

Int. J. Nonlinear Anal. Appl. 12 (2021) No. 2, 1513-1529 ISSN: 2008-6822 (electronic) http://dx.doi.org/10.22075/IJNAA.2021.5280

A novel deep learning framework for improving the quality of services using block chain technology

R.Parthiban^{a^*}, K. Santhosh Kumar^b

^a Department of CSE, IFET College of Engineering, Villupuram, India.

^bDepartment of IT, Annamalai University, Chidambaram, India.

(Communicated by Madjid Eshaghi Gordji)

Abstract

Electronic Health Record (EHR) holds immensely sensitive information and consisting of crucial data related to the patients. Storing and organising such data is highly arduous task. Researches still going on to improve the Quality of Service (QOS) of such data. Existing study focused only on improving the system throughput, privacy and latency issues. But they did not tend to scrutinize the scalability and privacy of such data records. In this paper, we propose a novel deep learning framework to improve the Quality of Service using block chain technology. Initially the data is classified into high priority and low priority based on its nature by using Recurrent Neural Network (RNN). Then, the classified high priority data is further allowed to each block of a block chain and the low priority data is stored and maintained as log file. Finally, the results are compared based on the evaluation metrics which demonstrates our proposed novel deep learning framework achieves better accuracy.

Keywords: Electronic Health Record (EHR), Quality of Service (QOS), Recurrent Neural Network (RNN), Block chain

1. Introduction

Recently, the health details about the patients had been increased tremendously. Hence, their health progress over a past few years had been maintained in the form of manual to electronic records. This record is known as Electronic Health Record (EHR). It contains crucial information about the patient's past medical history, medication complexity, radiology reports etc. Storing and organizing such crucial health details had been a cumbersome task. Hence healthcare data industries had extended Healthcare 1.0, Healthcare 2.0, Healthcare 3.0, Healthcare 4.0 and much more. Basically, healthcare 1.0 industries maintain all the details about the patient in the form of

^{*}Corresponding author: R.Parthiban

Email addresses: saranmds@gmail.com (R.Parthiban^{a^*}), santhosh09539@gmail.com (K. Santhosh Kumar^b)

manual records of paper format. So data about patient had been very transparent. Hence privacy and confidentiality had been a major concern. On basis of the concern of maintenance and to enhance better scalability healthcare 2.0 had been introduced. It is said to be e-health and mainly focussed on the advancement of technology using various devices and minimize the manual effort of humans. Hence effective storage and management mechanism is needed on the domain of healthcare. So cloud based server had been widely used in order to store and manage such data. Cloud server is the widely used data server, because of its accessibility is user friendly and its centralised server. Also the way of getting vulnerability is manifold, there have a possibility of numerous malicious attacks prone. So definitely the patient crucial medical histories will be steal. On the basis of this consideration, a decentralised server had been introduced with the same functionality which is known Healthcare 3.0. It is introduced mainly to focuses the EHR need to working on the mobile applications also manage services efficiently and need to take minimal cost. But it had been lacking of knowledge on the performance wise. In today's trends technology plays a versatile role, but it doesn't have ability to provide service on the basis of today's trend, means doesn't provide services in an intelligent way. So need an effective artificial intelligent mechanism over healthcare 3.0. In such a way that, we extract all our usage from healthcare record in an efficient manner. Hence the advancement of healthcare 3.0 is known as healthcare 4.0, which means importing various knowledge related today trends to healthcare 4.0 with help of artificial intelligent. Consequently effective decision making model are needed on the domain of healthcare 4.0 in order to take appropriate decision on the particular moment. Hence the advancement of artificial intelligence, effective deep learning models are used on the domain of healthcare which is known as healthcare 5.0. So it can able to deal with all the real time problem also satisfy all the patient expectations in a well advanced way. Parallelly the systems performance also enhanced and deals with various issues like handling complex mechanism, data fragmentation and lack of knowledge etc. So it provides a promising outcomes to the people who are accessing healthcare 5.0.



