REVIEW ARTICLE

An Integrated Approach for Analysis of Electronic Health Records Using Blockchain and Deep Learning

Pooja Singhal[1], Shelly Gupta[2], Deepak[3] and Jagendra Singh[4,*]

[1,2,3]ABES Engineering College, Ghaziabad, Dr. A.P.J. Abdul Kalam Technical University, India; [4]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India

ARTICLE HISTORY

Received: October 12, 2022
Revised: January 05, 2023
Accepted: January 25, 2023

DOI:
10.2174/2666255816666230509142714

Abstract: Blockchain is used to assess health records digitally, preserving the security and immutability of the records. The goal of this study is to make it easier for patients to access their medical records and to send them alert messages about important dates for their check-ups, healthy diet, and appointments. To achieve the above-mentioned objective, an integrated approach using Blockchain and Deep learning is initiated. The first approach is Hyperledger Fabric in Blockchain, i.e., private Blockchain, for storing the data in the medically documented ledger, which can be shared among hospitals as well as Health organizations. The second approach is incorporated with a deep learning algorithm. With the help of algorithms, we can analyse the ledger, after which an alert *i.e.* consultation, health diet, medication, *etc.*, will be sent to the patient's registered mobile device. The proposed work uses nine features from the dataset; the features are identification number, age, person gender, disease, weight, consultation date, medication, diagnosis, and diet specification. The study is conducted with several features to give accurate results. The integrated model used in this suggested piece of work automates the patient's alert system for a variety of activities. In terms of precision, recall, and F1 score, testing data demonstrate that the LSTM performs better than the other models. By working together with the calendar software on Android mobile devices, alert systems can be improved in the future.

Keywords: Blockchain, deep learning, integrated environment, hyperledger fabric.

1. INTRODUCTION

Blockchain is a stable, secure, shared and distributed platform. It is a ledger that processes and records data. It provides a trusted solution for attackers and tries to control the system by compromising the central controller. It is a new technology that is useful [1] for safeguarding both tangible items (such as money, homes, automobiles, and land) and non-tangible items (such as patents, digital records, and intellectual property rights). For the vast majority of the data, maintaining current accuracy serves as a snapshot of the current situation. Blockchain databases are now able to store meaningful as well as previous information. In Blockchain technology, data creation with its own consistent history. They grow as ever-growing repositories of their past over time and provide a true picture. It is a costly expense to reduce or modify the data, which has led to people calling the Blockchain database irreversible.

In this modern era, many health organizations do not keep a physical record of patients' medical information, including their diagnostic checkup and their treatments; however, they do maintain these records electronically, which are kept safe and guarded. The term "Electronic Health Record (EHR)" refers to a computerised record of a patient's medical history that is updated over time by the physician. It can include all pertinent clinical management data that is important to caregivers, such as progress notes, problems, medications, key indicators, past medical histories, vaccinations, laboratory information, and radiology reports. The EHR has access [2-6] to the data and the capacity to simplify medical tasks. Through a number of methods, including evidence-based decision support, quality management, and result reporting, the EHR can also directly or indirectly subsidies other operations. There are a few issues with current EHR maintenance, including:

1. Deciding whether to believe a company that stores health records digitally.
2. Tampering and loss of medical information.
3. It was challenging to find the patient's history to recommend treatments.
4. How to obtain patient information in an emergency and whether it can be trusted.

The paper presents a storage approach that uses a Blockchain Hyperledger fabric to store patient data with improved confidentiality and security in order to get beyond all these limitations. Without that patient's permission, no one else is

[*] Address correspondence to this author at the School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India; E-mail: jagendrasngh@gmail.com

2666-2558/XX $65.00+.00

allowed to examine their medical records. Other users, such as doctors and healthcare providers, should possess an electronic certificate from the government in order to join and have access to medical health records in the Blockchain network. Only doctors, nurses, and clinicians would be allowed to perform CRUD operations in the block. The block's data can be obtained using the hash value. The patient's block is then monitored using a recurrent neural network technique with long short-term memory (RNN-LSTM). Following that, the performances of RNN-LSTM and RNN-GRU are contrasted. Once the patient block has been verified, an alert will be sent to the patient's registered device.

1.1. Motivation

The incredibly sensitive data in electronic health records make it very likely that hackers will misuse the records when they are stored centrally [7,8]. The patients also keep track of their records for appointments for routine consultations, prescriptions, diagnoses, *etc.* The purpose of this work is to design an alert system for the sick person and evaluate the medical records electronically using a deep learning mechanism that is recorded in the Blockchain.

1.2. Improvement

A private, trusted Hyperledger fabric is used for storing the patient's medical records for security purposes. It employs the RNN-LSTM and RNN-GRU mechanisms to evaluate the blocks (the patient's EHR). For the benefit of the patient, an alert system is made for activities like reminders for the next appointment, prescription, and diagnosis. Analysis is performed on the RNN algorithm's behavior and effectiveness. As a result, the EHR is stored on a dependable Hyperledger fabric [9,10]. The deep learning Recurrent Neural Network algorithm examines the medical records and develops an alarm system to remotely monitor the patients.

1.3. Composition of the Paper

The structure of the paper is as follows: Literature Survey discussed in part II. Materials and procedures are described in part III. The results are discussed in part IV. The closing process is mentioned in part V.

