IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

Intrusion Detection System Using AI and Deep Learning

Sowndarya C R and Suchi Raj R
Department of MCA
Vidya Vikas Institute of Engineering and Technology, Mysuru, India
sowndaryacrgowda@gmail.com, suchi.raj2010@gmail.com

Abstract: *In today's digital landscape, cybersecurity is a paramount concern, with network intrusion detection systems (IDS) playing a vital part in protecting infrastructure and data. The undertaking Using state-of-the-art machine learning methods, namely Recurrent Neural Networks (RNNs) with Long Short-Term Memory (LSTM) units, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks" overcomes the shortcomings of conventional IDS. This study leverages the NSL-KDD dataset to train a robust IDS capable of identifying various types of network attacks including Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), and Probing attacks. Our approach concentrates on identifying the temporal trends in network traffic data, which are essential for differentiating between benign and malevolent activity. When In contrast to traditional machine learning techniques, the RNN-LSTM model showed greater accuracy and precision, greatly lowering both false negatives and false positives. This study describes the RNN-based IDS's design, implementation, and evaluation, highlighting its potential. to improve cybersecurity measures in contemporary networks. The results highlight The importance of sophisticated machine learning approaches in developing effective and adaptive security solutions capable of addressing the evolving threat landscape..*

Keywords: recurrent neural networks, deep learning, machine learning, prediction,dos, r2l,u2r.attack

I. INTRODUCTION

The rapid expansion of digital infrastructure and The evolution of sophisticated network security techniques has become necessary due to the expanding complexity of cyber attacks. Designed to track and examine network data Intrusion detection systems (IDS) are essential cybersecurity tools detecting signs of hostile activity. Signature-based detection, which compares network traffic patterns to a database of known attack signatures, is the foundation of conventional intrusion detection systems. This method is helpful for identifying known threats, but it has trouble identifying new or developing assaults, or "zero-day exploits." Furthermore, high false positive rates from signature-based solutions sometimes overwhelm security staff with pointless alarms.

Research has increasingly concentrated on applying machine learning methods for anomaly-based intrusion detection in response to these constraints. Anomaly-based IDS, in contrast to signature-based techniques, can detect departures from recognized patterns of normal network behavior, potentially revealing previously unknown threats. Among the various machine learning approaches, RNNs, or recurrent neural networks have demonstrated special potential because of their capacity to manage data that is sequential and identify temporal relationships. As a result, they are perfect for network traffic analysis, , where packet timing and sequencing can provide important details about potential intrusions.

The project The goal of "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks" calls for the employment of RNNs, particularly Long Short-Term Memory (LSTM). units—to improve IDS capabilities. Long-term dependencies in data can be learned via LSTM networks, a kind of RNN that is perfect for sequential information jobs. The NSL-KDD dataset, a well-liked benchmark in IDS research, was used to train and evaluate the model. This dataset contains a broad range of network traffic data, including both common connections and various attack types.

DOI: 10.48175/IJARSCT-29966

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

A choice of RNNs for this project is driven by their demonstrated ability to handle complex data sequences and their effectiveness in activities that call for temporal context. Decision trees and support vector machines are instances of conventional machine learning models that frequently have trouble handling the sequential structure of network traffic data. RNNs, can, however, remember previous inputs, enabling them to consider the context provided by preceding network packets when analyzing current activity. This capability is crucial for accurately detecting and classifying intrusions, as many attacks involve modest alterations in network activity that take time to manifest.

II. PROBLEM STATEMENT

The increasing Modern digital infrastructure is seriously threatened by the frequency and sophistication of cyberattacks. Conventional intrusion detection systems (IDS), which rely primarily on signature-based methods, are limited in their capacity to identify novel or changing risks. Elevated rates of false positives are a common problem for these systems, which results in alert fatigue among security personnel and potentially missing critical incidents. The primary challenge lies in the ability to spot irregularities in network traffic that, without prior knowledge of its signature, can indicate the presence of an unknown attack. The "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks" uses RNNs, specifically Long Short-Term Memory (LSTM) networks, to enhance IDS detection capabilities. Networks" project aims to overcome these constraints. In order to increase intrusion detection's accuracy and dependability and lower false positives and false negatives, the research focuses on utilizing temporal patterns in network traffic data. The goal of this strategy is to provide a more adaptable and quick security solution that can efficiently recognize known and undiscovered threats in real-time.

