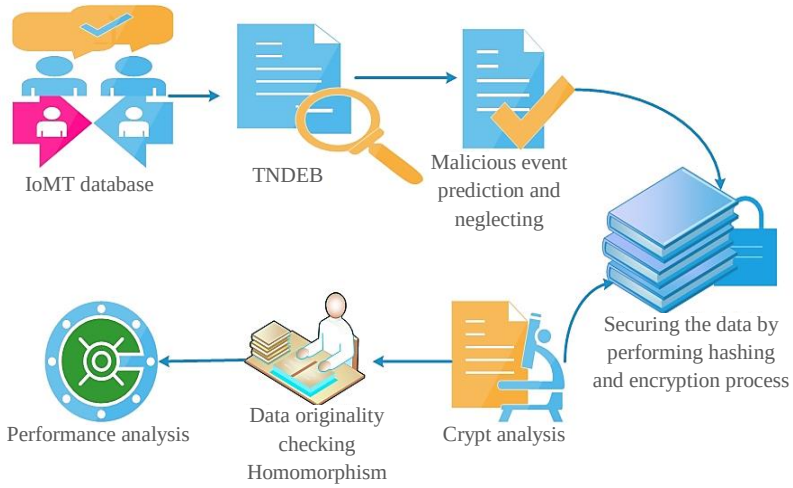

Figure 1 Proposed architecture

Finally, the crypt analysis has been performed by launching the brute force attack. Subsequently, the chief parameters such as Decryption and Encryption time, confidential rate, error rate, and execution time were measured and compared with other traditional approaches. The proposed architecture process is mentioned in Figure 1.

3.1 Process of TNDEB model

The presented TNDEB mechanism combined the functions of the transformer neural network [38] and the Data Encryption standard algorithm [39]. The proposed security mechanism is processed by the dataset collected from the medical cloud, which includes the patient's data from certain hospitals. The data initialization process was followed based on the transformer neural network's function, which is explained in Eqn. (1).

$$I(D_c) = \sum_{i=1}^{n} d_i \tag{1}$$

Here I indicate the data initialization functions D_c represent the medical data collected from the IoT cloud, n define the number of data, and d_i denote the original input data.

3.1.1 Malicious event prediction and neglecting

The initialized data are trained to the transformer model to trace the malicious activities present in the data and then neglected. The malicious event tracking and neglecting function is explained in Eqns. (2) and (3).

$$P_{ME} = \lambda(d_b, d_m) \times D_c(d_1, d_2, \ldots d_n) \tag{2}$$

$$N_{ME} = D_c - \lambda(d_m) \tag{3}$$

Here malicious prediction function is defined as P_{ME}, λ is the malicious event tracing variable, d_m are the malicious features d_b represent the benign features N_{ME} indicating the malicious event elimination function.

3.1.2 Hashing

After the malicious event detection and elimination process, the original benign data is sent to the hashing phase. In this phase, the hash values of each original data set are computed and named as hash 1 value. The hash value computation function is explained in Eqn. (4).

$$h_1(D_c) = d_i \bmod p \tag{4}$$

Here $h_1(D_c)$ represents the Hash 1 value of the original data and p denoted the prime number. The hash 1 value of the original data is computed and stored in the blockchain architecture through this function.

3.1.3 Encryption

The hash value calculated data are then encrypted using the principle of the DES algorithm. It is a commonly used encryption algorithm that encrypts data in groups of 64 bits. This algorithm uses a similar key for Decryption and Encryption; the length of the key is 48 bits, and sub-keys are created for each group. Primarily, the key is generated utilizing the document number and variables to encrypt the data. The key generation function is expressed in Eqn. (5).

$$K^e = a^f \bmod b \tag{5}$$

Where, K^e express the generated encryption key, a and b denotes the public variables, f indicates file number. The data is encrypted using the generated encryption key. In the DES, the plain text is split into two parts: left (L) and right (R), using the permutation function, and further, the encryption function is explained in Eqn. (6).

$$C_i = \begin{cases} L_g = R_{g-1} \\ R_g = L_{g-1} \oplus f(R_{g-1}, K^e{}_g) \end{cases} \quad (6)$$

Here C_i represented, the encrypted cipher data g denotes the number of groups f is the DES function and $\oplus$ defines the XOR function. Thus, the data are encrypted using the DES functions and entered into the Homomorphism to check the data integrity.

