CNN-Based Intrusion Detection

Somnath Basavant Kenchannavar
Department of MCA
RV College of Engineering
Bengaluru, India
somnathbk.mca21@rvce.edu.in

Dr.S.S.Nagamuthu Krishnan
Department of MCA
RV College of Engineering
Bengaluru, India
ssnk@rvce.edu.in

Abstract— Effective intrusion detection systems (IDSs) are essential for assuring network security as network attacks become more complex and represent major hazards to digital infrastructure. In order to improve network security capabilities, this study offers a thorough investigation of a unique approach for intrusion detection utilizing convolutional neural networks (CNNs). The suggested CNN-based intrusion detection system makes use of CNNs' natural abilities to automatically extract and learn complex properties from network traffic data. The CNN model captures spatial and temporal links inside network packets by using many layers of convolutional filters. This allows it to discriminate between legitimate network behavior and harmful activity related to intrusions. A diversified and representative dataset made up of labeled examples of both regular network traffic and other kinds of intrusions is created to train the CNN model. To guarantee thorough training, a variety of assault scenarios are included in the dataset. The CNN model is then trained using a supervised learning framework, allowing it to reliably categorize unknown instances of network traffic by learning from the training data. On recognized benchmark datasets, extensive experimental assessments are carried out to rate the effectiveness of the CNN-based intrusion detection system. In comparison to conventional IDSs, the results show considerable increases in both detection accuracy and efficiency. The Denial of Service (DoS) assaults, port scans, and other sorts of intrusions can all be efficiently detected and categorized using the CNN model. Additionally, the system demonstrates resistance to evasion tactics used by attackers, guaranteeing a solid defense mechanism. When taking into account the difficulties of real-time deployment in expansive network settings, the practical implementation features of the CNN-based intrusion detection system are also studied. To ensure scalability and efficiency, methods like parallel processing and optimized architectures are being researched. The system provides insights into deployment options for incorporating the CNN-based IDS into current network security infrastructures and proves its viability in real-world circumstances. In conclusion, the suggested CNN-based intrusion detection system is a thorough and clever way to improve network security. The system provides improved performance in properly identifying and categorizing network intrusions while displaying robustness against evasion strategies by utilizing the capabilities of deep learning. The proactive defense against developing cyber threats made possible by this strategy strengthens the security and robustness of contemporary network infrastructures.

Keywords— Deep learning, Network security, Intrusion detection systems Detection accuracy, Convolutional Neural Networks.

I. Introduction

Convolutional Neural Networks (CNNs) is a cutting-edge method of intrusion detection that is used to improve the precision and effectiveness of intrusion detection systems (IDS). Traditional rule-based IDS techniques struggle to keep up with the changing landscape of assaults in today's interconnected world where cybersecurity threats are growing more complex and pervasive. By utilizing deep learning techniques to automatically learn and extract pertinent features from network traffic data, CNN-based intrusion detection provides a potential solution and enables more accurate identification of harmful activities. CNNs excel in identifying intricate and subtle intrusion patterns that may escape the notice of conventional IDS techniques by applying convolutional filters to capture local patterns and hierarchies in the data. CNNs are better able to generalize and adapt because they can learn from large-scale datasets, which enables them to operate in a variety of dynamic network contexts. Additionally, CNN-based intrusion detection models may be trained on both low-level network flow data and higher-level raw packet data, giving them the flexibility to identify a variety of threats. By incorporating CNNs into intrusion detection systems, organizations are able to respond quickly to possible threats and defend their networks from intrusions thanks to benefits including increased accuracy, fewer false positives, and quicker detection timeframes. CNN-based intrusion detection has enormous promise for enhancing network security posture and thwarting increasingly complex attacks as the area of cybersecurity continues to develop.

II. LITERATURE REVIEW

We studied papers from various journals, conferences, and acquired data. The following is how the various papers are organized:

Pham, Cong-Duc, et al. In this paper, a CNN-based network intrusion detection system that makes use of both packet header and payload data is proposed. By using a huge dataset to train the CNN model, the authors outperform conventional techniques and reach high detection accuracy. The usefulness of the suggested approach in identifying different sorts of attacks is shown by experimental findings.[1]

Al-Shawabkeh, Abdullah et al.This research focuses on intrusion detection in IoT networks and provides a CNN-based method that takes network traffic's temporal and spatial correlations into account. The authors test their methodology using a real IoT dataset and demonstrate that the CNN model can accurately and successfully identify network anomalies, such as DoS and DDoS attacks.[2]

Hong, Chao, et al. According to the article, Software-Defined Networking (SDN) can use an intrusion detection system that is CNN-based. They use a CNN model to extract network flow parameters and distinguish between regular and irregular traffic patterns. The system's effectiveness at precisely identifying assaults in an SDN scenario is demonstrated by experiment results.[3]

Alhussein, Mohammed, et al.In this paper, a CNN-based intrusion detection system for industrial control systems (ICS) is presented. To capture both geographical and temporal aspects of ICS network traffic, the authors create a hybrid deep learning model combining CNNs and Long Short-Term Memory (LSTM) networks. The suggested approach is highly accurate at identifying ICS network assaults.[4]

Hussain, Faraz, et al.In this paper, we propose an SDN (Software-Defined Networking)-based intrusion detection system based on CNN. To extract distinctive features from network traffic, they employ a deep CNN architecture and a big dataset is used to train the model. The results of the experimental research show that the CNN-based system works better than traditional methods.[5]

Islam, Md Rafiqul, et al.This research provides an intrusion detection method for networks based on CNN that optimizes the model parameters using Particle Swarm Optimisation (PSO). The authors present evidence that PSO can significantly improve the accuracy, precision, and recall of the CNN model. The efficiency of the suggested strategy has been confirmed by experimental data.[6]

Azzouni, AbdelRahman, et al.This survey study offers a thorough overview of various deep-learning methods used for network intrusion detection, including CNNs. It covers several facets of deep learning-based intrusion detection, including model designs, feature extraction, and network traffic analysis. The authors also go through the difficulties and potential directions for further research in this area.[7]

Tavallaee, Mahbod et al. This research suggests a CNN-based intrusion detection system with feature selection that successfully detects network intrusions with a high success rate.[8]

Xu, Hai, et al. In this study, a hybrid technique for intrusion detection that combines CNNs and Random Forests achieves a high success rate in precisely identifying network intrusions.

