ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

Secure IoT-based healthcare multimedia data with deep intelligent blockchain technology

G. M. Karthik
Koneru Lakshmaiah Education Foundation, Guntur 522502, India
K saikumar, Department of ECE, Koneru Lakshmaiah Education Foundation, India-522302,
saikumarkayam4@ieee.org

SK ahammad , Department of ECE, Koneru Lakshmaiah Education Foundation, India-522302,

Abstract
Nowadays, Internet of Things (IoT) based applications are widely used in different sectors because of their high mobility, low cost, and efficiency. However, the wide usage of these applications leads to various security issues. Several security applications exist for protecting multimedia data, but the appropriate confidential range is not met due to the multi-variant features. Hence, the novel hybrid Elman Neural-based Blowfish Blockchain Model has been developed in this article to secure IoT healthcare multimedia data. Here, the Elman network features provided continuous monitoring for predicting malicious events in the trained multimedia data. In addition, the crypto analysis was performed to enhance the confidentiality rate by hiding the raw data from third parties. The presented model was verified using python software. Furthermore, the robustness of the developed model is validated with a crypt analysis by launching attacks. Finally, the outcomes were estimated and compared with the existing techniques in terms of Encryption time, decryption time, execution time, error rate and confidential rate. Here, the evaluation database is the multimedia data, which is high in data size. Henceforth, the performance of the security model for securing multimedia data depends on time

Keywords Blockchain · Healthcare framework · Elman neural network · Blowfish algorithm · Multimedia security ·Internet of Things

1 Introduction
People and their day-to-day activities are interconnected and managed with specific internet technology [1]. This process includes collecting and processing data in different forms based on the application's needs. IoT technology uses sensors and communication devices to collect, share, and process information from various sectors [2]. However,the IoT framework uses centralized system architecture, facing challenges in security, cost, and system capacity

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

[3]. Moreover, server failure affects the entire performance of the system. In the case of an IoT-based healthcare center, the patient's details and electronic health records are stored in the coud server [4]. Initially, a multimedia IoT healthcare dataset was collected from the standard site and imported into the system.

- Consequently, a novel hybrid ENbBBM model with security parameters was designed in the system.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

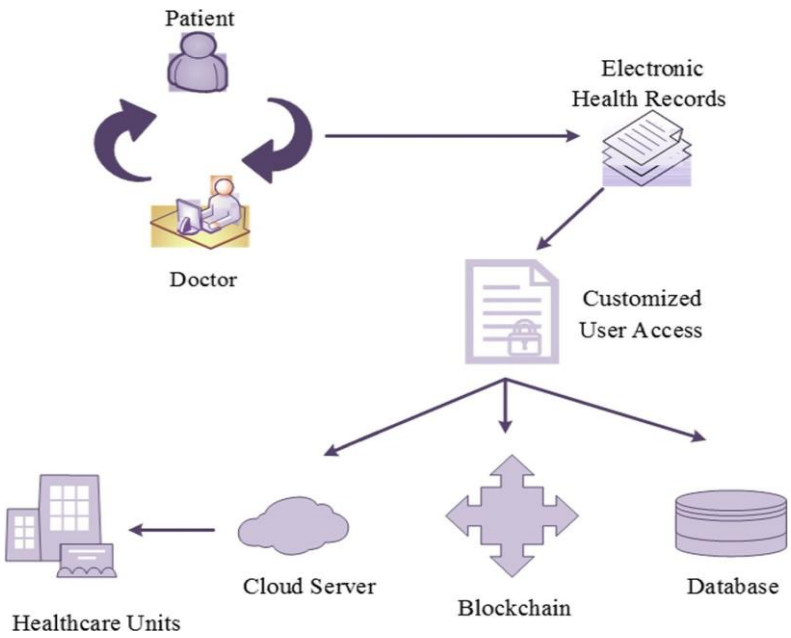


Fig. 1 Blockchain in healthcare management

- Then, a monitoring module was developed in the designed model to detect and neglect the malicious events in the dataset.
- Subsequently, crypto analysis was performed to hide the data from third parties.
- Finally, the security level of the developed model was analyzed with a crypt analysis, and the performances were estimated in two-phase.
- Furthermore, the outcomes of the developed model are validated in a comparative analysis in terms of confi- dential rate, error rate, and execution time.

