International Journal of Computer and Engineering Optimization (IJCEO)
Volume 1, Issue 1, September – October (2023)

RESEARCH ARTICLE

SECURE BLOCKCHAIN BASED DEEP LEARNING APPROACH FOR DATA TRANSMISSION IN IOT-ENABLED HEALTHCARE SYSTEM

R. R. Sathiya[1 *], S. Rajakumar[2] and J. Sathiamoorthy[3]

[1]Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Coimbatore, India
[2]Department of Electronics and Communication Engineering, Panimalar Engineering College, Chennai, India
[3]Department of Computer Science and Engineering, RMK Engineering College, Tamilnadu, India

[*]*Corresponding e-mail: rajamani3314@gmail.com*

Abstract – Healthcare service quality has been improved by integrating the Internet of Things (IoT) with conventional medical networks. In contrast, device-mounted sensors and wearables employed in Healthcare Systems (HS) monitoring and data transmission ongoing over unprotected open channels to adjacent devices. The effectiveness of operations is being improved by the link among IoT devices and computers, yet it allows attackers to commit a variety of cyber-attacks that could jeopardize patients under vital observation. Using Deep-BiLSTM in a healthcare IoT system for Secure Data Transmission is presented in this paper. In particular, the first unique there is a suggested blockchain design that assure data security and reliability transfer through the use of the Zero Knowledge Proof (ZKP) mechanism. The validated data is then utilized to create a deep learning framework for identification of intrusions in the HS network. A Bidirectional Long Short-Term Memory (BiLSTM) and Deep Convolutional Neural Network (DCNN) are integrated to create a highly efficient intrusion detection method. experiments using two sources of open data (CICIDS-2017 and ToN-IoT) has been used to compare the proposed method with 96% better performance. The suggested BD-BiLSTM methodology has 98% precision, accuracy, recall, and F1 score, which is pretty high when compared to other approaches. of BDL-SMDTA, PBDL and GWMNN.

Keywords *– Internet of things, health care system, cyber-attack, deep-BILSTM, Zero knowledge proof mechanism (ZKP), deep convolutional neural network*

1. INTRODUCTION

Traditional healthcare systems have been transformed into intelligent ones through the Internet of Things (IoT), which allows patient data is continuously monitored and accessible remotely. In medical field, a number of medical devices powered by the Internet of Things (IoT) collect real-time health information of patients, such as their body temperature and other important details.[8] In fact, IoT can help the medical field in diagnosing and treating patients remotely. [9]. It is, however, possible to eavesdrop, manipulate the data, and exploit other security vulnerabilities in an IoT-authorized Healthcare System (HS) when the nodes are related 24/7 over an open, insecure public channel. [10] whereby attackers try to take advantage of the dependability, and security of IoT data and devices.[11]

To address the issues raised above, IoT-enabled healthcare is possible with blockchain and deep learning (DL). To begin, A block and a chain make up a blockchain (a form of public database). It is impossible to modify data once it has been blocking chain of immutable blocks recording data attacks [12]. Furthermore, consensus mechanisms support the reliability of distributed data stored on a blockchain. [13] As a result, while transmission through IoT-enabled HS, it is safe and reliable to consider the patient's medical information. [6] Because of blockchain's immutability and decentralized architecture, smart contracts can boost trust between parties engaged in the data transfer by independently enforcing and carrying out the terms of the contract.

To detect aberrant network behaviors and prevent HS attacks, The majority of intrusion detection systems are DL-based typically utilized over deep learning technologies. However, most with some attack types, IDS developed in the literature perform badly in terms of the rate of false alarms and detections. since they take data directly from the network. [14,15]. Furthermore, one of the key challenges with IoT-authorized HS is scalability. The justification is that, as the number of as the number of IoT device rises, to keep up, more storage space will be required for data generation's exponential expansion. [16]. These attacks not only target hospital network components with malicious

software or malware, but they also target genuine IoT devices with the goal of limiting their operation [17].

This strategy assumes that the communication's endpoints (IoT devices and Edge servers) cannot be completely trusted. Additionally, it is presumed that they speak on a channel that is open, public, and insecure. IoT devices and edge servers, however, are thought of as semi-trusted. A message delivered between two entities can have its contents changed by an attacker [18].

Also, the assailant obtains entry to important data and able in order to carry out a data poisoning assault. As a result, in order to prevent the information from being viewed by unauthorized parties, verifying the involved parties is crucial before initiating secret communication. Therefore, it is crucial to consider this approach while investigating IoT data security. [19].

Prior to secret communication, it is necessary to confirm that the involved parties to stop them from gaining access to the information [20-25]. As a result, it is critical to consider this paradigm while analyzing the security of IoT data [26-27]. Furthermore, scalability is one of the more major challenges in IoT-enabled HS [28,29]. The argument is that additional storage space will be needed as the number of IoT devices rises to support the exponential growth in data generated [31-35].

In this article BD-BILSTM was developed and implemented, as a result of combining blockchain and deep learning approaches, the aforementioned issues can be addressed. There are several main contributions to this paper:

- The BD-BILSTM system combines blockchain technology with deep learning (DL) techniques in order to transmit data securely.
- It is planned to implement a blockchain-authorized security framework. The fundamental technique uses zero knowledge evidence to register and verify IoT devices.
- The above technique validates data records, provides a standardized method for transmitting medical information in the HS network, and protects against data contamination threats.
- A security architecture with DL capabilities is suggested. A Deep convolutional neural network by using the (DCNN) technique, raw data can be encoded into a format that is more suitable for storage.
- The development of an intrusion detection system makes use of the Bidirectional Long Short-Term Memory (BiLSTM) technology.
- ToN-IoT and CICIDS-2017 network he proposed BD-BiLSTM framework is evaluated using datasets.
- Suggested method has been determined by the evaluation metrices of accuracy, precision, F1 score and recall.

