

Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset

Jinsi Jose^{1,2}, Deepa V. Jose¹

¹Department of Computer Science, CHRIST University, Bangalore, India

²Department of Computer Science, Rajagiri College of Social Sciences, Cochin, India.

Article Info

Article history:

Received Jan 4, 2022

Revised Sep 25, 2022

Accepted Oct 8, 2022

Keywords:

CIC-IDS 2017 dataset

Convolution neural network

Deep neural network

Internet of things

Intrusion detection system

ABSTRACT

Due to technological advancements in recent years, the availability and usage of smart electronic gadgets have drastically increased. Adoption of these smart devices for a variety of applications in our day-to-day life has become a new normal. As these devices collect and store data, which is of prime importance, securing is a mandatory requirement by being vigilant against intruders. Many traditional techniques are prevailing for the same, but they may not be a good solution for the devices with resource constraints. The impact of artificial intelligence is not negligible in this concern. This study is an attempt to understand and analyze the performance of deep learning algorithms in intrusion detection. A comparative analysis of the performance of deep neural network, convolutional neural network, and long short-term memory using the CIC-IDS 2017 dataset.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Jinsi Jose

Department of Computer Science, Christ University Hosur Road

Bangalore, Karnataka-560029, India

Email: jinsi.jose@res.christuniversity.in

1. INTRODUCTION

Internet of things (IoT) can be considered as the boon of the latest century. The adoption of this technology in various walks of life and in every business, medical and engineering field showcases the extent to which this technology is being embraced by all. Since the concept of artificial intelligence (AI) is also incorporated into it, IoT devices become smarter and can take better decisions. According to International Data Corporation (IDC), IoT device-generated 73.1 ZB of data in 2025, and the estimated number of IoT devices will be 41.6 million [1]. Even though IoT helps to automate many applications and thereby reduce human interventions, security is the primary concern to be addressed. So, the identification of varying attacks is a significant concern among the researchers.

From the beginning of the design of the IoT network and smart devices, there were also attempts to protect data and devices from intruders. Security of the data collected and stored is always a major concern for researchers working in this area as the mode and type of attacks vary every moment. There are different approaches for attack detection such as filter packets—with firewalls and proxies, adopting encryption—with cryptographic protocols, data storage encryption or virtual private networks, password authentication method, audit and log activities—for web servers, database servers, and application servers, attack identification using intrusion detection system, intrusion prevention system [2].

An intrusion detection system (IDS) is a technique that can track network traffic and identify malicious traffic or any kind of attack and give alerts [3]. It is a combination of software and hardware. The idea of the IDS was started in 1970 [2]. The IDS are categorized into four based on the occurrence, placement strategies, and detection method. Based on occurrence strategy, the collection of information can be host-based, network-based, network node-based or hybrid mode. In the placement category, the placement

of IDS can be centralized, distributed, and hybrid. In detection method categorization, it can be signature-based IDS, anomaly-based IDS, and hybrid IDS. [4], [5]. The concept of IDS started with computer networks for identifying abnormal traffic. For this implementation of IDS, different methods were used based on game theory, complex event processing, automata [6], data mining, statistical model, payload model, rule-based [4], and AI. Even though other techniques exist, AI has a prominent role in intrusion detection as it has proved to detect attack better. AI based IoT IDS can overcome the shortcomings of the existing traditional methods. Most of the current IoT IDS technologies are static, unable to learn from the previous attack. AI is a powerful method that can learn from the previous attacks over time, identify attacks from the usual traffic, and alert the corresponding system. AI methods such as machine learning (ML) and deep learning can provide powerful capabilities to IoT security requirements [7].

From the earlier stages of AI implementation in IoT IDS, the researchers have experimented with different ML techniques. Though ML techniques give better accuracy and overcome other shortcomings of the traditional methods, it has some other limitations. In ML techniques, the classification and regression tree (CART) has a significant role. CART gives high performance with low training time, but it shows less performance for complex dataset [8]. In ML, conventional methods follow shallow learning which sometimes focuses on feature engineering and selection. In the traditional detection method, the learning capacity is less, reducing the complex dataset. The learning process gathers partial information from every data, so a large amount of data is needed for training. A large amount of data is very crucial in the case of the heterogeneous dataset. Deep learning has a significant role in a large amount of data and has the ability to automatic feature learning and handles advanced problems upon a bulk amount of data [9].

