iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: V Month of publication: May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71032

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Automated Intrusion Detection Using Deep Learning Techniques

B. Manivannan[1], K. Abarna[2], D. Radhika[3]
[1]Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tamilnadu, India
[2]PG Scholar, Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tamilnadu, India
[3]Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tamilnadu, India

Abstract: Intrusion Detection Systems (IDSs) are essential for keeping an eye on and identifying dangerous or unauthorized activity occurring within computer networks. Conventional intrusion detection systems, which frequently depend on rule-based detection techniques, find it difficult to adjust to new attack patterns and changing cyber threats. This work suggests a sophisticated IDS architecture that combines Long Short-Term Memory (LSTM) networks with Deep Convolutional Neural Networks (DCNN) in a hybrid deep learning technique to get over these drawbacks. In order to improve detection accuracy, LSTM is utilized to learn temporal and sequential relationships, whereas DCNN focuses on capturing spatial patterns within network traffic data to boost detection accuracy. The NSL-KDD dataset, a refined and generally recognized benchmark for intrusion detection research, is used to train and assess the suggested model. According to experimental results, indicate that the DCNN-LSTM system is an effective and trustworthy approach for detecting threats in real-time within complex and rapidly changing network environments, offering superior detection rates and classification accuracy.

Keywords: Intrusion Detection System (IDS), Deep Learning, Deep Convolutional Neural Network, Long Short-Term Memory, NSL-KDD Dataset.

I. INTRODUCTION

In order to keep computer networks safe and secure, intrusion detection systems, or IDSs, are crucial. Because of their static structure and reliance on pre-set rules, classic rule-based intrusion detection systems (IDSs) have difficulty identifying previously undiscovered attack patterns as cyber threats continue to increase in complexity and frequency. In order to overcome these constraints, machine learning and deep learning methods have become strong substitutes that can learn from vast amounts of network data and spot minute patterns that point to malicious behaviour. Long Short-Term

Memory (LSTM) networks are well-suited for handling sequential data, while Deep Convolutional Neural Networks (DCNN) excel at capturing spatial features. This combination offers a more thorough comprehension of the behaviour of network traffic. The NSL-KDD dataset, which provides a fair and sophisticated standard for intrusion detection research, is used in this study to create and assess a hybrid intrusion detection system (IDS) model that combines DCNN and LSTM. Improving IDSs' detection precision and flexibility in dynamic network contexts is the goal.

A. Intrusion Detection System (IDS)

An essential security tool for identifying irregularities or unwanted access to a network or computer system is an intrusion detection system (IDS). Intrusion Detection Systems (IDS) detect potential threats or policy violations by examining patterns in user actions, system logs, or network traffic. IDS can be classified into several types, such as Host-Based IDS (HIDS), which monitors individual devices, and Network-Based IDS (NIDS), which observes entire segments of a network. These systems employ different detection techniques, such as signature-based detection that recognizes familiar attack patterns, and anomaly-based detection that detects deviations from normal behaviour.

IDSs based on signatures are good at identifying attacks that have already been discovered, but they could have trouble identifying threats that haven't been discovered yet. On the other hand, anomaly-based systems provide greater flexibility but often result in higher false positive rates, as they use models of normal activity to identify unusual behaviour. IDSs are essential to the security infrastructure because they give network managers insight into possible breaches, allowing them to take the necessary precautions to preserve data confidentiality and integrity.

B. Deep Learning

Multi-layered neural networks are used in deep learning, a sophisticated area of artificial intelligence, to process data and identify complex patterns. In terms of experience-based learning, these models mimic how the human brain works. A deep neural network's layers can learn progressively more abstract features from the data. In the context of cybersecurity, the initial layers may detect straightforward patterns in network traffic, while the more advanced layers are capable of identifying complex threat indicators. Deep learning models may automatically learn features, which eliminates the requirement for domain-specific knowledge during pre-processing, in contrast to typical machine learning models that frequently require manual feature extraction. Methods such as LSTM, Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs) are commonly applied in the analysis of sequential and structured data. Because deep learning can generalize and adapt to complex data distributions and large-scale datasets, it has shown especially good results in applications like malware classification, phishing URL identification, and intrusion detection.