Therefore, the remainder of the paper will be organized as follows: A review of the literature is presented in Part 2, followed by an evaluation of the proposed work in Section 3, a discussion of the findings in Section 4, and a conclusion in Section 5.

2. LITERATURE SURVEY

The relevant work in these fields is presented in this section, with a focus on the Deep-BiLSTM technique for Secure Data Transmission and conventional healthcare systems with higher-quality healthcare services. Some of those methods have been discussed in this section.

In 2020, Li, J. et al., [1] proposed a secure architecture for IoT-enabled healthcare system's edge computing on SDN. IoT device authentication is handled employing a straightforward authentication technique via the Edge servers. After authentication, SDN controller manages Resource allocation, network optimization, and load balancing for the healthcare system is connected to the Edge servers. With a reduction in network control overhead, it improves throughput, latency, packet delivery ratio, average reaction time, and overall network performance.

In 2021 Wang, K. et al., [2] proposed an IoT-cloud-authorized healthcare data system with forward privacy and verifiability, as well as Verifying a multi-keyword search method constructed using a pseudo-random function (PRF). This technique overcomes the challenge of scenario for top-K searches with just partial results to evaluate the accuracy of search findings. The trial's findings demonstrate the FEncKV system is appropriate for IoT-authorized healthcare systems.

In 2021 Arul, R. et al., [3] proposed an adaptable service compliance (BASC) effort is based on the blockchain to prevent non-dormant health care services from becoming a liability. Regarding providing and facilitating end users' utilization of medical data, it is trustworthy in overcoming dormancy worries. Verification of affordability is the result of learning, and background checks vouch for the accuracy of the information. This improves the aid's honesty while preventing healthcare service failures and delays.

In 2021 Li, W. et al., [4] proposed a thorough review making use of applying machine learning (ML) techniques to extensive data analysis in healthcare industry. It makes it possible for government agencies and healthcare professionals to keep up with the most recent developments in ML-based large-scale data analysis in healthcare. Additionally, it offers extensive and recent studies on big data analytics techniques for the Internet of Things and smart health based on machine learning. Also, full analysis of their advantages and disadvantages is given.

In 2021 Said, O. and Tolba, A., [5] proposed a significant IoT-authorized to provide a broad spectrum of communication amongst healthcare devices, healthcare architecture uses satellites and high-altitude platforms in addition to Internet coverage technologies. (HAPs). Efficiency of the suggested IoT-authorized healthcare framework is assessed using NS3. The results of the simulation demonstrate that the proposed IoT-enabled healthcare system outperforms the conventional healthcare design.

In 2021 Peneti, S. et al., [6] proposed a modular neural network-based network approach with gray wolf optimization is used to handle security in smart environments. (GWMNN). An optimized neural network is utilized in IoT-enabled smart applications to maintain latency and compute resource usage. In contrast to multi-layer perceptrons and deep learning networks, the system has minimal latency and good security (99.12%), according to simulation findings that are used to analyses the system's effectiveness.

In 2022 Sardar, A. et al., [7] proposed a secure facial recognition solution for the Internet of Things in medical. Cancellable biometrics, BioCrypto-Circuits, and BioCrypto-Protection Schemes are the three stages template protection approaches that have been established to protect biometric data. FERET, CVL, IITK, Casia-Face-v5, and these benchmark face databases were used to evaluate how well the proposed system will operate. Results are provided using suggested system's correct recognition rate and equal error rate.

In 2022 Zhang, L. et al., [8] proposed a federated learning continues even if the quantity of internet users declines. remains above a predetermined level in a dropout-tolerant technique. The security analysis shows that the proposed solution protects data privacy. The costs of computing and communication are theoretically studied as well. The experimental findings show that, in comparison to earlier methods, the suggested scheme provided positive results while preserving anonymity.

In 2022 Neelakandan, S. et al., [9] proposed a new secure medical data transfer and diagnosis model powered by blockchain (BDL-SMDTD). The BDL-SMDTD model's objective is to determine diseases with maximum detection rate while securely transmitting medical images. Using feature extraction based on ResNet-v2, the recommended BDL-SMDTD model's highest classification performance was attained with 96.94% sensitivity, 98.36% specificity, and 95.29 accuracy.

In 2022 Kumar, R. et al., [10] proposed Deep learning (DL) techniques are coupled with smart contracts and permissioned blockchain to produce the PBDL, a special platform for secure and effective data transmission. By the use of a smart contract-based consensus mechanism, PBDL initially uses a blockchain approach communication entity to be registered, checked (using zero-knowledge proof), and validated. The IoT-Botnet and ToN-IoT datasets used in the security analysis and testing results demonstrate the PBDL framework's superiority to other exiting techniques.

It can be seen from the reviews above that these methods have some shortcomings. This research proposes a Deep-BiLSTM technique Enabling Safe Data Transfer in Internet of Things-Approved Medical Systems to address these disadvantages.

3. PROPOSED METHODOLOGY

This part presented BD-BILSTM, which combines block chain and deep learning methods to ensure the accuracy of the data and secure data transmission in order to identify intrusion in the HS network.