3.1.4 Homomorphism

To perform the homomorphism function, the hash values of the encrypted data should be computed. The hash value of the encrypted data was named the hash 2 value. It is computed by the function detailed in Eqn. (7).

$$h_2(D_c) = C_i \bmod p \quad (7)$$

The hash 2 value computation variable is defined as $h_2(D_c)$. After the hash two value calculation, the homomorphism function matches the hash 2 and hash one already stored in the blockchain. The system shows the specific data as "data attacked" if the hash values do not. The homomorphism condition is explained in Eqn. (8).

$$H = \begin{cases} if(h_1 = h_2) & data\ not\ attacked \\ if(h_1 \neq h_2) & data\ attacked \end{cases} \quad (8)$$

The system allows the user to access only when the hash values are matched by sharing the key for Decryption. Otherwise, the system will not allow the user to access it.

3.1.5 Decryption

The reverse process of Encryption is termed Decryption. The system sends the key to the user after the hash value validation. The encrypted cipher files are then decrypted to get the original data in the decryption process. The decryption process is given in Eqn. (9).

$$\delta(D_c) = d_i = \begin{cases} R_g = L_{g-1} \\ L_g = R_{g-1} \oplus f(L_{g-1}, K^s{}_g) \end{cases} \quad (9)$$

Where δ denotes the decryption function, which is the original data, and K^s is the system-shared secret key. At the decryption phase, the encrypted data were decrypted by applying the key in reverse order of the Encryption.

The processing functions are expressions of the TNDEB model and are explained in pseudo-code format in Algorithm 1. The Python code was implemented based on this algorithm. Additionally, the flow diagram of the TNDEB process is expressed in Figure 2.

Algorithm 1. TNDEB

Start
{
$input \rightarrow cloud\ medical\ data$
$D_c \rightarrow d_1, d_2, d_3 \ldots\ldots d_n$
//Iot Medical Data Are Initialized
Malicious Event Prediction ()
{
int $P_{ME}, \lambda, d_b, d_m$
// Malicious Data Detecting Variables Are Initialized
$P_{ME} \rightarrow \lambda(d_b, d_m)$
//The Malicious Event Of The Input Data Is Predicted
$N_{ME} \rightarrow D_c - \lambda(d_m)$
// The Malicious Data Are Eliminated From The Model
}
Hashing ()
{
int h_1, p
$h_1 \rightarrow d_i \bmod p$
//The Hash 1 Value Of The Original Data Are Calculated And Stored
}
Encryption ()
{
intK^e, C_i
//The Encryption Variables Are Initialized
The Key K^e Is Generated Using The Document Number And Public Variables
$C_i = K^e \oplus d_i$
//The Original Data Are Converted Into Cipher Data Using DES Encryption Key

```
        }
        Homomorphism ()
        {
                h_2 → C_i mod p
                //Hash 2 Value Is Calculated
                if (h_1 ≠ h_2)
                {
                        Display Data Attacked
                }Else
                {
                        Not Attacked
                }
        }
        Decryption ()
        {
                d_i = K^e ⊕ C_i
                //The Benign Data Is Decrypted Using Shared Key
        }
}
End
```

