International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Deep Learning Perspectives to Detecting Intrusions in Wireless Sensor Networks

Ashwini B. Abhale* and Dr. Jayaram Reddy A**

Submitted: 14/10/2022 **Revised:** 27/12/2022 **Accepted:** 20/01/2023

Abstract- Due to the increasing number of communication protocols being used to send and receive data, security concerns have been raised about the unauthorized access of this data. To address these issues, the development of advanced IDS has been carried out. Deep learning is a type of machine learning that is composed of several neurons. Due to the increasing number of large-scale data sets and the success of deep learning in various fields, researchers have focused on detecting intrusions using deep learning. Due to the increasing number of data transmissions through various communication protocols, there has been a rise in security concerns about the security of these networks. This has prompted researchers to develop advanced IDSs that can detect unauthorized access. Besides having an effective network intrusion detection system(NIDS), continuous improvement is also required to ensure that the security of the network is maintained. Deep learning techniques are commonly used in the detection of network intrusions. It can also perform various tasks, such as analyzing and reporting on data. Due to its success in various fields, researchers have been focusing on developing deep learning techniques for detecting intrusions. This paper aims to review the current state of deep learning-based IDSs and compare with proposed modified algorithms with the previous ones.

Keywords- *Deep learning, Anomaly detection, CNN, CNN-LSTM, GRU, RNN, LSTM*

1. Introduction-

According to the Ericsson Mobility Report, "*there will be over 500 million 5G subscriptions in 2022, and Asia Pacific will be the fastest-growing region. It also noted that the number of connected devices will increase by about 29 billion by 2022, with 18 billion of these being related to the Internet of Things*". The rapid emergence and evolution of 5G and the Internet of Things are some of the most talked about topics in the industry. According to a survey conducted by Ericsson, over 90% of executives from leading telecom companies believe that the next generation of wireless technology will allow the development of innovations. Various tools can help prevent cyber-attacks and keep the networks secure. These include firewalls, spam filters, antimalware tools, and anti-phishing software. These tools are universal across organizations regardless of their size and industry.

According to ALERTLOGIC^{TM} "*An intrusion detection system (IDS) is a device or application that can be used to monitor and detect unauthorized access to the network. It can then alert the appropriate person or organization when a breach occurs*". Despite the various security measures that can be implemented to prevent unauthorized access to a network, no matter how well they are designed, no system is impenetrable. Attackers constantly develop new ways to circumvent these measures. One of the most critical factors that you should take into account when it comes to protecting your network is the availability of an intrusion detection system[1]. This type of device can be used to monitor and detect unauthorized access to the network. It can then notify the appropriate person or organization when a breach occurs. It can also trigger alarms when it discovers certain types of suspicious activity.

Anomaly-based, signature-based or Hybrid based IDS can be used to identify and prevent unauthorized access to an organization's data.[2] In the former, the goal is to analyze monitored behaviors and compare them with pre-defined intrusion patterns. On the other hand, in the latter, the goal is to identify anomalous behavior and prevent unauthorized access. Different techniques such as machine learning and statistical-based methods, are used to detect anomalies. A deep learning system is a type of machine learning which uses multi-layer networks to

**Research Scholor, School of Information Technology & Engineering(SITE),Vellore Institute of Technology, Vellore, India.*
Email : ashwiniabhale@gmail.com
***Assistant Professor, School of Information Technology & Engineering(SITE),Vellore Institute of Technology, Vellore, India.*
Email : ajayaramreddy@vit.ac.in
**Corresponding Author : Ashwini B Abhale (+91 9970756938), ORCID ID : 0000-0002-6053-2282*

perform various tasks, such as natural language processing and image recognition. It has been shown to excel in various fields.[3].

A network intrusion detection system is used to identify and secure a wireless sensor network (WSN). It can detect security attacks and other unauthorized activities by analyzing the data collected by the devices and the network technologies. However, due to the increasing number of data collected by the networks and the high-tech devices, the detection rate of these attacks has decreased. Due to the complexity of detecting an intruder, the security systems must be equipped with the necessary tools and resources to efficiently handle the vast amount of data that is collected and stored in a distributed environment[3]. An intrusion is a type of unauthorized activity that can be carried out to gain access to a wireless sensor network. Two levels of security are provided for this type of network. The first level is designed to protect the network from unauthorized access. The second level detects and prevents unauthorized activities from happening on the network.