2. LITERATURE SURVEY

A distributed network of nodes' fixed data structure is known as a Blockchain. It was first made available as a technology through the cryptocurrency Bitcoin, which claims to have invested $ 180 billion in the market. Since “January 2018” [2] they have offered a solution to the issue of double money trading in digital transactions. Numerous platforms and applications have been proposed to make use of the advantages provided by the growing interest in Blockchain technology. Banks, healthcare, real estate, the Internet of Things, and other

Industries have all received papers outlining the advantages of this technology. Due to the growing concern about the use of fraudulent medical certificates and instructions in the healthcare sector. We have proposed a secretive e-Certificate site using Blockchain benefits. Many documents have discussed the appropriateness of Blockchain technology for digital certificates or education certificates, but we have not found any work related to e-certificates confirming confidentiality registered in the literature. Other activities in the same area are discussed next.

A study by Gordon and Catalini [9] examined the potential advantages of Blockchain technology for the healthcare sector. Hospitals, pharmaceutical corporations, and other stakeholders govern the healthcare sector. They cited the need for information exchange as the primary justification for using Blockchain in the healthcare industry. The study also identified four reasons or mechanisms for why Blockchain technology needs to be applied in the field of health care. This includes how to handle patient identity, instant access to clinical records, and digital access rights to data. It also covers the storage of data both on and off the chain. The study included difficulties or impediments to using Blockchain technology.

Using the Hadoop database, Sahoo and Baruah [10] have created an unrivalled Blockchain platform. They recommended leveraging the distribution offered by the fundamental Hadoop database and the power-sharing offered by Blockchain technology to address the issue of Blockchain failure. The Blockchain above this framework uses a Blockchain archive in the Hadoop database; nevertheless, blocks are saved in the Hadoop database to facilitate the development of Blockchain technology. This study proposes the usage of the Hadoop database system and the SHA-256 hashing used for Blockchain transactions to address the issue of scaling the Blockchain platform. Java was the programming language employed in this artwork.

When MedRec [11-23] was initially created, it became the initial working model implemented for a digital sick person health record system to manage that would be made possible using Blockchain technology. On the Ethereum Blockchain, comprehensive accessibility data may be backed up. Healthcare organizations do not maintain the Blockchain. This suggests that the data may still be stolen or used improperly. A health wellness management system, like Ivan's [22], encrypts sick person keys while data is kept on the Blockchain. Researchers and medical facilities decode the data using the patient's public key with the patient's consent. On the other hand, we provide our sick persons having complete authorization to be owners of their own data so that they can manage the rights of whosoever has access to it.

Each node in the Blockchain is given a distinct set of public and private keys when they sign up for the network. We may introduce authentication, non-repudiation, and integrity into the network by using asymmetric cryptography. Every time a transaction occurs, it is verified by the user's private key and broadcast to the surrounding nodes. Before relaying the transaction farther into the network, the other nodes cross-check and validate it using the public key. The fraudulent transactions are eliminated. Some of the nodes, known as miners, gather all the transactions in that time window after a predetermined amount of time and package them into a time-stamped block. As soon as a new block is mined, other nodes check to see if it contains valid transitions; if so, the block is broadcast; otherwise, it is discarded. After predetermined intervals of time, this procedure keeps repeating. The introduction of transactions and blocks gradually builds confidence while the nodes initially operate in a trustless environment. As a result, all transactions are verified before relaying, and similarly, blocks are mined by nodes with a specific level of trust. As a result, it is claimed that the confidence in a Blockchain develops into a network attribute [24-32, 33].

To mine the block and update the Blockchain at regular intervals, the nodes within it must unanimously agree on a set of ordered transactions. In a perfect world, the answer is to decide on the block that was mined by the most nodes. However, the Sybil attack, in which a single person adds several nodes to impact the block's mining decision, poses a serious risk. Transactions cannot be undone after a block is mined using a miner and after it has been locked [34]. Because the asymmetric key combination is used to validate the transactions so that no one can subsequently dispute their involvement in the transactions, this is how Blockchain maintains security. The set of transactions and transaction counter that comprise the block's body define how many transactions a block can carry based on the size of the transactions [34,35,36].

The Internet of Medical Things (IoMT) and smart contracts are discussed in this article along with how they can be applied to the e-healthcare industry. The research analyses the directions that smart contracts and decentralisation will take the IoMT in e-healthcare [37], suggests a novel architecture, and discusses the benefits, drawbacks, and potential future directions of their combination. In comparison to conventional methods, the suggested architecture demonstrates its effectiveness using average packet delivery ratio, average latency, and average energy efficiency performance characteristics.

The author of this paper proposed a widely accepted Blockchain-based educational framework for a broad range of stakeholders, including universities, enterprises, and other institutions of higher learning that are willing to cooperate as part of the framework [38]. This system helps stakeholders validate academic credentials and course credits for students enrolled in universities that can be distributed digitally. The planned project would grant credits to enrolled students at various universities when they successfully complete courses in tokens. The funds will function as transactions that are mined as blocks and added to the longest chain. It will function in a uniform setting where all stakeholders cooperate despite obstacles posed by governmental regulations and administrative procedures.

In this study, a novel concept known as patient-centric healthcare data management is proposed (PCHDM). This suggestion functions both on chain and off chain. In off-chain systems, genuine health data is encrypted and kept securely over the interplanetary file system, while hashes of health records are stored as health record chains in Hyperledger fabric in on- chain health record databases (IPFS). By confirming patient wishes before sharing health details, a secure smart contract hosted by container technology and Byzantine Fault Tolerance consensus ensures patient privacy [39]. Hyper ledger calliper benchmarks are used to measure the performance of distributed ledger technology in terms of transaction latency, resource usage, and transaction per second. The model gives participants greater confidence in working together and sharing their medical details.