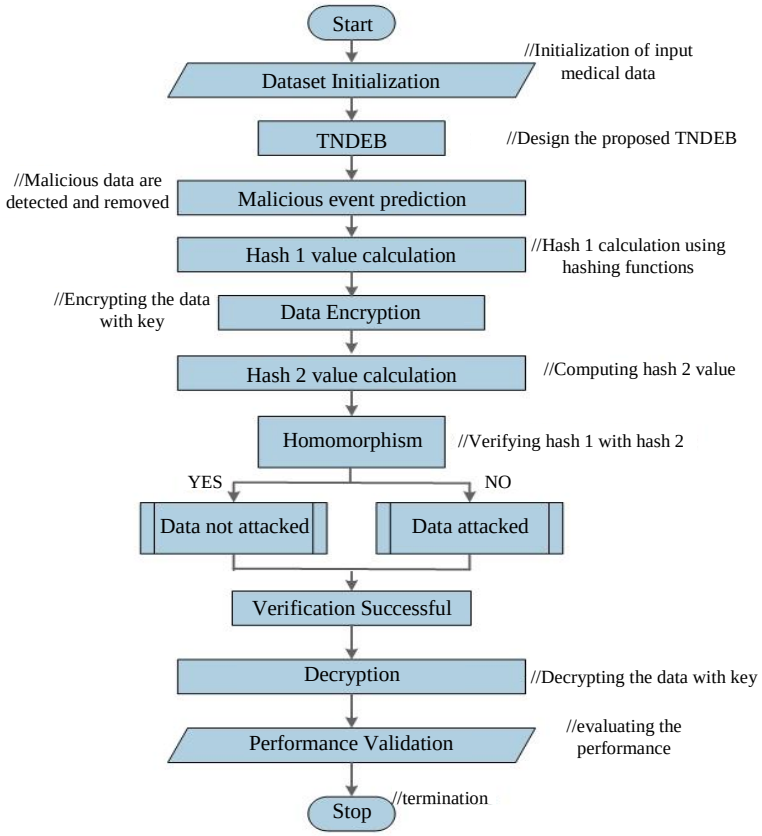

Figure 2 Flowchart TNDEB

4. Results and discussion

The TNDEB architecture is designed to secure cloud medical information from various attacks. This method integrated the features of the transformer neural structure and DES algorithm. The medical data is collected from the IoT cloud and processed to test the presented model. The other requirements for designing the presented model are tabulated in Table 2.

Table 2 Parameter requirements

Execution Parameters	
Parameters	**Details**
OS	Windows 10
Platform	Python
Version	3.10
Database	Disease Symptom Data
Launched Attack	Brute force

The malicious event in the data is traced and removed through the transformer network, and the DES process encrypts data. To perform the Homomorphism, the hash values of the original and encrypted data are matched and verified. The verified data is sent to the decryption stage. Also, the system is checked by launching a brute force attack.

4.1 Case study

In this section, the case study was explained to understand the functions of the TNDEB model. Primarily, the medical data was gathered and entered into the proposed framework. The number of samples collected is 4920. Further, the proposed TNDEB framework is modeled in the Python environment using the required parameters. The collected dataset includes the various diseases and their symptoms seen in the patients. These data are first imported to the transformer network to identify and eliminate the malware-injected data from the collected dataset. After the malware removal, the hash 1 point is computed and encrypted using the DES function. Then, hash two is calculated for the encrypted data, and the homomorphism process is carried out by matching the two hash values. If the values are reached, the decryption process is performed. Otherwise, the system displays as data is attacked. In addition to checking the system's efficiency, the cryptanalysis process is carried out by launching a brute-force attack.

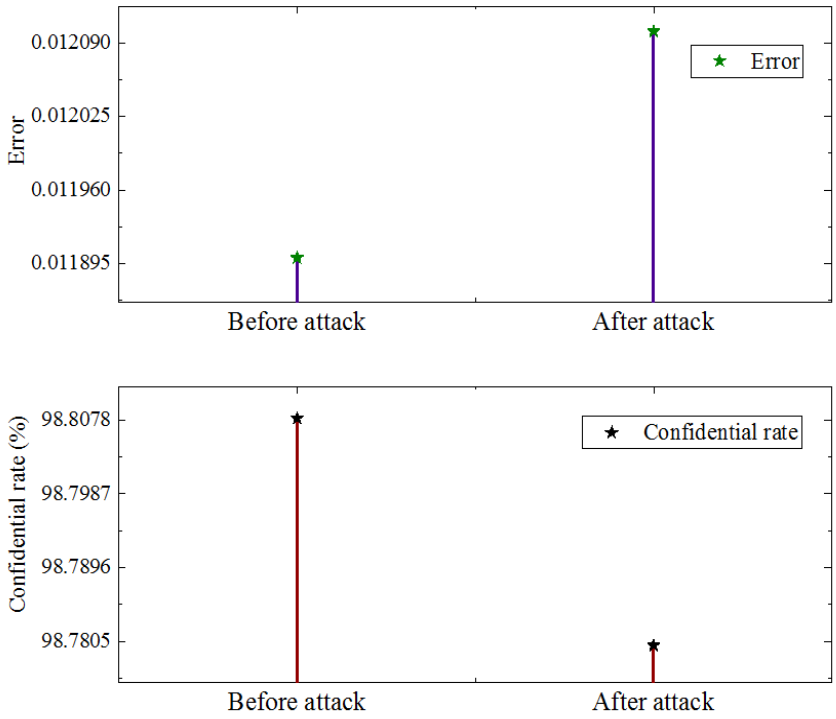

Figure 3 Performance before and after an attack

The error rate and confidential rate were calculated before and after an attack. It is described in Figure 3. The confidentiality and error values of the TNDEB system before launching the brute force attack are 98.808% and 0.0119. After inserting the brute force attack, the system's confidentiality percentage and error value change to 98.780% and 0.0121, respectively.

4.2 Comparative analysis

The proposed TNDEB model is designed and implemented in the Python environment. The performance of TNDEB was evaluated in terms of Decryption, execution and Encryption time, confidentiality, and error rate. The resulting values are then compared with prevailing blockchain cryptography mechanisms such as Elliptical Curve Cryptography (ECC) [40], Rivest-Shamir-Adleman (RSA) [40], Ring Hash Elliptical Curve Cryptography (RHECC) [40], Belief Network based Diffie Hellman (BNDH) [41] and Modified Blow Fish (MBF) [42] to validate the improvement of the proposed mechanism.