This research presents a comparative improvement in various deep learning algorithms with proposed enhanced algorithms on the NSL-KDD dataset. The significant contribution of this paper is to improve the performance of deep learning algorithms to provide better safety and security to WSN.

The remainder of the paper is arranged as follows: section 2 deals with the literature review, section 3 describes the dataset used, and the next section deals with WSN and algorithms used in this paper. Sections 6 and 7 deals with evaluation metrics and results. Section 8 concludes the paper.

2. Related Work

Zhendong Wu et al.[4] proposed SRDLM method is used to re-encode the semantics of network traffic. It enhances the algorithm’s ability to distinguish between traffic and improves its robustness. Through deep learning, it can also be used to improve the accuracy of the algorithm. For instance, the SRDLC algorithm for detecting Web character injection attacks has a 99% accuracy. The NSL-KDD data set can be easily detected using machine learning techniques, and its average performance improved by over 8%.

Ashfaq Hussain Farooqi et al.[5] proposed a novel; distributed system that aims to detect intrusions is designed to work with its neighbors to identify and prevent unauthorized access to its nodes. It can be done in two modes: offline detection and online prevention. Online prevention allows the system to protect the nodes that are already considered malicious, while offline detection scans the nodes that an adversary exploits. A simulation of a proposed detection scheme shows that it can achieve high and low false positive rates.

Congyuan Xu et al.[6] introduce a novel IDS that combines a neural network with a resilient multi-layered perceptron, a softmax module, and a gated recurrent unit. The results of the experiments show that the system has exceptional performance. The KDD 99 and NSL-KDD systems were able to achieve a detection rate of 99.42% and 99.31%, respectively. Furthermore, they could detect denial of service attacks with 99.98% and 99.55% accuracy. In addition, comparing the performance of these two systems, it was revealed that the GRU is more suitable for IDS than the LSTM.

Pascal Maniriho et al.[7] presented a new approach to analyzing the performance of Internet of Things networks using a hybrid feature selection engine and random forest algorithm. The system's performance was evaluated using IoTID20, a dataset collected from the IoT Environment. The proposed method was able to achieve high accuracy while detecting various types of attacks, such as DoS, MITM, and scanning.

Christian Miranda et al.[8] develop a framework that combines a lightweight authentication method with an intrusion detection system and a real-time monitoring system. This will allow for enhanced anomaly detection in SDWSNs.

Yakubu Imrana et al.[9] develop a deep learning model that can detect network intrusions. The proposed model performed well and achieved accurate results. The model was trained to validate its performance using the NSL-KDD dataset, a widely used benchmark for network intrusion detection. The BiDLSTM model performed well in the experiment and was able to improve its recall, F-score, and accuracy compared to the conventional LSTM model. It also outperformed other models in detecting different attack classes.

Shaimaa Ahmed Elsaid et al.[10] proposed a system for detection of illicit substances with a detection rate of 97.9% and a false alarm rate of 1.8%, which is significantly better than the other systems. The small standard deviation of the proposed system shows that it has an advantage over other detection systems. Also able to determine the impact on the system’s performance. They found that the NSL-KDD dataset exhibited the lowest false alarm rate and highest detection rate

Jorge Granjal et al.[11] proposed approach to protect devices from attacks is based on a multi-class problem that can be easily solved by analyzing the patterns of intrusions. The accuracy of the proposed system is at 93%, which is higher than the 92% achieved with the binary class problem. Despite the lower accuracy, the researchers achieved a recall of 98% and a F1-Measure of 98%.

Tanya Sood et al.[12] proposed a conditional generative adversarial network (CGAN) in an unsupervised learning model for analyzing data. It used to generate fake data to fool an intruder. Method reduces the need for deploying additional sensors to achieve the desired results.

Sandeep Sharma et al.[13] analyze the probability that an intruder follows a particular path to reach a specific target area within a mobile sensor network. It then formulates a barrier coverage strategy to prevent intruders from entering the network.

Muder Almiani et al.[14] proposed model for detecting IoT network security based on a Fog computing-based neural network. It uses a modified backpropagation algorithm to train a recurrent neural network. The model considers the various types of attacks that can affect the development of an IoT network, such as DoS attacks. It can also detect other attacks, such as R2L, U2R, and probes.

Georgios Efstathopoulos et al.[15] proposed an anomaly-based IDS developed for the Smart Grid that handle the data collected from a real power plant. Through the use of deep learning and machine learning models, the system was able to improve its accuracy by 29%.