In this article, integrated deep learning and Blockchain services were proposed. Two steps are required to complete this. Lattice cryptography is required for authentication in the first section, and deep learning services are employed in the second section to store a data set of electronic health record details for disease prediction in the future in accordance with the performance KPIs provided. In order to increase accuracy, data must then be compared across many parameters. With regard to the parameters used for comparison, the recently concluded suggested framework called BinDaas performs better than the other existing approaches [38-40].

According to the findings of the above survey, there are several important areas that require additional attention. First, the timely availability of patient health records, followed by the necessity to raise medication alarms and any alarms for urgent appointments. In order to give more security, immutability, and the requirement to foster confidence between doctor and patient, so that both can reap equal benefits, an integrated approach is created while keeping the above factors in mind. This method also allows us to assess how useful these records are for medical professionals.

3. METHODOLOGY

A. Hyperledger Fabric

When Blockchain technology first emerged, the MedRec Hyperledger fabric was a plug-and-play (modular) open-source platform that built distributed ledgers, enabling high levels of data security and privacy. (Fig. **1**) depicts the Hyperledger fabric architecture [12]. Through the fabric SDK, the client surrenders the transaction pool to the endorser. Peers who endorse each other validate the transaction, carry it out, and produce the read and write sets. The client is then informed of the response. The client gathers all peer responses and then sends them to the "orderer." In this instance, the orderer places all transactions in ascending order, which is followed by the formation of a block. Each committer verifies this block and as a result, adds a new block to their individual copy of the ledger.

The key part of Fabric is the Membership Service Provider, which establishes a rule to admit members only after authentication and verification [14, 15]. It oversees the client's legitimacy and User ID. The customer is the one who originates the transaction proposition. In Blockchain, every transaction must be recorded in the shared ledger in a specific order. The order in which updates are made must be established for the world state to be legitimate.

B. RNN Long Short-Term Memory

A recurrent neural network is a special kind of deep learning that uses the results of one phase as the input for the subsequent. Recurrent neural networks can understand the long-term dependencies of data because of a special type called LSTM. The repeating module of the LSTM, which consists of a combination of four separate layers coupled to one another, facilitates this form of learning [16, 4]. The procedure

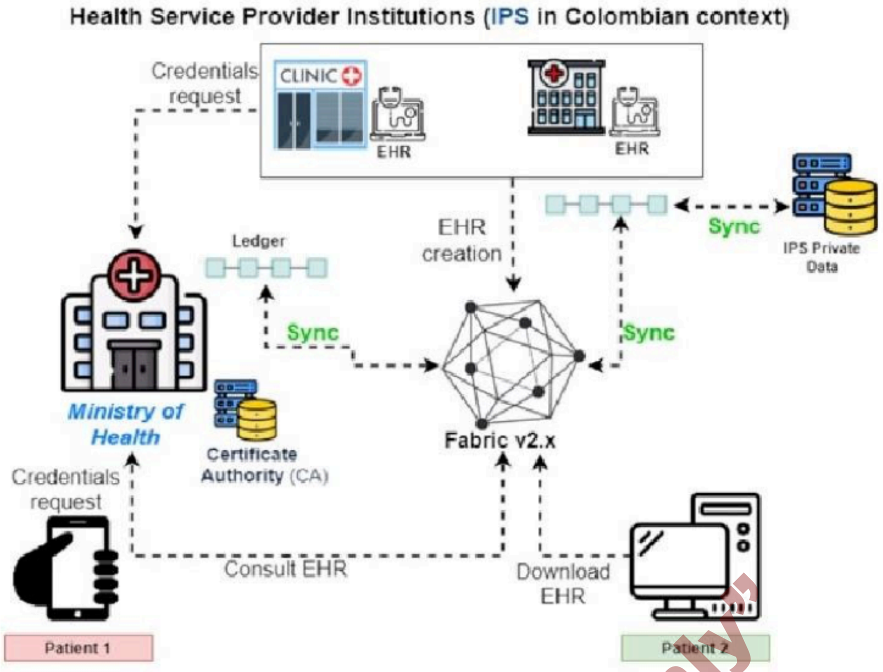

Fig. (1). Hyperledger fabric layered architecture. (*A higher resolution / colour version of this figure is available in the electronic copy of the article*).

Table 1. Abbreviations.

EHR	Electronic Health Record
SP1	Sick Person
PH1	Physician
EU1	End User
SPK	Sick Person Private Key
SUK	Sick Person Public Key
SK	Session Key
PPK	Physician Private key
SPV	Sick Person View of Data

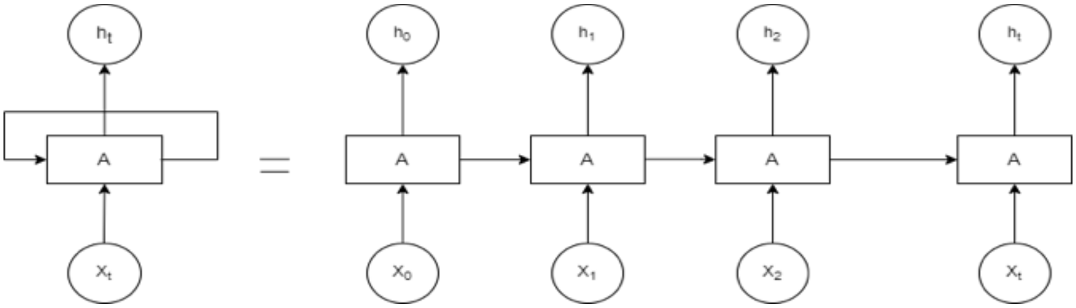

Fig. (2). LSTM RNN Layered Architecture.

is shown in Fig. (**2**), along with the three-layered architecture, where the embedding layer feeds the Encoder-LSTM network with the pre-processed input. Then it moves on to the attention layer, which serves as the intermediary layer, where it helps the decoder focus on particular areas of the fixed-size vectors.