The presented article is sequenced as follows, the research articles related to the presented work are listed in Sect. 2, the problems in the existing techniques are described in Sect. 3, the presented approach is explained briefly in Sect. 4, the outcomes of the developed model are analyzed in Sect. 5, and the conclusion of the work is mentioned in Sect. 6.

2 Related works

Some of the recent research articles related to the study are described as follows, Over the past

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

decades, IoT applications have been widely used in various fields. This rapid growth leads to several problems like central server overload, privacy, and data security. Thus, blockchain technologies are introduced to build a trustworthy transaction between the sender and the receiver. Therefore, [5] presented a novel IoT framework embedded with the Ethereum blockchain approach to overcome the above demerits. Here, the designed Ethereum blockchain environment is validated by the healthcare data. This developed model is suited for different IoT applications and provides better results. However, it depends on the load distribution between the resources.

The development of electronic devices leads to security and surveillance issues in the private lives of the user. Thus, the present cyber security system aims to secure the users' data from third parties. This efficient cyber security model shares, interact and process the data securely with minimum latency. Hence, [6] developed a decentralized e-healthcare framework, which enables only the user to access their data stored on the server. In this model, several security building blocks are embedded, which provides data integrity and security. But, the cryptographic approach used in this model is complex and difficult to understand.

Recently, it has been noticed that blockchain technologies solve interoperability issues in IoT healthcare frame- works

3 System model with problem statement

Recently, IoT-based applications have been widely used in various sectors because of their high efficiency and advancements, particularly in the medical field. However, this growth of IoT applications gives rise to several

security and privacy issues [7]. Generally, in IoT-based healthcare units, patient-sensed data are stored in the cloud server. Thus, the possibility of data injection and security threats is high. Hence, a blockchain mechanism is intro- duced to overcome these security challenges in IoT appli- cations. Blockchain is a decentralized framework that enhances the confidentiality between the sender and the receiver in a transaction.

Video surveillance is the required smart monitoring system to monitor and update the current public events to the management. However, securing the video surveillance data is the most needed task for maintaining the confi- dential score for the monitoring. Considering this, edge computing is introduced for the IoT-based smart video surveillance system [8]. Here, if any third party is entered, it alerts the control system. However, transaction data is remained public to everyone.

In addition, the cloud assists diagnosis system is implemented for the diabetic retinopathy application for detecting the diabetes types by analyzing the image fea- tures. Here, the retina

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

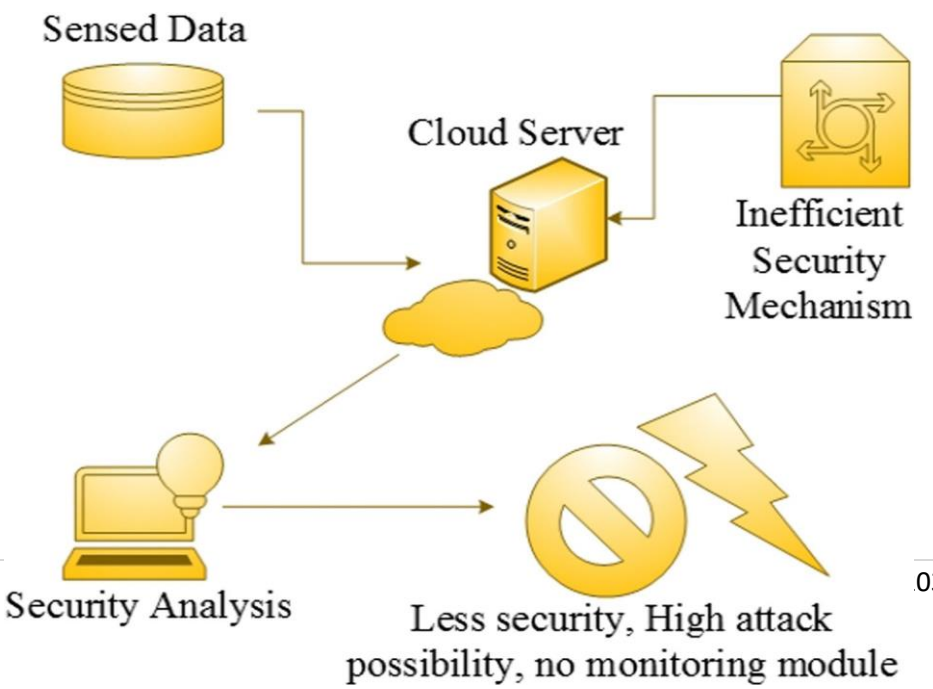
image data was secured at a high confidential rate. But retrieving the data reported more computational time.

