International Journal of Communication Networks and Information Security

ISSN: 2073-607X, 2076-0930

*Volume **14** Issue **3** Year **2022** Page **257:268***

Blockchain Technologies in Healthcare System for Real Time Applications Using IoT and Deep Learning Techniques

Alcides Bernardo Tello[1*], Jiuhong Xing[2], Dr. Aparna Lalitkumar Patil[3], Dr. Lalitkumar Premchandra Patil[4] and Dr Shabnam Sayyad[5]

[1]Universidad de Huanuco, Huanuco 10001, Peru

[2]Zhengzhou University of Science and Technology, Zhengzhou city, 450064, China

[3]Assistant Professor, Parle Tilak Vidyalaya Association's Institute of Management, Vile Parle, Mumbai

aparna.patil1011@gmail.com

[4]Associate Professor, VIVA Institute of Management & Research, Virar

0000-0002-1959-0317

[5]Associate Professor, Department of Computer Engineering, AISSMS College of Engineering, Pune, India

shabnamfsayyad@gmail.com

Article History

Received: 24 August 2022
Revised: 28 October 2022
Accepted: 29 November 2022

Abstract

Data transparency, flexible access, immutability, privacy, audit, traceability, data provenance, trust, and security are fundamental issues for modern healthcare data management systems. As a promising new technology, blockchain has the potential to enhance healthcare data management functions by boosting data efficiency and guaranteeing trust. The present research looked into the benefits of blockchain technology in healthcare and the challenges that have prevented its widespread implementation so far. Healthcare organisations around the world are using a variety of methods to modernise into more effective, coordinated and user-cantered structures. There is an increase in both human effort and security risks when dealing with massive amounts of data, such as reports and images for each individual. Internet of Things (IoT) solutions in healthcare aim to address these problems by enhancing patient care while reducing costs through more effective use of healthcare resources. However, many different types of intrusion can pose serious risks to IoT devices. In some cases, doctors will insist that their patients use only certain labs or pharmacies, regardless of the quality of the services they provide, simply to increase the doctor's bottom line. Because of this, protecting data is essential when discussing the Internet of Things. To solve these problems, Blockchain technology has emerged as the most reliable method for protecting the privacy of control systems in real time. In this paper, we will introduce a CNN-based healthcare data security framework using the blockchain technique by generating the hash of each data point, which will alert all users of the blockchain network to any unauthorised changes to data or breaches in the supply of medicines.

Keywords: Blockchain, Healthcare, IoT, Deep Learning

1. Introduction

Smart healthcare is the delivery of medical care by means of electronic devices and networks (such as smartphones, smartwatches, wireless blood pressure monitors and wireless smart glucometers). The smart devices process data from a wide variety of sensors and biological systems to improve patient care (i.e., the application having information about medical science such as diagnosis, treatment and prevention of disease). In a nutshell, smart healthcare paves the way for people from all walks of life (including doctors, nurses, patient caretakers, family members and patients [1]) to have timely and accurate access to the information and solutions they need to reduce medical errors, boost efficiency and cut costs in the healthcare system.

Internet of Things, as defined by the IoT European Research Cluster (IECR) project [2], is a dynamic network infrastructure that may self-configure on the basis of interoperable and standard communication protocols. The Internet of Things (IoT) refers to the infrastructure of networks that may connect users, devices, locations and services at any time and in any way [3]. When it comes to healthcare, the internet of things has several potential uses, including remote monitoring, smart sensors and device integration. These days, it's common to find D2D communications integrated into the design of sensor-based systems.

Blockchains are decentralised ledgers that are shared among computers in an encrypted peer-to-peer network. Following the confirmation of each transaction, the ledger is updated across the network and stored at each node. Despite its roots as a network for Bitcoin digital currency transactions, blockchain technology is well-suited for cyber security solutions due to its encryption and decentralised nature. The hashing method is used to establish the connections between the ledger's blocks. The number of verified and finalised transactions is recorded in the first of two halves that make up each block. The second portion is the block's header and it comprises the block's time stamp and a hash of the previous and current blocks. By connecting multiple pre-existing blocks in this way, a block chain is formed; the longer the block chain, the more difficult it is to forge.

A privacy-isolation zone is set up at the origin to collect data and sounds from the body that are not speech. This strengthens the safety of transferring and storing data on the cloud. A security module including access control and trust generating servers is developed in addition to a bespoke deep CNN approach for data extraction from the cloud. The privacy of patient information is ensured in this manner. We evaluate the security of the system in the face of hypothetical attacks that involve both data manipulation and privacy leaks. Data on the user's identification and gait is often linked with data on the user's gestures, movements, and health from a wearable device. The privacy of the user can be compromised if the data is stolen from the cloud and then disassociated from the gait data. Data should be partitioned and analysed in a **data-security enclosure** before being sent to the cloud. The signal is zeroed out and contained within the window using a smooth window technique. The gathered signal is multiplied by the signal inside the region of interest.

