International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

THE MOST EFFECTIVE FRAMEWORKS FOR CLOUD BASED INTERNET OF THINGS USING DEEP LEARNING BASED CYBER ATTACK DETECTION

***Ankita Harshad Tidake[1], Selva Kumar. S[2] , Vijayalaxmi H Manjunatha[3], Veera Jyothi. B[4], Nethravathi. B[5] Chawngsangpuii[6], Saravana Selvam. N [7], Mukta Nivelkar[8]**

[1]Assistant Professor, Department of Artificial Intelligence and Data Science, Ajeenkya DY Patil School of Engineering, Pune, Maharashtra, India, ankita.tidake@gmail.com

[2]Associate Professor, Department of Computer Science and Engineering, B.M.S. College of Engineering, Bengaluru, Karnataka, India, selva.cse@bmsce.ac.in

[3]Assistant Professor, Department of Computer Science and Engineering (IoT & Cyber Security with Block Chain Technology), Mangalore Institute of Technology and Engineering, Moodabidri, Karnataka, India, burukule@gmail.com

[4]Associate Professor, Department of Information Technology, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India, veerajyothi_it@cbit.ac.in

[5]Associate Professor, Department of Information Science and Engineering, JSS Academy of Technical Education, Bengaluru, Karnataka, India, nethravathi.sai@gmail.com

[6]Associate Professor, Department of Information Technology, Mizoram University, Aizawl, Mizoram, mzut126@mzu.edu.in

[7]Professor, Department of Artificial Intelligence and Data Science, PSR Engineering College, Sivakasi, Tamilnadu, India, n.saravanaselvam@gmail.com

[8]Assistant Professor, Department of Information Technology, Fr. Conceicao Rodrigues Institute of Technology, Vashi Navi Mumbai, Maharashtra, India, mukta.nivelkar@fcrit.ac.in

Abstract

The rise of IOT has sparked revolutionary developments in advanced technology, driven by the integration of connected smart devices. While these innovations bring immense benefits, they also introduce complex security challenges. Cyberattacks are a critical problem, especially the context of Intrusion Detection Systems (IDS) as these systems are responsible for detecting and preventing Cyberattacks on the IOT devices. Deep learning has appeared as a promising tool for enhancing the capability of IDS in the detection and prevention of cyber threats targeting IOT networks. However, traditional IDS methods often require you to address unique challenges in an IOT environment, such as the wide selection of connected devices and the diversity of network traffic generated. This article examines the latest progress in intrusion recognition technology for IOT security and focuses on a deep

Received: August 03 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

learning-based approach. Deep Learning Used in IDS-Provides an overview of algorithms, data records involved, different types of cyberattacks, IOT device threats, and criteria for assessing IDS performance. Furthermore, we highlight the challenges of applying deep learning to IOT security and suggest areas that warrant further investigation. Deep learning models are particularly effective in identifying abnormal patterns or potential threats in real-time. By continuously monitoring and responding to security issues, these systems significantly improve the protection of IoT networks from cyber risks, ensuring robust defense against evolving threats.

Keywords: IOT; DL; IDs; Cyberattacks

Introduction

IOT transforms the industry by enabling seamless data recording, analysis and communications between billions of connected devices. The technology is expected to revolutionize sectors such as healthcare, real estate and intelligent cities, achieving 30 billion related devices by 2025. However, the rapid expansion of IOT also poses considerable security challenges. Many IOT devices have limited processing and memory capabilities, making them vulnerable to cyberattacks. As these devices expand further, the risk of data injury and malicious activity increases, and the safety of IOT networks becomes a serious concern. The growing threat of hackers, malware, and other security risks underscores the need for robust IOT security solutions. Traditional security measures, such as systemic security architectures and cryptographic techniques, are important but not sufficient. The complexity and scale of IOT systems demand more advanced solutions to ensure data protection and network reliability. An effective safety measure for IOT networks is the use of IDS. These device monitoring network activity for doubtful actions and warning administrators when a potential security violation occurs. However, conventional IDSs, designed for larger and more powerful networks, struggle to cope with the unique challenges of IOT environments. Due to limited skills on IOT system, it is tough to implement complex IDSS, leading to security gaps. To deal with these limitations, deep learning is required powerful tool to improve the effectiveness of IDSs in IOT networks. By leveraging deep learning algorithms, IDSs can more accurately detect and respond to threats, even in the face of large volumes of information and complex event patterns generated by IOT devices. As the IOT landscape continues to evolve, it is necessary to explore existing research and advancements in deep learning-based IDSs. Understanding the strengths and weaknesses of current systems will help drive improvements in IOT security and ensure the safe and reliable operation of connected devices. With the continued growth of IOT, investing in advanced security solutions, including deep learning-powered IDSs, is crucial to safeguarding IOT networks and protecting sensitive data from cyber threats.