4.2.1 Encryption and decryption time

The framework's time to convert the initial data into cipher data is validated as encryption time. The key generating time is included in the encryption time. While the time of the restoration process of the initial data from the cipher data is computed as decryption time. It is generally calculated after the encryption and decryption process. The main motive for calculating the decryption and encryption time is to show the system's efficiency during the security process.

The comparison of the encryption time of the TNDEB scheme with various prevailing cryptography models is shown as a graphical representation in Figure 4. The ECC algorithm scored an encryption time of 500ms, the RSA algorithm completed the encryption process in 470ms, RHECC resulted in 300ms and BNDH process scored 3.55ms for the encryption time. At the same time, the proposed TNDEB model recorded the encryption time as 1.01ms. Compared to the existing approaches, the proposed achieved much less encryption time. This less encryption time indicates the speed of the encryption process of the TNDEB architecture is higher than that of the other existing approaches.

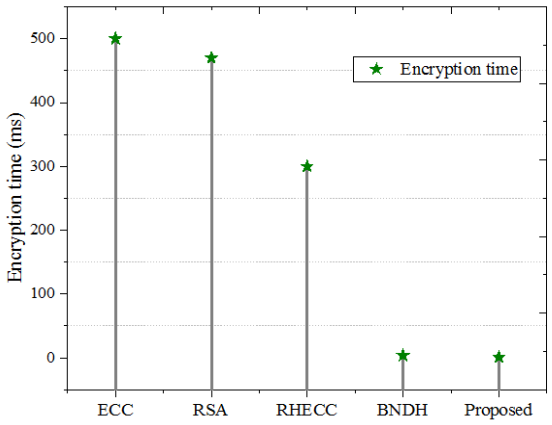

Figure 4 Encryption time evaluation

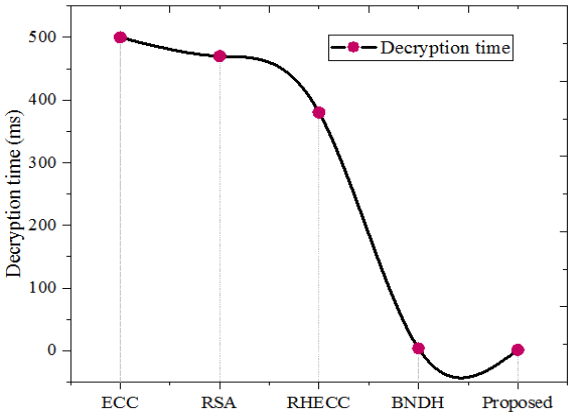

Figure 5 Decryption time evaluation

Similarly, the duration of the decryption process of the proposed TNDEB model is evaluated and competes with the other current blockchain models, as shown in Figure 5. The ECC schema validated the decryption time as 500ms, RSA result 470ms, RHECC recorded 380ms, and BNDH scored the encrypting time of 3.6ms. However, the proposed TNDEB model validated the decryption time of 1.26ms which is lower than all other compared prevailing schemas. Large files require excess time to decrypt and encrypt. Therefore, the TNDEB strategy hashing process with Encryption reduced the Encryption and Decryption.

4.2.2 Confidential rate

The data rate the proposed TNDEB model safeguarded is evaluated as the confidentiality rate.

The values of the existing and proposed encryption scheme's confidential rate are compared in Figure 6. The confidentiality percentage of the ECC algorithm is 91%, RSA scored 93.5%, RHECC achieved 98%, and BNDH framework scored 95% of the confidential rate. Further, the proposed model showed a confidentiality rate of 98.8%. Compared to the other related models, the confidentiality rate of the proposed is increased, which shows the security improvement in the healthcare system. In the proposed system, the confidentiality of the medical records is checked with and without attack conditions. Confidentiality is maintained even in the presence of the attack, which shows the security efficiency of the presented model.