In this work, we propose a novel hash processing technique to deal with the issue of data integrity issues brought on by the proliferation of IoT devices in public cloud settings. By routing hashes from on-premises servers (data centres) near IoT devices directly to a blockchain rather than to cloud servers, the proposed solution ensures the authenticity of IoT data. To be more precise, the proposed approach groups index information of geographically dispersed IoT data into the blockchain to guarantee its authenticity, and then hierarchically distributes two-way authentication of n bits of IoT data. Throughout the process of incorporating data collected from IoT devices into a blockchain, it is important to verify the hash value of the data to ensure its veracity. The proposed method used polynomial multiplication and security comparison to configure IoT data as building blocks for distributed environment optimisation, and this was done after an asymmetric hash of IoT data was calculated to limit the possibility of faults in IoT data integrity. This is how the proposed strategy ensures the linkage of IoT data while minimising the likelihood of error in the resulting data.

The rest of the paper is organised as follows. Describes our literature review of this paper Section 2. In Section 3, we discuss our proposed algorithms. Performance evaluation of the suggested

algorithms is discussed in Section 4. Finally, Section .5 concludes this paper with directions for future research.

2. Literature Survey

When block-chain technology is used to a database's worth of information, such blocks of information remain secure and aid in guaranteeing privacy while providing maximum transparency [4]. After being encrypted, these records are placed on the cloud, where they can eventually aid in the treatment of patients by allowing doctors to compare current information with past records. Similarly, 5G services can be used to transmit cloud-stored data to medical professionals. The ultimate consumers of healthcare are the doctors and nurses who recommend certain procedures to their patients. Further, the system's primary goal is to offer the fastest possible response to the patient for treatment while maintaining their anonymity and the confidentiality of their information.

This method was created to take full advantage of the numerous advantages of cloud computing. Similarly, nonparametric models can be used in situations where we either lack necessary background knowledge or do not have enough data to make an informed decision. Fog computing is used by similar Internet of Things devices to set limits on inter-device cooperation, allowing for instantaneous data transmission and response [5].

Deep learning, according to M. Kathuria and colleagues [6], was instrumental in the discovery of architectures like the Hierarchical Computing Architecture (HiCH), which, when combined with algorithms like Internet of Things , convolutional neural network (CNN) , will lead to the development of wireless body area networks (WBAN) for wearable devices. A variety of machine learning algorithms, including KNN ,EM, C5.0 , C4.5 and, are used to enhance AI by filling in missing data and building decision trees. Recently, several meta-algorithms have been developed with the express purpose of enhancing the efficiency of ML programmes. There are a number of access control problems inherent to IoT-Healthcare approaches and a number of algorithms have been developed to solve them.

Griggs et al. [7] suggest using smart contracts built on the blockchain to conduct medical sensor research and management in a secure environment. Using the Ethereum protocol and a private blockchain, the author designed a network in which sensors can exchange data with a portable computer that can then invoke smart agreements and monitor all Blockchain activity.

In [8], G. G. Dagher et al. propose a blockchain-based system for protecting patients' privacy while allowing patients, clinicians and third parties secure, interoperable and effective access to medical data. The system uses smart contracts on an Ethereum-based blockchain to improve access control and code obfuscation, adding a layer of security through cryptographic techniques.

A novel Blockchain-based architecture for storing medical records was presented by L. Zhu et al. [9]. Important data should be kept permanently in case claims of interference arise and its original state needs to be confirmed. To safeguard its users' privacy, the author employs a number of cryptographic strategies in addition to stringent data management procedures.

Recently occurring coronavirus epidemics have wreaked havoc on hospital IT systems, making it harder to maintain and process patient records. These experts believe that the Internet of Things is the best strategy for overcoming the challenges of developing intelligent healthcare systems in the future. The Internet of Things improves data processing, access management, and intelligent identification in healthcare administration by combining artificial intelligence (AI), network technology (networks), and sensor technology (sensing). As a result, we can create a healthcare system that is not only more secure, but also more affordable, user-friendly, and robust. On the other hand, data tampering and leakage are the primary concerns in the field of IoT healthcare [10]. Because of this, it is more important than ever to restrict access to patients' medical records. Access restrictions and role-based access control are frequently used in conventional centralised computing settings to address these security concerns.

Sun et al. [11] illustrate that the user attributes and access control policies are converted into vectors of predefined lengths, which simplifies the protocol for accessing the encrypted data. Fan et al. [12]

used blockchain technology for user certification and nonrepudiation to facilitate data transmission and access management. There are two problems that may be traced back to these terms, which are unique to the field of access control: (i) How to leverage the user's social data to win their trust and sway without compromising their privacy, and (ii) How to use the user's occupation and trust to construct a failsafe access control system without compromising their privacy (iii) Consequently, the suggested method for the IoT-Healthcare system makes use of a secure access control module that operates in accordance with the user attributes.

3. Proposed System

Fig.1 depicts the proposed system's primary elements. First, healthcare apps will gather patient information and safely save it to the electronic health record (EHR). But then the blockchain was found and it turned out to be the best way to keep a control system's data private and secure in real time. In this piece, we'll present a CNN-based security framework for healthcare data using the blockchain approach, by generating the hash of each data, so that any changes to the data or breaches in the security of pharmaceuticals will be immediately visible to all participants in the blockchain network.