Related Work

In this division includes the evaluation of the related work used by DL techniques for Intrusion recognition in the IOT. It covers both centralized and distributed approaches aimed at improving the detection of various network intrusions.

Received: August 03 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

Centralized DL-based Intrusion Detection Systems:

Alom [1]: We developed the first IDS based on deep face network and tested it on the NSL KDD dataset. Their model achieved 97.5% accuracy, significantly higher than 42% accuracy of the training data.

Kim [2]: This study focused the attacks (distributed rejection) using LSTM networks (long short memory) to record complex patterns in time series data. Their approach achieved 98.8% accuracy on the KDD Cup 99 dataset.

Shone [3]: They proposed system that uses a stacked removal autocoder (NDAES) and random forests in classification. The models tested with the data record KDD cup 99 and NSL-KDD achieved 98% accuracy comparable to previous approaches.

Kwon et al. [4]: We trained the system of NSL-KDD datasets after using MLP model (Multilayer Perfect) to code numerical normalization and categorical features. Your best model achieved 90% accuracy.

Ferrag et al. [5]: Comparative inspections of various DL models including RNN, DNN, Limited Boltzmann Machine (RBM), CNN, Deep Boltzmann Machine (DBM), and DAE were performed. Their results showed that CNN and DAE models of the Bot-Iot datasets of CSE-CIC IDS2018 and Coroniotis versions achieved the highest accuracy of 97% and 98%.

Distributed DL-based Intrusion Detection Systems:

Yadav and Subraman [8]: Your work proposed a solution that recognizes DDOS attacks on the application layer with the help of stacked automatic coders (SAEs) for traffic classification. They reported a DR of 98.98% and an incorrectly (FPR) of 1.28%.

Lopez-Martin [9]: They proposed a system based on Conditional Variable Automatic Code (CVAE) that not only recognizes intrusions, but also reconstructs missing functions from incomplete data records. Their approach achieved 99%, 92%, and 71% accuracy when recovered at 3, 11, and 70 by using NSL-KDD datasets to accommodate NSL KDD datasets.

Luo and Nagarajan [10]: Focuses on reducing high computing costs for deep learning in wireless sensor networks (WSNs). They developed a distributed anomaly recognition system based on automatic (AES) in which sensors independently recognize abnormalities.

Diro and chilamkurti [11]: The proposed distributed architecture on IOT networks of fog nodes estimate model training and attack detection, and master node manages parameter release and optimization. This approach improves the scalability and efficiency of intrusion recognition.

Loupak, et al. [12]: CNN+LSTM combination achieved a maximum accuracy of 97.16%. Data records were compensated by replicating DDOS attack data to improve performance of the DL model.

Received: August 03 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

Contribution of this work

The most important contributions from the work are outlined as follows:

1. In this step, lettering, converts categorical data into numerical values, making it easier to use in subsequent stages of the model.

2. The data is then normalized using standard coal-breading methods to ensure consistency between scales. Given the fact that IOMT data often have several dimensions, PCA is used to reduce dimensions, not only improving performance, but also reducing compensation complexity and making the model more efficient.

3. A K-fold cross-validation technology is used to assess training rate variability, improving both the accuracy and generalizability of the model.

4. In the final stage, multi-tiered building sequentially is used for the process of recognition of preprocessed data records. The algorithm is trained on this data.

5. The proposed approach is compared with algorithms to present its effectiveness through comparative analysis. Ultimately, this study shows that the combination of PCA and deep learning is very effective when recognizing potential security threats.

The structure of the proposed work is as follows: Section 2 provides an overview of related work on topics. Section 3 describes the proposed system covering the data set used, the processing methods, and the deep learning algorithm used. The results and discussion are presented and analyzed in Section 4.

Proposed System

The approach used in this study aims to examine and evaluate the effectiveness of a learning-based system, depth, for recognizing cyberattacks in an IOT environment. This study begins with a comprehensive review of existing literature and provides theoretical analysis of various intrusion methods based on deep learning techniques. We examine key factors in detail, including the prevalence of cyberattacks on IOT networks, existing IDS and cybersecurity related challenges. The theoretical framework establishes a foundation for understanding the complexities of cyber threats in IOT environments.

3.1 Distributed DL Attack Detection Framework:

Modern IOT networks have shared solutions across the border to identify cyberattacks. Due to the distributed IOT environment, the intrusion detection service needs to be revised. Traditional centralized IDS have proven ineffective in preventing novel (zero-day) attacks. This approach consists of four key stages, as shown in Figure 1 data processing and preprocessing, deep learning models training and testing.