Hence, the traditional blockchain technique faces high time costs and computational time challenges. In addition, it lacks in the malicious event detection phases, which makes the system inefficient and provides less security.

Thus, an intelligent blockchain mechanism is required to Further, the encrypted dataset is stored in the cloud server. In addition, the security level of the designed model is validated with a crypt analysis. A brute force attack is launched in the crypt-analysis phase, and system performance is checked. Finally, the outcomes regarding confidential rate, error rate, encryption time, and decryption time are estimated. Moreover, the obtained outcomes are verified by comparing the results of the existing techniques in a comparative analysis. The framework of the developed model is illustrated in Fig. 3.

4 Proposed ENbBBM for healthcare framework

A novel hybrid Elman Neural-based Blowfish Blockchain Mechanism (ENbBBM) was developed to secure the IoT- based healthcare dataset. This presented approach incorporates the attributes (features) of the Elman Neural System and the Blowfish cryptography. Initially, an IoT-based healthcare multimedia dataset was collected from the standard site and imported into the system. The collected multimedia dataset contains sensed health features in image, audio, and video. The presented model includes two important phases: the monitoring phase and the crypto analysis phase. In the monitoring module, the system removes the attacks present in the dataset and provides continuous monitoring of the system. The crypto analysis module encrypts the dataset with a generated key.



ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

Fig. 2 System model and its problem statement

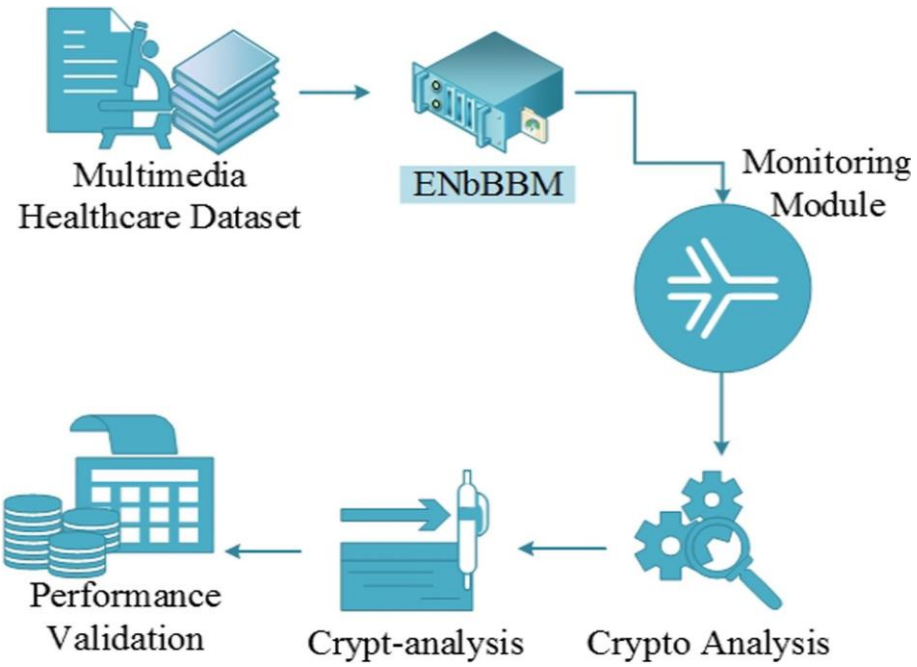


Fig. 3 ENbBBM framework

Thus, the developed model secures the healthcare mul- timedia dataset from security threats (attacks) and provides high data integrity. The flowchart of the designed block- chain model is shown in Fig. 4. Moreover, the step-by-step process of the presented work is in pseudocode format visualized by algorithm 1. In this designed novel ENbBBM, the monitoring process is continuously updated for malicious actions and user misbehaviour. This contin- uous monitoring process has provided stable security for every case and all format data.

5 Result and discussion

A deep neural blockchain mechanism is designed in python software to secure the healthcare dataset from security threats. To verify the presented model, a multimedia IoT- based

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

healthcare dataset was collected from Kaggle. The gathered dataset contains healthcare information in images, audio, and video. Then, a monitoring phase is introduced inthe system to detect and remove malicious events from the dataset. Further, the dataset is encrypted and stored on the server. Moreover, the system's security level is validated with a crypt analysis. Table 1 lists the designation of implementation parameters.