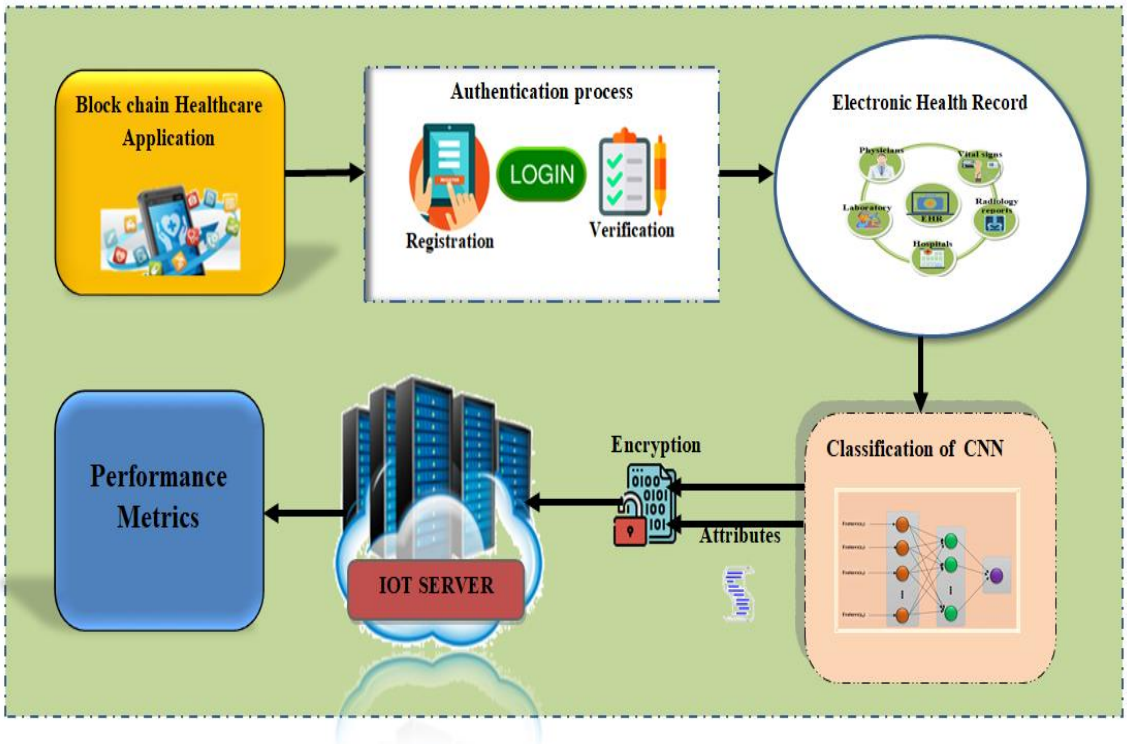

Figure 1: CNN-based healthcare data security framework using the block chain technique

3.1 Health Care applications

Pulse-Rate Sensor. A human's heart rate can be determined by monitoring their pulse. This sensor is highly recommended by professionals for continuous heart rate monitoring. A biometric sensor that can measure pulse or heart rate is another name for this device. Anxiety trackers, fitness trackers, sleep monitors, high-end video game consoles and a remote patient monitoring/alarm system are just some of the applications for the pulse-rate sensor.

Blood Pressure Sensor. The venous pressure of a person can be measured with a blood pressure cuff. The patient's blood pressure can be measured precisely with the aid of a blood pressure sensor.

Oximeter Sensor. The MAX30100 is a sensor used in pulse oximeters, which determine how much oxygen is in the blood. Besides its role in the respiratory process, the body has its own oxygen requirements. When oxygen levels in the blood drop too low, cell damage, organ failure and eventually death can result. The Max30100 pulse oximeter sensor is used for gauging the amount of oxygen carried by haemoglobin. Between 95% and 100% oxygen saturation is considered "normal."

3.2 Authentication

(1)The user must become accustomed to authenticating in the aforementioned ways before beginning the solution flow management section at the management level.

(2)Once the user has been authenticated, they will be able to access the solution's administrative dashboard. Users can then enter their domain via the administration APIs.

(3)To respond to requests made by users with admin API blockchain solution manager REST.

(4)The blockchain solution manager that is linked to the CNN blockchain platform has updated the ledger.

3.3 Electronic Health Record (EHR)

Electronic health records are digital archives of patient information that are securely transmitted between authorised parties, as recommended by the International Organization for Standardization. The major goal of this document is to keep the patient happy and ensure that they receive the best possible care, hence it contains sensitive information about their health. Numerous EHR platforms are now built on the Blockchain.

Medrec: It is based on the principle of decentralised data storage. It is a paradigm built on the Blockchain that allows users to verify their identities, keep their information private and pool their resources. Smart contracts and the idea of distributed data are key to this model's operation.

3.4 Classification of CNN

In order to collect data and sounds from the body that are not spoken, a privacy-isolation zone must be set up at the origin. The safety of cloud-based information exchange and storage is thereby enhanced. A security module consisting of servers for access control and trust generation is used in conjunction with a modified deep CNN algorithm to extract data from the cloud. This protects the privacy of all patient information. System performance is measured using data tampering attack scenarios and hypothetical privacy leakage. Data on the user's gait and identity are often combined with data on the user's gestures, movements and health from a wearable device. The privacy of the user can be compromised if the records is filched from the cloud and then disassociated from the gait data. Data should be divided up and analysed in a secure environment before being sent to the cloud. We use a smooth window function to keep the signal constant inside the boundary while setting it to zero outside. The accumulated signal is multiplied by the signal inside the region of interest.