This paper focuses on three deep learning models deep neural network (DNN), long short-term memory network (LSTM), and convolutional neural network (CNN). Section 1 gives an introduction to IoT, its security issues, and existing solutions. Section 2 details the impact of deep learning in IoT IDS from recent studies available in the literature. A detailed explanation of the method adopted for this study is mentioned in section 3. Section 4 presents the results and discussions, followed by conclusions and future scope in section 5.

2. RELATED WORK

Deep learning has had a vital role in IoT intrusion detection rather than any conventional method. This section gives a glimpse of the importance of deep learning in IoT attack detection. Yin *et al.* [10] proposed a recurrent neural network (RNN) with the NSL-KDD dataset and performed binary and multi-classification. In another study, the DNN model using the KDD CUP 99 dataset is presented [11]. It was focused on multi-classification, and the first epochs onwards result showed 99% accuracy.

Bi-directional long short-term memory recurrent neural network (BLSTM-RNN) for binary classification in IoT intrusion detection was carried out [12]. The results show the proposed model achieved 95% accuracy. CNN gives more accuracy on intrusion detection [13]. A comparison of CNN with other deep learning methods was performed. The CNN model was proposed and tested with two datasets: NSL-KDD and UNSW-N15. The result shows the proposed CNN model gives better results with existing deep learning models. In another study, Ding and Zhai [14] presented an intrusion detection model based on CNN. They focused on multi-classification with the NSL-KDD dataset. The performance of the proposed model was evaluated with other ML and deep learning models such as radio-frequency (RF), support vector machine (SVM), deep belief network (DBN), and LSTM.

A novel feed-forward neural network (FNN) is proposed for binary and multi-classification using the BoT-IoT dataset [15]. This study gave a detailed explanation of the proposed framework and used accuracy, precision, recall and F1-score as evaluation metrics. Wu and Guo [16] proposed the LuNet model and tested it with two datasets. In another study, a DNN model is proposed for binary and multi-classification and tested with six datasets [17]. Sindian [18] proposed an enhanced autoencoder approach called EDSA for detecting DDoS attacks. Ahmad *et al.* [19] proposed a new DNN model for identifying attacks from both authentic and non-authentic sources. Nowadays, most researchers are stepping forward to work with new datasets rather than traditional datasets. Using the BoT-IoT dataset, Popoola *et al.* [20] proposed a hybrid model to detect BoT attacks in IoT. The researchers worked on both binary and multi-classification.

Syed *et al.* [21] introduced intrusion detection system IoT time-series data using RNN and bi-LSTM with feature selection. In this study, they worked in the BoT-IoT dataset with different feature selection methods to evaluate the model. A model is proposed to identify three different DDoS attacks using the DNN and LSTM model for binary classification [22]. An enhanced UNSW-NB 15 dataset is used for intrusion detection using deep learning models [23]. A network anomaly detection method is suggested for the NSL-KDD dataset by using deep learning in the unsupervised active inferences layer [24]. It can be inferred from the literature reviewed that the majority of the research is done using the existing dataset and the newly proposed models are not that much compared with the latest deep learning models.

3. METHOD

This section focuses on data pre-processing and detailed implementation of three deep learning algorithms. The CIC-IDS2017 dataset is used for DNN, CNN and LSTM models. The proposed method illustrates the overall idea of the work. The pictorial representation of the proposed method is shown in Figure 1.