3. Dataset

This paper used the dataset developed by Mahbod Tavallaee et al. named NSL-KDD dataset. This is the modified and updated version of KDD dataset.

4. Lexicon Related to Wsn

Wireless Sensor Network- A wireless sensor network (WSN) as shown in fig.1 is a distributed communication system that enables users to establish and manage their own networks without needing a central hub or fixed infrastructures. It is one of the most promising innovations in the wireless transmission industry[16]. The system utilizes a set of dynamic nodes to provide a secure and reliable communication experience. In addition to industrial automation, this technology can also be used to monitor various other fields such as agriculture, environment monitoring, and military surveillance. These wireless sensors can be connected to a network to collect and interpret data. Traditional WSNs usually consist of switches and routers as their components. As their size grows, they become difficult to update and monitor. Also, large-scale WSNs are often heterogeneous due to their different communication protocols. These networks are composed of different clusters that only communicate at low levels[17]. Due to the nature of the WSN's distributed management system, it is very complex to implement and manage security mechanisms in the network. This makes it an ideal platform for developing and managing applications. As the system's size and complexity increase, it also faces various constraints. Some of these include energy restrictions, memory limitations, and processing capabilities[18]. Due to the system's complexity, the need for a lightweight security framework is also becoming more prevalent. This can be achieved through the use of intelligent features.

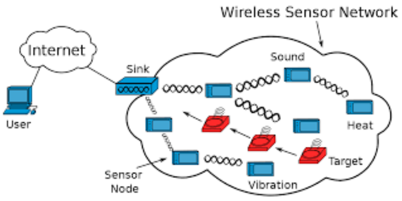

Fig. 1 Wireless Sensor Network *(img src- wikidata)*

A network-based security system can help organizations monitor their hybrid and cloud environments for signs of a potential security compromise. It can also detect policy violations and port scanning. Instead of being actively deployed, security technologies known as NIDS are typically only used to alert on suspicious activities. This means that they are often partnered with intrusion prevention systems. Organizations use NIDS system to enhance their security visibility by monitoring and analyzing events from multiple sources[18]. Basic architecture is shown in fig.2

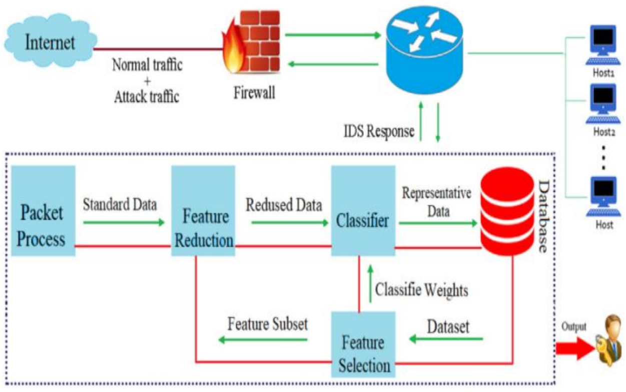

Fig. 2 Basic Architecture of NIDS[19]

Method of analysis of Intrusion Detection System

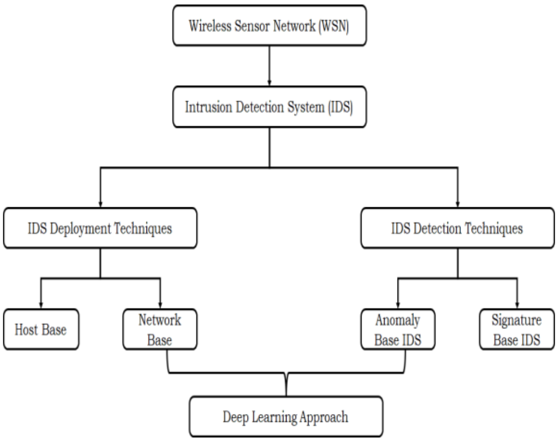

Fig. 3 Types of IDS

4.1.1 Host Intrusion Detection System

(HIDS) is an IDS security that monitors a single device's network traffic and logs. It uses a series of regular file sets to capture the system's state. When a snap is taken, the IDS verifies that all settings are intact by comparing the previous state to the present state.. A HIDS provides a deeper understanding of the host device's activity, such as permissions, files, registry, and configuration changes. It can also detect malicious packets sent from inside the organization. Its second line of defense against unauthorized changes to files is useful when trying to prevent software integrity breaches. A HIDS is more cost-effective than a NIDS in analyzing encrypted traffic. The main disadvantages of a HIDS are its limited visibility and lack of context for decision-making. Large organizations can be hard to manage due to the complexity of handling all the details for each host. Also, it's not good at detecting network scans and other network-wide attacks.