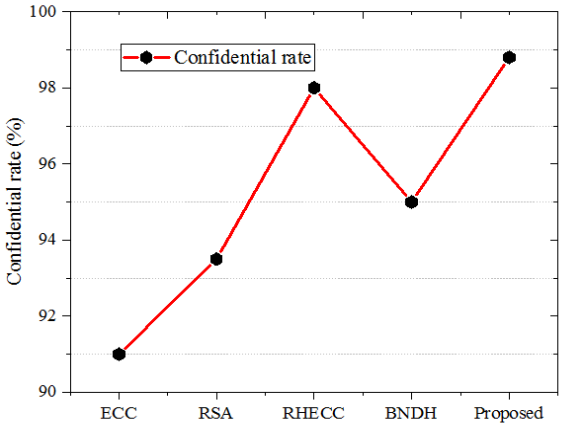

Figure 6 Confidential rate

4.2.3 Error rate

The error rate is calculated to ensure whether the data that arrived is the data the user or recipient sent. The error rate of the proposed method was calculated for two conditions: before and after an attack. Then, the average error rate of both conditions is compared with the existing cryptography models for evaluation of improvement.

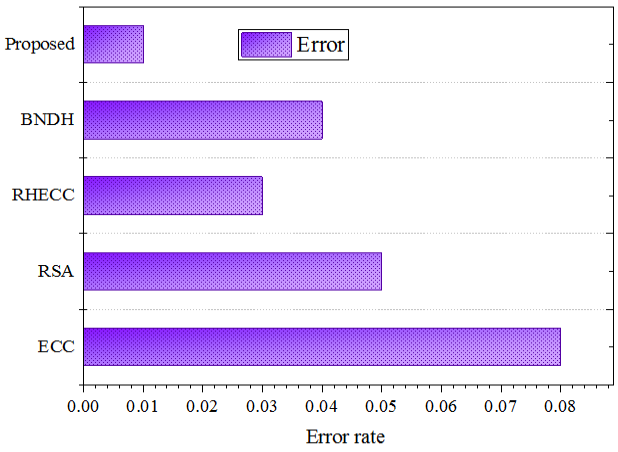

Figure 7 Error comparison

Table 3 Overall performance

Methods	Decryption time (ms)	Encryption time (ms)	Confidential rate (%)	Error rate
ECC	500	500	91	0.08
RSA	470	470	93.5	0.05
RHECC	380	300	98	0.03
BNDH	3.6	3.55	95	0.04
Proposed	1.26	1.01	98.8	0.01

Moreover, a comparative error rate analysis is performed to check the similarity between encrypted and decrypted data. The comparison is shown in Figure 7. The proposed TNDEB framework attained an error rate of 0.01. The error values of other related models, such as ECC, RSA, RHECC, and BNDH, are 0.08, 0.05, 0.03, and 0.04. The proposed model achieved a very low error rate compared to these values. The overall comparison of the error value, confidentiality, Decryption, and encryption time is mentioned in Table 3.

4.2.4 Execution time

The time the proposed TNDEB system takes to complete the entire security process of the healthcare system is calculated as execution time or run time. The execution time is calculated using the expression given in Eqn. (10).

$$X_t = \left(\frac{E_t + D_t}{M_t}\right) \tag{10}$$

Here X_t denotes execution time, E_t defines encryption time, D_t represented as decryption time, and M_t is the maximum time allocated for the process.

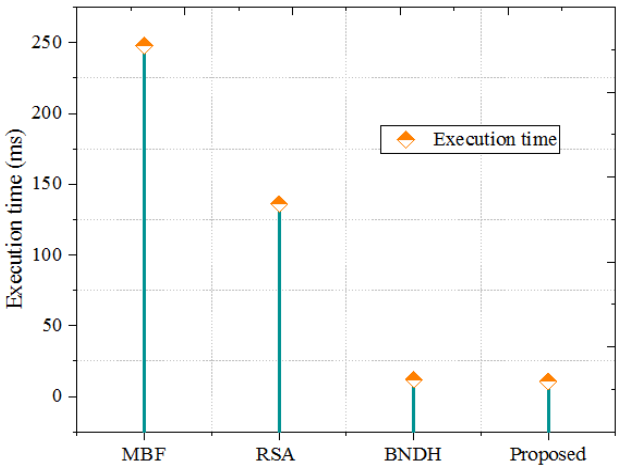

Figure 8 Execution time

The execution time includes the duration of hash value calculation, Encryption, Homomorphism, and Decryption time. The comparison of TNDEB's total execution time with existing models is shown in Figure 8. Here, the execution time is compared with existing works such as MBF, RSA, and BNDH. The run time of the MBF is 248ms, RSA is 136ms, and BNDH is 12ms. The total execution of the TNDEB framework is only 10ms, which is lower than the other existing models. The values of the execution time are arranged in Table 4.