Figure 1: EHR records medical entities

Due to the advancement needed in the domain of healthcare sector, deep learning models are employed. Usually deep learning model plays a most significant role in the almost all the field of data science. It extract features easily from the dataset based on its functionality. It encompasses all the top trends of technology within its hands. While processing enormous amount of real time dataset, deep learning are widely used in today world. Usually with help of healthcare medical record, deep learning model has a wider capacity to diagnosis and predict the diseases in effortless fashion. In order to extract certain features from real time dataset, machine learning algorithm usually follows traditional approaches, which consist of i)Analyse ii)Select iii)Evaluate. So it is quite time consuming and performance wise lagging. So most powerful Deep learning models are deployed, for processing real time dataset. It is time efficient as well as effectively recognize features, extract pattern and provide best testing accuracy. DL models directly extract features from the dataset. So the performance had been enhanced. In recognition of images, DL model usually takes that corner and separate the image a fixed block. Each block is taken and train that block using activation function [11].

Deep learning model contributes its services to numerous domains which includes Natural language processing, Speech Recognition, computer vision [6, 17] etc. Because of its capacity of training, diversified domains make use this. Healthcare domain which includes various end-to-end learning mechanism with feature engineering, capability to manage multimodality, and complex dataset. Unsupervised data representation is the most complex function, because the class label is not available for prediction tasks. It actually forms clusters as the dataset, based on the common functionality of data items presented in the dataset. Therefore, the core concept in the backend of deep learning algorithms is artificial neural network (ANN). It consists of input nodes along with hidden layers. Hidden layers are associated to the training samples. Each layer is initialized with random weights. All nodes are known as neurons. Moreover, activation function associated with it, means the performance is based on that activation function (i.e. Sigmoid, Tanh, Relu).

The network is converged by minimizing cost function and optimizing weights by using:



Figure 2: Deep Neural Network Architecture

Blockchain technology is widely used nowadays, almost all the sector. Because of its privacy preservation mechanism everyone prefer block chain. It engineering world, this technology plays a versatile role and enhance secure transactions [29]. This technology enabled business with technological influence, and make a secured environment. Furthermore, it is a block of network in which each block are connected in a single chain and each block is using proper cryptography algorithm (ie. AES, SHA-256, RSA etc). If malware attacked at one block means, entire block will destroy its performance. By means of solving numerous problem, blockchain technology handles and managing various functionality [26]. It is widely used in almost today's sector like product origin tracking, logistics, supply chain management etc [23, 1]. Though it provides managerial functions in a secured way, chances of getting attacked also considerably high. Purpose of deal with this issue, we enhance a high energy values associated with each block. Hence the transaction would be processed in a secured way.



Figure 3: Block chain involved transaction

2. Related work and literature survey:

Nowadays, medical health records are widely used in the field of healthcare. Due to the advancement of technology, deep learning model had been deployed into that. Healthcare data is the crucial data, also the availability of resources from that data is widely needed. Hence healthcare 1.0, healthcare 2.0, healthcare 3.0, healthcare 4.0, healthcare 5.0 had been introduced [6]. In order to enhance security and privacy, EHR passed over each block of a blockchain network proposed by Christian et al. [6] . Lanxiang et al. [8] proposed the extended version of blockchain in the EHR, that is the logical expression. By using that expressing all index terms had been calculated. But each it calculates, means the system transaction had widely reduced and scalability is affected. Hence QOS had been affected.

In order to achieve mutual authentication for separate server, a medical health architecture is introduced. It allows unusual features and toughness at the lowest communication cost proposed by Amin et al. [3]. Also the client server communication is not discussed, hence it considered to be one of the trust issue. Gope et al. [12] introduced Secured IOT-based anonymous RFID structure at low rate of latency, which deal the anonymous attacks from various network. But identification and authorization of permission, FHIR Chain is applied over blockchain. It is successfully functioned and proposed by Peng et al. [30]. Though it provide authenticated service but it does not address interoperability functions. So deep learning framework is allowed over the EHR data, in which feature selection and extraction functions are carried over and it was proposed by Weng et al. [27]. It provides a distributed federated, collaborative DL models and reduce the scalability and effectively expose the functions as much as possible. However the learning function of trained model is not fixed in a proper sequence.