4.1.2 **Network intrusion detection system (NIDS)**

Network-based utility that monitors and analyses incoming and outgoing network traffic. It can be deployed at various points within the network, such as data chokepoints. An IDS security system is a good thing for an enterprise network. It can monitor and secure the various parts of the network. A few NIDS can be placed strategically around the network to provide visibility into the security of the network. However, the setup of an NIDS can be very expensive, especially if it has to monitor a large and busy network. It can also suffer from low specificity, as it cannot detect attacks within encrypted traffic.

4.1.3 **Anomaly-Based Intrusion Detection System**

(AIDS) is an IDS that monitors the traffic patterns of a network. It uses machine learning to identify malicious behavior instead of relying on data patterns. This type of IDS also sets a baseline for expected system behavior. Through a system analysis, the system can check for new behaviors similar to those observed in a signature-based IDS. It can then identify attacks that are not supported by the signature. However, an anomaly-based attack might be a cause for investigation. AIDS can detect new threats and signs of unauthorized activity. It can also build a model of trustworthy behavior based on machine learning. The complexity of an AIDS is one of its main disadvantages. It requires more processing resources to manage.

4.1.4 **Signature-Based Intrusion Detection System (SIDS)**

is a network security tool that monitors the movement of packets through a network. It compares those packets' attributes and attack signatures to a database of known patterns. A SIDS can be used against attackers who use known attack signatures. It can also be helpful in discovering low-skill attacks. It can efficiently process a large amount of network traffic. Without a signature in the database, a SIDS cannot identify a breach. An attacker can modify an attack by changing its attack signature. This can be done by changing the character code or letters of a symbol. Therefore, the database needs to update regularly to keep up with the latest threats.

5. Various Algorithm Used in This Paper

5.1 Deep Learning

Deep learning is a type of artificial intelligence that can be used to learn complex tasks. This type of learning is part of a larger family of machine learning techniques. Developers can use deep learning techniques in various fields, such as medical image analysis, computer vision, natural language processing, and machine translation. These techniques have been widely used in various applications, such as board game development and scientific research. They have been able to produce exceptional results in some cases, surpassing the performance of human experts. Deep learning is a type of machine learning that uses multiple layers in the network. Although a linear perceptron can be considered a universal classifier, it can also be equipped with a non-polynomial activation function that allows it to perform unsupervised. This type of learning is a modern variation of the same concept, and it allows for optimal implementation and practicality. In deep learning, the layers are often heterogeneous, which allows them to deviate from the biologically informed models. This is because deep learning aims to improve its understandability and efficiency.

5.2 CNN

Convolutional Neural Networks are a form of Deep Learning algorithm that can analyse an input image and give weights to its many features. It can then differentiate one from the other. ConvNets are much cheaper to implement than other classification tools. In primitive methods, the process of learning these types of filters was manually performed. ConvNets can acquire these properties with sufficient training[20]. The Convolutional Operation seeks to extract high-level characteristics from the input image, such as the edges. Unlike other methods, it does not need to be limited to one ConvNet. Instead, it can be expanded to include other layers to provide a more comprehensive understanding of the data. ConvNets can perform two types of operations: One of which is to reduce the dimension of the feature that it takes concerning the input. The other is to increase or remain the same.

5.3 CNN-LSTM

The CNN Long-term Storage Memory Network or CNN LSTM is a type of architecture that can be used for sequence prediction problems. It combines the capabilities of a neural network and long-term memory to form a classification module. The module is ideal for security applications due to its ability to consider the correlation between data.

5.4 LSTM

The LSTM is a neural network that can be used for various tasks, such as speech recognition and machine translation. It has become the most cited network of the 20th century. The term long-term memory refers to an artificial neural network that can be used in the fields of deep learning and artificial intelligence. Unlike other neural networks, which only process single data points, the LSTM uses feedback connections to process data sequences[21]. The LSTM is an analogy to a standard RNN, which has both short-term and long-term memory. The LSTM architecture aims to create a short-term memory that can be used for RNNs that can last thousands of time steps.