Table 4 Execution time comparison

Method	Execution time (ms)
MBF	248
RSA	136
BNDH	12
Proposed	10.64

4.3 Discussion

In this section, the overall parameters of the TNDEB model are discussed. The system acquired an encryption time of 1.010ms and a decryption time of 1.2607ms. Compared to the other current models, the presented mechanism has shown lesser Encryption and decryption time, as verified by the comparative analysis. The system used a transformer network for attack detection and elimination. The network processes large data in less time, giving all data equal importance. Also, the utilization of the DES algorithm completes the Encryption and Decryption in a short time. Also, for accurate verification, the homomorphism function is performed using the hash two and stored hash one values. To offer further justification, the state of approach in Table 5 is executed in the same platform and compared with the present novel proposed model. In every performance metrics case, the proposed approach received the finest outcome, revealing the proposed system's robustness in securing medical records.

Table 5 Performance of state-of-the-art models

References	Decryption time (ms)	Encryption time (ms)	Confidential rate (%)	Error rate	Execution time (ms)
CoAP [25]	10	10	78	9	450
ASE [26]	9	8	85	10	370
identity-based blockchain [27]	79	76	64	18	320
Hybrid ML with blockchain [28]	67	66.8	67	26	210
Tensor decouple blockchain [29]	87	87	59	22	178
FLGAN [30]	75	74.2	87	19	152
BHLS [31]	82	80	72	30	213
BHLBE [32]	40	41	79	25	80
SHSA [33]	52	50	90	20	89
PSANN [34]	13	16	25	15	62
DCNPS [35]	27	26.6	70	13	108
LPCAB [36]	33	31	84	36	158
LPET [37]	44	43	88	33	23
Proposed	1.26	1.01	98.8	0.01	10.64

When compared to the most advanced methods for protecting medical records, Table 5 shows the effective performance of the proposed model. The proposed model outperforms the existing approaches by achieving the highest confidentiality rate of 98.8% and the lowest error rate of 0.01%. It shows that the model has robust data security, and encryption, making it difficult for any attackers to capture or decode important data. This ensures that the confidentiality of the information remains intact, even under attempted breaches or vulnerabilities, and demonstrates that it can effectively safeguard sensitive data. Furthermore, compared to the other models, the encryption and decryption speeds of 1.26 ms and 1.01 ms, respectively, are much quicker, guaranteeing effective data processing. Moreover, the overall execution time of 10.64 ms is notably lower, highlighting the proposed approach’s efficiency. These results emphasize the robustness of the proposed system in securing medical records, offering a balance of high security and low latency, making it an optimal solution in healthcare environments.

Finally, the data was processed to check the system's ability by launching the brute force attack in the proposed model. The confidential and error rates were calculated for before and after attack conditions. The overall performance assessment of the presented TNDEB model is tabulated in Table 6.

Table 6 Performance Assessment

Metrics	Performance
Decryption Time (ms)	1.2607ms
Encryption Time (ms)	1.010ms
Confidential rate (Before attack)	98.808%
Error Rate (Before Attack)	0.0119
Confidential Rate (After Attack)	98.780%
Error Rate (After Attack)	0.0121
Execution Time (ms)	10.643ms

5. Conclusion

In the IoT healthcare system, security is the major concern for data sharing. Therefore, a novel TNDEB model is introduced in this article to provide security to the healthcare system. The collected IoMT database processes the system. Initially, malicious events present in the collected dataset were identified and removed. Further, the value of hash one is computed. Moreover, the data is encrypted, and the hash two value is calculated. The hash values are matched to verify the data. The verified data is then sent to the user with a private key to restore the initial data from the encrypted one. In addition, the system is checked by injecting the brute force attack. The model is implemented in Python software, and results are compared with prevailing techniques. The encryption and decryption time of the TNDEB model is 1.010ms and 1.260ms, and the total execution time is 10.643ms. It is reduced from the existing models. Also, the confidential and error rate is measured as 98.8% and 0.0119 before the attack and 98.78% and 0.0121 after the attack. The confidential rate has been increased, and the error rate has been reduced. Thus the presented model improves the reliability of the healthcare system and prevents attacks. However, if the medical records are in an increased manner, then it causes blockchain storage limitations. In the future, automatically concatenating the blockchain based on medical records needs will help tackle storage limitation issues.

6. References

[1] Verma G, Kanrar S. Secure document sharing model based on blockchain technology and attribute-based Encryption. Multimed Tools Appl. 2024;83:16377-94.

[2] Kiania K, Jameii SM, Rahmani AM. Blockchain-based privacy and security preserving in electronic health: a systematic review. Multimed Tools Appl. 2023;82:28493-519.

[3] Mahajan HB, Junnarkar AA. Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing. Multimed Tools Appl. 2023;82:44335-58.