C. System Model

Due to the high security and privacy of medical data, this study uses the Blockchain [18,19] to store all of the patient's electronic health records, which cannot be accessed by outside parties or online attackers. These kinds of medical data can be saved using Hyperledger Fabric. Inter Planetary File System (IPFS) is used, which offers a remedy for file storage issues. Large files may be stored and retrieved effectively with IPFS. To protect privacy, medical records are encrypted with symmetric key encryption. The record is kept secure by being saved in an encrypted format on an IPFS server that is overseen by the proper authorities. An organization must first receive permission to access the patient's record.

1. To decode the record, a private key is required.
2. The key is encoded using the asymmetric key and public key RSA key pair. Access to a health records may be removed if:
3. The asymmetric key is decrypted by the private key connected to the EHR owner.
4. The EHR is decoded using the asymmetric key.
5. The record is once more encoded using a new asymmetric key.
6. The public keys of all allowed users are used to complete the encoding of theasymmetric key.

The model of the system is shown in Fig. (**3**). It accepts the input (digital medical records) from physicians or medical experts as well as health wellness providers, which is to be fed into the Hyperledger Fabric using Inter Planetary File System (IPFS), with the help of which the data is fetched by a deep learning agent for analyzing the EHR. This data-feeding record is shown using Algorithm 1. After this, an alert signal, as shown in Algorithm 2, is generated with the help of RNN-LSTM for several activities, like the medical expert consultation and wellness schedule, to the sick person's registered device.

The proposed work offers an efficient alert system by utilizing different EHR characteristics. Some of the features naming Access control, Confidentiality, Interoperability, Data Integrity, Patient Data access and storage. Taking into account all of these characteristics, we can create a reliable alarm system that will allow for ongoing patient monitoring. The data reduction process is then completed to identify the best dataset model that has been suggested in order to maximize efficiency.

D. Preprocessing Data

Pre-processing data is a crucial task that must be completed. It aids in achieving the model's maximum efficiency. The dataset is now pre-processed through four significant phases,including:

1. Cleaning of data
2. Integration of data
3. Changes to data
4. Data minimization

To obtain the pre-processed data needed to train the model, these four stages must be carried out in the correct order. The dataset is initially cleaned up by adding missing values, assigning null values, removing invasive data, resolving inconsistencies, and eliminating outliers. The data is then utilized for data integration, which is the process of combining data from various sources into one, more substantial data storage, like a data warehouse [21].

Algorithm 1: The creation and updating of health data on the Hyperledger Blockchain.

Updating and storing data () Factors: (EHR) from a variety of sources result: 0 or 1.

1. Process Store EHR
2. For every
3. EU1 contacts SP1
4. If (role==Physician && permission== GRANT) then
5. Make a SPV of the EHR in IPFS
6. (Encrypt (HR)) PV Decryption
7. Make Sk
8. Send SPK (Sk), PPK (Sk), and SPV (Sk) Encrypted to SP1, PH1, and SPV
9. Create Update ()
10. EHR [(Decrypt SPK (Encrypted SUK (EHR) + Encrypt (SP1).
11. Pan Commit (EHR) IPFS

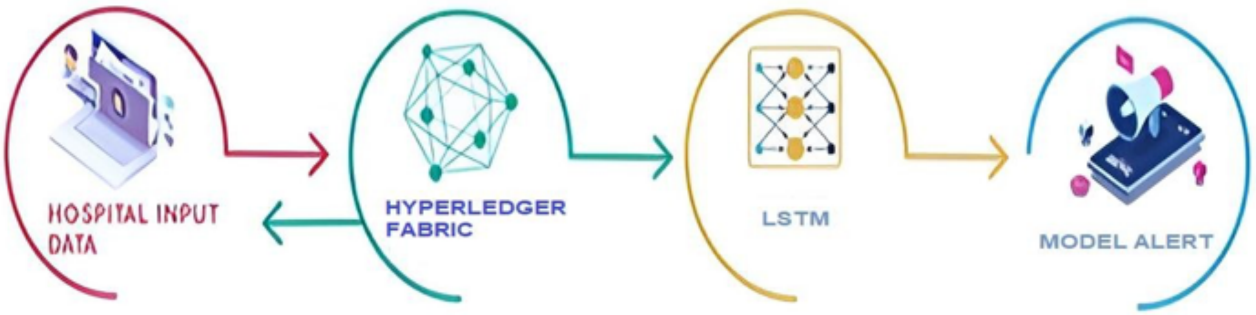

Fig. (3). Model of the system. (*A higher resolution / colour version of this figure is available in the electronic copy of the article*).

```
12. IPFS EHR hash
13. Hash EHR, HyperledgerFabric Blocks
14. Return 1
15. Else
16. Permission=Deny
17. Return 0
18. Exit if
19. Exit for ()
20. Exit procedure Store_EHR
```

E. Evaluation Metrics

A variety of assessment indicators are employed to assess the effectiveness of our model.

$$\text{Accuracy} = (TZ+AN)/(TZ+AN+UZ+CN) \qquad (1)$$

$$\text{Precision} = (TZ + UZ)/(TZ) \qquad (2)$$

Examining True Positive (TZ) units in relation to False Positive (UZ) units is the goal of precision. Examining True Positive (TZ) units in relation to unclassified False Negative (CN) units is the goal of recollection. The following equation gives the recall's arithmetic arrangement:

$$\text{Recall} = TZ/(TZ + CN) \qquad (3)$$

Using the F1-measure, which has a mean recall and precision, this problem is solved. One way to calculate F1-measure is as follows:

F1score is calculated as [2 (Precision * Recall)/ (Precision + Recall)] (4)

The recall and accuracy of the performance evaluation may occasionally be subpar. A differentalgorithm is required, for instance, if a mining algorithm has a high precision but a low recall. Then the issue of which algorithm is more efficient arises.