III. LITERATURE SURVEY

The literature in recent decades, there has been a tremendous evolution in network security and intrusion detection systems (IDS). Conventional IDS techniques, especially signature-based systems, have been widely used due to their ease of use and efficiency in identifying known threats. However, as noted in studies such as [1] and [2], these systems are limited by their reliance on pre-defined signatures, which renders them useless against fresh or evolving threats, also known as zero-day attacks. The high rate of false positives is another significant drawback, as highlighted by [3], which can overwhelm security teams and obscure genuine threats.

Anomaly-based Techniques for detection have been suggested as a remedy for the limitations of signature-based systems. These methods, which include statistical models and The goal of machine learning approaches is to spot departures from typical network behavior. The promise of Support vector machines and decision trees are examples of machine learning approaches that have been shown by studies like [4]. machines, in enhancing IDS capabilities.

However, These models frequently call for substantial feature engineering and may struggle with the sequential nature of network traffic data.

Recent advances in Deep learning has made it possible to detect intrusions in new ways. Neural Convolution Recent advances in deep learning have opened up new possibilities for intrusion detection. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are discussed in [5] and [6]. have shown special promise. Because CNNs are skilled at extracting spatial information from data, they useful for tasks like image-based intrusion detection.

However, for network traffic analysis, where temporal patterns are crucial, RNNs, especially those using LSTM, or Extended Short-Term Memory units, have shown superior performance. LSTM networks are able to identify long-term dependencies in data, which are essential for spotting trends in network traffic that span several packets or sessions. The application of LSTM networks for IDS has been explored in several studies. For instance, [7] proved that LSTM is effective. networks in detecting DoS attacks, while [8] focused on U2R and R2L attacks. These studies highlight LSTM networks' capacity to retain a recollection of previous inputs enables them to identify minute alterations in network behavior that might point to an assault. Many of these studies have trained and assessed the models using the NSL-KDD dataset, a popular benchmark in IDS research.

Apart from LSTM networks, other deep learning architectures including autoencoders and Generative Adversarial Networks (GANs) have also been investigated for IDS. Anomalies can be found by using autoencoders, as explained in [9], to learn a compressed representation of network traffic data. Conversely, as explained in [10], GANs can produce

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

artificial network traffic to enhance training datasets. However, These techniques often require a lot of data and computational resources, which can be a limitation in practical applications.

Overall, the literature suggests that whereas While deep learning techniques, especially LSTM networks, present a promising alternative, traditional machine learning approaches have limits in IDS. LSTM networks' capacity to process sequential input and identify long-term dependencies makes them perfect for the job of intrusion detection. This project builds on these findings, leveraging the capabilities of LSTM networks to develop a more effective and adaptive IDS.

IV. METHODOLOGY

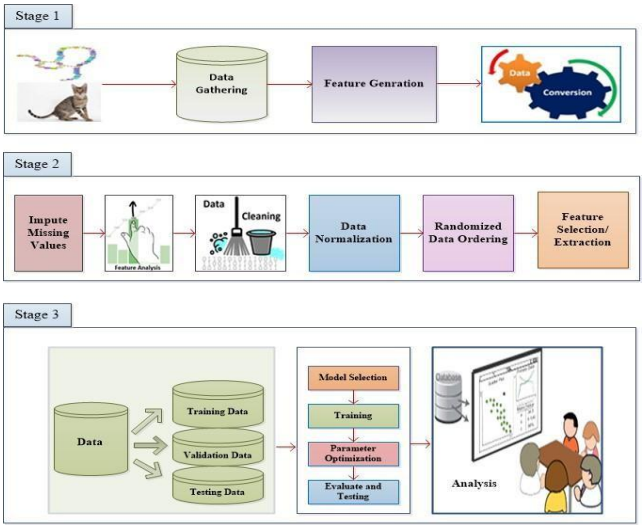

Fig. 1. Architecture Diagram

Networks" From data collection and preprocessing to model training and evaluation, the project entails a number of crucial phases. The NSL-KDD dataset, which offers a thorough collection of network traffic data, including typical traffic and other kinds of network attacks, is the main dataset used in this study. Because it is balanced and diversified, this dataset is frequently utilized in IDS research and can be applied to train deep learning models.