C. DCNN-LSTM Model

The DCNN-LSTM model is a powerful hybrid framework that improves pattern recognition and prediction accuracy in sequential data settings by combining the strengths of Long Short-Term Memory (LSTM) networks with Deep Convolutional Neural Networks (DCNN). DCNNs excel at uncovering spatial hierarchies and local relationships in data by applying convolutional filters to the input features. This allows the model to capture unique characteristics linked to various activity categories and is especially helpful for extracting low-level and high-level representations from structured network traffic. On the other hand, LSTM networks, a specific type of RNN, are made to handle long-term dependencies in data sequences. They do this by solving problems like vanishing gradients that are frequently seen in conventional RNNs. By selectively updating memory cells, LSTMs enable the network to discard irrelevant data while preserving crucial information from past inputs. When combined, DCNN and LSTM work effectively together, with DCNN handling spatial abstraction and LSTM focusing on learning from sequential patterns. This design is particularly helpful when examining network logs or packet streams, as both temporal patterns and spatial correlations are essential for spotting malicious behaviour.

D. NSL-KDD Dataset

The KDD Cup 1999 dataset, one of the most popular benchmarks in intrusion detection research, has been improved and polished into the NSL-KDD dataset. The original KDD dataset faced the issue of high redundancy, which compromised the accuracy of model training and evaluation results. By eliminating duplicate records and guaranteeing a more equitable distribution of attack and normal cases, the NSL-KDD dataset overcomes these constraints. It comprises four primary types of attacks: DoS (Denial of Service), R2L (Remote to Local), U2R (User to Root), and Probe. The dataset is appropriate for assessing classification performance across a variety of intrusion types since these categories reflect various ways an attacker could jeopardize system integrity. Each record in the dataset contains 41 features, both continuous and categorical, extracted from network connections. Dividing the dataset into training and testing sets allows for a comprehensive assessment of the model's generalization ability. Because of its increased quality, diversity, and applicability in evaluating the efficacy of contemporary intrusion detection techniques, such as deep learning models, NSL-KDD continues to be a typical benchmark.

II. LITERATURE REVIEW

In this study, Maxat Akbanov [1] et al. have suggested The likelihood of retrieving data is almost zero due to the sophisticated encryption and distribution techniques used by contemporary ransomware families. We investigate how software-defined networking (SDN) can be used to detect and stop sophisticated ransomware assaults. We introduce our SDN-based security framework along with the findings from our ransomware analysis. They used the notorious Winery ransomware as a proof of concept. In light of the results, we develop a framework for SDN detection and mitigation and offer an Open Flow-based remedy. By adding flow table entries to Open Flow switches in real time, the developed solution blocks compromised hosts and detects suspicious activities through network traffic monitoring. Lastly, our tests using several WannaCry samples show that the developed system is capable of promptly identifying affected PCs and stopping the spread of WannaCry. These days, ransomware poses a serious and quickly growing threat to users of all sizes, from small families to large corporations and governmental organizations. Five ransomwares have evolved over time, beginning with extremely simple fake antivirus software in 2008 and progressing to more sophisticated variants like crypto type ransomware. The culmination of this development is the appearance of a novel ransomware variant that spreads throughout internal and external networks by fusing flaws with worm-like propagation techniques.

In this study, Joseph W. Mikhail [2] et al. proposed that in order to counter new cybersecurity threats, efficient network intrusion detection techniques are crucial. Traditional business networks have historically been the subject of extensive research in this field. However, wireless networks are now included in the cyber threat scenario. This article's authors present a novel model that can be applied to two distinct intrusion detection applications: 802.11 wireless networks and conventional corporate networks, and it can be trained on completely different feature sets. In each of the previously stated applications, this is the first method to show enhanced performance. A one-versus-all binary architecture with many layered sub-ensembles forms the basis of the model. Each sub-ensemble has a collection of sub-learners, with only a subset of the sub-learners utilizing boosting, in order to provide great generalization potential. Sub-ensembles of each class are given a class weight determined by the true-positive rate, or sensitivity measure, which is fully learned from training data. It is also investigated how pruning can be used to eliminate sub-learners that don't contribute or negatively affect system performance as a whole.