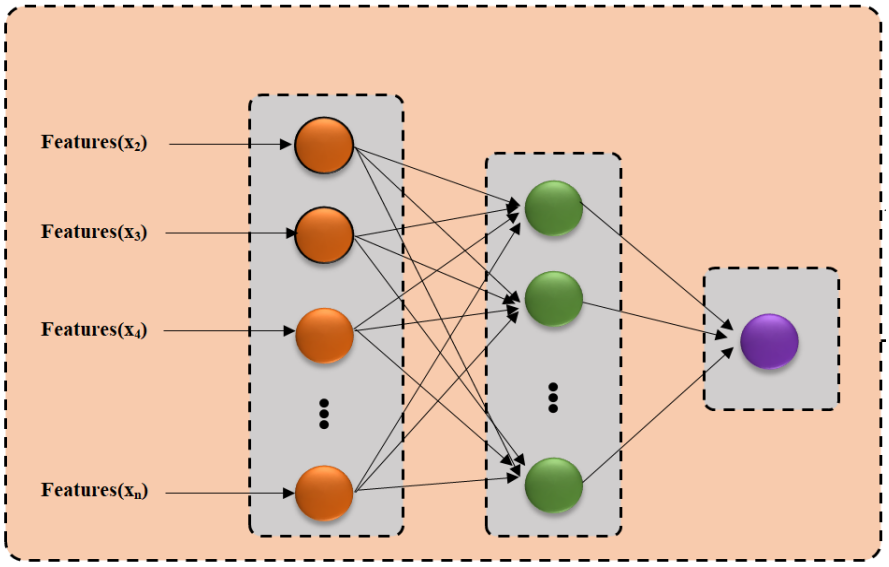

Figure 2: Classification of CNN Structure

3.5 Creation of IoT Information

Before any Internet of Things (IoT) data can be produced using the proposed method, all IoT devices in a distributed cloud environment must first generate blockchain-based data. With the purpose of improving cloud server throughput, the suggested method employs a correlation matrix similar to Equation to pre-process IoT data generated in 64-bit information blocks (1)

$$b_m = Map:(id_m, Block_m) \tag{1}$$

Information-type Preprocessed IoT data can be used to generate blocks in 64-bit units, as shown in Equation (1), which can then be processed in a variety of ways depending on the type of service. (2).

$$B_i = b_m \in \{Z \mid b_1, b_2, ..., b_i\} \tag{2}$$

The i-th "block," denoted by the letter V_m. When handling various forms of IoT information in a distinct manner, the letter Z is used to sequentially order the various forms of IoT data. The amount of od/ven replications in IoT data determines which of two hash chains make up the block formed by Equation (2). The processing of continuous hashes is made possible by this technology and it does so without compromising any information in the surrounding IoT data. It can optimise Internet of Things (IoT) data in distributed cloud settings and makes it simpler to validate the authenticity of IoT data using signatures. Each block of IoT data is assigned a weight in blockchain units that may be used to verify the data, and then the values of those attributes are extracted using the proposed approach (3).

$$V_m = v_m \in \{P_m \mid 1 \le m \le n \bmod 64\} \tag{3}$$

In this case, V_m represents the 64-bit value of the i-th block's property and pi represents the 64-bit value of the corresponding IoT information property.

3.6 Block Processing for Hash Processing of IoT Data

During the data collection phase, it takes into account the cloud scheduler policy and makes an informed decision about which scheduler policy is best suited for the data to be sent to cloud servers. **Error! Bookmark not defined.**The suggested method organises n blocks of information $y_1, y_2, \ldots, y_n$ so that they are orthogonal to each other, allowing for the processing of the connected information of IoT data obtained from IoT devices. During the data collection phase, it takes into account the cloud scheduler policy and makes an informed decision about which scheduler policy is best suited for the data to be sent to cloud servers.

$$g \cong c_1 y_1 + c_2 y_2 + ... + c_n y_n \tag{4}$$

In Equation (4), a probability function like Equation (9) is used to condition on the significance of linked information (5).

$$E\left(B_m^y\right) = -\sum_{m=1}^{n} \frac{1}{n} \log \frac{1}{n} = \log n \tag{5}$$

The proposed method utilises a matrix-like representation to establish a hierarchical link between weighted IoT data and establishes a relationship between seemingly unrelated blocks of data based on outcomes such as high access paths or regular expression filtering checks. The proposed method uses hash-processed load-balancing data for the linkage information, which aids in lowering bandwidth consumption and getting rid of superfluous IoT data while still keeping the information connection between IoT data intact.

4. Result and Discussion

4.1 Experimental Setup

Python 3.8 is used for the simulation and TensorFlow2.2 is used to simulate the CNN. An advanced computing engine (CPU) with 16 cores and 32 threads, 16 GB of primary memory and a graphics acceleration unit (GPU): GTX 1060 is used to run the simulations. The simulation runs on a powerful computing platform that allows for the integration of blockchain technology and a healthcare management system equipped with a categorisation module.