For the purpose of predicting time series and diagnosis of hardly possible disease, LSTM (Long short term memory) proposed by Pham et al. [22] have been significantly used. It deploys all the functionality within a simple fashion. This approaches also used word2vec for pre-training the dataset. Further advancement, need to process image with best accuracy, CNN (Convolution Neural Networks) are widely used and it successfully process the Electronic Health Record(EHR) and it was proposed by Suo et al. [21].

Then transfer learning approach is widely used and it is based on VGG-16 and it's an extension

of CNN model and it was proposed by Musaed et al. [2]. Jacobson et al. [16] compared the stacked Aes and RBM (Restricted Boltzmann Machine) and embedded that into word2vec-based approach for clinical evidences. They got better comparison result, when compared to [27].

The deep learning approaches applied over the EHR and its functionalities and sub-functionalities is mentioned in Table 1.

I G I I I I I I I I I I I I I I I I I I									
INPUT DATASET	Functionalities provided	Sub-functionalities provided							
Clinical evidences	Extraction of information	Concepts regarding to single							
		event							
		Event regarding to temporal							
		knowledge							
		Concepts regarding to Relative							
		based							
		Concepts regarding to							
		abbreviation based							
Codes regarding medical	Learning representation	Representation related to							
records		conceptual view							
		Details of representation							
		related to patient							
Correlated information	Prediction based on outcomes	Prediction based on static and							
		temporal							
Correlated information	Phenotyping	Identification of noval							
		phenotype							
		Available phenotypes must be							
		improved.							
Clinical evidences	De-identification	De-identification based clinical							
		text							

Table 1: Deep learning functionalities implements on EHR

3. System Model and Problem formulation:

This section delineate about the available system model and the problem formulation

i) System model:

Consider an Electronic Health Record (EHR) that is block chain based network, which consist of 4 layers of network that means layer 0, layer 1, layer 2, layer 3. The data flow movement is from layer 0 to layer 3, which means lowest level to higher level. In system model, layer 0 represents the various users belonging to healthcare. i.e. Healthcare Researchers, Laparoscopic Technician, Insurance agents, Patients, Doctors etc. Data generated by using automated sensor such as i) amperometic biosensor, ii) electrochemical biosensor iii) glucose biosensors etc. from various lab reports, lab test reports, drug research, insurance bills etc. The overall collected data is passed to the data level. In that level homogeneous reading is achieved by using sensor fusion algorithms [13] shown in **figure 4**. By use of Bayesian classifier, classification of every layer is done. In that, it takes mapping every layers to the corresponding organization. Hence the each and every user communication with the network will able share their resources to the authenticated user. Also the data is gathered from the HU and by means of processing, the appropriate features had been extracted. Additionally every layer forwarded that to next layer. By means of this, auto-updated is done. Consequently, every layer worked in distributed fashion, so the information processing is much more efficient also updation is done as well. Each and every layer security and privacy had been preserved by use of proper cryptography function. Hence the data stored in every layer must follow the sequence of security parameters.



Figure 4: Tradition Healthcare architecture using Blockchain architecture

ii) Problem Formulation:

Here, the data is not organized in a proper way, means while organizing a large amount of real time dataset. Need to much concentrate on various functionalities associated with it. This model does not categorized their sequence. Also that processing takes much time consuming as well as space consuming is much required. Hence the performance corresponding to every layer takes enormous amount of time, so the scalability have been affected, in such a way QOS has been affected. Additionally, the data performance over every layer takes random bit generation. So most of it process unnecessary lower order data. So effective classification algorithm is required, in which it need to classify the given data into higher order and lower order data. To address this problem, we will proposed a novel deep learning framework using blockchain technology.

4. Methodology

This section describes the proposed novel deep learning framework using block chain approach. The core idea behind this work is to increase the Quality of Service over EHR (Electronic Health Record). Usually Electronic Health Record (EHR) contains very crucial information about the patients. Hence processing of this record is a challenging task. From existing work, we found that the data classification is not done in an efficient way.