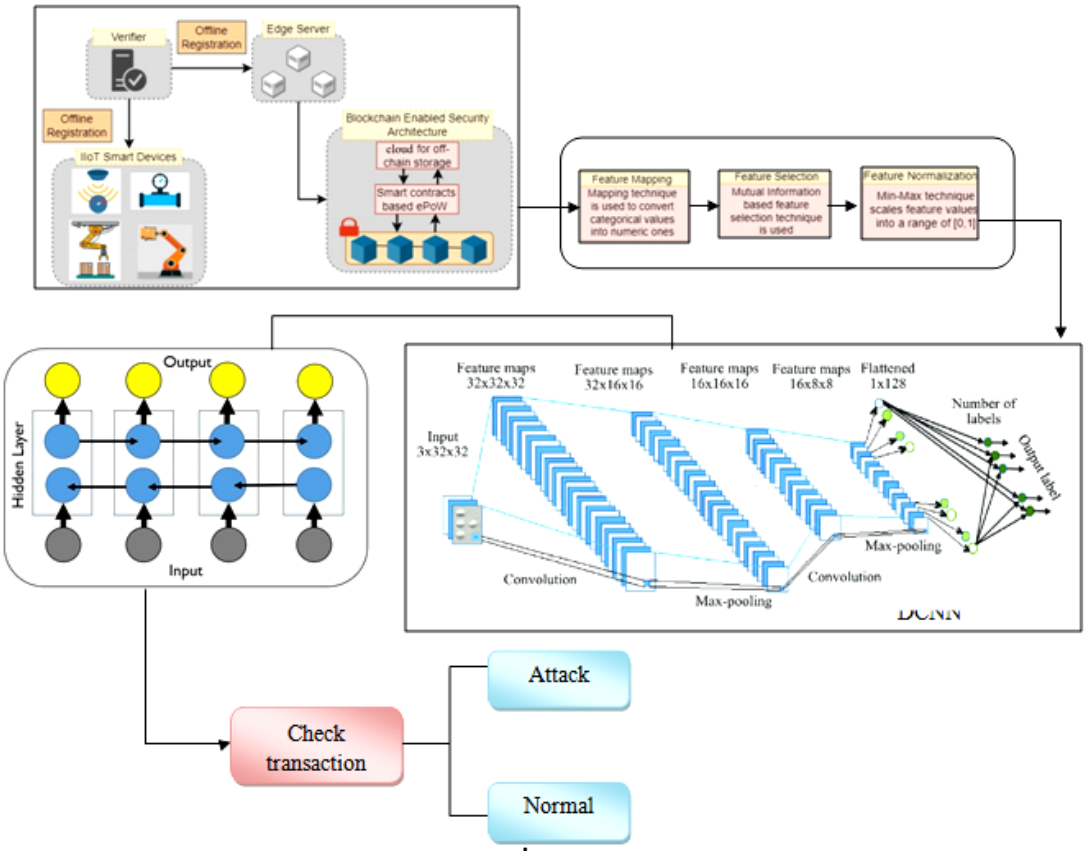

Figure 1. Overall block diagram of proposed method

The proposed BD-BILSTM is summarized in Figure 1, which shows the communication taking place among various parties. IoT devices are just one of the many communication entities included in this architecture. Verification *(V)*, edge servers (*EDGE*). All participating entities must be registered by V before being added to the network. Few resources and computational power are available to the S_{di}. The computing resources and power are constrained. Since each $S_{di}$is connected to the Internet, data can be sent and received online. (*EDGE*) includes data analysis servers, industrial computers, and other like gadgets. To undertake mining activities, one or more S_{di} are connected to EDGE. The BD-BILSTM systematic design consists of two major components: (i) a blockchain-authorized security framework and (ii) a deep learning-authorized security framework, this is illustrated in Figure.2 below and explained below,

To identify IoT device and safe data transfer, blockchain technology is employed. In the deep learning authorized security framework, transforming the original datasets' dimensions into a new structure using a DCCN approach. The way that these structures' function is explained in full below,

3.1. Block chain authorized security framework

The BD-LSTM is divided into six distinct phases in the first level of security: (i) initialization, (ii) registration and verification, (iii) encryption and decryption, (iv) block creation and validation, (v) data generation and block updation, and (vi) consensus. As shown below, all steps must be performed in a detailed manner.

(i) initialization phase

This stage is evaluated by trusted verifier *V* in order to bootstrap the framework settings. *V* adds the IoT sensor node S_d to the suggested framework.,

Step 1: With a Non-singular representation for the elliptic curve E_{P_N}(a, b): $y^2 = x^3 + ax + (b \bmod P_N)$, the verifier V selects the suitable biggest prime number P_N

Step 2: The verifier selects at random PR_{VK}(private key) ∈, Z_{P_N}Rk ∈ {0,1}Z_{P_N} and sets PR_{VK}as private key. Next, PB_{VK}(public key) is generated using $PB_{VK} = PR_{VK}$.

Step 3: Then, the Hash function H(.) based on one-way cryptography is chosen by V, and makes the required elements public.

(ii) Verification and Registration phase

IoT sensor node S_{di} asks the verifier *V* to join the blockchain network during the registration step. Once the *PK* is developed successfully, timestamp TS_i is stored for verification of the Sdi registration. • The PK is made up of ID_{sdi} vand M_{sd_i}which is submitted to verifier V with the time included.