In their research, Yuyang Zhou [3] et al. have promoted In network design, intrusion detection systems (IDS) are often employed techniques to guarantee the availability and integrity of sensitive assets in secured systems. Even though a variety of supervised and unsupervised machine learning techniques have been used to increase the effectiveness of intrusion detection systems, current intrusion detection algorithms still have trouble performing well. First, the categorization process of an IDS is hampered by the abundance of redundant and superfluous data in high-dimensional datasets. Second, a single classifier might not be able to identify every kind of attack. Third, many models are less adaptable to new attacks since they were created for out-of-date datasets. Therefore, in this study, we propose a novel intrusion detection system based on ensemble learning and feature selection techniques. The initial phase includes developing CFS-BA, a heuristic approach to dimensionality reduction that identifies the best subset of features based on their correlation. Following that, we provide an ensemble approach that combines the Random Forest (RF), Forest by Penalizing Attributes (Forest PA), and C4.5 algorithms.

In this system, Gulshan Kumar [4] et al. proposed. In addition to minimizing financial loss and service interruptions brought on by network assaults, network security is essential for safe communication. Usually, hackers use flaws in widely used software to attack network computer systems in a variety of ways. Network attacks can cause anything from little service interruptions to large financial losses. Machine learning-based intrusion detection systems (IDSs) have developed recently to address unauthorized network resource access and use. Numerous machine learning techniques have been created and implemented into IDSs over time. However, in terms of false positives and detection rates, the majority of intrusion detection systems reported subpar intrusion detection results. Researchers focused on creating ensemble classifiers, which combine predictions from multiple individual classifiers, to overcome these difficulties. Ensemble classifiers enhance performance by pooling their knowledge to make up for the shortcomings of individual classifiers.

In this work, Bayu Adhi Tama [5] et al. have suggested in the information age we live in today, a Web attack defense system is essential. Classifier ensembles have been suggested for online traffic anomaly-based intrusion detection. However, poor ensemble design makes their performance awful. This study introduces a stacked ensemble model for anomaly-based intrusion detection in web applications. The suggested stacked ensemble is an ensemble architecture, but its base learners are various ensemble learners, such as random forest, gradient boosting machine, and XG Boost, in contrast to traditional stacking, which frequently uses single weak learners. To demonstrate the generalizability of the proposed approach, the experiment utilizes two datasets—CSIC-2010v2 and CICIDS-2017—both specifically designed for detecting attacks in web applications. Additionally, the suggested model performs better in terms of accuracy and false positive rate than current web attack detection methods. The CICIDS-2017, NSL-KDD, and UNSW-NB15 datasets provide validation results that are superior to those derived from a number of existing methods. Lastly, a two-step statistical significance test is used to evaluate the effectiveness of all classification techniques, contributing to the body of current knowledge.

In this study Vanlalruata Hnamte [6] et al. Several studies have proposed the use of deep convolutional neural networks (DCNNs) to enhance IDS performance by automatically extracting meaningful features from network traffic data. In particular, DCNN-based IDS has demonstrated superior detection accuracy, with studies indicating near-perfect performance levels. For example, research utilizing large-scale datasets such as ISCX-IDS 2012, DDoS (Kaggle), CICIDS2017, and CICIDS2018 highlights the effectiveness of DCNN in accurately distinguishing between benign and malicious traffic, with GPU acceleration further enhancing computational efficiency and enabling real-time threat detection. DCNNs excel in capturing spatial features from raw network data, making them a promising solution for modern IDSs. The combination of high accuracy and low false positive rates underscores the value of DCNNs in detecting emerging cyber threats.