5.5 RNN

Neural network is a sort of computation in which the outcome of the previous step is used as the input for the following phase. In most instances, the network's inputs and outputs are independent of one another. In specific circumstances, such as when predicting the following word in a sentence, the prior words are necessary. Recurrent Neural Network (RNN) created to solve this issue by implementing a hidden layer. This feature allows the system to remember certain details about a sequence.

7. Results and Discussion

The proposed study shows that proposed methods are more efficient than the traditional methods. Table -1 and Table 2 shows the comparison between various evaluation metrics namely accuracy, precision, recall and F1-score. Fig. 4 and fig.5 shows the graphical representation of the comparison. Fig 6 to fig.10 shows the roc curve comparison between traditional and proposed method.

5.6 GRU

A basic Recurrent Neural Network can often encounter issues with the vanishing-exploding gradients to resolve the issue Gated Recurrent Unit Network (GRU) is introduced. The main difference between a GRU and a basic RNN is that the latter involves gates that modulate the current state and the previous hidden state of the network..

6. EVALUATION MATRIX

6.1 Classification Accuracy: The accuracy of a classification model is one of the most critical factors that can affect its performance. It measures the number of times the model correctly predicts the output.

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN}$$

6.2 Precision: The precision metric is used to measure the number of outputs that the model has provided that were correct.

$$\text{Precision} = \frac{TP}{TP+FP}$$

6.3 F1-measure: F1-measure is a tool that helps determine the recall and precision of a model. It can be used to evaluate both the recall and the precision of a given model.

$$\text{F1-measure} = \frac{2*Precision*Recall}{Precision+Recall}$$

6.4 Recall: The recall metric is used to determine the percentage of positive values that the model can correctly predict.

$$\text{Recall} = \frac{TP}{TP+FN}$$

6.5 Area Under Curve (AUC)**:** Area Under Curve is the area of the two-dimensional area that’s under the ROC curve. It’s commonly used to evaluate binary classification problems. The Area Under the Curve is the probability that a given classifier will rank a given positive or negative example higher than a given negative example. This feature allows a system to distinguish between classes.

Table 1 Accuracy Comparison between various model (Traditional vs Proposed)

Models	Traditional (%)	Proposed(%)
CNN	99.39	99.42
CNN - LSTM	98.69	99.18
RNN	98.91	98.99
LSTM	98.53	98.87
GRU	98.56	99.17

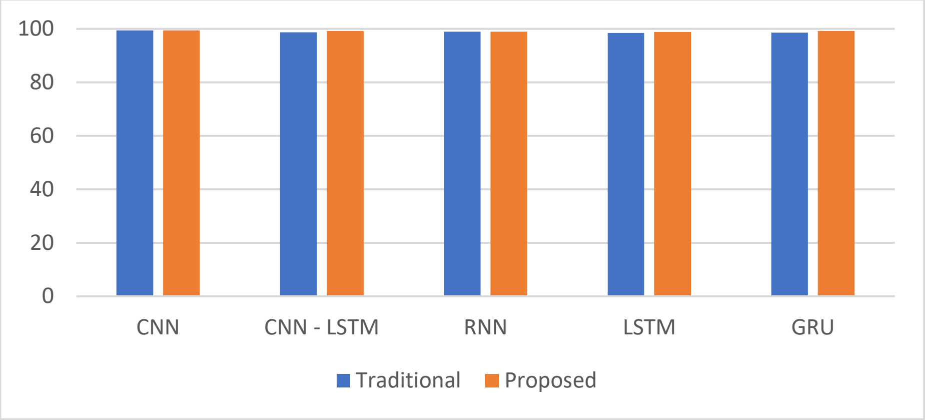

Fig. 4 Accuracy Comparison Traditional vs Proposed Model

Table 2 Table 1 Precision, Recall and F1-score Comparison between various model (Traditional vs Proposed)

	Precision		Recall		F1-score	
Models	Traditional	Proposed	Traditional	Proposed	Traditional	Proposed
CNN	99.95	99.99	99.01	98.98	99.91	99.95
CNN - LSTM	98.8	99.44	98.32	98.86	99.51	99.73
RNN	98.9	99.01	98.86	98.74	99.77	99.77
LSTM	98.69	98.51	98.46	98.71	99.16	98.85
GRU	97.63	99.37	98.27	98.98	98.67	99.73