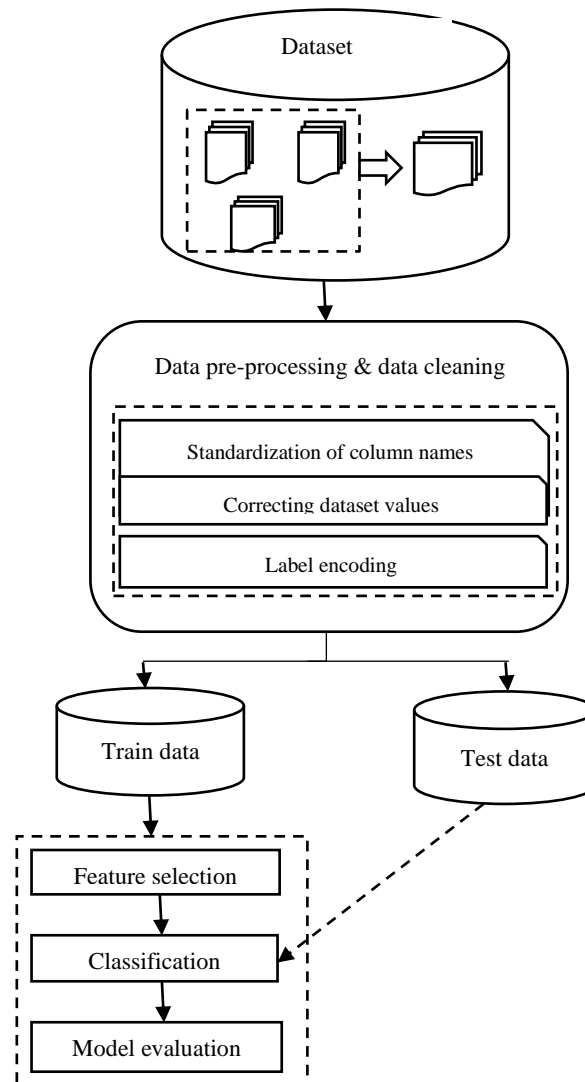


Figure 1. Proposed method

3.1. Data pre-processing

Data pre-processing is an inevitable step before feeding the data into the model. The entire dataset contains eight CSV files. First, append all the available datasets into a single dataset, then perform data pre-processing and data cleaning. In the standardization of column names, check whether any comma or other special characters exist, and such kind of values are removed. To correct the dataset, check whether any infinite values are present and find out that *'flowbytes/s'* and *'flowpackets/s'* contain 1,509, 2,867 infinite values, respectively. Then, check for the null values in the columns, generate the total number of null values of each column, and identify that *'flowbytes/s'* and *'flowpackets/s'* have 2,867 values. Next, generate the description of all the columns with count, mean, standard deviation, minimum values, 25%, 50%, 75%, and maximum values. Here, all the null values are replaced by zeros and generated in the dataset head details.

The next focus was on exploratory data analysis (EDA). It is a method to analyze data and summarizes the data characteristics frequently through the visual approach. Using principal component analysis (PCA) method to remove the highly correlated data, perform standardization and label encoding of

the data, subsequently. The entire data was reduced to 71 features, including the label. The dataset was split into training (70%) and testing (30%) data and then checked with normalization and transformation of both train and test data, followed by summarizing the transformed data with precision 3.

3.2. Deep learning models

Deep learning is a subset of machine learning and tries to learn from a vast dataset using a multi-layered neural network. Deep learning follows a transfer learning methodology rather than a shallow learning approach. So, deep learning can provide better accuracy in terms of classification, which gained weights from the previous layers. This section focused on the implementation of different deep learning architectures such as DNN, LSTM and CNN. To evaluate models used confusion matrix, accuracy, precision, recall, and F1-score as an evaluation metrics. A confusion matrix is a table which summarizes the predictions of classification models. It contains a total summarization of corrected and incorreced predictions based on each class. To draw up the confusion matrix, calculating true positive (TP), true negative (TN), false positive (FP), and false negative (FN) is needed. Then, we calculated metrics as in (1) to (4).

$$\text{Accuracy} = \frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \quad (1)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP}+\text{FP}} \quad (2)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP}+\text{FN}} \quad (3)$$

$$\text{F1 score} = 2 \times \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