Algorithm 2: Building a Hyperledger Blockchain alert for health records.

```
1. Input: BLOCKCHAIN EHR
2. Output: Dynamic suggestion
3. An alternative way of action
4. Initialize P and Q;
5. Prepare the content of the items;
6. For I to J do
7. For each (P sample, Q sample) samples, do
8. Train Autoencoder (P sample, Q sample);
9. End
10. Theta ← Autoencoder(P);
11. PtP ← PTP;
12. For each, I ϙ items do
13. PtP ← PtP + αPOB ∗T POB + λQ I;
14. Ptr ← (1+α) POBrOB+ λvtheta
15. Qi ← Solve (PtP,Ptrob)
16. End
17. QtQ ← QTQ;
18. Foreach q ϙ users do
19. QtQ ← QtQ+α QOB∗T QOB+ λpI;
20. Qtr ← (1+α) QOBrOB
21. Pp ← Solve (PtP,Ptrob)
22. Exit For
23. Exit For each
```

4. EXPERIMENTS & RESULT

The personal alert system in the suggested model is created for sick persons with registered mobile numbers. The alert is generated for certain events like the date of the next appointment, the prescription due date, the diet requirements, and the diagnostic data. Initially, the Blockchain's IPFS protocol is used to store the patient's EHR. The Blockchain will increase the security and distribution of the data stored there.

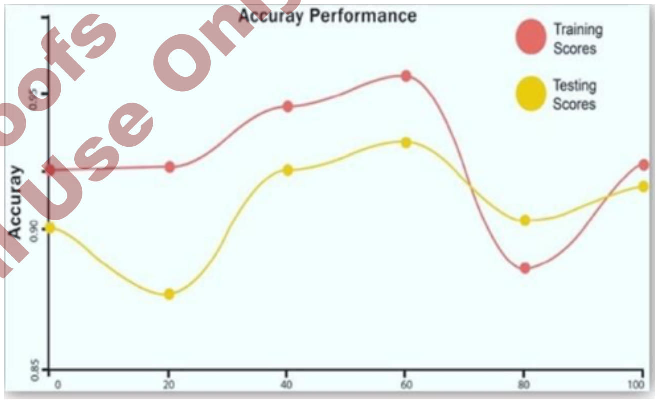

Fig. (4). Shows verified values & measures for LSTM. (*A higher resolution / colour version of this figure is available in the electronic copy of the article*).

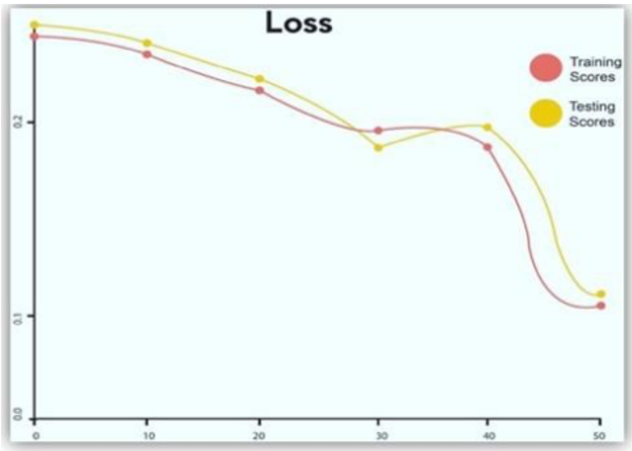

Fig. (5). Shows verified values & measures for LSTM (Loss). (*A higher resolution / colour version of this figure is available in the electronic copy of the article*).

Table 2. Characteristics used for model.

Sequence	Characteristics	Data Type
I	Sick Person Identification	Number
II	Sick Person Age	Number
III	Sick Person	Definite
IV	Sick Person Weight	Number
V	Sick Person illness	Definite
VI	Medicine schedule	Text
VII	Next meeting time	Date
VIII	Next examine time	Date
IX	Balanced regime Specification	Text

Table 3. Description for Precision, Recall & F1 scores.

Domain	Mark	Hyperledger Fabric(LSTM)	Hyperledger Fabric (GRU)
Precision	Allowed	0.9877	0.9655
	Not Allowed	0.8943	0.9924
Recall	Allowed	0.9947	0.9987
	Not Allowed	0.7232	0.3744
F1 Scores	Allowed	0.9922	0.9724
	Not Allowed	0.8277	0.5524

The deep learning mechanism, Long Short-Term Memory, retrieves the data that is kept on the Blockchain and uses it for analysis. A customized alarm system is sent to the registered cell phone number, and an extensive review of the sick person's electronic health record. The dataset's nine features—Identification number, age, gender, illness, body weight, time of consultation, medication, analysis, and regime specification—are used in the proposed work.

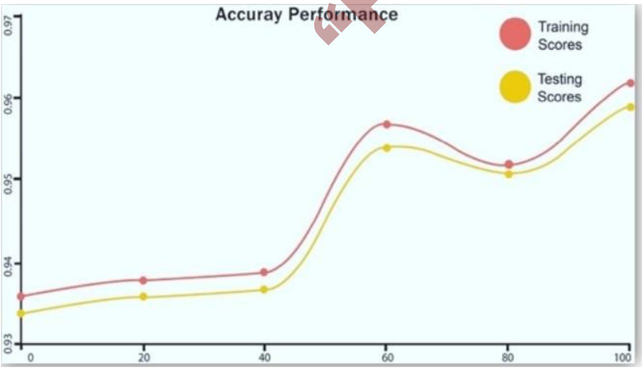

Fig. (6). Shows verified values & measures for GRU. (*A higher resolution / colour version of this figure is available in the electronic copy of the article*).