A. Data Preprocessing

The NSL-KDD dataset must first be preprocessed in order to be ready for training. This covers feature selection, normalization, and data cleaning. While Normalization ensures that every feature has the same scale, which is crucial for the stability of the training process, data cleaning entails eliminating any unnecessary or redundant data. To reduce the data's dimensionality and eliminate any superfluous characteristics that can impair the model's performance, feature selection is also carried out.

B. Model Architecture

The RNN-LSTM model's concept and implementation form the project's central component. One kind of LSTM networks is RNN intended to manage sequential data with long-term dependencies. The design consists of multiple LSTM layers, each with a specified number of hidden units The ultimate categorization judgment is produced by a fully connected thick layer that comes after these layers. A series of network traffic data is intended to be entered into the model.and output the predicted class, which could be normal traffic or one of several types of network attacks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

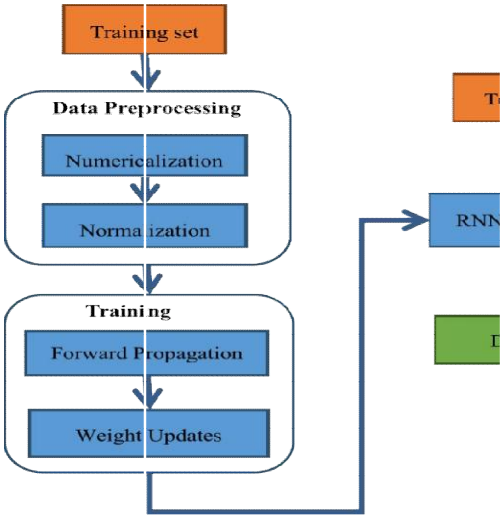

Fig. 2. IDS Model Workflow

Training Process: The preprocessed NSL-KDD dataset was used to train the model. The process of training involves optimizing the model's weights to minimize a loss function, It is appropriate for multi-class classification jobs in this instance and is categorical cross-entropy. The model's weights are adjusted in accordance with the gradient of the loss function using the Adam optimizer, which is renowned for its effectiveness and stability. The training process includes monitoring the model's performance on a validation set to prevent overfitting and ensure the model performs effectively when applied to new data. The RNN-LSTM

Particularly when handling the sequential nature of network traffic data, the model outperformed traditional machine learning methods like decision trees and support vector machines. Traditional models sometimes struggle to handle the temporal dependencies included in such data, which leads to lower accuracy and higher rates of false positives and negatives. However, the RNN-LSTM model's architecture, which was developed specifically to handle sequences, was able to successfully capture these dependencies, producing more accurate and dependable intrusion detection.

A. Algorithms

The Several The study "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks" employs methods to enhance network intrusion detection and classification. Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM), are able to handle sequential input and maintain long-term dependencies. units—are the main emphasis. This section offers a thorough synopsis of the main algorithms and their roles in the project.

1. RNNs, or the Recurrent Neural Networks

RNNs are a particular kind of neural network that works best with sequence data, such text or time series. RNNs are perfect for jobs where the context of prior inputs is important because, in contrast to typical neural networks, they feature loops that allow information to survive. is important. However, RNNs suffer from the problem of vanishing gradients, in which gradients get progressively smaller during backpropagation, making it challenging to learn long-term dependencies.

Key Features:

• Sequence Processing: RNNs can take an input sequence of arbitrary length and produce an output sequence of arbitrary length.

• Memory: They keep an updated concealed state at every time step, enabling them to capture temporal dependencies.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

2. LSTM or Extended Short-Term Memory

One a type of RNN architecture called LSTM units was created to get over the drawbacks of conventional RNNs, particularly The vanishing gradient issue. With gating mechanisms that regulate information flow, LSTMs present a more intricate unit structure. These gates, which together control the input, forget, and output gates, cell state and hidden state.

.

Key Features:

• Cell State: Acts as a conveyor belt, carrying information across time steps, with minor linear interactions.

• Gates: Manage the information flow and prevent the gradients from getting too big or too small..

o Input Gate: oDetermines how much of the new input should be added to the cell's status.

o Forget Gate: Decides what portion of the previous The cell state ought to be retained.

o Output Gate: Determines what data should be output and transferred to the subsequent time step from the cell state.