[4] Verma P, Mishra R. IoT based smart remote health monitoring system. 2020 International Conference on Electrical and Electronics Engineering (ICE3); 2020 Feb 14-15; Gorakhpur, India. USA: IEEE; 2020. p. 467-70.

[5] Jeddi Z, Bohr A. Chapter 9 - Remote patient monitoring using artificial intelligence. In: Bohr A, Memarzadeh K, editors. Artificial Intelligence in Healthcare. London: Academic Press; 2020. p. 203-34.

[6] Tscholl DW, Rössler J, Said S, Kaserer A, Spahn DR, Nöthiger CB. Situation awareness-oriented patient monitoring with visual patient technology: a qualitative review of the primary research. Sensors (Basel). 2020;20(7):2112.

[7] Moghadas E, Rezazadeh J, Farahbakhsh R. An IoT patient monitoring based on fog computing and data mining: cardiac arrhythmia usecase. Internet of Things. 2020;11:100251.

[8] Adeniyi EA, Ogundokun RO, Awotunde JB. IoMT-based wearable body sensors network healthcare monitoring system. In: Marques G, Bhoi AK, de Albuquerque VHC, Hareesha KH, editors. IoT in healthcare and ambient assisted living. Singapore: Springer; 2021. p. 103-21.

[9] Chander B, Kumaravelan. Chapter 9 - Wearable sensor networks for patient health monitoring: challenges, applications, future directions, and acoustic sensor challenges. In: Balas VE, Pal S, editors. Healthcare Paradigms in the Internet of Things Ecosystem. London: Academic Press; 2021. p. 189-221.

[10] Abugabah A, Nizamuddin N, Alzubi AA. Decentralized telemedicine framework for a smart healthcare ecosystem. IEEE Access. 2020;8:166575-88.

[11] Bhatt V, Chakraborty S. Real-time healthcare monitoring using smart systems: a step towards healthcare service orchestration smart systems for futuristic healthcare. 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS); 2021 Mar 25-27; Coimbatore, India. USA: IEEE; 2021. p. 772-7.

[12] Anikwe CV, Nweke HF, Ikegwu AC, Egwuonwu CA, Onu FU, Alo UR, et al. Mobile and wearable sensors for data-driven health monitoring system: state-of-the-art and future prospect. Expert Syst Appl. 2022;202:117362.

[13] Comito C, Falcone D, Forestiero A. Current trends and practices in smart health monitoring and clinical decision support. 2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM); 2020 Dec 16-19; Seoul, South Korea. USA: IEEE; 2020. p. 2577-84.

[14] Al-Humairi SNS, Hajamydeen AI. IoT-Based healthcare monitoring practices during Covid-19: prospects and approaches. In: Mehra PS, Goyal LM, Dagur A, Dwivedi AK, editors. Healthcare Systems and Health Informatics. Boca Raton: CRC Press; 2022. p. 163-85.

[15] Philip NY, Rodrigues JJPC, Wang H, Fong SJ, Chen J. Internet of things for in-home health monitoring systems: current advances, challenges and future directions. IEEE J Sel Areas Commun. 2021;39(2):300-10.

[16] Abdulmalek S, Nasir A, Jabbar WA, Almuhaya MAM, Bairagi AK, Khan MAM, et al. IoT-Based healthcare-monitoring system towards improving quality of life: a review. Healthcare. 2022;10(10):1993.

[17] Poongodi M, Sharma A, Hamdi M, Maode M, Chilamkurti N. Smart healthcare in smart cities: wireless patient monitoring system using IoT. J Supercomput. 2021;77:12230-55.

[18] Alshamrani M. IoT and artificial intelligence implementations for remote healthcare monitoring systems: a survey. J King Saud Univ Comput Inf Sci. 2022;34(8):4687-701.

[19] Zahid A, Poulsen JK, Sharma R, Wingreen SC. A systematic review of emerging information technologies for sustainable data-centric healthcare. Int J Med Inform. 2021;149:104420.

[20] Mourtzis D, Angelopoulos J, Panopoulos N, Kardamakis D. A smart IoT platform for oncology patient diagnosis based on AI: towards the human digital twin. Procedia CIRP. 2021;104:1686-91.

[21] Ranjan AK, Kumar P. Ensuring the privacy and security of IoT-medical data: a hybrid deep learning-based encryption and blockchain-enabled transmission. Multimed Tools Appl. 2024;83:79067-92.

[22] Sudhakar K, Mahaveerakannan R. Prospects of deep learning with blockchain for securing the digital radiography data in smart healthcare. 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT); 2024 Mar 15-16; Bengaluru, India. USA: IEEE; 2024. p. 1-7.