To get correct findings, the taxonomical analysis is performed using a number of features. Long-Short Term Memory (LSTM) and Gated Recurrent Unit (GRU), both Recurrent Neural Network approaches, are used in the study of the EHR. The list of acronyms is shown in Table **1**, and the features employed in the model are shown in Table **2**. As a result, Table **3** compares the precision, recall, and F1 score of the two combined Blockchain and Recurrent Neural Networks when analyzing the EHR. (Fig. **4**) displays the training and testing results for the LSTM. The training curve is represented by the red line in the graph, while the testing curve is shown by the yellow line. Training curves begin at 94% and increase to 94.6% after 51 epochs. The testing curve begins at 95%, increases to 98%, and then decreases to 97%. (Fig. **5**) displays the training and testing losses for the LSTM. The testing loss is shown in yellow, whereas the training loss is shown in red. The training loss starts out at 0.26 and dropsto 0.127 over time.

The measurement for downfall begins at 0.20 and reaches 0.074 with a time period. (Fig. **6**) displays the results from the GRU training and testing, whereas "(Fig. **7**) displays the results from the GRU training and testing in terms of losses. The training curve is shown in Fig. (**5**) as a red curve. The testing and training results for GRU range from 92% to 96%. Similar to this, the yellow curve showing the testing results for the LSTM starts at 95% and increases to 97.5%. (Fig. **7**), shows the loss begins at 0.4 and starts to decline after 51 iterations. Then, it approaches 0.2. The testing loss behaves similarly, starting at 0.3 and fallinguntil it hits 0.06.

According to Table **3**, the LSTM model performs better than another model in terms of F1 score, recall, and preci-

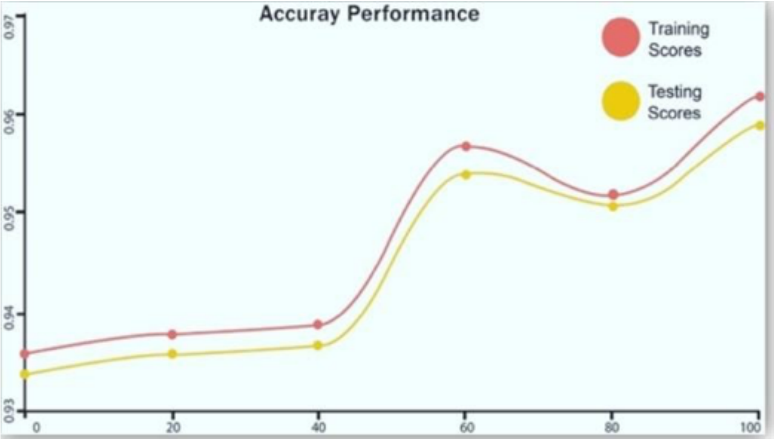

Fig. (7). Shows verified values & measures for GRU(Loss). (*A higher resolution / colour version of this figure is available in the electronic copy of the article*).

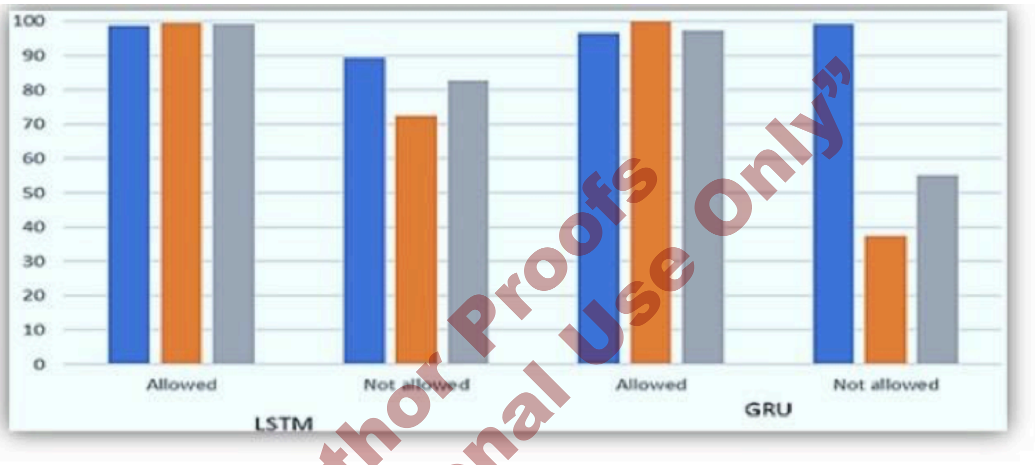

Fig. (8). Detailed analysis of LSTM & GRU. (*A higher resolution / colour version of this figure is available in the electronic copy of the article*).

sion. The accuracy, recall, and F1 measure scores for the Allowed LSTM were 97%, 98%, and correspondingly. The precision, recall, and F1 measure scores for the Not Allowed class were 86%, 76%, and 80%, respectively. Although not as good as LSTM, the performance of other model named Integrated Blockchain-GRU is also went well. In Fig. (**8**), a contrast model is shown for both outputs.