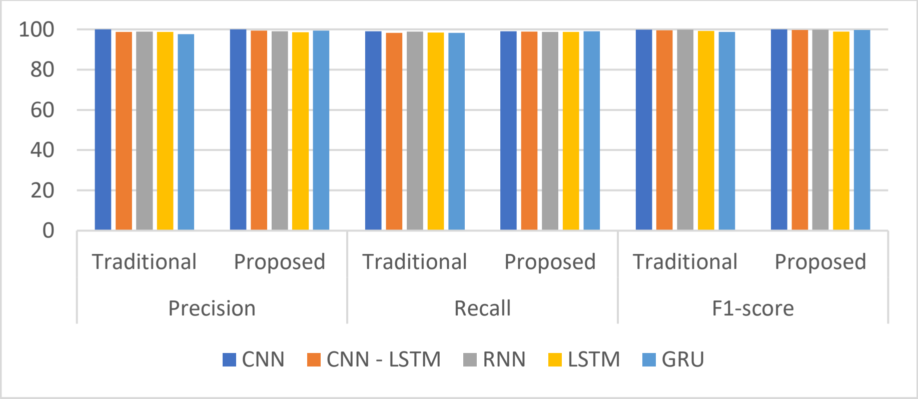

Fig. 5 Precision, Recall and F1-Score Comparison Traditional vs Proposed Model

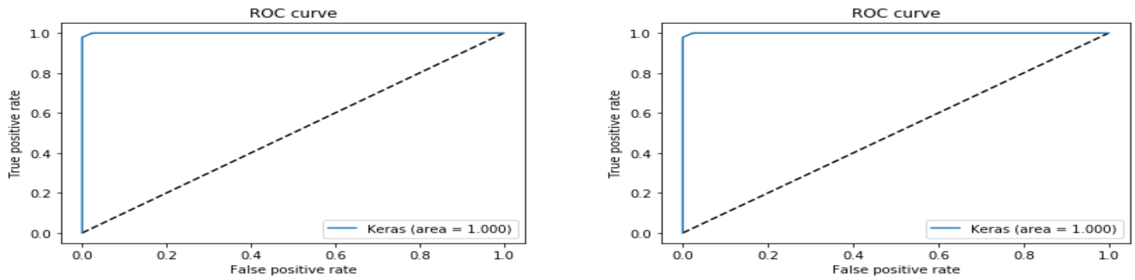

Fig. 6 ROC comparison of Traditional CNN and Proposed CNN

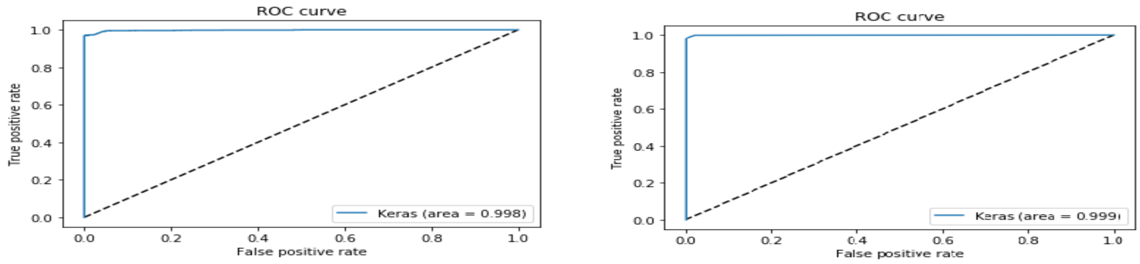

Fig. 7 ROC comparison Traditional CNN and Proposed CNN

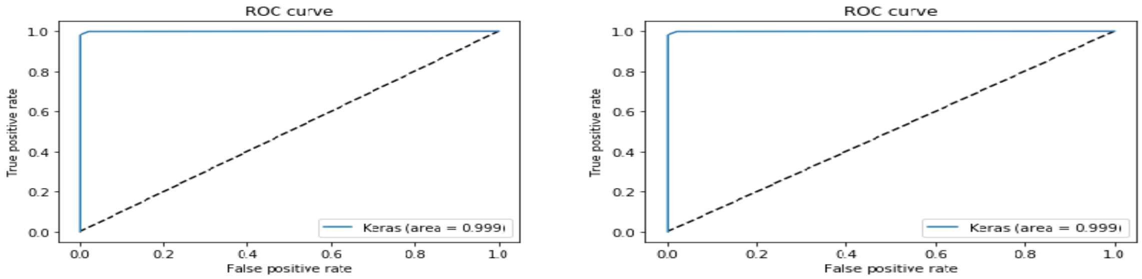

Fig. 8 ROC comparison Traditional RNN and proposed RNN

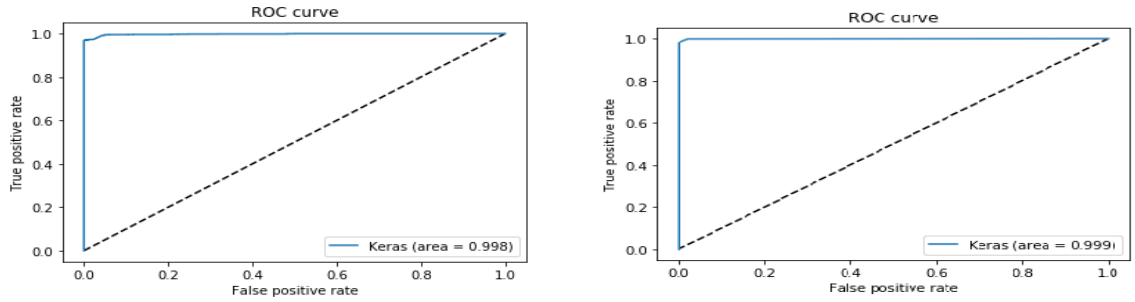

Fig. 9 ROC comparison Traditional LSTM and Proposed LSTM

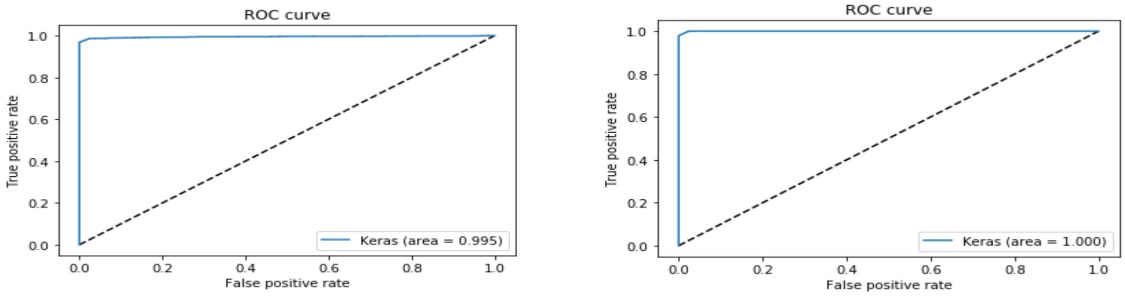

Fig. 10 ROC comparison Traditional GRU and Proposed GRU

8. Conclusion

The proposed IDS work is able to provide excellent precision and accuracy under certain constraints. It also applied to different dimensions and datasets. In this paper, we show the model's efficacy under various metrics. In the field of computer science, deep learning is used to process large and complicated datasets. Additionally, it does not require any human assistance to discover correlations between the many input features. New technologies, such as traffic transmission, are developing at a breakneck pace, prompting academics to explore the potential of deep learning in intrusion detection.. This work conducted to compare the various existed algorithm with proposed algorithm.