4.2. Metrics of Performance

The detection model's performance is often measured using the metrics listed below.

a) Accuracy: The model's ability to predict the appropriate proportion.

$$\text{Accuracy} = \frac{TN + TP}{TP + FN + TN + FP} \tag{6}$$

4.3 Encryption Time Analysis

Table 1. Encryption Time Analysis of CNN based Security for healthcare data

Messages	Random Forest	Naïve Bayes	Neural Networks	CNN
100	11.946	10.432	9.247	8.471
200	12.235	10.674	9.732	8.324
300	12.456	10.903	9.983	8.673
400	13.043	11.219	10.887	9.034
500	13.549	11.548	10.594	9.274

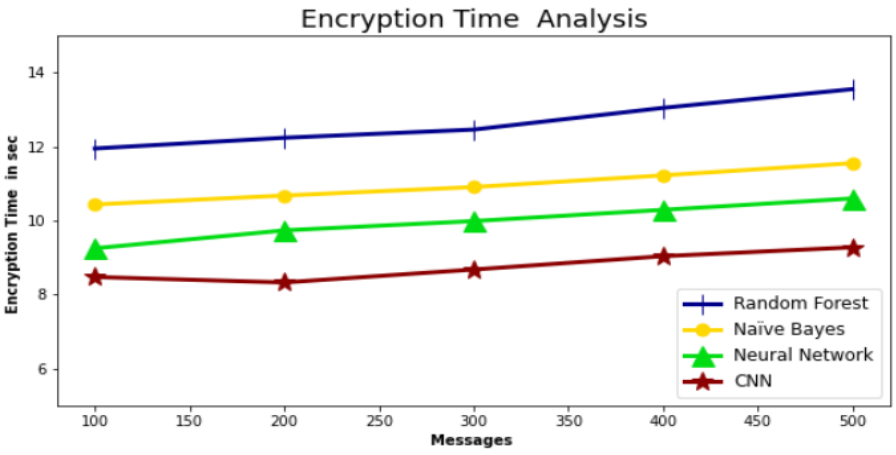

Figure 3. Encryption Time Analysis of CNN based Security for healthcare data

The Encryption Time analysis of the CNN technique with existing methods is described in Tab 1 and Fig 2. The data clearly demonstrates that the CNN method outperformed the other techniques. For 100 operations, the CNN method took only 8.471 seconds to encrypt, whereas other existing techniques such as Random Forest, Nave Bayes and Neural Networks have Encryption

Time of 11.946 seconds, 10.432 seconds, and 9.247 seconds, respectively. Similarly, for 500 operations, the CNN method has an Encryption Time of 9.274sec, while other existing techniques such as Random Forest, Nave Bayes and Neural Networks have Encryption Times of 13.549 sec, 11.548 sec and 10.594 sec respectively.

4.3 Decryption Time Analysis

Table 2. Decryption Time Analysis of CNN based Security for healthcare data

Messages	Random Forest	Naïve Bayes	Neural Networks	CNN
100	18.156	17.341	16.914	16.314
200	18.211	17.456	17.011	16.432

300	18.345	17.611	17.101	16.586
400	18.628	17.951	17.194	16.701
500	18.909	18.031	17.315	16.815

Tab 2 and Fig 3 show the decryption Time analysis of the CNN technique using existing methods. The data clearly demonstrates that the CNN method outperformed the other techniques in every way. For 100 operations, the CNN method took only 16.314 seconds to decrypt, whereas other existing techniques such as Random Forest, Nave Bayes and Neural Networks have decryption time of 18.156 seconds, 17.341 seconds and 16.914 seconds, respectively. Similarly, for 500 operations, the CNN method has an decryption time of 16.815 sec, while other existing techniques such as Random Forest, Nave Bayes and Neural Networks have decryption times of 18.909 sec, 18.031 sec and 17.315 sec respectively.