(iii) Encryption and decryption phase:

A public key PB_{sd_i} and a private key PB_{sd_i} are produced once the IoT device S_{d_i} has been successfully registered by the verifying authority V.

$$CP1 = (P_N 1 * P_N) + SKEY_{sd_i} \quad (1)$$

$$CP2 = MSG_{sd_i} + \left(P_N 1 * PB_{sd_i}\right) + SKEY_{sd_i} \quad (2)$$

Here CP1 and CP2 denote the ciphertext. Finally, equation is used to decrypt the message (3)

$$MSG_{sd_i} = \left(\left(CP2 - PB_{sd_i}\right) * CP1\right) - SKEY_{sd_i} \quad (3)$$

(iv) Block generation and testing phase:

Beginning of S_{d_i} the block generation and evaluation procedure, For the Appropriate Recognition, brand-new block $ID_{sd_i}{}^{BLOCK}$ is performed by, which forwards it for inclusion into the blockchain with credentials. $PB_{sd_i}$and IB_{sd_i}. The real data is then preserved by the IPFS storage layer.

(v) Data generation and block updation:

This stage illustrates how S_{d_i} produces data and the corresponding block updates. $ID_{sd_i}{}^{TX}$ and makes updation in block. Furthermore, $ID_{sd_i}{}^{BLOCK}$ Becomes part of the blockchain network after being successfully updated.

(vi) Consensus phase:

Following the satisfactory ZKP verification, the ID_{sd_i} is produced, given to the appropriate Blockchain sensor node update, and IoT sensor node. In order to add transactions to the blockchain network and perform transaction verification, the *ePoW* consensus method is used i.e., I$ID_{sd_i}{}^{NEWIX}$by ID_{sd_i}.

3.2. Deep learning enabled security architecture

3.2.1. Deep convolutional neural network (DCNN)

In-depth learning Cyberattacks are recognized through a convolutional neural network (DCNN). Deep learning has the ability to reveal higher-level features and more abstract concepts that reveal links that are more complicated and interconnected than what is currently known about deep neural network methodologies.

Deep learning is defined by a significantly higher number of sequentially connected neural layers. Moreover, as a result of additional modifications, more data is typically needed for training and computational burdens as complexity increases. These developments provide the ability to quickly calculate repeated non-linear modifications of the crucial input data, which is the main strength of the architecture for deep learning and allows for end-to-end learning.

Three key ideas form the foundation of the CNN topology: temporal or spatial sampling, shared weights, as well as regional receptive domains. Hence, CNNs are often composed of various layers known as convolutional layers, and that small kernels comprise each convolutional layer that enable efficiently extracting high-level data. Layers that are fully connected receive input from the final convolutional layer.

The basic CNN model is composed of an alternating convolutional layer, input layer, non-linear layers and pooling or subsampling layers. In this case, has fewer completely linked layers, however a sofmax classifier is frequently found as the very last layer. Convolutional layers are made up of convolutional stages, detector stages, and pooling stages in accordance with a complex layer terminology.

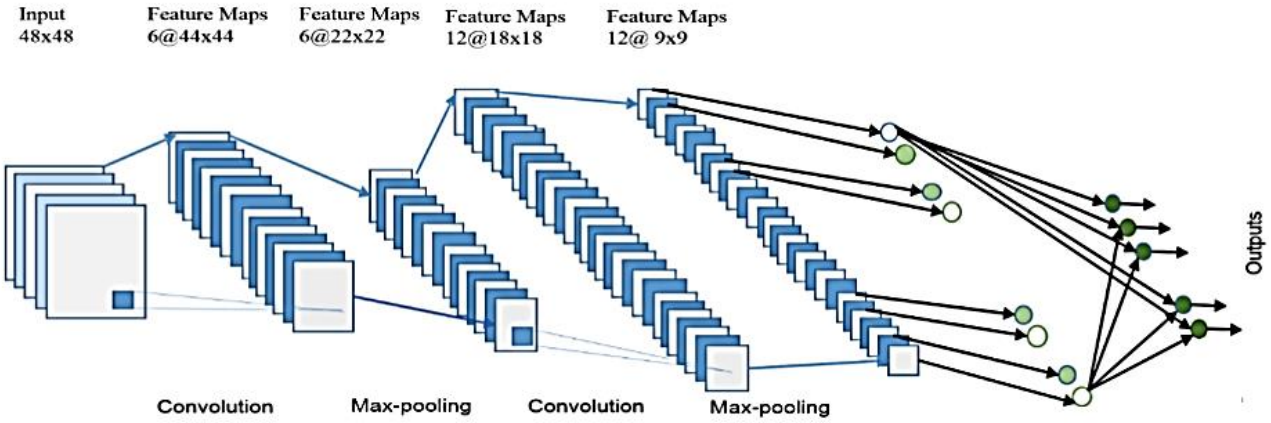

Figure 2. DCNN architecture

This indicates that there are multiple stages in each convolutional layer. Convolutional layers are routinely switched out with sub-sampling layers in order to speed up computation and eventually strengthen spatial and configurational invariance. This is a list of a CNN's fundamental layers.

Input layer:

Typically, a multidimensional array of data serves as the input. Where the network is fed data, Patterns, video signals, time series, or image pixels or their transformations can all be used as input data.

Convolutional layer:

It serves as CNN's main foundation. Convolution's main objective is to separate different characteristics from the input. Edges, corners, textures, and lines are among the low-level significant characteristics from which the first convolutional layer extracts information.