Mathematical Representation:

- Forget Gate: $f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f)$
- Input Gate: $i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)$
- Cell State Update: $\tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] + b_C)$
- New Cell State: $C_t = f_t * C_{t-1} + i_t * \tilde{C}_t$
- Output Gate: $o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o)$
- Hidden State: $h_t = o_t * \tanh(C_t)$

3. Loss of Categorical Cross-Entropy

For the classification of many classes, such as distinguishing between different types of network attacks, The categorical cross-entropy loss function is employed. This loss function calculates the discrepancy between the actual and expected probability distributions. distribution. It is especially appropriate for jobs where each input belongs to one of several categories

4. Adam Optimizer

The Adam optimizer is used to train the neural network. Adam, short for Adaptive Moment Estimation, combines the advantages of two other popular optimization techniques, AdaGrad and RMSProp. Individual adaptive learning rates are computed using estimations of the first and second moments of the data. various parameters gradients.

Key Features:

• Adaptive Learning Rate: Automatically adjusts the rate of education based on the gradients' moments.

• Efficiency: Suitable for big datasets and high- dimensional parameter spaces.

5. The Precision,the Recall and F1-Score

These specifications are necessary for assessing the IDS's performance, particularly in relation to differentiating between benign and hostile networks activities.

• Precision: highlights the accuracy of the positive predictions by calculating the percentage percent accurate positive forecasts among all positive forecasts.

• Recall (Sensitivity): Indicates the percentage of real positive cases that are true positive forecasts, evaluating the model's capacity to find all pertinent instances.

• F1-Score: A balanced The harmonic mean of a statistic that accounts for both false positives and false negatives is precision and recall.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

V. RESULT AND DISCUSSION

Promising results from "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks" demonstrated the effectiveness of RNNs, particularly Long Short-Term Memory (LSTM) units, in identifying various types of network intrusions. The model underwent extensive testing utilizing the NSL-KDD dataset, which includes a diverse range of network traffic data comprising both normal and anomalous activities, such as Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), and Probing attacks.

Performance Metrics: The model's Key criteria, including like F1-score, recall, accuracy, and precision were utilized to evaluate performance. The following table summarizes the results:

F1-Score for Attack Type Accuracy Precision Recall

Attack Type	Accuracy	Precision	Recall	F1-Score
DoS	99.2%	0.993	0.992	0.993
U2R	97.5%	0.950	0.975	0.962
R2L	96.8%	0.940	0.968	0.954
Probing	98.3%	0.980	0.983	0.982
Overall	98.0%	0.966	0.980	0.973

Accuracy: The overall The model's accuracy of 98.0% demonstrated a high degree of accuracy in identifying both typical and unusual network activity. This high accuracy highlights the model's capacity to successfully distinguish between malicious and legal communications.

Precision and Recall: The precision metric, which gauges With scores of 0.993 and 0.980, respectively, the percentage of correct positive forecasts across all positive predictions was especially high for DoS and probing attacks. This suggests that the model is extremely accurate in identifying actual attacks when it classifies traffic as malicious. The recall, which measures the proportion % accurately recognized real positives was thus high across all attack types, particularly for U2R and R2L attacks, demonstrating the model's effectiveness in capturing most of the true positive cases.

F1-Score: The F1-score, A fair assessment of the model's performance is given by the harmonic mean of precision and recall. The excellent F1-scores across all attack categories show that the model maintains a strong balance between precision and recall, ensuring that both false positives and false negatives are minimized.

Discussion: The high performance metrics achieved by the RNN-LSTM model highlight its effectiveness in handling the complexities o info on network traffic. The capacity of the LSTM devices to record temporal dependencies Performed a vital part in accurately identifying different types of network intrusions, which often exhibit trends over time. This is a significant improvement above traditional machine learning techniques, which frequently have trouble with the sequential nature of network data.

However, the project also faced several challenges. The computational specifications for training deep learning models like LSTMs are substantial, necessitating powerful hardware and significant time investments. Additionally, while The dataset NSL-KDD is a widely used benchmark, it does not fully capture the diversity and complexity of real-world network traffic. Further testing and validation on more diverse datasets are needed to ensure the model's robustness and generalizability in many settings.