- i) Initially, we introduced Recurrent Neural Network (RNN) over the dataset, in which it classified the entire data set into higher order and lower order.
- ii) Then consider only the resultant higher order data, and passed that data into the each block in a chain. Also the lower order data is kept in a separate log file.
- iii) We proposed a new block-chain based mechanism, means of facilitating to share the over energy among neigh boring nodes. In such a way to enhance privacy preservation, also employed hash functions along with bilinear pairing.
- iv) Finally the resultant showed that proposed framework provides secured communication, also the Quality of Service had been increased.

The proposed work flow of the work is demonstrated as figure 5. Initially the input is taken from electronic health record. In experimentation purposes we used cardiography dataset. Then the dataset is split for training and testing purpose of the ratio 80:20. Then the dataset is classified by using Recurrent Neural Network (RNN). The classified dataset contains higher order and lower order data. The higher order data contain the all the necessary information for predicting the particular disease. Whereas the lower order data contains not unnecessary information, but it is not highly recommended in order to predict a particular diseases. And the lower order data is kept as a log file. Then the classified higher order data is allowed over each block of a network, their proper cryptography algorithm is maintained. Then that block chain network is the final output block which means, their all the necessary information about the patient is maintained. Also that is known as secured log file. While storing this, the scalability and integrity of a EHR is maintained, which means QOS is improved in our proposed system.



Figure 5: The proposed workflow

- 1: Input: Electronic Health Record
- 2: Split dataset: Training and Testing (80 : 20)
- **3:** If (Dataset = limited)
- 4: Do Passed over every block in a network
- 5: Else
- 6: Do Recurrent Neural Network // classified the higher and lower order data
- 7: Blockchain (Higher order data)
- 8: Log file(Lower order data)
- 9: Output: Secured log file

4.1. Classification using RNN:

From the viewpoint of EHR, usually hold a large amount of data because of its vast nature. Therefore, the processing of data sequence takes much time. Additionally, the data complexity has been increased. RNN generally takes input data from the sequence of order also by means of remembering the input data by use of internal memory. It a kind of promising algorithms, in which it does all its works in a powerful and efficient way. Recurrent neural network is usually works on the weather prediction, time series, speech recognition, financial data, audio, video etc. It involves much deeper grasping power over the dataset.

By selecting all the information over the network and fed to each input layer. Each neuron takes the input and each input as associated with weight. Also every neuron associated with hidden layer depends on its training the dataset.

While predicted, a set of input in a sequenced manner, RNN initially works just like an artificial neural network in which keep on applying activation function over every hidden layer[28, 25]. The output layer of RNN is expressed as:

$$o_t = \varphi(V_{st}) \tag{2}$$

$$s_t = f(U_{xt} + W_{st-1})$$
 (3)

V – Final matrix weight which is corresponding to each hidden layer.

st – Output value which corresponding to each hidden layer.

U – Initial matrix weight which is corresponding to each hidden layer.

 W_{st-1} – Like some influence weight, st-1 represent the output state of each hidden layer at time t - 1.

xt – value of input layer.

By combing the above 2 equation, we get the following equation, i.e.

$$o_t = \varphi(VfU_{xt} + Wf(U_{xt-1} + Wf(U_{xt-2} + Wf(U_{xt-3} + W_{st-4}))))$$
(4)

The equation stated above, determines that each output value related to RNN is closely associated to the output value related to it. The memory function of RNN determines this fact. So while find out solution of each sequence related to problem has to get positive effect. Hence classifying every state will determines the higher order as well as lower order data. The memory function needed, while performing some sequential functioning. Hence the determined sequence would

$$Ft = \sigma(Wf \cdot [ht - 1, xt] + bf) \tag{5}$$

where,

Wf – The weight matrix

bf – Paranoid term

xt – The input value which is corresponding time

ht - 1 – The previous time external state.

The Input Gate can be expressed as:

$$I_t = \sigma(Wi \cdot [ht - 1, xt] + bi) \tag{6}$$

Where

W – Input gate related to the weight matrix.

Bi - paranoid term related to Input gate.

Also, the output gate be represented as,

$$Ot = \sigma(Wo \cdot [ht - 1, xt] + bo) \tag{7}$$

Where

Wo - output gate related to the weight matrix.

Bo - paranoid term related to output gate.