CONCLUSION

The paper suggests using the Inter Planetary File System protocol and an integrated Blockchain-deep learning algorithm to store the digital medical records in the Hyperledger Fabric platform to make data decentralized as well as secure and easily accessible. While storing data, an integrated approach of deep learning mechanism, namely Recurrent Neural Network techniques and Long-Short-Term Memory and Gated Recurrent Units, is used to assess the recorded digital health records for a sick person. This combined approach also sends an alert regarding medical advice, a schedule for medicine, any health wellness alert, and a regime specification to the sick person's registered device. In this proposed study, the major concern lies in generating alarm on the basis of different attributes like age, gender, body weight, illness, medication chart, and meeting date. The LSTM outperforms the other models in terms of precision, recall, and F1 score, according to testing results. Although this work is realistically feasible, compared to the conventional model, the maintenance cost is higher. The android calendar application and fitness apps can work together in the future to improve the alert system and offer a solution for a more affordable model.

LIST OF ABBREVIATIONS

EHR	=	Electronic Health Record
EU1	=	End User
PH1	=	Physician
PPK	=	Physician Private key
SK	=	Session Key
SP1	=	Sick Person
SPK	=	Sick Person Private Key
SPV	=	Sick Person View of Data
SUK	=	Sick Person Public Key

CONSENT FOR PUBLICATION

Not applicable.

FUNDING

None provided.

CONFLICT OF INTEREST

The authors declare no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] R.K. Siva, M.K. Manoj, R.G. Thippa, K. Neeraj, K.R.M. Praveen, S. Bhattacharya, D.Y. Suh, and M.J. Piran, "A Blockchain-Based Credibility Scoring Framework for Electronic Medical Records", *IEEE Access, Globecom Workshop,* 2020, pp. 978-1-7281-7307-8 **INCOMPLETE..**

[2] M. Pilkington, "Blockchain technology: Principles and Applications", In: F.X. Olleros, and Z.E.E. Majlinda, Eds., *Research Handbook on Digital Transformations.* 2016. **INCOMPLETE..**

[3] I. Eyal, A.E. Gencer, E.G. Sirer, and R.V. Renesse, "Bitcoin-NG: A scalable blockchain protocol", *13th Usenix Conference on Networked Systems Design and Implementation (NSDI'16),* 2020, pp. 45-59 Berkeley, CA,USA.

[4] CoinMarketCap.Com, "Crypto Currency Market Capitalization", Available from: https://coinmarketcap.com/currencies/ (Accessed on: August 15, 2018).

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", Available from: http://www.bitcoin.org/bitcoin.pdf

[6] "Universa, (2016), Blockchain is Reshaping the Banking Sector", Available from: https://medium.com/universablockchain/blockchain-is-reshaping-the-

[7] I. Kar, "Estonian Citizens Will Soon Have the World's Most Hack-Proof Health-Care Records", Available from: http://qz.com/628889/this-eastern-european-country-is-moving-its-

[8] D. Oparah, "3 Ways That the Blockchain Will Change the Real Estate Market", Available from: http://techcrunch.com/2016/02/06/3-

[9] P. Joshi, "The Blockchain of Things: Why it is a major game changer for Internet of Things", Available from: http://www.forbesindia.com/blog/health/the-blockchain-of-things-why-

[10] W.J. Gordon, and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability", *Comput. Struct. Biotechnol. J.,* vol. 16, pp. 224-230, 2018. http://dx.doi.org/10.1016/j.csbj.2018.06.003 PMID: 30069284

[11] M.S. Sahoo, and P.K. Baruah, "HBasechainDB – A scalable blockchain framework on Hadoop ecosystem", *Asian Conference on Supercomputing Frontiers,* pp. 18-29 http://dx.doi.org/10.1007/978-3-319-69953-0_2

[12] A. Zhang, and X. Ma, "Decentralized Digital Certificate Revocation System Basedon Blockchain", Available from: https://www.researchgate.net/publication/327325392_Decentralized_Digital_Certificate_Revocation_System_Based_on_Blockchain

[13] A. Yakubov, W.M. Shbair, A. Wallbom, and D. Sanda, "Blockchain-BasedPKI Management", Available from: https://orbilu.uni.lu/bitstream/10993/35468/1/

[14] M.Y. Kubilay, M.S. Kiraz, and H.A. Mantar, "A new PKI model with certificate transparency based on blockchain", *arXiv,* 2018. **INCOMPLETE..** http://dx.doi.org/10.48550/arXiv.1806.03914

[15] *"Accredited certificate authentication system",* Patent WO2018008800A1 **INCOMPLETE..**

[16] "Vitalik Buterin Ethereum white paper made simple", Available from: https://blockchainreview.io/wpcontent/uploads/2013/02.01._final_Ethereum-White-Paper-Made-Simple.pdf

[17] D. Emmons, "White paper and Demo: UX for Authenticated & Verified ERC20 Payments Using MetaMask and EthSigUtil", Available from: https://medium.com/coinmonks/whitepaper-and-demo-ux-

[18] G. Sabarmathi, and R. Chinnaiyan, "Investigations on big data features research challenges and applications", *2017 International Conference on Intelligent Computing and Control Systems (ICICCS),* 2017, pp. 782-786, Madurai. http://dx.doi.org/10.1109/ICCONS.2017.8250569

[19] M. Asif-Ur-Rahman, F. Afsana, M. Mahmud, M.S. Kaiser, M.R. Ahmed, O. Kaiwartya, and A. James-Taylor, "Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things", *IEEE Internet Things J.,* vol. 6, no. 3, pp. 4049-4062, 2019. http://dx.doi.org/10.1109/JIOT.2018.2876088

[20] S. Biswas, T. Akhter, M. Kaiser, and S. Mamun, "Cloud based healthcare application architecture and electronic medical record mining: An integrated approach to improve healthcare system", *2014 17th International Conference on Computer and Information Technology (ICCIT),* pp. 286-291, 2014. **INCOMPLETE..**

[21] T.D. Gunter, and N.P. Terry, "The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions", *J. Med. Internet Res.,* vol. 7, no. 1, pp. e3, 2005. http://dx.doi.org/10.2196/jmir.7.1.e3 PMID: 15829475

[22] D. Ivan, "Moving toward a blockchain-based method for the secure storage of patient records", In: *ONC/NIST Use of Blockchain for Healthcare and Research Workshop.* ONC/NIST: Gaithersburg, MD, United States, 2016, pp. 1-11.