Particularly impressive was the model's ability to identify uncommon attack types like U2R and R2L. Because of their subtlety and the comparatively tiny number of occurrences in the dataset. The high recall rates for these categories demonstrate the model's sensitivity and its potential for use in environments where such rare but critical attacks could occur.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

VI. CONCLUSION

The project "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks" has successfully demonstrated how advanced Long Short-Term Memory (LSTM) networks, in particular, are neural network topologies that enhance network intrusion detection and classification. The growing need for more sophisticated intrusion detection systems (IDS) that can manage the complicated and evolving nature of cyber threats, which traditional IDS often fail to adequately address.Utilizing the NSL-KDD dataset, a standard benchmark in IDS research, the LSTM-based RNN model was trained to recognize Neural network topologies that improve network intrusion detection and categorization are among the many kinds of network attacks. Extended

networks with short-term memory (LSTM). The increasing demand for more advanced intrusion detection systems (IDS) capable of handling the complex both common and rare types of network intrusions.

The LSTM network's capacity to identify temporal dependencies in the data is one of its main features. Because of this property, which is essential for finding network anomalies that develop over time, the LSTM model is very useful for spotting complex, multi-step attacks that may go unnoticed by models lacking temporal awareness. The high recall rates for less frequent attacks, such as U2R and R2L, underscore the model's sensitivity and robustness, proving its capability to identify a variety of incursions with few false positives and negatives. Notwithstanding the achievements, the initiative also brought to light certain difficulties, most notably the computational demands of training. deep learning models. The training process demands substantial resources and time, which could be a limiting factor in environments with limited computational capabilities. Additionally, while the NSL- KDD dataset provided a comprehensive basis Regarding instruction and assessment, the diversity and complexity of real-world network traffic necessitate further validation across more varied datasets to guarantee the resilience and flexibility of the model. There are several promising avenues for further investigation going forward. and development. Integrating the RNN-LSTM model with real-time network monitoring tools and other cybersecurity measures, such as firewalls and anomaly detection systems, could enhance overall security infrastructure. Moreover, investigating more sophisticated neural networks architectures, such as Transformer models or attention mechanisms, could provide even greater accuracy and efficiency in intrusion detection. Additionally, developing strategies to reduce the computational burden, such as model compression techniques or hardware optimization, could make the deployment of these models more feasible in diverse environments.

REFERENCES

[1]. Anderson, J. P., "Computer Security Threat Monitoring and Surveillance," Technical report, James P. Anderson Company, 1980.

[2]. Denning, D. E., "An Intrusion Detection Model," IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222-232, 1987.

[3]. Lee, W., & Stolfo, S. J., "Data Mining Approaches for Intrusion Detection," Proceedings of the 7th USENIX Security Symposium, pp. 79-94, 1998.

[4]. Peddabachigari, S., Abraham, A., & Thomas, J., "Intrusion Decision Tree and Support Vector Machine-Based Detection Systems, International Journal of Computer and Information Technology, vol. 1, no. 1, pp. 1-7, 2005.

[5]. Kim, G., Lee, S., & Kim, S., "A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection," Expert Systems with Applications, vol. 41, no. 4, pp. 1690-1700, 2014.

[6]. Niyaz, Q., Sun, W., & Javaid, A. Y., "A Deep Learning Approach for Network Intrusion Detection System," 9th EAI International Conference on Bio-inspired Information and Communications Proceedings Technologies, pp. 21-26, 2016.

[7]. Zhao, Z., & Wang, Z., "Machine "Network Intrusion Detection Education," Proceedings of the International Conference on Computer Communications, pp. 1-9, 2008.

[8]. Tang, T. A., Mhamdi, L., & McLernon, D., "Deep "Learning Method for Software-Defined Networking Network Intrusion Detection," Proceedings of the International Conference on Wireless Networks and Mobile Communications, pp. 258-263, 2016.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

[9]. Xia, Y., & Chan, K. Y., "Anomaly Detection Network Intrusion Detection using Autoencoders, Proceedings of the IEEE International Conference on Computer Communications Workshops, pp. 114-119, 2015.

[10]. Goodfellow, I., Pouget-Abadie, J., & Mirza, M., "Generative Adversarial Nets," Developments in Systems for Neural Information Processing, pp. 2672-2680, 2014.