Received: August 03 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

Two data records are considered to create a comprehensive solution. A BOT-IOT dataset involved in IOT-specific attacks and an NSL KDD dataset that expands the area of cyberattacks being considered. Both data records are processed to be prepared for use in neural networks. This section focuses on the selection of corresponding deep learning models of the proposed framework. This is because it is suitable for monitored learning and has strong performance. Both networks are originally evaluated in a centralized model, followed by deep learning model in a distributed framework. Finally, performance of the distributed framework can be evaluated in a realistic, distributed environment with limited data.

3.2 Datasets

This paper aims to effectively determine powerful frame to effectively detect IOT cyberattacks. To achieve this, use both BOT-IOT (specific data records for IoT cyberattacks) and NSL-KDD (common cyberattack data records).

The training and test dataset consists of five output masses and four types of attacks: DDO, DOS, Keylog, Data Theft. Keylog refers the attacks in which data theft involves leaking private user information while still capturing information. However, for the purposes of this paper, network traffic of all network sizes is considered. T he introduction of advance network category (such as 5G) leads to a variety of network sizes and scenarios. All attacks in the data record create flooding and features in relation to traffic rates, parcel counts and protocol types that are particularly important by IOT devices.

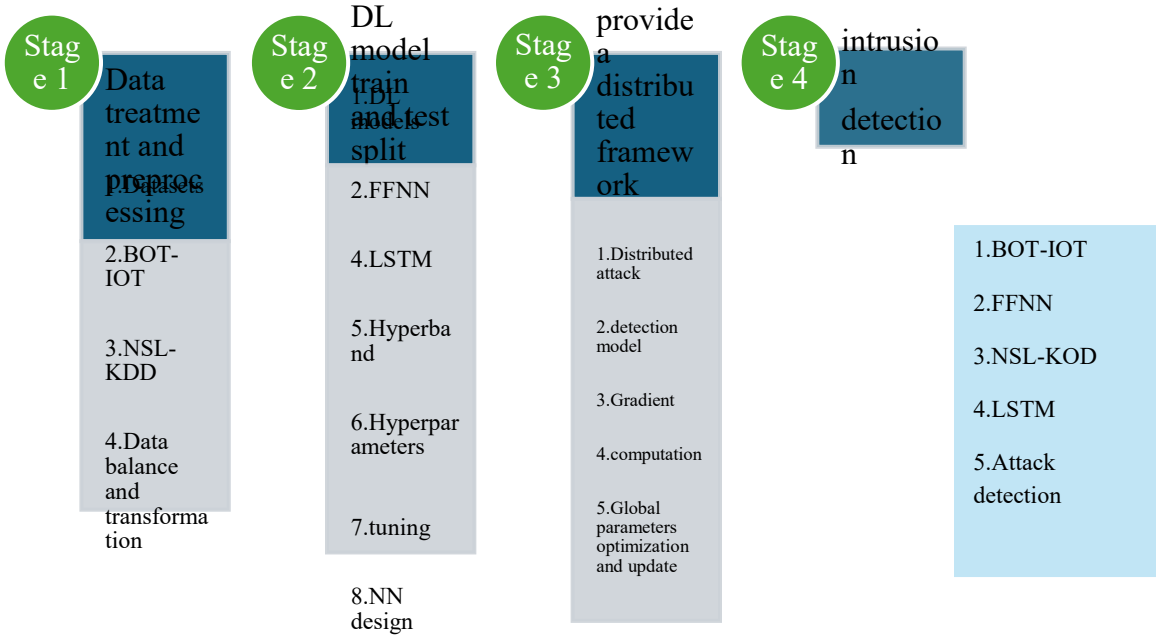

Fig 1: Attack detection framework phase

3.3 Data Pre-processing

Received: August 03 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

Information is processed earlier in the deep learning model. With proper pre-processing of network traffic, the DL model can make fair predictions and reduce the risk of overhangs. The preprocessing process can be divided into two phases: Gathering and information processing.

3.3.1 Attribute Selection

In BOT IOT are functions that contain information about installments, number of packages and protocol category used on IOT devices. Reason for this choice lies on the attack properties available on these devices. Many characteristics are shared between two data records, taking into account the commonality of attacks such as DOS. However, the NSL-KDD dataset also handles network cyberattacks with a variety of characteristics, such as: probing Attack. These attacks target network vulnerabilities rather than just the devices, making their scope broader than those in the BOT -IOT dataset, which focuses primarily on device-centric attacks. As a result, additional network-related features are included in the framework, such as urgent packets, service type, and logged-in status.

3.3.2 Data Processing

Both datasets are imbalanced, with significantly more records for normal traffic than for attacks. Various methods, such as oversampling and under sampling, can be used to address this imbalance. Given the large volume of records, we opted for an under sampling approach. This involves decreasing the number of normal traffic documents (by selected subsets), but attack documents remain intact. In this way, I created a balanced data record with 50% attacks and 50% regular traffic documents.