For each state, ct the calculation and expression represents the,

$$ct^{\sim} = tanh(Wc \cdot [ht - 1, xt] + bc) \tag{8}$$

where, $ct \tilde{}$ - Inside state at each moment. For RNN, the corresponding final output is the solution of hybrid action of ot and ct, which will be denotes as:

$$ht = Ot \odot tanh(ct) \tag{9}$$

Furthermore, each set of input neuron of network will be following matrix format,

$$A = \begin{bmatrix} node1 & node2 & node3 & node4\\ node5 & node6 & node7 & node8\\ node9 & node10 & node11 & node12\\ node_m & node_m + 1 & node_m + 2 & node_m + 3 \end{bmatrix}$$
(10)

The nodes on the network is expected as

$$R = \begin{bmatrix} node_pre1\\ node_pre2\\ node_pre3 \end{bmatrix}$$
(11)

The softmax activation function is widely used to calculate the output in the output layer. Hence it is

$$Softmax(uj) = \frac{\exp(u_j)}{\sum U_q}$$
(12)

4.1.1. Higher order classified Data:

This data contains all the necessary details about the patient, in which it is classified by the RNN by using softmax activation function. Though is it the classified data, but need a proper normalization mechanism is needed over the higher order data. Also while classifying this, error function had been obtained for the given cost function.

i) Mean Squared Error: It is usually helpful to findout the error, so that backpropagate and keep on updating the weight function. The formula used to find out this is,

$$MSE = \frac{1}{n}\sum(y-\widehat{y})^2$$
, $(y-\widehat{y})$: The square of the difference between actual and prectifed.

ii) Mean absolute Error: It is also used for the performance evaluation of the model in which used to findout the deviation between the actual and predicated value. The formula used to find out is that,

$$MAE = \frac{1}{n} \sum_{\substack{i=1\\ \text{test set}}}^{n} |y_i - \hat{y}_i|$$

The below graph shows the exact difference between the predicted as well as actual value and their differences.



Figure 6: Difference between actual and predicted value

4.1.2. Lower order Classified Data:

This data contains the unnecessary data and it increases the complexity of an processing time and space. Hence while, classifying the entire data, we separate this by using recurrent neural network also it is kept stored as a log file. The activation function is softmax.

4.2. Block chain based scheme:

For security purposes, the environment depends on a secured platform. Hence we applied all our higher order classified data is passed over the blockchain. The neighboring nodes and some other excess energy is also passed into the block. This network aims to provide strengthen the entire network strong as well as reduce the malicious situation such as possible attacks. Hence the creation of block been more secured as well as stable based on the current environment. The following algorithm demonstrates the distribution of block on entire network, which means the created sequence is allocated as well as destroy the block, once the participation is done. The provided cryptography algorithm makes a sequence of action in which the random sequence of block will not hold the information.

Algorithm : Allow data over each Block.

Input: $t, N = \{createx, Allocatex, key_functionsx, logfilex\},\$

// where x is the set of numbers range from $(1, \ldots, n)$

// means block generation

Initialization: Time function is set also the view as **VIEW** Output: Log file generation

1: Set VIEW = 0;

- 2: Q_x which initialize a message <PRE-PREPARE_FUNCTION, *blockcreationi*, σi , *sec*>, with a sequence of random number in *Sec*;
- 3: After the time t, the Q_x node sends <PRE-PREPARE_FUNCTION, *blocki*, σi , *sec>* to N; //N denotes function of numbering of block from 0 to n.
- 4: After completion of block creation, each node ∈ N replies
 with a consistent message at a given time which means allocation of block space
 <PREPARE, blocki, sec> to all N_the Px and EB node do not participate in sending the replies phase;
- 5: Each node $\in N$, upon receiving at least 2f<PRE-PREPARE_FUNCTION, *blocki*, σi , *sec>* and <PREPARE,*blocki*, *Sec>*, sends a message <COMMIT, *Blocki*, *sec>* to all *N*_the *EB* node which does not participate in this exact step;
- 6: Every node ∈ N, upon receiving at least 2f + 1
 <COMMIT, Blocki, sec>, reaches an consensus and publishes a set of full block also return Reached;
- 7: if the EB node does not receive a response after 2VIEW t then;
- 8: run the algorithm 3 and **return** not reached;
- 9: **end if**