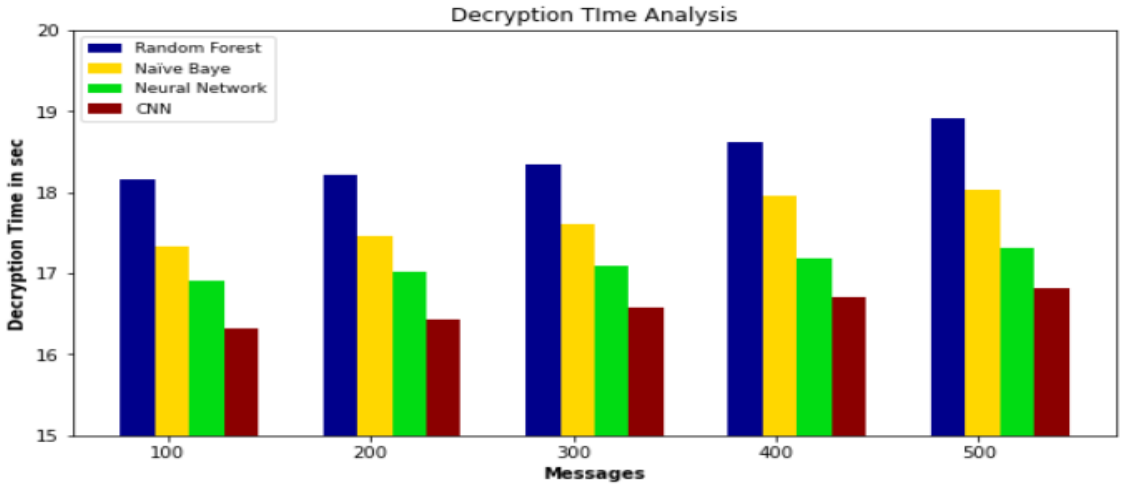

Figure 4. Decryption Time Analysis of CNN based Security for healthcare data

4.4 Execution Time Analysis

Table 3. Execution Time Analysis of CNN based Security for healthcare data

No of Data from dataset	Random Forest	Naïve Bayes	Neural Networks	CNN
100	5.171	4.252	3.219	2.375
200	5.241	4.185	3.417	2.567
300	5.543	4.658	3.675	2.374
400	5.982	4.854	3.151	2.943
500	6.034	5.280	4.065	3.094

The CNN technique's Execution Time analysis with existing methods is described in Tab 3 and Fig 4. The data clearly demonstrates that the CNN method outperformed the other techniques in every way. For example, with 100 operations, the CNN method took only 2.375 seconds to execute, whereas other existing techniques such as Random Forest, Nave Bayes and Neural Networks have execution times of 5.171 seconds, 4.252 seconds and 3.219 seconds, respectively. Similarly, for 500 operations, the CNN method takes 3.094 seconds to execute, while other existing techniques such as Random Forest, Nave Bayes and Neural Networks take 6.034 seconds, 5.280 seconds and 4.065 seconds, respectively to execute.

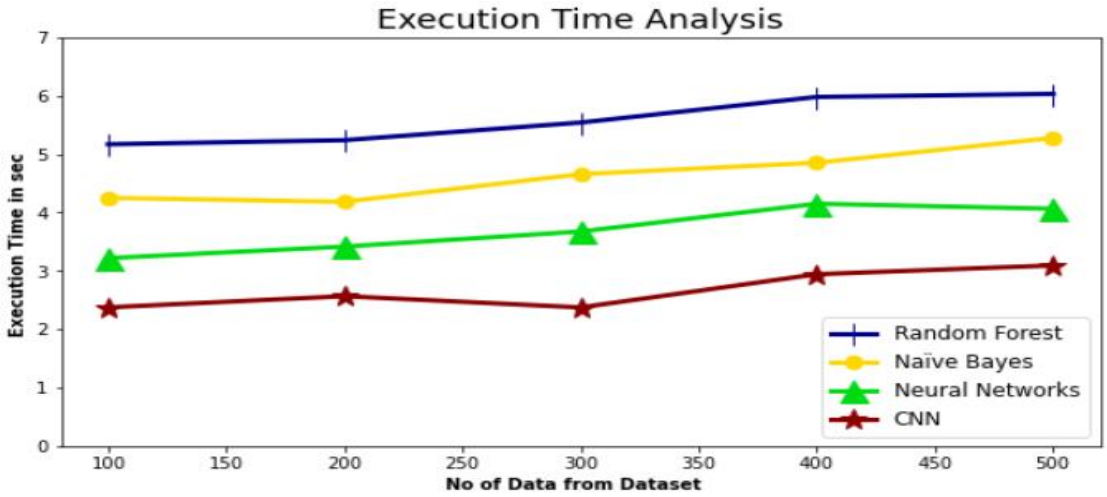

Figure 4. Execution Time Analysis of CNN based Security for healthcare data

4.6 Throughput Analysis

Table 4. Throughput Analysis of CNN based Security for healthcare data

No of Data from dataset	Random Forest	Naïve Bayes	Neural Networks	CNN
100	752.87	845.26	978.38	1189.54
200	794.37	882.59	993.31	1238.25
300	754.72	877.93	1045.73	1248.32
400	819.27	902.65	1089.45	1293.83
500	832.87	947.18	1127.85	1314.27

Tab.4 and Fig.6 describe the throughput analysis of the CNN technique with the existing methods. The data clearly shows that the proposed method outperforms the other techniques in all aspects. For example, with 100 data points, the CNN method has a throughput of 1189.54kbps while the other existing methods like Random Forest, Nave Bayes and Neural Networks have a throughput of 752.87kbps, 845.26 kbps and 978.38kbps, respectively. Similarly, with 500 data points, the proposed method has 1314.27kbps of throughput while the other existing methods like Random Forest, Nave Bayes and Neural Networks have a throughputs of 832.87kbps, 947.18kbps and 1127.85 kbps, respectively. This proves that the CNN technique has higher performance with greater throughput.