3.4 Neural Network Models

As soon as the data is processed, a second phase of the frame begins, and the DL model is trained and tested. DL, computing models can learn about different representations and stages of abstraction, allowing them to efficient record complex relationships within the input information. The DL algorithm works starting with preprocessed raw data and converting modules into abstract shapes. Integrating several levels facilitates the learning of highly complex models often used in classification tasks by identifying the category and associated input functions for minimizing the effects of smaller variations.

FFNN is a frequently used model of artificial neuronal networks (ANNs), in which information flows from the input layer through layers hidden in the output layer, moving forward only. Neurons in the input and output layers is determined by the number of input and output variables.

Received: August 03 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

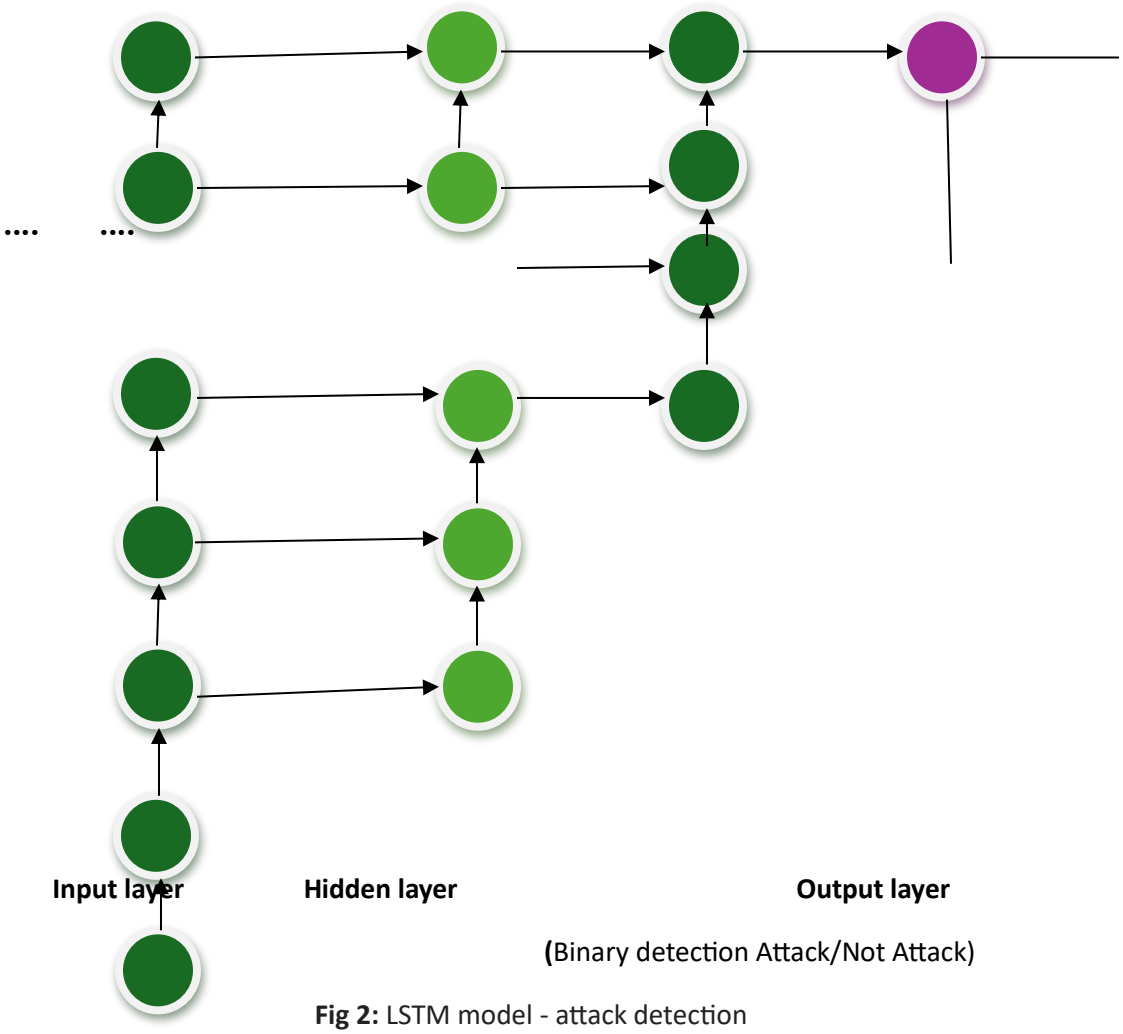

Fig 2: LSTM model - attack detection

The three FFNN layers are fully connected. That is, each neuron is connected to each neuron in the next layer of shift. In real-world applications, the network consists of many neurons. The LSTM model structure used attack detection in IOT environment using BOT-IOT data records follows a similar structure as shown in Figure 1 and 2 but there is an LSTM configuration.