4.2.1. Key Generation:

An Gaussian distribution function over a secret key generation in which Z symbol is used, so that the sent E[P] is derived from root block in which the polynomial function had been introduced also defined the root block as (root0, root1, root2,..., rootek). Then corresponding criteria of each root value must satisfies $|R| < R_N$, which means that the range depends on every lattice polynomial associated with it. Each counter is initialized as 1 that means session key is generated over the sequences in order to maintain the uniqueness of a function. Also the secret key generation is mainly based on the reduced polynomial function. At the final step, the secret key parameter as $(R_N, ID_1, ID_2, nonce)$ is send along with each block through secure communication channel.

4.2.2. Signature Generation:

Each time, at the time of creating the block, and random sequence number is generated in which the corresponding signature parameters are computed also received X1 and X2 from generated key phase. The generated signature takes each values from pos_list and sign_list. Then the rejected signature is again passed to each counter space. Hence the computed sequence would be (S, SK, counter).



Figure 7: Blockchain network to provide network channel

5. Results

For Experimentation purposes, we used EHR (Cardiography dataset). In order to increases Scalability and integrity QoS, Initially the dataset is classified into higher order and lower order data by using RNN classifier. We used google colaboratory under Python 3 using TensorFlow library and which also includes the packages such as keras, numpy, pandas. Numpy is used for doing vectorization. Pandas library is used for analysing and manipulating the data. Our experimentation consist of three main stage. The dataset is initially classified into the ratio of 80:20 for training and test purposes.

- 1. Initially, we compare the unclassified data accuracy along with RNN classified data accuracy.
- 2. Then the performance of our blockchain network will be calculated and compared with exisiting blockchain network.

5.1. Evaluation Metrics

The accuracy of the RNN classification process is classified using the formula(12). The detection of an attack in a block chain is proportional to the detection rate. Furthermore, the accuracy TP denotes true positive means predict positive as positive, TN denotes true negative means predict negative as negative, FP denotes False positive means predict negative as positive, FN denotes False negative means predict positive as negative.

Accuracy =
$$\frac{TP + TN}{TP + TN + FP + FN}$$
 (12)

Detection rate =
$$\frac{TT}{TP + FN}$$
 (13)

False alarm rate =
$$\frac{FP}{FP + TN}$$
 (14)

5.2. Dataset Description:

S. No	Attribute Name	Туре		
1	LB	Real		
2	AC	Real		
3	FM	Real		
4	UC	Real		
5	DL	Real		
6	DS	Real		
7	DP	Real		
8	ASTV	Real		
9	MSTV	Real		
10	ALTV	Real		
11	MLTV	Real		
12	Width	Real		
13	Min	Real		
14	Max	Real		
15	Nmax	Real		
16	NZeros	Real		
17	Mode	Real		
18	Mean	Real		
19	Median	Real		
20	Variance	Real		
21	Tendency	Real		
22	FHR pattern class code	Real		
23	Fetal state class code	Categorical		

Table 2: Description of Cardiography dataset

Cardiography dataset consist of 23 attributes in which each attributes contains, the corresponding data associated with it.

The fetal class code contains 3 values (1,2,3). Also replaced the integer 1 with the variable "one", 2 with the variable "two", 3 with the variable "three". The summary of the dataset as given below.

- i) #Classes: 3 (one, two, three)
- ii) #Instances: 2126
- iii) #Total attributes: 23

	Recurrent Neural			Unclassified Data(Testing time)				
	Network(Testing time)							
	Accuracy	CPU	GPU	TPU	Accuracy	CPU	GPU	TPU
HL=10	97.784%	2.15	1.82	1.32	63.964%	83.232	82.343	73.343
HL=20	97.982%	3.82	1.99	1.67	65.983%	122.983	98.123	87.232
HL=30	98.862%	9.85	2.32	2.06	67.387%	223.98	212.232	193.243
HL=40	98.998%	40.76	33.68	32.74	69.983%	343.932	330.232	234.343
HL=50	99.251%	42.65	38.87	36.43	71.232%	543.938	520.343	432.178
HL=60	99.376%	82.87	78.33	65.93	72.343%	653.983	620.432	539.232

Table 3: Comparison of Accuracy of the classified data (RNN) over unclassified data

Table 2 summarizes the comparison of accuracy of the RNN classified data to the unclassified data in which HL stands for hidden Layer and number of epochs= 46. As the number of hidden layer increases, the accuracy is improved. The Bold letter indicates the highest accuracy we achieved. Also corresponding CPU, GPU, and TPU time are mentioned in the table. The bold indicates the maximum time required in order to compute the entire computation.