Non-linear layer or detector layer:

Each linear activation is detected by the detector stage using a nonlinear activation function. Many nonlinear activation functions are shown here. A neuron's output f as a function of its input x is typically represented as $f(x) = \tanh(x), sigmoid(x)$ or Rectified Linear Unit (ReLU). ReLU applies the function$y = \max(x, 0)$. The nonlinear properties are increased of the decision function in convolutional layer.

Pooling or down sampling layers:

Typically, a pooling layer decreases the feature maps' size of the feature maps and creates down sampled versions in the input map. Through pooling, the inputs are divided into regions of size $R \times R$with each region producing a single output. If a pooling layer receives an input of size $W \times W$, the output size P is calculated by,

$$P = \left|\frac{W}{R}\right|$$

The maximum output inside a rectangular region is the focus of the max pooling activity. Invariance is introduced using max pooling.

Fully connected layers:

The last level of the CNNs' topology, which is made up of a general multi-layer network, has been attained. In the subsequent layers, every activation from the previous layer will be a fully connected 1D layer. It is feasible to pull features from these layers to train another classifier.

3.2.2 Bidirectional Long Short-Term Memory (BiLSTM)

A model for sequence processing called Bi-LSTM comprises two LSTMs. One processing the information forward and the other processing it backward. The network can access more data with the aid of Bi-LSTMs, which is advantageous for the context of the algorithm. Bidirectional LSTM connects both of the hidden LSTM (Bi-LSTM) layers to the output layer. In the application, using two LSTM as one layer encourages improving the learning long-term dependency, which subsequently will increase model performance. Bi-LSTM architecture shows in Figure 3.

The reversed inputs from time $t-1$ to $t-n$ are used to calculate the backward LSTM layer output sequence $\overleftarrow{h}$ just because the unidirectional and forward LSTM layer output sequences, h and h′, are generated similarly. The function was then applied to these output sequences to create the output vector y_t. Similar to an LSTM layer, a Bi-LSTM layer's final output can be denoted by a vector, $Y_t = y_{t-n}, \ldots, y_{t-1}$ where the final element, y_{t-1}, is the anticipated heart rate for the subsequent iteration.

Given input tasks $X = (x_1 \ldots, x_T)$, the hidden vector tasks $h = (h_1, \ldots, h_T)$ and the output vector tasks $Y = (y_1, \ldots, y_T)$ using the subsequent equations from $t = 1$ to T.

$$h_t = H(W_{xh}x_t + W_{hh}h_{t-1} + b_h) \quad (4)$$

$$y_t = W_{hy}h_t + b_0 \quad (5)$$

Where W and b stand for weight and bias matrices, respectively, and the function for a hidden layer is H. H is often a sigmoid function applied element by element.

$$i_t = \sigma(W_{xi}x_t + W_{hi}h_{t-1} + W_{ci}c_{t-1} + b_i) \quad (6)$$

$$f_t = \sigma(W_{xf}x_t + W_{hf}h_{t-1} + W_{cf}c_{t-1}b_f) \quad (7)$$

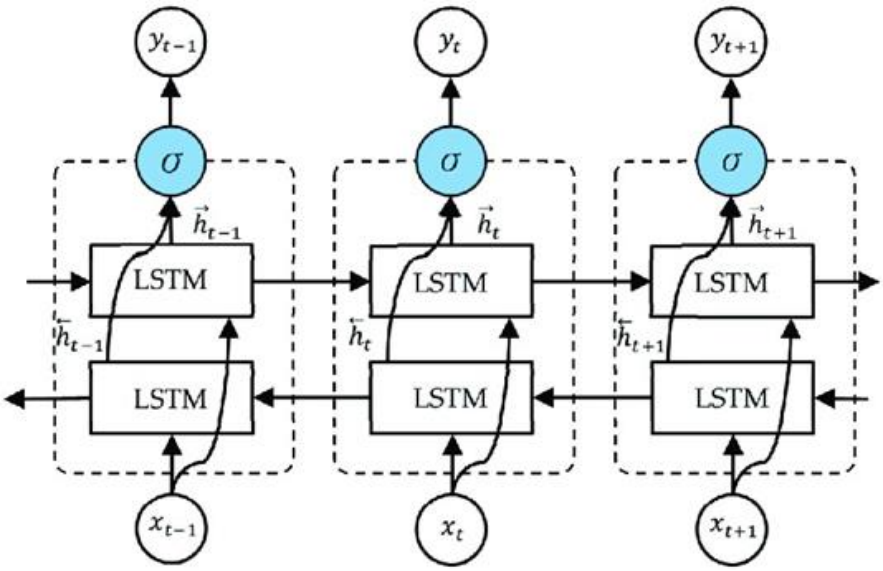

Figure 3. Bi-LSTM architecture

$$c_t = f_t c_{t-1} + i_t \tanh(W_{xc}x_t + W_{hc}h_{t-1} + b_c)$$

$$O_t = \sigma(W_{xo}x_t + W_{ho}h_{t-1} + W_{co}c_t + b_o) \quad (9)$$

$$h_t = O_t \tanh(c_t) \quad (10)$$

The input gate, forget gate, output gate, and cell activation vectors, respectively, are represented by the letters *i f, o* and c, while the logistic sigmoid function is represented by σ. These variables all have the same size as the hidden vector h. Input-output gate matrix W_{x0} and hidden input gate matrix W_{hi} are both used in computers.

The following formula is used to determine the output vector y(t).

$$y(t) = \sigma y(\overrightarrow{h_t}, \overleftarrow{h_t}) \quad (11)$$

where the σy function combines the hidden layer output neuron sequences. and is capable of adding, concatenating, multiplying, and averaging any of the four operations.