[23] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management", *2016 2nd International Conference on Open and Big Data (OBD),* pp. 25-30, 2016. **INCOMPLETE..** http://dx.doi.org/10.1109/OBD.2016.11

[24] B. Vardhini, and N. Shreyas, "A blockchain based electronic medical health records framework using smart contracts", *International Conference on Computer Communication and Informatics (ICCCI -2021),* 2021, Coimbatore, INDIA. **INCOMPLETE..** http://dx.doi.org/10.1109/ICCCI50826.2021.9402689

[25] K. Sears, and D. Stockley, "Influencing the quality, risk and safety movement in healthcare", In: *Conversation with International Leaders.*. CRC Press, 2017. **INCOMPLETE..** http://dx.doi.org/10.1201/9781315588476

[26] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records", *IEEE Access,* vol. 7, pp. 147782-147795, 2019. http://dx.doi.org/10.1109/ACCESS.2019.2946373

[27] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with finegrained access control in decentralized storage systems", *IEEE Access,* vol. 6, pp. 38437-38450, 2018. http://dx.doi.org/10.1109/ACCESS.2018.2851611

[28] Md. Abdullah Al Mamun, F.J. Umor, A. Sami, M.K. Shamim, A. Sami, and K. Asif, "A combined framework of interplanetary file system and blockchain to securely manage electronic medical records", *Proceedings of International Conference on Trends in Computational and Cognitive Engineering, Advances in Intelligent Systems and Computing,* 2021p. 1309 **INCOMPLETE..** http://dx.doi.org/10.1007/978-981-33-4673-4_40

[29] S. Hohenberger, and B. Waters, "Online/offline attribute-based encryption. In: Public-Key Cryptography - PKC 2014", *17th International Conference on Practice and Theory in Public-Key Cryptography,* Buenos Aires, Argentina, 2014.

[30] (30) B. David, P. Gaži, A. Kiayias, and A. Russell, "Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain", *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.,* Springer: Tel Aviv, Israel, pp. 66-98, 2018. http://dx.doi.org/10.1007/978-3-319-78375-8_3

(30) "First Bitcoin Cash Block Mined", Available from: https://news.bitcoin.com/fork-watch-first-bitcoin-cash-block-mine (Accessed on: Sep. 1, 2019).

[31] "Lumino Transaction Compression Protocol(LTCP)", Available from: https://docs.rsk.co/ LuminoTransactionCompressionProtocolLTCP.pdf (Accessed on: Sep. 1, 2019).

[32] R. Yang, F.R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges", *IEEE Commun. Surv. Tutor.,* vol. 21, no. 2, pp. 1508-1532, 2019. http://dx.doi.org/10.1109/COMST.2019.2894727

[33] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things characterization of fog computing", *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing,* 2012, Helsinki, Finland, pp. 13-15. http://dx.doi.org/10.1145/2342509.2342513

[34] D. Koo, K. Piratla, and C.J. Matthews, "Towards Sustainable Water Supply: Schematic Development of Big Data Collection Using Internet of Things (IoT)", *Procedia Eng.,* vol. 118, pp. 489-497, 2015. http://dx.doi.org/10.1016/j.proeng.2015.08.465

[35] N. Fotiou, V.A. Siris, S. Voulgaris, and G.C. Polyzos, "Bridging the cyber and physical worlds using blockchains and smart contracts", *Workshop on Decentralized IoT Systems and Security,* 2019 San Diego , California , United States **INCOMPLETE..** http://dx.doi.org/10.14722/diss.2019.23002

[36] P. Giungato, R. Rana, A. Tarabella, and C. Tricase, "Current Trends in Sustainability of Bitcoins and Related Blockchain Technology", *Sustainability,* vol. 9, no. 12, pp. 2214, 2017. http://dx.doi.org/10.3390/su9122214

[37] A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, and B-G. Kim, "Blockchain based smart contracts for internet of medical things in e-healthcare", *Electronics,* vol. 9, no. 10, pp. 1609, 2020. http://dx.doi.org/10.3390/electronics9101609

[38] A. Srivastava, P. Bhattacharya, A. Singh, A. Mathur, O. Prakash, and R. Pradhan, "A distributed credit transfer educational framework based on blockchain", *2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T),* pp. 54-59, 2018. **INCOMPLETE..** http://dx.doi.org/10.1109/IAC3T.2018.8674023

[39] V. Mani, P. Manickam, Y. Alotaibi, S. Alghamdi, and O.I. Khalaf, "Hyperledger healthchain: patient-centric IPFS-based storage of health records", *Electronics,* vol. 10, no. 23, pp. 3003, 2021. http://dx.doi.org/10.3390/electronics10233003

[40] P. Bhattacharya, S. Tanwar, U. Bodke, S. Tyagi, and N. Kumar, "BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications", *IEEE Trans. Netw. Sci. Eng.,* vol. **•••**, pp. 1-1, 2019. **INCOMPLETE..** http://dx.doi.org/10.1109/TNSE.2019.2961932