3.2.1. Deep neural network

A DNN architecture is a type of neural network which follows a feed-forward network. It contains multiple fully connected hidden layers rather than input and output layer. From the input layer, information passes to hidden layers in a feed-forward manner, and by using the backpropagation algorithm, the output layer learns weights repetitively [25]. Equation of the DNN architecture can be:

- $d \in \mathbb{N}$: input layer dimension
- L : number of layers
- N : number of neurons
- $\sigma: \mathbb{R} \rightarrow \mathbb{R}$: non-linear function
- $W_\ell: \mathbb{R}^{N^{\ell-1}} \rightarrow \mathbb{R}^{N^\ell}, \ell = 1, \dots, L$: affine linear maps $X \mapsto AX + b$
- Then $\phi: \mathbb{R}^d \rightarrow \mathbb{R}^{NL}$, given by

$$\phi(x) = W_L \sigma \left(W_{L-1} \sigma \left(\dots \sigma \left(W_1(x) \right) \right) \right), x \in \mathbb{R}^d \quad (5)$$

The proposed DNN architecture contains an input layer with 250 neurons, three hidden layers with 32, 72, and 32, respectively, and the output layer with five neurons. The connection mode was fully connected. The hidden layer activation function is rectified linear unit (ReLU), and SoftMax is used as the output layer activation function. To identify the loss used categorical cross-entropy as a loss function, and Adam optimizer was used to minimize the error function. Table 1 shows the values of evaluation metrics of DNN.

Table 1. Values of evaluation metrics of DNN

Evaluation Metrics	Accuracy	Precision	Recall	F1-score
Percentage	90.61	80.85	84.60	84.60

3.2.2. Long short-term memory

LSTM works efficiently for time series data. LSTM architecture uses looping feedback connections and feedforward connections, which is helpful to model to hold information for a while. LSTM can learn from long and short dependencies without loose and excess accumulation of data, and, at the same time, is smart enough to remember things from the past and predict the subsequent scenarios. LSTM uses a series of gates such as forget gate, input gate, and output gate to control the flow of information in each cell present in the architecture [25], [26]. The formulations of LSTM architecture are shown below.

The output of the forget gate is denoted as F_t and W_F, U_F, b_F are weights and bias parameters of forget gate. I_t is the output of forget gate and W_I, U_I, b_I are the input gate weight and bias. During training, these weight and bias parameters are optimized. x_t and h_t are input vector and hidden vector at time t .

$$F_t = \sigma(W_F x_t + U_F h_{t-1} + b_F) \quad (6)$$

$$I_t = \sigma(W_I x_t + U_I h_{t-1} + b_I) \quad (7)$$

C_t holds the value kept in the memory cell which calculated by the output of input and forget gate along with current value of input. By using these values, the output and hidden states are calculated. \odot is the element-wise vector product.

$$O_t = \sigma(W_O x_t + U_O h_{t-1} + b_O) \quad (8)$$

$$C_t = F_t \odot C_{t-1} + I_t \odot \tanh(W_C x_t + U_C h_{t-1} + b_C) \quad (9)$$

$$h_t = O_t \odot \tanh(C_t) \quad (10)$$

$$O_t = f(W_O h_t + b_O) \quad (11)$$

The LSTM model implemented contains four hidden layers having 64, 64, 128, and 128 neurons. ReLU is used as the activation function of hidden layers, and SoftMax was used as an activation function of the output layer. In fitting model two, the loss function in categorical data used the categorical cross-entropy function and binary cross-entropy function for binary data. Table 2 gives values of evaluation metrics of LSTM.

3.2.3. Convolutional neural network

CNN is a supervised learning method that is used to classify labelled data into a different pattern. CNN has several building blocks such as convolution layer, pooling layer, and fully connected layer. The CNN architecture can train multiple nonlinear layers with fully connected layers. So, it can automatically learn important hierarchical features from the raw data. CNN is mostly dealing with more complex feature extraction with better accuracy. The CNN architecture can reduce the number of parameters and gradient diffusion problem also. It leads to the successful training of the model in an effective manner [17], [25], [27].