The presented model is executed in the Python software, version 3.10, and the outcomes are estimated as confiden- tial rate, execution time, error rate, and encryption anddecryption time. The designed model estimates the results in two phases, before and after the attack. Furthermore, a comparative assessment was done to validate the perfor- mance of the designed model.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **© 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021**

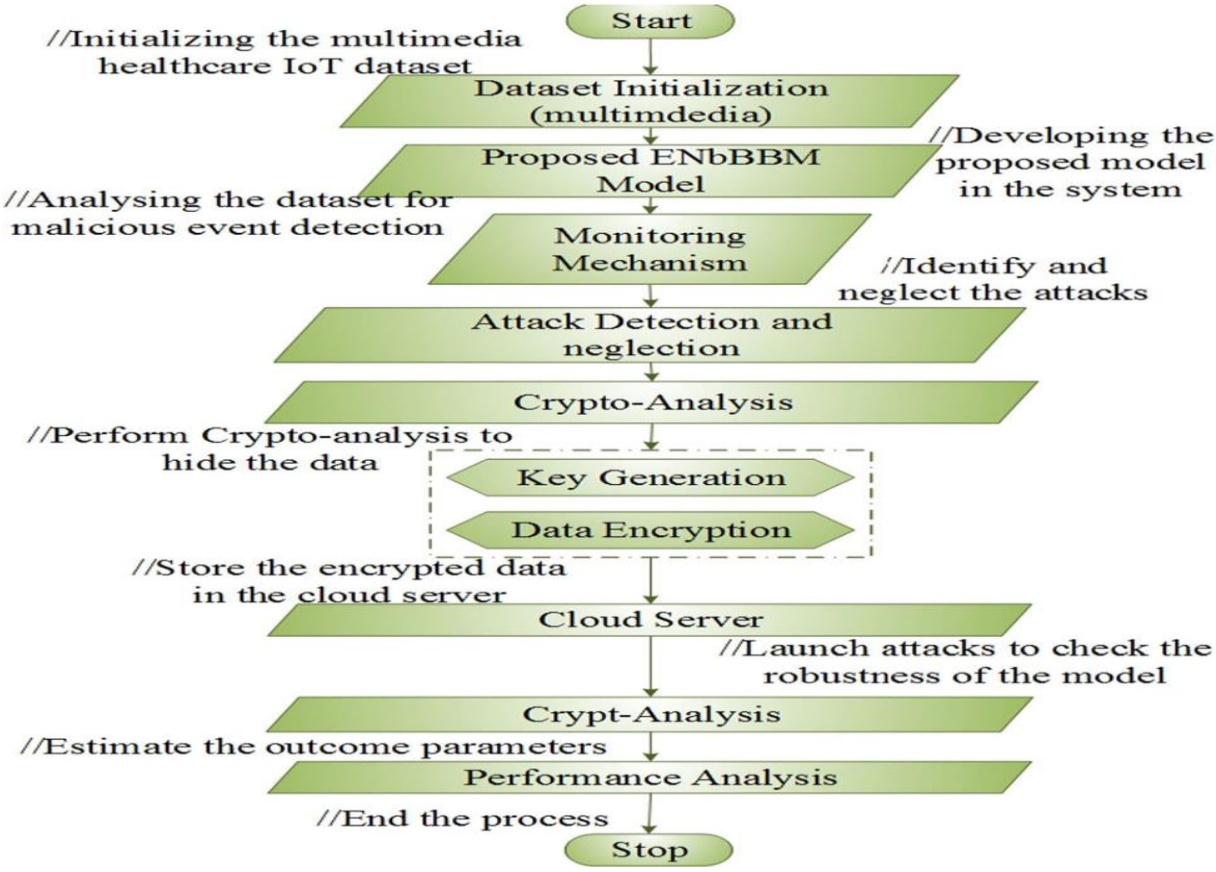
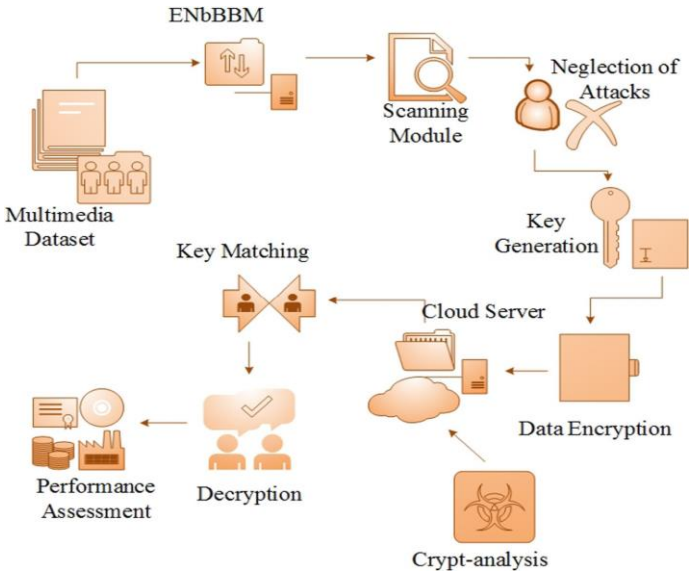