4. RESULT & DISCUSSION

This section rates the effectiveness of proposed BD-BiLSTM. The proposed model has been evaluated using the conventional numerical parameters listed below,

4.1 Evaluation Metrics

4.1.1. Accuracy

The accuracy of all correctly predicted categories to the dataset's actual classifications represents the prediction algorithm's accuracy. Equation (12) determines the model's accuracy. Each prediction model typically yields four distinct outcomes: False Negative (FN)., False Positive (FP), True Negative (TN), and True Positive (TP).

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

4.1.2. Precision

(8) Precision is an exact definition of the frequency of positive abnormalities in a particular picture. The higher proportion of information is highlighted by precision. Equation (13) calculates the precision of the model.

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} = \frac{\text{True position}}{\text{Total predicted position}} \quad (13)$$

4.1.3. Recall

The amount of accurate phishing URL predictions made over all URLs in the dataset is known as the prediction algorithm's recall. Equation (14) determines the model's recall.

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} = \frac{\text{True position}}{\text{Total prediction position}} \quad (14)$$

4.1.4. F1 score

The method of calculating the classifier's harmonic mean for recall and precision. It is possible to turn it into a single metric. Equation (15) determines the model's F1 score.

$$\text{F1 score} = \frac{2\times(\text{precision}\times\text{recall})}{(\text{precision+recall})} \quad (15)$$

4.2 Performance metrics

Figure 4 displays the comparability analysis's accuracy and F1 score for the suggested and existing methods.

The new BD-BiLSTM approach is compared to the existing PBDL, BDL-SMDTD, and GWMNN. The prediction results were examined using measures for precision, F1 score, recall, and accuracy.

The proposed BD-BiLSTM is high in comparison to other existing approaches. The size of the F1 is 0<100 in size, shown in figure 4.

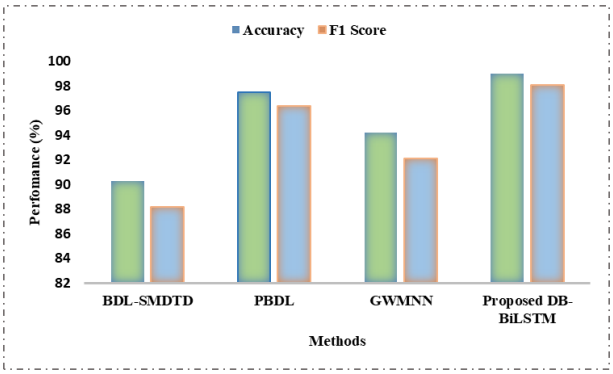

Figure 4. Comparative analysis with existing and Proposed method

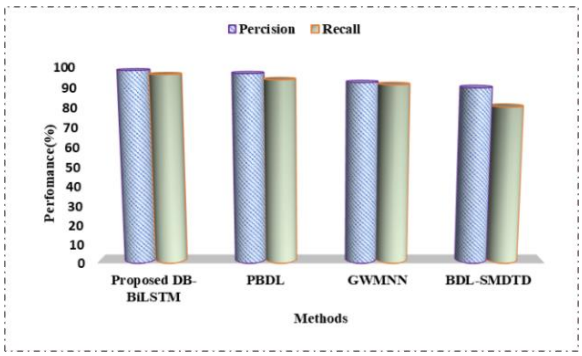

Figure 5. Comparative analysis with existing and Proposed method

Figure 5. Shows the Recall and precision of the analysis in comparison to the suggested and existing methods. The existing PBDL, BDL-SMDTD, GWMNN are compared with proposed BD-BiLSTM method. Performance analysis of existing CICIDS, TON-IOT vs proposed DB-BiLSTM shown in Figure 6.

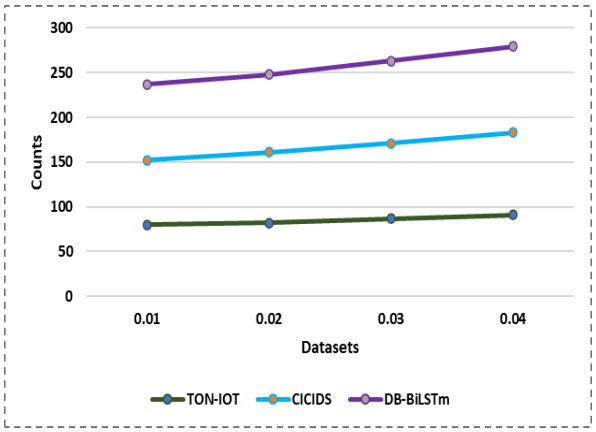

Figure 6. Performance analysis of existing CICIDS, TON-IOT vs proposed DB-BiLSTM

TON-IOT covers nine aberrant observations, the majority of which are encountered in IoT/IoT environments, including backdoors and DDoS., it consists of 43 labelled features. Ransomware, SSH-Patator, and other updated attack observations are included in CICIDS., it consists of 78 labelled features. As a result, the proposed BD-BiLSTM has high performance than CICIDS and TON-IOT.