III. RELATED WORK

Network intrusion detection systems (NIDSs) based on machine learning (ML) use flow characteristics derived from flow export protocols such as NetFlow. Recently successful ML and Deep Learning (DL) based NIDS systems are supposed to collect average packet size and other flow information from each packet in the flow. Actually, commodity electronics where packet sampling is inevitable frequently utilize flow exporters. However, whether such machine learning-based network intrusion detection systems perform in the presence of sampling—that is, when flow information is obtained from a sampled set of packets rather than the entire traffic—is not entirely known. In this study, we explore how packet sampling affects the performance and effectiveness of ML-based NIDSs. Unlike previous studies, our proposed evaluation procedure is robust to varying flow export stage parameters. Therefore, it can offer a trustworthy evaluation of NIDS even when sampling is used. Through sample investigations, we discovered that hostile flows with a smaller size (i.e., number of packets) are more likely to go undetected, even at low sampling rates like 1/10 and 1/100.

IV. METHODOLOGY

Deep Convolutional Neural Networks (DCNN) and Long Short-Term Memory (LSTM) networks are used in the hybrid deep learning architecture used to develop the suggested intrusion detection system. By utilizing the advantages of both models, this integrated technique improves the system's capacity to detect intricate and dynamic network intrusions. In order to identify trends that can point to possible dangers, DCNN is used to extract significant geographical characteristics from the input network traffic data. The LSTM network, which is in charge of examining the data's temporal and sequential components, receives these extracted features after that. The system can learn the time dependencies an spatial structure of network traffic thanks to this combination. The NSL-KDD dataset, which offers a varied and organized collection of network traffic samples categorized by different kinds of intrusions, is used to train and evaluate the model. The system seeks to correctly categorize network behaviors and differentiate between benign and malevolent activity using this approach. Because this hybrid technique increases detection precision, it can be used in contexts where high accuracy in threat identification and security monitoring is required.

A. Load Data

The initial step of the system, the data loading module, is responsible for importing the NSL-KDD dataset into the workspace. Labeled network connection records representing both typical activity and other kinds of attacks are included in this collection. The records contain a variety of information that are essential for training and testing the detection model, such as protocol kinds, service types, and connection durations. When the dataset is loaded correctly, all values are formatted and structured correctly, facilitating a seamless transition to the following processing steps.

B. Data Preprocessing

To get the raw data ready for analysis, the preprocessing module is crucial. In this step, the dataset is cleaned by addressing missing values, eliminating duplicate records, and applying encoding techniques like label encoding or one-hot encoding to transform category variables into numerical form. To make sure that every feature contributes equally to the learning process, normalization or scaling is also used. Preprocessing makes the data more organized and consistent, which lowers noise and boosts the deep learning model's effectiveness and performance.

C. Feature Extraction

The feature extraction module enhances the model's learning capacity by extracting valuable information from the processed dataset. Spatial features are automatically derived from network traffic data using Deep Convolutional Neural Networks (DCNN). These characteristics draw attention to significant patterns and structures that could be signs of benign or malevolent conduct. By creating a simplified representation of the original data, the extracted features assist the system in concentrating on the most pertinent traits for intrusion detection.

D. Training And Testing

In this module, the dataset is split into two subsets: one for model training and another for performance evaluation. In order for the hybrid DCNN-LSTM model to learn the patterns connected to various forms of network activity, the extracted features must be fed into the model during the training phase. To reduce categorization mistakes, the model iteratively modifies its internal parameters. Following training, the model's ability to identify previously undiscovered instances of both typical and invasive behaviors is evaluated using the distinct data set.

E. Model Evaluation

Using common measures like accuracy, precision, recall, and F1-score, the assessment module evaluates the trained model's performance. These measurements offer a thorough understanding of the model's capacity to accurately categorize network traffic. To show the proportion of accurate and inaccurate predictions for each class, confusion matrices and classification reports are frequently produced. This assessment aids in assessing the suggested system's efficacy and pinpoints potential areas for enhancement in subsequent model revisions.