3.4.2 Overfitting Prevention

DAEs and AEs are also well developed, with data records with similar properties being more than 95% accurate. A possible approach to prevent excessive adaptation is to delete the IP address during preprocessing of the data record. However, because various IP attackers are used for training and verification rates, there are no repeating addresses, and the model cannot remember specific swimming point numbers that satisfy the attacker's IP address. Additionally, understanding the nature of IP attackers is important, as this knowledge can help in implementing future preventive measures through tracking. A promising area for future research involves using explainable AI to determine Whether there

Received: August 03 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

is an actual connection between the IP address and the method used in the attack, especially the method associated with DOS.

3.5 Distributed Framework

Proposed solution improves existing methods by bringing attack detection through acceleration . Additionally, unloading global parameter updates to the cloud reduces arithmetic and storage. The resulting updates are output to the fog node. This approach also helps to shorten detection periods.

3.5.1 Framework Description

Distributed attack recognition architecture based on DL is designed to integrate intrusion detection into fog computer systems in an IOT environment. As shown in Figure 3, IOT architecture consists of three layers: edge, fog and cloud. The edge layer consists of millions on IOT devices with limited resources, such as smart phones, sensors, surveillance cameras, and intelligent vehicles. These devices generate a large amount of unstructured data transferred to the fog layer. Initially, as is common in most deep learning techniques, the weights of the model are initialized first.

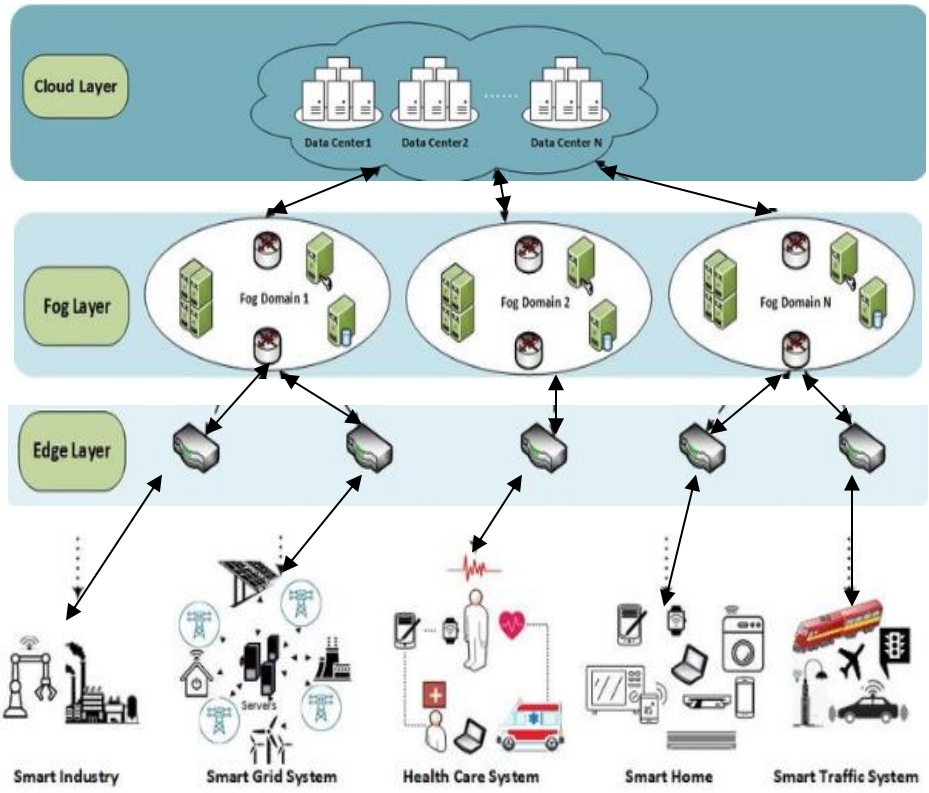

Fig 3: DL-based distributed attack architecture for distributed architectures of fog/ on IOT networks

Received: August 03 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

Objective	DL model	Dataset	Hidden layers	Units	Dropouts (%)	Epochs
Detection	FFNN	BOT-IOT	2	110/55/110	–	12
		NSL-KDD	3	49/129/89/187	25/45/25/35	15
	LSTM	BOT-IOT	4	110/63/34	–	32
		NSL-KDD	6	55/101/201/110/55	–	22

Table 1 FFNN and LSTM DL models to detect cyber-attacks on IOT networks

Table 1 summarizes the equipped FFNN and LSTM-DL models to recognize and classified cyberattacks on IOT networks.

Algorithm 1 represent the steps involved preprocessing, updating the model and updating the gradient weight, verifying the model of the new distributed attack system.