Figure 8 shows the comparison of accuracy over the unclassified and recurrent neural network classified data. Resultant shows that the our proposed deep learning framework provides better accuracy, which means Quality of Service of the given model had been increased.



Figure 8: Comparison graph of Recurrent neural network(Classified data) and unclassified data

Conclusions In this work, we introduced a deep learning framework for improving the Quality of Services using blockchain. Also, we achieved the highest accuracy at the testing phase. Our deep learning framework consists of RNN which actually classifies the dataset into higher order and lower order based on its preferences. Moreover, the proposed method achieved the highest accuracy of 99.376% and the corresponding CPU, GPU, TPU time were 82.87, 78.33, and 65.93, respectively. Then, the classified higher order dataset is further applied over each block of a network in which the scalability and integrity is improved which is the most important QOS. In future works, we are going to integrate this into an IoT environment. In addition, in order to maintain data processing speed, we will incorporate big data into it.

References

- N. Z. Aitzhan and D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, IEEE Trans. Dependable Secure Comput., 15(5), Sep./Oct. 2018, pp. 840-852.
- M. Alhussein and G. Muhammad, Voice pathology detection using deep learning on mobile healthcare framework, IEEE Access, 6, 2018, pp. 41034-41041.
- [3] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan and N. Kumar, An efficient and practical smart card based anonymity preserving user authentication scheme for tmis using elliptic curve cryptography, Journal of Medical Systems, 39, Oct. 2015, pp. 1-18.
- [4] G. S. Aujla, R. Chaudhary, K. Kaur, S. Garg, N. Kumar and R. Ranjan, Safe: Sdn-assisted framework for edge-cloud interplay in secure healthcare ecosystem, IEEE Transactions on Industrial Informatics, 15(1), 2019, pp. 469-480.
- [5] H. Bao and R. Lu, Comment on privacy-enhanced data aggregation scheme against internal attackers in smart grid, IEEE Transactions on Industrial Informatics, 12(1), 2016, pp. 2-5.
- [6] P. Bhattacharya, S. Tanwar, U. Bodke, S. Tyagi and N. Kumar, Bindaas: Blockchain-based deep-learning as-aservice in healthcare 4.0 applications. IEEE Transactions on Network Science and Engineering, 2019.
- [7] P. Bhattacharya, S. Tanwar, R. Shah and A. Ladha, Mobile edge computing-enabled blockchain framework-a survey, in Proceedings of ICRIC 2019 (P. K. Singh, A. K. Kar, Y. Singh, M. H. Kolekar and S. Tanwar, eds.), Springer International Publishing, (Cham), 2020, pp. 797-809.
- [8] L. Chen, W. K. Lee, C. C. Chang, K. K. R. Choo and N. Zhang, Blockchain based searchable encryption for electronic health record sharing, Future Generation Computer Systems, 95, 2019, pp. 420 -429.
- [9] C. Esposito, A. De Santis, G. Tortora, H. Chang and K. K. R. Choo, Blockchain: A panacea for healthcare cloudbased data security and privacy, IEEE Cloud Computing, 5(1), 2018, pp. 31-37.
- [10] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, Blockchain technologies for the Internet of Things: Research issues and challenges, IEEE Internet Things J., 6(2), Apr. 2019, pp. 2188-2204.
- [11] I. Goodfellow, Y. Bengio and A. Courville, *Deep Learning*, MIT Press, 2016.
- [12] P. Gope, R. Amin, S. H. Islam, N. Kumar and V. K. Bhalla, Lightweight and privacy-preserving rfid authentication scheme for distributed iot infrastructure with secure localization services for smart city environment, Future Generation Computer Systems, 83, 2018, pp. 629 - 637.
- [13] R. Gravina, P. Alinia, H. Ghasemzadeh and G. Fortino, Multi-sensor fusion in body sensor networks: State-ofthe-art and research challenges, Information Fusion, 35, 2017, pp. 68- 80.
- [14] Z. Guan et al., Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities, IEEE Commun. Mag., 56(7), Jul. 2018, pp. 82-88.
- [15] J. J. Hathaliya, S. Tanwar, S. Tyagi and N. Kumar, Securing electronics healthcare records in healthcare 4.0: A biometric-based approach, Computers & Electrical Engineering, 76, 2019, pp. 398-410.
- [16] O. Jacobson and H. Dalianis, Applying deep learning on electronic health records in Swedish to predict healthcare associated infections, In Proceedings of the 15th Workshop on Biomedical Natural Language Processing, (Berlin, Germany), Association for Computational Linguistics, Aug. 2016, pp. 191-195.
- [17] N. Kabra, P. Bhattacharya, S. Tanwar and S. Tyagi, Mudrachain: Blockchain-based framework for automated cheque clearance in financial institutions, Future Generation Computer Systems, 102, 2020, pp. 574-587.
- [18] H. J. Kim and H. S. Kim, Auth hotp-hotp based authentication scheme over home network environment, In International Conference on Computational Science and Its Applications Santander, Spain, Springer, 2011, pp. 622-637.
- [19] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta and K. K. R. Choo, Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks, Computer Networks, 129, 2017, pp. 429-443.
- [20] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng and Y. Zhang, Consortium blockchain for secure energy trading in industrial Internet of Things, IEEE Trans. Ind. Inform., 14(8), Aug. 2018, pp. 3690-3700.
- [21] Y. Liu, T. Ge, K. Mathews, H. Ji and D. McGuinness, *Exploiting task-oriented resources to learn word embeddings for clinical abbreviation expansion*, In Proceedings of BioNLP, (Beijing, China), Association for Computational Linguistics, 15, July 2015, pp. 92-97.
- [22] T. Pham, T. Tran, D. Phung and S. Venkatesh, Deepcare: A deep dynamic memory model for predictive medicine, In Pacific-Asia Conference on Knowledge Discovery and Data Mining, Macau, China, Springer, 2016, pp. 30-41.
- [23] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie and M. Bertoncini, Blockchain based decentralized management of demand response programs in smart energy grids, Sensors, 18(1), 2018, p. 162. [Online]. Available: https://www.mdpi.com/1424-8220/18/1/162.