The time series network traffic data input vector is $y = (y_1, y_2 \dots y_{n-1}, cl)$, where $y_n \in R^d$ is features and $cl \in R$ is class label. The feature map fm applying in convolution operation on the input data with filter $w \in R^{f \times d}$, and f is the feature. The feature map fm from the set of features f is obtained as (12),

$$hl_i^{fm} = \tanh(w^{fm} x_{i:i+f-1} + b) \quad (12)$$

where bias term denotes as $b \in R$ and hl is implemented in each set of features f in record $\{x_1: f, x_2: f + 1, \dots x_{n-f+1}\}$ to generate feature map as (13),

$$hl = [hl_1, hl_2, \dots hl_{n-f+1}] \quad (13)$$

where $hl \in R^{n-f+1}$ and applying max pooling operation on each feature map as $\vec{\rightarrow}_{hl} = \max\{hl\}$. A fully connected layer mathematically as (14).

$$O_t = \text{softmax}(w_{ho} hl + b_o) \quad (14)$$

In the implemented model, there are three hidden layers with a ReLU activation function. Each hidden layer contains 120, 60, 30 neurons, respectively, and the output layer contains 15. In between the hidden layer, it used MaxPooling layer with pool size 2. This architecture used sparse categorical cross-entropy as a loss function with Adam optimizer. Table 3 gives values of evaluation metrics of CNN.

Table 2. Values of evaluation metrics of LSTM

Evaluation Metrics	Accuracy	Precision	Recall	F1-score
Percentage	97.67	94.96	95.95	93.55

Table 3. Values of evaluation metrics of CNN

Evaluation Metrics	Accuracy	Precision	Recall	F1-score
Percentage	99.61	97.05	95.00	93.09

4. RESULTS AND DISCUSSION

This section focuses on comparing implemented three architectures such as DNN, LSTM, CNN as well as existing models. In this result evaluation used accuracy, precision, recall and F1-score as evaluation metrics of the model. Figure 2 illustrates the evaluation metrics comparison of three implemented models.

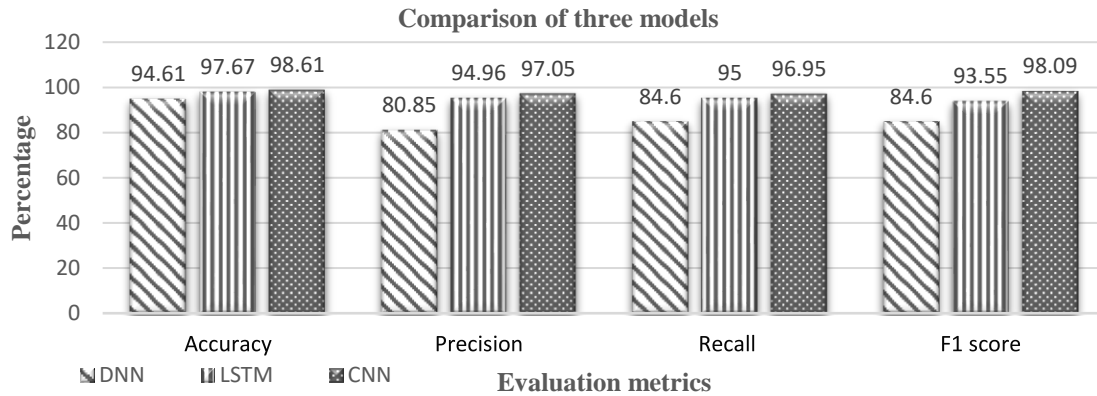


Figure 2. Comparison of DNN, LSTM and CNN models

The comparative analysis of the graph shows that CNN yielded much better results in terms of accuracy, precision, recall, and f1score. Table 4 gives the overview of the comparative study of the models with other existing models. From the results, we can identify except DNN model other two models have better accuracy. The main reasons are system dependencies and lack of correct feature selection. The main advantage of LSTM is that it has the edge over any other conventional feedforward neural network. The CNN allows the model both time and space correlations for better performance.