Algorithm 1 Distributed learning algorithm

Require: Global parameters M_w →Random values

1: for all epochs do

2: for all nodes do

3: for all devices do

4: Pre-process user raw data RD_x →PD_x

5: Send pre-processed user data to the corresponding fog-node

6: M_w: Download the updated model from the Cloud Server

7: Train the model (M_w) with the local dataset (PD_x)

8: and get the new model weights (W_x)

9: end

10: Get the mean weights from all devices in the fog node:

Received: August 03 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

11: $\Delta W_f = \Sigma_{i=1}^{X}(W_i - W_{global})/x$

12: Send the gradient weights (ΔWf) to the Cloud server

13: end

14: Update the global model with the following criteria:

15: $Mw = Mw + mean(\Sigma_{i=x}^{X}(\Delta W_i))$

16: end =0

Validated model

The two best DL models that recorded the data, FFNN and LSTM, have been combined into a distributed framework with BOT-IOT and NSL-KDD. Performances are presented and analyzed in the next section.

Results

These models are evaluated using a variety of metrics to assess their effectiveness. Metrics include accuracy (ACC), loss, accuracy, and recall. These metrics are derived from a confusion matrix that specifies the numerous of attacks and ordinary data records to which true positive (TP) and true negative (TN) are correctly classified, and shows the classification results that FP and FN correctly classify the numerous of regular attack rates.

The Accuracy (Equation 1) is the ratio of the correct classification predictive to the total number of authorities evaluated.

$$Accuracy = (TP + TN) / (TP + TN + FP + FN) \quad (1)$$

Accuracy (Equation 2) is the ratio of the overall predictive elements of the accurately classified element.

$$Predictive = TP / (TP + FP) \quad (2)$$

A callback (Equation 3) is the ratio of the correct classification elements (attack or normal) for all elements.

$$Recall = TP / (TP + FN) \quad (3)$$

To ensure stability and consistency of neural networks, all conclusions in a distributed environment are repeated 20 times to prevent unnecessary redundant calculations that are overloaded by the cloud server.

Received: August 03 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

4.1 Distributed Framework Results

Objective	DL model	Dataset	Accuracy (%)	Predictive (%)	Recall (%)
Detection	FFNN	BOT-IOT	98.96	98.94	99.98
		NSL-KDD	99.68	99.32	98.23
	LSTM	BOT-IOT	98.96	98.92	98.94
		NSL-KDD	97.45	96.75	98.68

Table 2 FFNN and LSTM realize cyberattacks on IOT networks

FFNN is proven and is an ideal download model for cyberattack recognition in a centralized IOT environment.

Table 2 shows the results of FFNN and LSTM deep learning models for detecting cyberattacks on IOT networks. The results for the BOT-IOT dataset are roughly the same, but there are significant differences in the NSL-KDD dataset.

The structure of the distributed framework allows only FFNN to be integrated and tested with data records for BOT-IOT and NSL-KDD. Figures 4 and 5 show the accuracy, while Figures 6 and 7 show the results for the NSL KDD dataset. Because data records compensated, that is, approximately equal proportions, accuracy, and recalls of benign and malicious samples serve as representative metrics. The loss function is used to identify potential overadaptations on the model.

Thus results reflect the network performance during the validation phase that occurs in the cloud environment after individual training of the model on all fog nodes. The poor performance remains below 1% for all metrics, resulting in losses well below 1%. As a result, the ultimate performance of distributed systems remains strong and achieves high results.

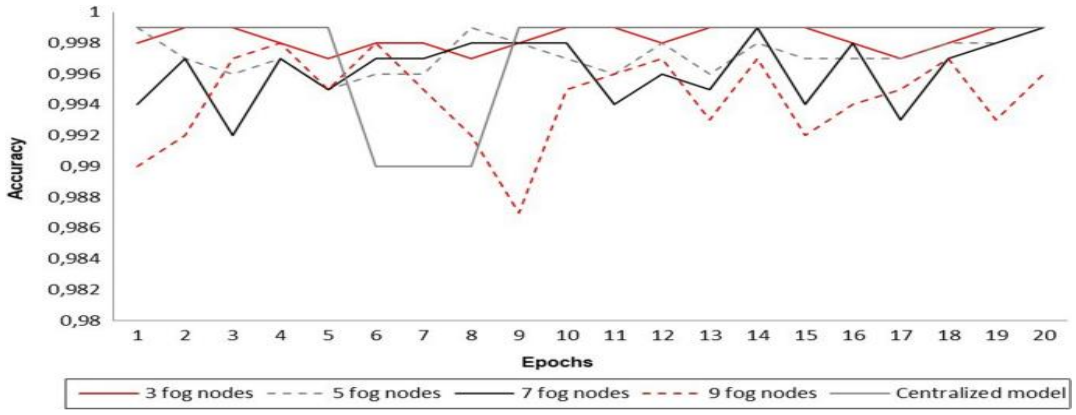

Fig 4: BOT - IOT dataset FFNN leads to a distributed framework of 1, 3, 5, 7, 9 fog nodes