5. CONCLUSION

In this paper, a new Deep-BiLSTM technique based on Blockchain is created to transmit data securely in IoT-approved healthcare systems. To guarantee security, BD-BiLSTM offers a two-level design. At the initial level, a blockchain architecture was shown in particular, the first unique a scalable blockchain architecture using the Zero Knowledge Proof (ZKP) technique is suggested to guarantee data security and integrity. The bidirectional long short-term memory is used by the deep convolutional neural network on the second level's deep learning architecture to recognize network intrusions. The validated data is then utilized to develop a deep learning framework for identifying HS network breaches. The use of IPFS-based off-chain storage enhances the scalability of BD-BiLSTM. The latter combines Bidirectional Long Short-Term Memory (BiLSTM) and Deep Convolutional Neural Network to create an efficient intrusion detection system. The suggested solution has been compared Using analysis with two public datasets (CICIDS-2017 and ToN-IoT), our proposed Bi-LSTM performs 96% better. According to experimental findings of F1 score, recall precision, and accuracy the proposed BD-BiLSTM technique has 98% in which is relatively high compared to existing methods of BDL-SMDTA, PBDL and GWMNN.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

No funding was received to assist with the preparation of this manuscript.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for all of their careful, constructive and insightful comments in relation to this work.

REFERENCES

[1] J. Li, J. Cai, F. Khan, A.U. Rehman, V. Balasubramaniam, J. Sun, and P. Venu. “A secured framework for sdn-based edge computing in IOT-enabled healthcare system”, *IEEE Access*, vol. 8, pp.135479-135490, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] K. Wang, C.M. Chen, Z. Tie, M. Shojafar, S. Kumar, and S. Kumari. “Forward privacy preservation in IoT-enabled healthcare systems”, *IEEE transactions on industrial informatics*, vol.18, no. 3, pp.1991-1999, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] R. Arul, R. Alroobaea, U. Tariq, A.H. Almulihi, F.S. Alharithi, and U. Shoaib. “IoT-enabled healthcare systems using block chain-dependent adaptable services”, *Personal and Ubiquitous Computing*, pp.1-15, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] W. Li, Y. Chai, F. Khan, S.R.U. Jan, S. Verma, V.G. Menon, and X. Li. “A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system”,*Mobile networks and applications*, vol.26, pp.234-252, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] O. Said, and A. Tolba, "Design and evaluation of large-scale IoT-Enabled healthcare architecture", *Applied Sciences*, vol.11, no. 8, p.3623, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] S. Peneti, M. Sunil Kumar, S. Kallam, R. Patan, V. Bhaskar, and M. Ramachandran. "BDN-GWMNN: internet of things (IoT) enabled secure smart city applications", *Wireless Personal Communications*, vol.119, pp.2469-2485, 2021, [CrossRef] [Google Scholar] [Publisher Link]

[7] A. Sardar, S. Umer, R.K. Rout, S.H. Wang, and M. Tanveer, "A Secure Face Recognition for IoT-Enabled Healthcare System", *ACM Transactions on Sensor Networks (TOSN)*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] P. Zhang, F. Liu, N. Kumar, and G.S. Aujla, "Information classification strategy for blockchain-based secure sdn in iot scenario", In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1081-1086. IEEE, 2020, July. [CrossRef] [Google Scholar] [Publisher Link]

[9] S. Neelakandan, J.R. Beulah, L. Prathiba, G.L.N. Murthy, E.F. Irudaya Raj, and N. Arulkumar. "Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model", *International Journal of Modeling, Simulation, and Scientific Computing*, vol.13, no. 04, p.2241006, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] R. Kumar, P. Kumar, R. Tripathi, G.P. Gupta, A.N. Islam, and M. Shorfuzzaman, "Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems", *IEEE Transactions on Industrial Informatic*s, vol.18, no. 11, pp.8065-8073, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] S. Aggarwal, R. Chaudhary, G.S. Aujla, N. Kumar, K.K.R. Choo, and A.Y. Zomaya, 2019. "Blockchain for smart communities: Applications, challenges and opportunities", *Journal of Network and Computer Applications*, vol.144, pp.13-48. [CrossRef] [Google Scholar] [Publisher Link]

[12] W. Zhao, C. Jiang, H. Gao, S. Yang, and X. Luo. "Blockchain-enabled cyber–physical systems: A review", *IEEE Internet of Things Journal*, vol.8, no. 6, pp.4023-4034, 2020 [CrossRef] [Google Scholar] [Publisher Link]

[13] M. Zolanvari, M.A. Teixeira, L. Gupta, K.M. Khan, and R. Jain. "Machine learning-based network vulnerability analysis of industrial Internet of Things", *IEEE Internet of Things Journal*, vol.6, no. 4, pp.6822-6834, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] O. Alkadi, N. Moustafa, B. Turnbull and K.K.R. Choo. "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks", *IEEE Internet of Things Journal*, vol.8, no. 12, pp.9463-9472, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] S. Rathore, B.W. Kwon, and J.H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network", *Journal of Network and Computer Applications*, vol.143, pp.167-177, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[16] C. Liang, B. Shanmugam, S. Azam, M. Jonkman, F. De Boer, and G. Narayansamy. "Intrusion detection system for Internet of Things based on a machine learning approach", In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), pp. 1-6. IEEE, 2019, March. [CrossRef] [Google Scholar] [Publisher Link]

[17] M. Hasan, M.M. Islam, M.I.I. Zarif, and M.M.A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches", *Internet of Things*, vol.7, p.100059, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] R. Gupta, S. Tanwar, F. Al -Turjman, P. Italiya, A. Nauman, and S.W. Kim. "Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges", *IEEE access*, vol.8, pp.24746-24772, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K.K.R. Choo. "A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks", *IEEE Transactions on Industrial Informatics*, vol.16, no. 8, pp.5110-5118, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[20] I. Namatēvs, "Deep convolutional neural networks: Structure, feature extraction and training", *Information Technology and Management Science*, vol. 20, no.1, pp.40-47, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[21] J. Xu, P. Vijayakumar, P.K. Sharma, and U. Ghosh, "Homomorphic encryption-based privacy-preserving federated learning in iot-enabled healthcare system", *IEEE Transactions on Network Science and Engineering*, 2022., [CrossRef] [Google Scholar] [Publisher Link]