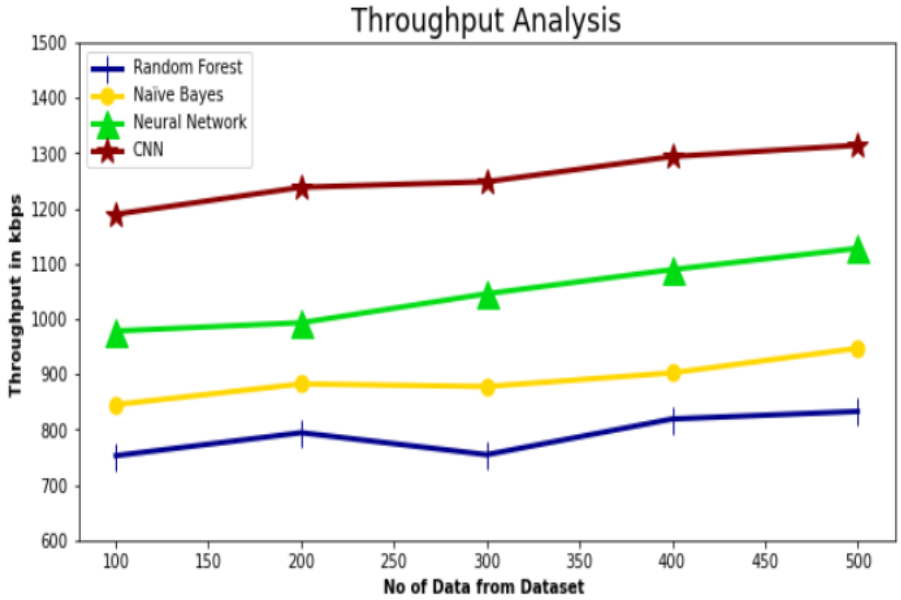

Figure 6. Throughput Analysis of CNN based Security for healthcare data

4.7 Accuracy Analysis

Table 5. Accuracy Analysis of CNN based Security for healthcare data

No of Data from dataset	Random Forest	Naïve Bayes	Neural Networks	CNN
100	87.26	89.16	92.63	94.27
200	87.63	89.64	93.46	95.75
300	88.94	90.28	92.91	96.82
400	88.13	90.83	93.81	97.37
500	88.94	91.27	94.96	97.92

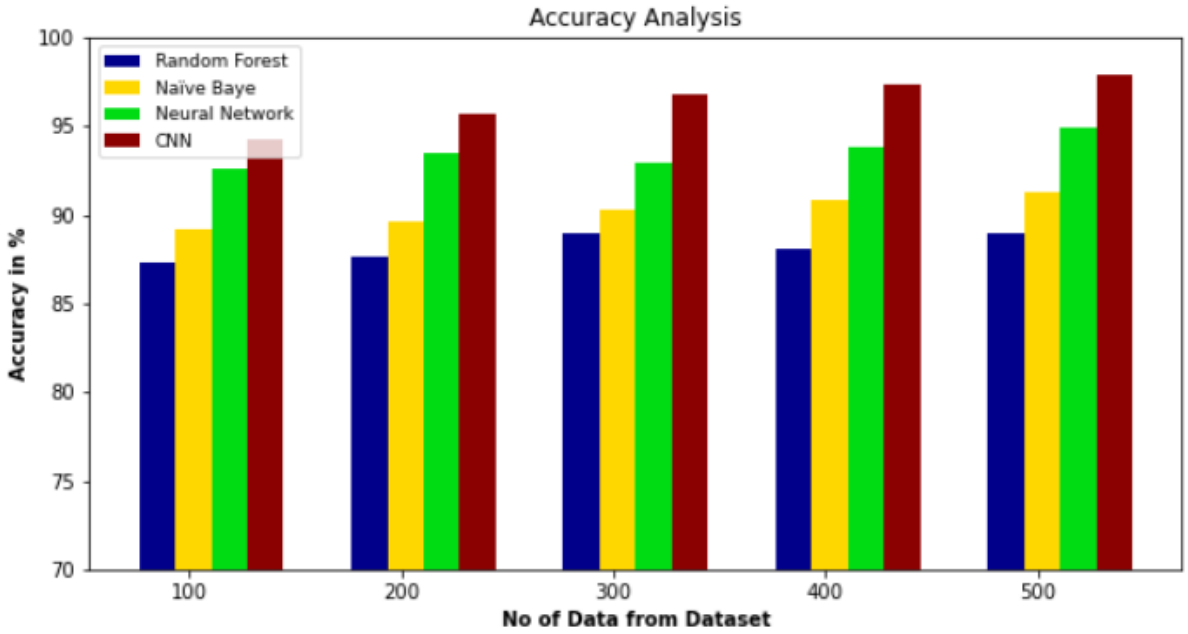

Figure 7. Accuracy Analysis of CNN based Security for healthcare data

Fig. 7 and Tab.5 illustrate a comparative accuracy examination of the CNN approach with other existing methods. The figure shows that the Block chain approach has resulted in higher performance with greater accuracy. For example, with data 100, the accuracy value is 94.27% for CNN, whereas the Random Forest, Nave Bayes and Neural Networks models have obtained accuracy of 87.26%, 89.16% and 92.63%, respectively. However, the CNN model has shown maximum performance with different data set size. Similarly, under 500 data, the accuracy value of CNN is 97.92%, while it is 88.94%, 91.27% and 94.96% for Random Forest, Nave Bayes and Neural Networks models, respectively.