[23] Velmurugan S, Prakash M, Neelakandan S, Martinson EO. An efficient secure sharing of electronic health records using IoT-based hyperledger blockchain. Int J Intell Syst. 2024;2024:1-16.

[24] Liu X, Shah R, Shandilya A, Shah M, Pandya A. A systematic study on integrating blockchain in healthcare for electronic health record management and tracking medical supplies. J Clean Prod. 2024;447:141371.
[25] Jamil F, Ahmad S, Iqbal N, Kim DH. Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. Sensors. 2020;20(8):2195.
[26] Mamta, Gupta BB, Li KC, Leung VCM, Psannis KE, Yamaguchi S. Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system. IEEE/CAA J Autom Sin. 2021;8(12):1877-90.
[27] Saidi H, Labraoui N, Ari AAA, Maglaras LA, Emati JHM. DSMAC: Privacy-aware decentralized self-management of data access control based on blockchain for health data. IEEE Access. 2022;10:101011-28.
[28] Khan MI, Jan MA, Muhammad Y, Do DT, Rehman AU, Mavromoustakis CX, et al. Tracking vital signs of a patient using channel state information and machine learning for a smart healthcare system. Neural Comput Appl. 2021:1-15.
[29] Aujla GS, Jindal A. A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring. IEEE J Sel Areas Commun. 2021;39(2):491-9.
[30] Khan AA, Laghari AA, Elmannai H, Shaikh AA, Bourouis S, Hadjouni M, et al. GAN-IoTVS: a novel internet of multimedia things-enabled video streaming compression model Using GAN and Fuzzy logic. IEEE Sens J. 2023;23(23):29434-41.
[31] Khan AA, Laghari AA, Baqasah AM, Alroobaea R, Almadhor A, Sampedro GA, et al. Blockchain-enabled infrastructural security solution for serverless consortium fog and edge computing. PeerJ Comput Sci. 2024;10:e1933.
[32] Khan AA, Laghari AA, Gadekallu TR, Shaikh ZA, Javed AR, Rashid M, et al. A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. Comput Electr Eng. 2022;102:108234.
[33] Khan AA, Laghari AA, Shaikh ZA, Dacko-Pikiewicz Z, Kot S. Internet of Things (IoT) security with blockchain technology: a state-of-the-art review. IEEE Access. 2022;10:122679-95.
[34] Khan AA, Laghari AA, Baqasah AM, Alroobaea R, Gadekallu TR, Sampedro GA, et al. ORAN-B5G: a next generation open radio access network architecture with machine learning for beyond 5G in industrial 5.0. IEEE Trans Green Commun Netw. 2024;8(3):1026-36.
[35] Khan AA, Laghari AA, Alroobaea R, Baqasah AM, Alsafyani M, Bacarra R, et al. Secure remote sensing data with blockchain distributed ledger technology: a solution for smart cities. IEEE Access. 2024;12:69383-96.
[36] Mehmood F, Khan AA, Wang H, Karim S, Khalid U, Zhao F. BLPCA-ledger: a lightweight plenum consensus protocols for consortium blockchain based on the hyperledger indy. Comput Stand Interfaces. 2025;91:103876.
[37] Khan AA, Dhabi S, Yang J, Alhakami W, Bourouis S, Yee PL. B-LPoET: a middleware lightweight Proof-of-Elapsed Time (PoET) for efficient distributed transaction execution and security on Blockchain using multithreading technology. Comput Electr Eng. 2024;118:109343.
[38] Natarajan A, Chang Y, Mariani S, Rahman A, Boverman G, Vij S, et al. A wide and deep transformer neural network for 12-lead ECG classification. 2020 Computing in Cardiology; 2020 Sep 13-16; Rimini, Italy. USA: IEEE; 2020. p. 1-4.
[39] Reyad O, Mansour HM, Heshmat M, Zanaty EA. Key-based enhancement of data encryption standard for text security. 2021 National Computing Colleges Conference (NCCC); 2021 Mar 27-28; Taif, Saudi Arabia. USA: IEEE; 2021. p. 1-6.
[40] Devmane V, Lande BK, Joglekar J, Hiran D. Preserving data security in cloud environment using an adaptive homomorphic blockchain technique. Arab J Sci Eng. 2022;47(8):10381-94.
[41] Goel A, Neduncheliyan S. An intelligent blockchain strategy for decentralized healthcare framework. Peer-to-Peer Netw Appl. 2023;16:846-57.
[42] Adeniyi AE, Misra S, Daniel E, Anthony Bokolo Jr. Computational complexity of modified blowfish cryptographic algorithm on video data. Algorithms. 2022;15(10):373.