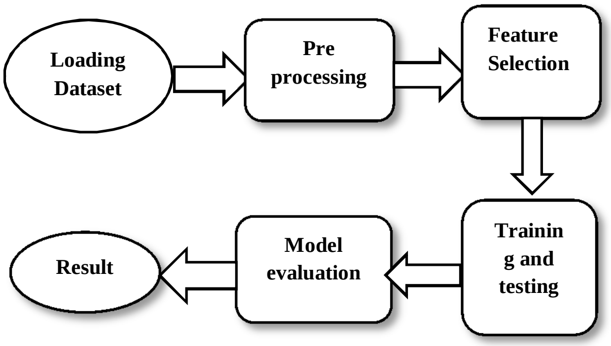

Figure 1. System flow diagram

V. ALGORITHM DETAILS

To enhance intrusion detection capabilities, the suggested system employs a hybrid deep learning technique that blends Long Short-Term Memory (LSTM) networks with Deep Convolutional Neural Networks (DCNN). Because DCNN is good at identifying spatial dependencies in network traffic data, it is used. In order to extract local features that reflect behavioural patterns in the data, it passes the input through a number of convolutional and pooling layers. The LSTM network, which focuses on learning sequential dependencies, is then given these properties. A particular kind of Recurrent Neural Network (RNN) called LSTM is made to retain information for extended periods of time, which makes it appropriate for spotting temporal patterns in the order of network events. The system can better classify traffic into normal or attack categories by analyzing the temporal and structural aspects of network activity thanks to the combination of DCNN and LSTM. The NSL-KDD dataset's labeled instances are used to train the model, which uses feature patterns to differentiate between different kinds of intrusions. The system's robustness against a variety of network threats and detection accuracy are improved by this hybrid design.

VI. RESULT ANALYSIS

Standard measures like accuracy, precision, recall, and F1-score were used to assess the suggested intrusion detection system's effectiveness. The system successfully distinguished between benign and malevolent network traffic, as evidenced by its high classification accuracy. The model correctly recognized the majority of attack cases while retaining a low false positive rate, according to a thorough analysis of precision and recall scores for each attack type, including DoS, Probe, U2R, and R2L. The system's resilience was further validated by the F1-score, which strikes a balance between recall and precision and shows that it can function effectively against a variety of network threats. Furthermore, the model's performance across several categories was visualized using confusion matrices, which shed light on the system's precise advantages and disadvantages in categorizing distinct assault types. The hybrid DCNN-LSTM model's efficacy as an intrusion detection tool is demonstrated by the results, which demonstrate that it performs noticeably better than conventional techniques, particularly when handling intricate patterns and adjusting to different attack circumstances.

VII. CONCLUSION

To sum up, the suggested intrusion detection system successfully tackles the difficulties of identifying network intrusions by using a hybrid architecture of Deep Convolutional Neural Networks (DCNN) and Long Short-Term Memory (LSTM) networks. The system performs better in classifying network traffic and recognizing different kinds of attacks by fusing the sequential learning strengths of LSTM with the spatial feature extraction capabilities of DCNN. High accuracy, precision, recall, and F1-score are among the evaluation outcomes that support the efficacy of this method in differentiating between benign and malevolent activity. The model's capacity to manage intricate and varied assault patterns is further confirmed by the usage of the NSL-KDD dataset for testing.

Compared to conventional rule-based systems, this hybrid model offers notable advantages, offering a viable way to increase network security and lessen possible dangers. The model could be improved and made more capable of handling different attack vectors and network settings in future research.

VIII. FUTURE WORK

Several areas for improvement can be the focus of future study on this intrusion detection system. To further increase classification accuracy and robustness, one possible approach is to investigate the integration of additional machine learning methods, such as Support Vector Machines (SVM) or Gradient Boosting. The model may be better able to generalize to unknown attack patterns if the training dataset is expanded to cover a wider variety of attack types and network traffic circumstances. Furthermore, by including strategies like distributed learning or parallel processing, the system might be made more scalable, enabling it to manage bigger and more complicated datasets. Examining the deep learning model's interpretability is also crucial since knowing how the model generates decisions can increase usability and confidence. Finally, to confirm the system's adaptability and performance under various circumstances, it might be tested against a greater range of network protocols and in more varied network environments. These developments would help the system become more flexible, effective, and relevant to a wider variety of network security issues.