5. Conclusion

Current security solutions are inadequate due to central system restrictions, but privacy and security of healthcare data is one of the most serious academic topics. In this study, we developed a process for building a complete healthcare system that connects two previously separate technologies—**the electronic health record and the remote patient monitoring system**—under a single roof. To ensure the security and confidentiality of patient information, this study used blockchain technology. Our technology helps bring down costs by doing away with the need for a trusted third party in a blockchain transaction and replacing them with a lightweight smart contract. In addition, the proposed method hash-processes IoT data to reduce errors in its integrity prior to performing load balancing. Connectivity and data integrity in the IoT are both protected by this technique. The goal of this piece is to provide a detailed description of how IoT and Blockchain can be applied in the healthcare sector to improve efficiency and quality of care. Remote patient monitoring, drug tracing and medical records management are three of the most important areas of healthcare where the Internet of Things and Blockchain technologies have been studied in depth. Moreover, the potential

difficulties and issues that may arise from implementing these two revolutionary technologies—the Internet of Things and the Blockchain—in the healthcare sector were discussed and analysed. In the future, we hope to overcome the work's time and money limitations by generalising its performance using larger data sets. Enhancing user identity protection policies is one area where adopting a blockchain-based security module can help. It is possible to enable real-time sample collection and system upgrades, both of which can boost system performance over time.

Consent For Publication

The authors read and aware of publishing the manuscript in International Journal of Communication Networks and Information Security

Declarations

Authors declares that all works are original and this manuscript has not been published in any journal.

References

1. W. D. De Mattos and P. R. L. Gondim, "M-Health Solutions Using 5G Networks and M2M Communications," IT Prof., vol. 18, no. 3, pp. 24-29, 2016. https://doi.org/10.1109/MITP.2016.52
2. Ejaz, W., Anpalagan, A., Imran, M.A., Jo, M., Naeem, M., Qaisar, S.B. and Wang, W., "Internet of Things (IoT) in 5G wireless communications," IEEE Access, vol.4, pp.10310-10314, 2016. https://doi.org/10.1109/ACCESS.2016.2646120
3. Agbo C, Mahmoud Q, Eklund J. 2019. Blockchain Technology in Healthcare: A Systematic Review. Healthcare.7(2):56. https://doi.org/10.3390/healthcare7020056
4. E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir and A. A. A. El-Latif, "DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems," IEEE Access, vol. 8, pp. 111223- 111238, 2020. https://doi.org/10.1109/ACCESS.2020.2999468
5. I. H. Sarker, "Machine learning: algorithms, real-world applications and research directions," SN Computer Science, vol. 2, no. 3, pp. 1-21, 2021 https://doi.org/10.1007/s42979-021-00592-x
6. M. Kathuria and S. Gambhir, "Reliable packet transmission in WBAN with dynamic and optimised QoS using multiobjective lion cooperative hunt optimizer," Multimedia Tools and Applications, vol. 80, no. 7, pp. 10533-10576, 2021 https://doi.org/10.1007/s11042-020-10144-9
7. K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," J. Med. Syst., vol. 42, no. 7, pp. 1-7, Jul. 2018. https://doi.org/10.1007/s10916-018-0982-x
8. G. G. Dagher, J. Mohler, M. Milojkovic and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," Sustain. Cities Soc., vol. 39, pp. 283-297, May 2018. https://doi.org/10.1016/j.scs.2018.02.014
9. H. Li, L. Zhu, M. Shen, F. Gao, X. Tao and S. Liu, "Blockchain-based data preservation system for medical data," J. Med. Syst., vol. 42, no. 8, pp. 1-13, Aug. 2018. https://doi.org/10.1007/s10916-018-0997-3
10. Y. Sun, J. Liu, J. Wang, Y. Cao and N. Kato, "When machine learning meets privacy in 6G: a survey, "IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2694-2724, 2020. https://doi.org/10.1109/COMST.2020.3011561
11. J. Sun, H. Xiong, X. Liu, Y. Zhang, X. Nie and R. H. Deng, "Lightweight and privacy-aware fine-grained access control for IoT-oriented smart health," IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6566-6575, 2020. https://doi.org/10.1109/JIOT.2020.2974257

12. K. Fan, Q. Pan, K. Zhang et al., "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks," IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5826-5835, 2020. https://doi.org/10.1109/TVT.2020.2968094
13. F. Jamil, S. Ahmad, N. Iqbal and D.-H. Kim, "Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals," Sensors, vol. 20, no. 8, p. 2195, 2020. https://doi.org/10.3390/s20082195
14. V. D. Ambeth Kumar, S. Malathi, Abhishek Kumar, Prakash M and Kalyana C. Veluvolu, "Active Volume Control in Smart Phones Based on User Activity and Ambient Noise" Sensors 2020, 20(15), 4117. https://doi.org/10.3390/s20154117
15. E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir and A. A. A. El-Latif, "DITrust chain: towards blockchain-based trust models for sustainable Journal of Food Quality 19 healthcare IoT systems," IEEE Access, vol. 8, pp. 111223-111238, 2020. https://doi.org/10.1109/ACCESS.2020.2999468