Received: August 03 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

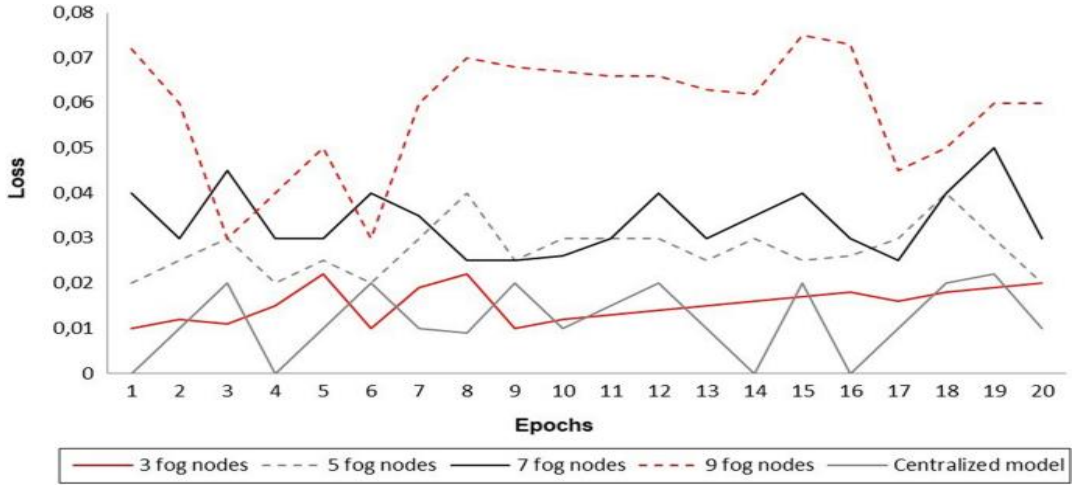

Fig 5: BOT - IOT dataset FFNN loss leads to a distributed framework of 1, 3, 5, 7, 9 fog nodes

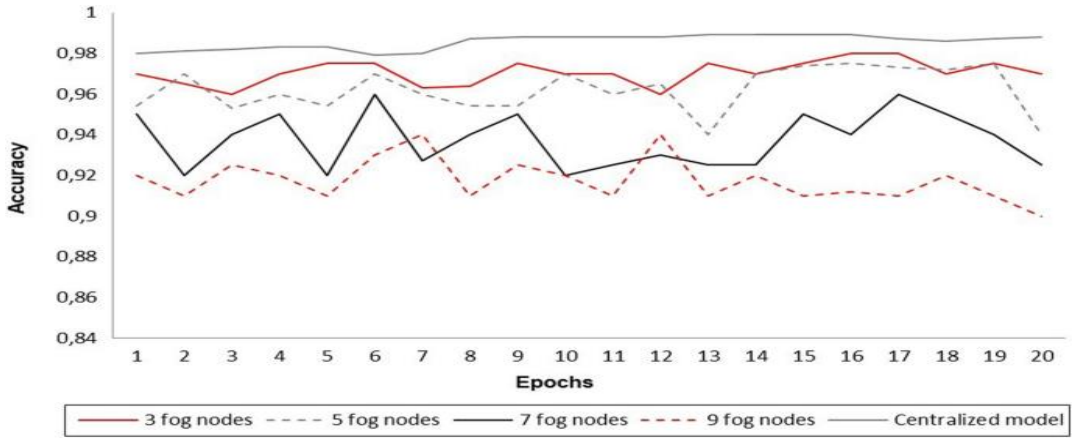

Fig6: NSL-KDD dataset FFNN ACC leads to a distributed framework for 1, 3, 5, 7, 9 fog nodes

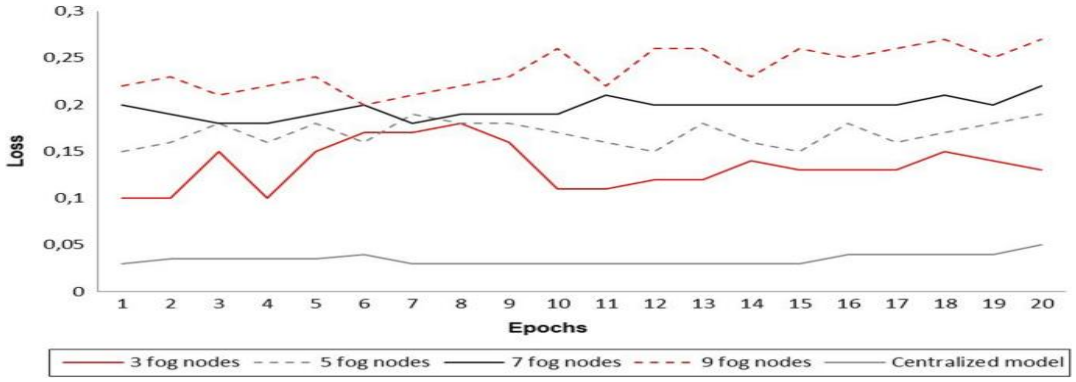

Fig 7: NSL-KDD dataset FFNN loss leads to a distributed framework of 1, 3, 5, 7, 9 fog nodes