- [24] A. Srivastava, P. Bhattacharya, A. Singh, A. Mathur, O. Prakash and R. Pradhan, A distributed credit transfer educational framework based on blockchain, In 2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T), Allahabad, India, IEEE, 2018, pp. 54-59.
- [25] S. Srivastava and S. Lessmann, A comparative study of LSTM neural networks in forecasting day-ahead global horizontal irradiance with satellite data, Sol. Energy, 162, Mar. 2018, pp. 232-247.
- [26] The essential eight technologies board byte: Blockchain, Accessed: 30, Apr. 2019. [Online]. Available: https://www.pwc.com.au/pdf/essential-emerging-technologies-blockchain.pdf.
- [27] J. S. Weng, J. Weng, M. Li, Y. Zhang and W. Luo, Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive, IACR Cryptology ePrint Archive, 14, 2019, pp. 1-18.
- [28] T. K. Whangbo, S. J. Eun, E. Y. Jung, D. K. Park, S. J. Kim and C. H. Kim et al., *Personalized urination activity recognition based on a recurrent neural network using smart band*, Int. Neurourology J., 22(Suppl 2), Jul. 2018, pp. 91-100.
- [29] 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. Surveys Tut., 21(2), Apr./Jun. 2019, pp. 1508-1532.
- [30] P. Zhang, J. White, D. C. Schmidt, G. Lenz and S. T. Rosenbloom, *Fhirchain: applying blockchain to securely and scalably share clinical data*, Computational and structural biotechnology journal, 16, 2018, pp. 267-278.