Table 4. Comparison of models with other existing models

Algorithm	Reference	Dataset used	Accuracy
DNN	[28]	NSL-KDD	86.00
	[25]	UNSW-NB 15	88.00
	[17]	KDD Cup 99, CIC IDS-2017	92.5
	[29]	BoT- IoT	94.00
	[30]	MQTT-IoT-IDS2020	97.13
Implemented DNN	-	CIC IDS-2017	94.61
LSTM	[31]	KDD 99	85.65
	[32]	KDD Cup 99	93.72
	[33]	Kitsune	95.00
	[34]	IoT- BoT	96.26
	[35]	NSL-KDD	96.9
Implemented LSTM	-	CIC IDS 2017	97.67
CNN	[36]	NSL-KDD	81.33
	[37]	NSL- KDD	83.31
	[38]	UNSW-NB 15	91.2
	[39]	UNSW-NB15	91.27
	[25]	UNSW-NB 15	92.16
Implemented CNN	-	CIC IDS 2017	98.61

5. CONCLUSION

In this emerging technological era, IoT devices have a very important role in the day-to-day life of all human beings. We can see various applications of IoT in all fields such as automation, health care, enhancement of customer experiences, and smart safety. Even for most people depending on the IoT devices security is the major concern for all of them. For this security purpose, researchers are focused on IoT intrusion detection systems. Even though there are various traditional methods and machine learning models available for the implementation of IoT IDS, deep learning models have a significant role in that, because deep learning method has ability to maximize the utilization of unstructured data as well as it can work on huge amount of data and perform better than other techniques.

This paper carried out a brief study of the relevance of deep learning in IoT IDS and did a comparative study with three deep learning models such as DNN, LSTM, and CNN. The results show DNN gives 94.61% accuracy, while LSTM and CNN achieves 97.67% and 98.61%, respectively. From this comparative study and literature review, it has been proven that deep learning models outperform the other methods applied in IoT IDS environment. Despite the deep learning models having better accuracy, our future scope is to develop a hybrid deep learning model for IoT intrusion detection with better accuracy in attack prediction and experimenting with the real-time dataset. The hybrid model is not only for combining two models but also for detection methods and IoT IDS placement strategy. Developing a hybrid deep learning model for IoT intrusion detection for better accuracy in attack prediction and experimenting with real-time dataset is the future scope which is the need of the hour.