Fig. 4 Flowchart of ENbBBM

are determined for three different classes individually. The encryption time of image, audio and video classes is 3.57ms, 3.89ms, and 4.12ms, respectively. Similarly, the decryption time of the developed model for image, audio, and video class

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021



5.1.1 Encryption and decryption time

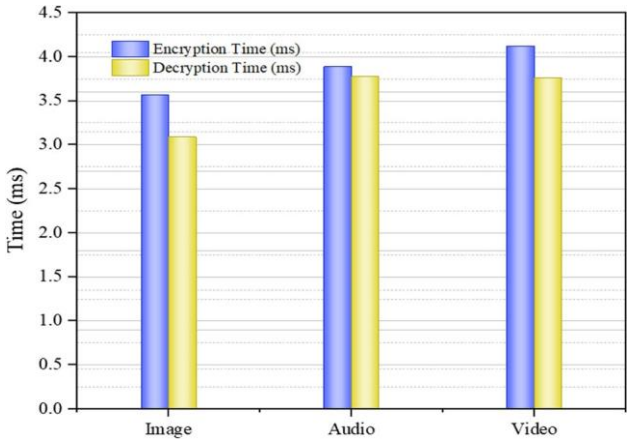


Fig. 6 Performance of the developed model

Sensitive Aware Elliptic Curve Cryptography (HSOA_D- SAECC) [27], and Secure Sharing and Storage of Educa- tional Records using Encryption Scheme (SSSER_ES) [28]are used for comparison.

References

1. Rahman, M. A., Rashid, M. M., Hossain, M. S., Hassanain, E., Alhamid, M. F., & Guizani, M. (2019). Blockchain and IoT-based cognitive edge framework for sharing

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

economy services in a smart city. Ieee Access, 7, 18611-18621.

2. Tavana, M., Hajipour, V., & Oveisi, S. (2020). IoT-based enterprise resource planning: Challenges, open issues, applications, architecture, and future research directions. Internet of Things, 11, 100262.
3. Tripathi, G., Abdul Ahad, M., & Paiva, S. (2020). Sms: A secure healthcare model for smart cities. Electronics, 9(7), 1135.
4. Egala, B. S., Priyanka, S., & Pradhan, A. K. (2019, December). SHPI: smart healthcare system for patients in ICU using IoT. In 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (pp. 1-6). IEEE.
5. Raju, K., Pilli, S. K., Kumar, G. S. S., Saikumar, K., & Jagan, B. O. L. (2019). Implementation of natural random forest machine learning methods on multi spectral image compression. Journal of Critical Reviews, 6(5), 265-273.
6. Saba, S. S., Sreelakshmi, D., Kumar, P. S., Kumar, K. S., & Saba, S. R. (2020). Logistic regression machine learning algorithm on MRI brain image for fast and accurate diagnosis. International Journal of Scientific and Technology Research, 9(3), 7076-7081.
7. Saikumar, K. (2020). RajeshV. Coronary blockage of artery for Heart diagnosis with DT Artificial Intelligence Algorithm. Int J Res Pharma Sci, 11(1), 471-479.
8. Saikumar, K., Rajesh, V. (2020). A novel implementation heart diagnosis system based on random forest machine learning technique International Journal of Pharmaceutical Research 12, pp. 3904-3916.