Declarations

Funding: NA

Conflicts of interest: The authors have no competing interests related to the submission of this manuscript.

References

[1] A. Thakkar and R. Lohiya, *A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges*, vol. 28, no. 4. Springer Netherlands, 2021.

[2] R. Ganeshan, C. S. Kolli, C. M. Kumar, and T. Daniya, "A Systematic Review on Anomaly Based Intrusion Detection System," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 981, no. 2, 2020, doi: 10.1088/1757-899X/981/2/022010.

[3] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowledge-Based Syst.*, vol. 189, p. 105124, 2020, doi: 10.1016/j.knosys.2019.105124.

[4] Z. Wu, J. Wang, L. Hu, Z. Zhang, and H. Wu, "A network intrusion detection method based on semantic Re-encoding and deep learning," *J. Netw. Comput. Appl.*, vol. 164, no. March, 2020, doi: 10.1016/j.jnca.2020.102688.

[5] A. H. Farooqi, F. A. Khan, J. Wang, and S. Lee, "A novel intrusion detection framework for wireless sensor networks," *Pers. Ubiquitous Comput.*, vol. 17, no. 5, pp. 907–919, 2013, doi: 10.1007/s00779-012-0529-y.

[6] C. Xu, J. Shen, X. Du, and F. Zhang, "An Intrusion Detection System Using a Deep Neural Network with Gated Recurrent Units," *IEEE Access*, vol. 6, pp. 48697–48707, 2018, doi: 10.1109/ACCESS.2018.2867564.