REFERENCES

[1] The article "An intellectual intrusion detection system using hybrid hunger games search and remora optimization algorithm for IoT wireless networks" by R. Kumar, A. Malik, and V. Ranga was published in the journal Knowledge-Based Systems in November 2022.

[2] W. Wang, S. Jian, Y. Tan, Q. Wu, and C. Huang developed a representation learning-based network intrusion detection system that records both explicit and implicit feature interactions. In January 2022, the journal Computer Security published their findings.

[3] J. Kusuma, W. Lehr, K. Katsaros, I. Selinis, D. Bubley, and J. Oughton examined the distinctions between Wi-Fi 6 and 5G wireless internet connectivity options. In June 2021, the journal Telecommunication Policy published their findings.

[4] A thorough mapping study and cross-benchmark evaluation of ensemble learning for intrusion detection systems were carried out by B. A. Tama and S. Lim. In February 2021, the journal Computer Science Review published their findings.

[5] S. Lei, C. Xia, Z. Li, X. Li, and T. Wang presented a novel model called HNN for investigating intrusion detection based on temporal-spatial analysis and multi-feature correlation. In October 2021, the IEEE Transactions on Network Science and Engineering published their research.

[6] Vanlalruata Hnamte, Jamal Hussain, Dependable intrusion detection system using deep convolutional neural network: A Novel framework and performance evaluation approach, Telematics and Informatics Reports, Volume 11, September 2023. https://doi.org/10.1016/j.teler.2023.100077.

[7] Y. Cheng, Y. Xu, H. Zhong, and Y. Liu, "Leveraging semisupervised hierarchical stacking temporal convolutional network for anomaly detection in IoT communication," IEEE Internet Things Journal, January 2021, edition 8, number 1, pages 144-155.

[8] In the July/August 2021 issue of IEEE Transactions on Dependable Secure Computing, "Sustainable ensemble learning driving intrusion detection model," pp. 1591-1604. X. Li, Z. Ma, C. Zhong, H. Li, M. Zhu, L. T. Yang, and Y.

[9] Using ensemble classifiers and feature selection to create an effective intrusion detection system, M. Dai, S. Jiang, G. Cheng, and Y. Zhou. Article number 107247, Journal of Computer Networks, vol. 174, June 2020.

[10] G. Kumar, K. Thakur, and M. R. Ayyagari's paper, "MLEsIDSs: Machine learning-based ensembles for intrusion detection systems—A review," J. Supercomput., vol. 76, no. 11, November 2020, pp. 8938–8971.

[11] B. A. Tama, L. Nkenyereye, S. M. R. Islam, and K. Kwak, "An enhanced anomaly detection in web traffic using a stack of classifier ensemble," IEEE Access, vol. 8, pp. 24120-24134, 2020.

[12] Bhushan Deore and Surendra Bhosale, Hybrid Optimization Enabled Robust CNN-LSTM Technique for Network Intrusion Detection, IEEE Access (Volume: 10), June 2022, 10.1109/ACCESS.2022.3183213.

[13] Jiawei Du, Kai Yang, Yanjing Hu, And Lingjie Jiang, NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning, IEEE Access (Volume: 11), March 2023,10.1109/ACCESS.2023.3254915

[14] Vanlalruata Hnamte, Hong Nhung-Nguyen, Jamal Hussain, Yong Hwa-Kim, A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE, IEEE Access (Volume:11), April 2023, 10.1109/ACCESS.2023.3266979.

[15] Rachid Ben Said, Zakaria Sabir, ImanAskerzade, CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software-Defined Networking with Hybrid Feature Selection, IEEE Access (Volume: 11), December 2023, 10.1109/ACCESS.2023. 3340142.