REFERENCES

- [1] T. Rago and A. Afuang, "IoT growth demands rethink of long-term storage strategies, says IDC," 2020. <https://www.idc.com/getdoc.jsp?containerId=prAP46737220> (accessed Jul. 23, 2021).
- [2] N. Chaabouni, "Intrusion detection and prevention for IoT systems using machine learning," PhD, Université de Bordeaux, 2020.
- [3] Y. Otoum and A. Nayak, "AS-IDS: Anomaly and signature based IDS for the internet of things," *Journal of Network and Systems Management*, vol. 29, no. 3, Jul. 2021, doi: 10.1007/s10922-021-09589-6.
- [4] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of things: Evolution, concerns and security Challenges," *Sensors*, vol. 21, no. 5, Mar. 2021, doi: 10.3390/s21051809.
- [5] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, vol. 4, no. 1, Dec. 2021, doi: 10.1186/s42400-021-00077-7.
- [6] Y. Fu, Z. Yan, J. Cao, O. Koné, and X. Cao, "An automata based intrusion detection method for internet of things," *Mobile Information Systems*, vol. 2017, pp. 1–13, 2017, doi: 10.1155/2017/1750637.
- [7] H. Wu, H. Han, X. Wang, and S. Sun, "Research on artificial intelligence enhancing internet of things security: A survey," *IEEE Access*, vol. 8, pp. 153826–153848, 2020, doi: 10.1109/ACCESS.2020.3018170.
- [8] N. Thapa, Z. Liu, D. B. KC, B. Gokaraju, and K. Roy, "Comparison of machine learning and deep learning models for network intrusion detection systems," *Future Internet*, vol. 12, no. 10, Sep. 2020, doi: 10.3390/fi12100167.
- [9] G. Kocher and G. Kumar, "Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges," *Soft Computing*, vol. 25, no. 15, pp. 9731–9763, Aug. 2021, doi: 10.1007/s00500-021-05893-0.
- [10] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.
- [11] J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, "Method of intrusion detection using deep neural network," in *2017 IEEE International Conference on Big Data and Smart Computing, BigComp 2017*, 2017, pp. 313–316, doi: 10.1109/BIGCOMP.2017.7881684.
- [12] B. Roy and H. Cheung, "A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural network," in *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, Nov. 2018, pp. 1–6, doi: 10.1109/ATNAC.2018.8615294.
- [13] S. Potluri, S. Ahmed, and C. Diedrich, *Convolutional neural networks for multi-class intrusion detection system*, vol. 11308 LNAI, Springer International Publishing, 2018.
- [14] Y. Ding and Y. Zhai, "Intrusion detection system for NSL-KDD dataset using convolutional neural networks," *ACM International Conference Proceeding Series*, pp. 81–85, 2018, doi: 10.1145/3297156.3297230.
- [15] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for IoT networks," in *2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*, Dec. 2019, pp. 256–25609, doi: 10.1109/PRDC47002.2019.00056.
- [16] P. Wu and H. Guo, "LuNet: A deep neural network for network intrusion detection," in *2019 IEEE Symposium Series on Computational Intelligence (SSCI)*, Dec. 2019, pp. 617–624, doi: 10.1109/SSCI44817.2019.9003126.
- [17] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.
- [18] S. Sindian, "An enhanced deep autoencoder-based approach for DDoS attack detection," *WSEAS Transactions on Systems and Control*, vol. 15, pp. 716–724, 2020, doi: 10.37394/23203.2020.15.72.
- [19] S. Ahmad, F. Arif, Z. Zabeehullah, and N. Iltaf, "Novel approach using deep learning for intrusion detection and classification of the network traffic," in *2020 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*, Jun. 2020, pp. 1–6, doi: 10.1109/CIVEMSA48639.2020.9132744.
- [20] S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui, and H. Gacanin, "Hybrid deep learning for botnet attack detection in the internet-of-things networks," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4944–4956, Mar. 2021, doi: 10.1109/JIOT.2020.3034156.
- [21] N. F. Syed, M. Ge, and Z. Baig, "Intrusion detection for time-series IoT data with recurrent neural networks and feature selection intrusion detection for time-series IoT data with recurrent neural networks and feature selection," *TechRxiv*, no. M1, pp. 0–9, 2021, doi: 10.36227/techrxiv.13525409.v1.
- [22] T. Khempetch and P. Wuttidittachotti, "DDoS attack detection using deep learning," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 10, no. 2, pp. 382–388, Jun. 2021, doi: 10.11591/ijai.v10.i2.pp382-388.
- [23] A. Aleesa, M. Y. Thanoun, A. A. Mohammed, and N. M. Sahar, "Deep-intrusion detection system with enhanced UNSW-NB15 dataset based on deep learning techniques," *Nan M Sahar*, vol. 16, no. 1, pp. 711–727, 2021.
- [24] D. U. M. N. Dr.R.Venkatesh, Kaviitha S, "Network anomaly detection for NSL-KDD dataset using deep learning," *Information Technology In Industry*, vol. 9, no. 2, pp. 821–827, Mar. 2021, doi: 10.17762/itii.v9i2.419.
- [25] H. Dhillon and A. Haque, "Towards network traffic monitoring using deep transfer learning," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Dec. 2020, pp. 1089–1096, doi: 10.1109/TrustCom50675.2020.00144.
- [26] G. Van Houdt, C. Mosquera, and G. Nápoles, "A review on the long short-term memory model," *Artificial Intelligence Review*, vol. 53, no. 8, pp. 5929–5955, Dec. 2020, doi: 10.1007/s10462-020-09838-1.