[7] P. Maniriho, E. Niyigaba, Z. Bizimana, V. Twiringiyimana, L. J. Mahoro, and T. Ahmad, "Anomaly-based Intrusion Detection Approach for IoT Networks Using Machine Learning," *CENIM 2020 - Proceeding Int. Conf. Comput. Eng. Network, Intell. Multimed. 2020*, no. Cenim 2020, pp. 303–308, 2020, doi: 10.1109/CENIM51130.2020.9297958.

[8] C. Miranda, G. Kaddoum, E. Bou-harb, S. Garg, and K. Kaur, "for Software-Defined Wireless Sensor Networks," vol. 15, pp. 2602–2615, 2020.

[9] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for intrusion detection," *Expert Syst. Appl.*, vol. 185, no. July, p. 115524, 2021, doi: 10.1016/j.eswa.2021.115524.

[10] S. A. Elsaid and N. S. Albatati, "An optimized collaborative intrusion detection system for wireless sensor networks," *Soft Comput.*, vol. 24, no. 16, pp. 12553–12567, 2020, doi: 10.1007/s00500-020-04695-0.

[11] J. Granjal, J. M. Silva, and N. Lourenço, "Intrusion detection and prevention in CoAP wireless sensor networks using anomaly detection," *Sensors (Switzerland)*, vol. 18, no. 8, 2018, doi: 10.3390/s18082445.

[12] T. Sood, S. Prakash, S. Sharma, A. Singh, and H. Choubey, "Intrusion Detection System in Wireless Sensor Network Using Conditional Generative Adversarial Network," *Wirel. Pers. Commun.*, vol. 126, no. 1, pp. 911–931, 2022, doi: 10.1007/s11277-022-09776-x.

[13] S. Sharma and J. Nagar, "Intrusion Detection in Mobile Sensor Networks: A Case Study for Different Intrusion Paths," *Wirel. Pers. Commun.*, vol. 115, no. 3, pp. 2569–2589, 2020, doi: 10.1007/s11277-020-07697-1.

[14] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simul. Model. Pract. Theory*, vol. 101, no. November 2019, p. 102031, 2020, doi: 10.1016/j.simpat.2019.102031.

[15] G. Efstathopoulos *et al.*, "Operational data based intrusion detection system for smart grid," *IEEE Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD*, vol. 2019-September, 2019, doi: 10.1109/CAMAD.2019.8858503.

[16] V. Gowdhaman and R. Dhanapal, "An intrusion detection system for wireless sensor networks using deep neural network," *Soft Comput.*, vol.

0123456789, no. Manoharan, 2021, doi: 10.1007/s00500-021-06473-y.

[17] B. A. Ashwini and S. S. Manivannan, “Supervised Machine Learning Classification Algorithmic Approach for Finding Anomaly Type of Intrusion Detection in Wireless Sensor Network,” *Opt. Mem. Neural Networks (Information Opt.*, vol. 29, no. 3, pp. 244–256, 2020, doi: 10.3103/S1060992X20030029.

[18] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, “Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges,” *IEEE Access*, vol. 8, pp. 3343–3363, 2020, doi: 10.1109/ACCESS.2019.2962829.

[19] M. Masdari and H. Khezri, “A survey and taxonomy of the fuzzy signature-based Intrusion Detection Systems,” *Appl. Soft Comput. J.*, vol. 92, p. 106301, 2020, doi: 10.1016/j.asoc.2020.106301.

[20] P. Sun *et al.*, “DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system,” *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/8890306.

[21] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, “A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions,” *Electron.*, vol. 9, no. 7, 2020, doi: 10.3390/electronics9071177.

[22] Alaria, S. K. "A.. Raj, V. Sharma, and V. Kumar.“Simulation and Analysis of Hand Gesture Recognition for Indian Sign Language Using CNN”." *International Journal on Recent and Innovation Trends in Computing and Communication* 10, no. 4 (2022): 10-14.

[23] Rajput, B. S. .; Gangele, A. .; Alaria, S. K. . Numerical Simulation and Assessment of Meta Heuristic Optimization Based Multi Objective Dynamic Job Shop Scheduling System. *ijfrcsce* 2022, *8*, 92-98.

[24] Rajput, B. S. .; Gangele, A. .; Alaria, S. K. .; Raj, A. . Design Simulation and Analysis of Deep Convolutional Neural Network Based Complex Image Classification System. *ijfrcsce* 2022, *8*, 86-91.