Received: August 03 ,2025

International Journal of Applied Mathematics

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

Conclusion

The proposed frame is distributed, these fog nodes process information close to the margin, while simultaneously improving detection and classification accuracy. This framework uses two data records to compare LSTM with two models, BOT-IOT and NSL-KDD. FFNN exceeds LSTM in the detection rate of both data records, particularly for NSL-KDD data sets. This experiment demonstrates the effectiveness of distributed DL models on IOT networks to recognize various attacks with high accuracy. Framework improves cyberattack awareness on IOT networks resource-limited devices, and identifies several attacks, particularly for BOT option datasets. In future, we plan to datasets by implementing information expansion technology ensure sufficient information in the event to an increase the number of FOG nodes. This helps to achieve results of comparable accuracy to those received on BOT IOT dataset. As a result, the accuracy, accuracy and recall of centralized architectures remain similar. Finally, both NSL-KDD and BOT-IOT data records may spread similar characteristics and allow for uniform models for attack detection on distributed environments. As a result, the distributed framework represent in this article will extended for future projects and can applied to a variety of fields using a variety of transfer learning techniques.

References

[1] Intrusion detection using deep belief networks. Alom, M.Z., Bontupalli, V., Taha, T.M.:. National Aerospace and Electronics Conference (NAECON), pp. 339–344 (2015). : s.n., In: 2015.

[2] Short Term Memory Recurrent Neural Network classifier for intrusion detection. Kim, J., Kim, J., Thi Thu, H.L., Kim, H.:. International Conference on Platform Technology and Service (PlatCon), pp. 1–5 (2016). : s.n., In: 2016.

[3] A deep learning approach to network intrusion detection. Shone, N., Ngoc, T.N., Phai, V.D., Shi, Q.:. IEEE Trans. Emerg. Topics Comput. Intell. 2(1), 41–50 (2018). : s.n., (2018).

[4] A survey of deep learning-based network anomaly detection. Kwon, D., Kim, H., Kim, J., Suh, S., Kim, I., Kim, J. Clust. Comput. 22(5), 949–961 (2019) : s.n., (2019).

[5] Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study. Ferrag, M.A., Maglaras, L., Moschoyiannis, S., Janicke, H. J. Inform. Secur. Appl. 50, 102419 (2020). : s.n., (2020).

[6] Dataset IDS 2018. Cibersecurity, C.I. CSE-CIC-IDS2018 on AWS. : s.n., Accessed 17 Mar 2021.

[7] Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Koroniotis, N., Moustafa, N., Sitnikova, E., Turnbull, B. Futur. Gener. Comput. Syst. 100, 779–796. : s.n., (2019).

Received: August 03 ,2025

Volume 38 No. 5 2025,

ISSN: 1311-1728 (prnted version); ISSN: 1314-8060 (on-line version)

[8] Detection of application layer DDoS attack by feature learning using Stacked AutoEncoder. Yadav, S., Subramanian, S. International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), pp. 361–366 (2016). : s.n., In: 2016 .

[9] Conditional variational Autoencoder for prediction and feature recovery applied to intrusion detection in IoT. Sensors. Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., Lloret, J. (Basel) 17(1967), 1–17 . : s.n., (2017).

[10] Distributed anomaly detection using autoencoder neural networks in WSN for IoT. . Luo, T., Nagarajan, S.G. IEEE International Conference on Communications (ICC), pp. 1–6 (2018). : s.n., In: 2018.

[11] Distributed attack detection scheme using deep learning approach for Internet of Things. Diro, A.A., Chilamkurti, N.:. Futur. Gener. Comput. Syst. 82, 761–768 (2018). : s.n., (2018).

[12] Deep learning models for cyber security in IoT networks. . Roopak, M., Yun Tian, G., Chambers, J. IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 452–457 (2019). : s.n., In: 2019.

[13] Toward generating a new intrusion detection dataset and intrusion traffic characterization. . Sharafaldin., I., Habibi Lashkari., A., Ghorbani., A.A. In: Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), vol. 1, pp. 108–116 : s.n., (2018).

[14] Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection. Vijayanand, R., Devaraj, D., Kannapiran, B. Comput. Secur. 77, 304–314 : s.n., (2018).

Received: August 03 ,2025