[22] G.S. Aujla, and A. Jindal, "A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring", *IEEE Journal on Selected Areas in Communication*s, vol.39, no. 2, pp.491-499, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] A.A. Khan, A.A. Laghari, M. Shafiq, O. Cheikhrouhou, W. Alhakami, H. Hamam, and Z.A. Shaikh, "Healthcare Ledger Management: A Blockchain and Machine Learning-Enabled Novel and Secure Architecture for Medical Industry", *Human-Centric Computing and Information Sciences*, vol.12, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] T.R. Gadekallu, M.K. Manoj, N. Kumar, S. Hakak, and S. Bhattacharya, "Blockchain-based attack detection on machine learning algorithms for IoT-based e-health applications", *IEEE Internet of Things Magazine*, vol.4, no. 3, pp.30-33, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] N. Al Asad, M.T. Elahi, A. Al Hasan, and M.A. Yousuf, November. "Permission-based blockchain with proof of authority for secured healthcare data sharing", *In 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT)*, pp. 35-40, IEEE, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[26] H. Babbar, S. Rani, and S.A. AlQahtani. "Intelligent Edge Load Migration in SDN-IIoT for Smart Healthcare", *IEEE Transactions on Industrial Informatics*, vol.18, no. 11, pp.8058-8064, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] B.S. Egala, A.K. Pradhan, V. Badarla, and S.P. Mohanty, "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control", *IEEE Internet of Things Journal*, vol.8, no. 14, pp.11717-11731, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[28] E. Ashraf, N.F. Areed, H., Salem, E.H. Abdelhay, and A. Farouk, "Fidchain: Federated intrusion detection system for blockchain-enabled iot healthcare applications", In Healthcare Vol. 10, No. 6, pp. 1110. MDPI, 2022, June. [CrossRef] [Google Scholar] [Publisher Link]

[29] S.A. ElRahman, and A.S. Alluhaidan, "Blockchain technology and IoT-edge framework for sharing healthcare services". *Soft Computing*, vol.25, no. 21, pp.13753-13777, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[30] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar. "Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications", *IEEE transactions on network science and engineerin*g, vol.8, no. 2, pp.1242-1255, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[31] S. Pal. “Internet of Things and Access Control: Sensing, Monitoring and Controlling Access in IoT-Enabled Healthcare Systems”, vol. 37, 2021. Springer Nature. [CrossRef] [Google Scholar] [Publisher Link]
[32] M. Javaid, and I.H. Khan. “Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic”, *Journal of Oral Biology and Craniofacial Researc*h, vol.11, no. 2, pp.209-214, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[33] S. Rani, M. Chauhan, A. Kataria, and A. Khang. “IoT equipped intelligent distributed framework for smart healthcare systems”, arXiv preprint arXiv:2110.04997, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[34] G. Hameed, Y. Singh, S. Haq, and B. Rana, “Blockchain-based model for secure IoT communication in smart healthcare. In Emerging Technologies for Computing”, *Communication and Smart Cities: Proceedings of ETCCS* 2021, pp. 715-730. Singapore: Springer Nature Singapore, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[35] T. Veeramakali, R. Siva, B. Sivakumar, P.C. Senthil Mahesh, N. Krishnaraj, “An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model”, *The Journal of Supercomputing.* 2021 Sep 1:1-21. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

R.R. Sathiya completed her Bachelor’s Degree in Information Technology from Bharathiar University, Coimbatore, Tamilnadu, India, in the year 2004 and her Master’s Degree in Computer Science and Engineering from Anna University, Coimbatore, Tamilnadu, India, in the year 2010. Her areas of interest include cloud computing, Internet of Things, and Image processing. She has published technical papers in International Conferences and Journals.

S. Rajakumar, is currently working as Professor in the department of Electronics and Communication Engineering, Panimalar Engineering College, affiliated to Anna University, Chennai. He has organized several Conferences and Seminars related to Image Processing and Signal Processing. He completed his B.E., degree in Electronics and Communication Engineering from Sun College of Engineering and Technology, Nagercoil affiliated to Manonmaniam Sundaranar University, Tirunelveli. He obtained his M.E., degree in Applied Electronics and Ph.D in Image Processing from Sathyabama University, Chennai, India in the year 2006 and 2013 respectively. He has published several research articles in National and International Conferences and Journals. His areas of interest include Digital Signal Processing, Image Processing, Pattern Recognition, VLSI and Communication Engineering.

J. Sathiamoorthy is currently working as an Associate Professor, Department of Computer Science and Engineering in RMK Engineering College, Chennai. He has completed M. Tech (CIT) and Ph.D from Manonmaniam Sundaranar University, Tirunelveli Tamilnadu, India. He has over 18 years of teaching experience. He has published papers in Network Security in National and International journals and has presented in International Conferences and Seminars. He has published more than 20 research papers in reputed journals in the area of ad-hoc networks especially MANET, VANET, FANET and Underwater Communication. He has acted as a reviewer in many reputed international journals.

Arrived: 10.08.2023
Accepted: 19.10.2023