- [27] J. Shara, "Deep learning methods for cybersecurity," in *Fifteenth International Conference On: Social and Natural Sciences – Global Challenge 2021 (ICSNS XV – 2021)*, 2021, pp. 73–90.
- [28] J. Jose and D. V. Jose, "Performance analysis of deep learning algorithms for intrusion detection in IoT," in *2021 International Conference on Communication, Control and Information Sciences (ICCISc)*, Jun. 2021, pp. 1–6, doi: 10.1109/ICCISc52257.2021.9484979.
- [29] J. P. J. Shareena, A. Ramdas, and H. A. P., "Intrusion detection system for IOT botnet attacks using deep learning," *SN Computer Science*, vol. 2, no. 3, May 2021, doi: 10.1007/s42979-021-00516-9.
- [30] M. A. Khan *et al.*, "A deep learning-based intrusion detection system for MQTT enabled IoT," *Sensors*, vol. 21, no. 21, Oct. 2021, doi: 10.3390/s21217016.
- [31] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)," *Journal of Big Data*, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-021-00448-4.
- [32] R. C. Staudemeyer, "Applying long short-term memory recurrent neural networks to intrusion detection," *South African Computer Journal*, vol. 56, Jul. 2015, doi: 10.18489/sacj.v56i1.248.
- [33] Y. Xu, Y. Tang, and Q. Yang, "Deep learning for IoT intrusion detection based on LSTMs-AE," in *Proceedings of the 2nd International Conference on Artificial Intelligence and Advanced Manufacturing*, Oct. 2020, pp. 64–68, doi: 10.1145/3421766.3421891.
- [34] Z. Ahmad *et al.*, "Anomaly detection using deep neural network for IoT architecture," *Applied Sciences*, vol. 11, no. 15, Jul. 2021, doi: 10.3390/app11157050.
- [35] S. Shende, "Long short-term memory (LSTM) deep learning method for intrusion detection in network security," *International Journal of Engineering Research and*, vol. V9, no. 06, Jul. 2020, doi: 10.17577/IJERTV9IS061016.
- [36] Y. Li *et al.*, "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," *Measurement*, vol. 154, Mar. 2020, doi: 10.1016/j.measurement.2019.107450.
- [37] X. Zhang, J. Ran, and J. Mi, "An intrusion detection system based on convolutional neural network for imbalanced network traffic," in *2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT)*, Oct. 2019, pp. 456–460, doi: 10.1109/ICCSNT47585.2019.8962490.
- [38] M. Azizjon, A. Jumabek, and W. Kim, "1D CNN based network intrusion detection with normalization on imbalanced data," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC)*, Feb. 2020, pp. 218–224, doi: 10.1109/ICAIIIC48513.2020.9064976.
- [39] B. Susilo and R. F. Sari, "Intrusion detection in IoT networks using deep learning algorithm," *Information*, vol. 11, no. 5, May 2020, doi: 10.3390/info11050279.

BIOGRAPHIES OF AUTHORS



Jinsi Jose     completed her post-graduation in Master of Computer Applications (MCA) in the year 2017 from CHRIST University, Bangalore, India. Currently, she is a research scholar in the same university working in the domain of network security in IoT, Department of Computer Science. Her areas of interest include the Internet of things, intrusion detection, artificial intelligence, machine learning, and deep learning. She is a faculty of Rajagiri College of Social Sciences, Kalamassery, India. She can be contacted at jinsi.jose@res.christuniversity.in.



Deepa V. Jose     holds a Ph.D. in Computer Science from CHRIST University, India. Her area of research interest includes wireless sensor networks, security in Internet of things, block chain technology, natural language processing (NLP), and cyber forensics. She has authored several research papers in national and international levels. She is a reviewer for leading computer science journals such as peer to peer networks. She can be contacted at Email: deepa.v.jose@christuniversity.in.