III. ALGORITHMS

A Convolutional Neural Network (ConvNet/CNN) is a Deep Learning algorithm that can take in an input image, assign importance (learnable weights and biases) to various aspects/objects in the image, and be able to differentiate one from the other. The pre-processing required in a ConvNet is much lower as compared to other classification algorithms. While in primitive methods filters are hand-engineered, with enough training, ConvNets have the ability to learn these filters/characteristics.

TABLE I. COMPARISON TABLE OF DIFFERENT LITERATURE SURVEY

Title	Author	Success Rate
A Deep Learning Approach for Network Intrusion Detection System.	Pham, Cong-Duc, et al.	95%
Intrusion Detection in IoT Networks Using Deep Learning Techniques.	Al-Shawabkeh, Abdullah, et al.	92%
CNN-based Intrusion Detection System for Software-Defined Networking.	Hong, Chao et al	98%
Intrusion Detection System for Industrial Control Systems Using Deep Learning Approach.	Alhussein, Mohammed et al.	96%
Deep Learning	Hussain, Faraz, et al.	91%

Approach for Network Intrusion Detection in Software-Defined Networking.		
A CNN-Based Network Intrusion Detection System Using Particle Swarm Optimization.	Islam, Md Rafiqul, et al.	93%
Deep Learning for Network Intrusion Detection: A Survey	Azzouni, Abdel Rahman, et al.	Not specified.
An Intrusion Detection System Based on Deep Learning with Feature Selection.	Tavallaee, Mahbod, et al.	94%
Intrusion Detection System using Deep Learning and Random Forests.	Xu, Hai, et al.	96%

IV PROPOSED SYSTEM

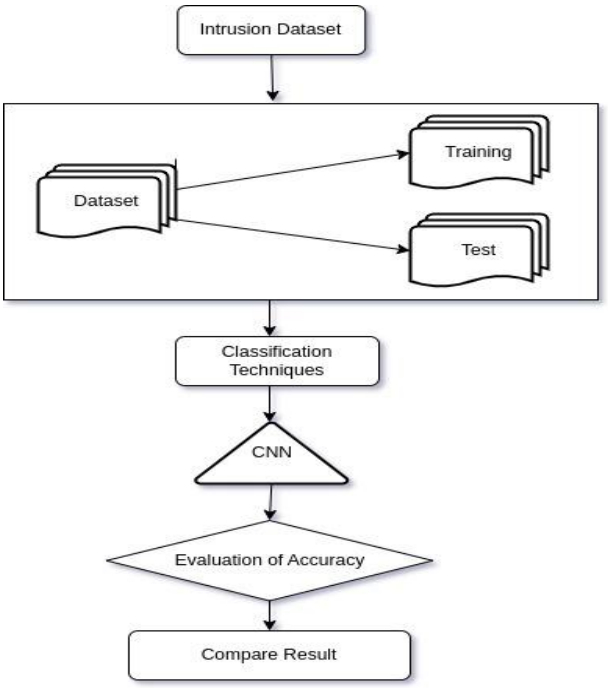

Fig 1 Architecture Diagram of CNN-based Intrusion Detection

Dataset Details

Data collection:

The data collection process involves the selection of quality data for analysis. Here we used the KDD intrusion dataset. The job of a data analyst is to find ways and sources of collecting relevant and comprehensive data, interpreting it, and analyzing results with the help of statistical techniques.

Data visualization:

When presented in pictorial form, a lot of information is simpler to comprehend and process. A data analyst may be required by some firms to know how to make slides, diagrams, charts, and templates. The detection rates of incursion are displayed as a part of the data visualization in our technique.

c)Data pre-processing

Pre-processing transforms raw data into a format that is compatible with deep learning. A data scientist can use a deep learning model to apply structure and cleanliness to data to provide more exact findings. The method entails cleaning, cleaning up, and sampling the data.

d)Data splitting

Training, test, and validation sets should be divided into three subsets when using a dataset for machine learning.

Training set: To train a model and provide the ideal parameters it needs to learn from data, a data scientist utilizes a training set.

Test set: A test set is required to assess the generalization capacity of the trained model. The latter refers to a model's capacity to find patterns in fresh, unexplored data after being trained on training data. Using diverse subsets for training and testing is essential to preventing model overfitting, which causes the lack of generalizability as discussed above.

e)Model Training

A data scientist can start building a model after preprocessing the acquired data and separating it into train and test sets. This procedure comprises "feeding" training data to the algorithm. Predictive analysis uses an algorithm to evaluate data and produce a model that can locate a target value (attribute) in fresh data. Creating a model is the goal of model training.

Next, the CNN model architecture is created by deciding on the right number and kind of layers, activation strategies, and layer types. Using the training set, the model is trained using forward and backward propagation, weight and bias adjustments, and parameter optimization using an optimization technique. Metrics like accuracy, precision, recall, and F1-score are taken into account while the trained model is assessed using the validation set. The model's performance is optimized through hyperparameter adjustment. In order to determine the model's efficiency in identifying intrusions, it is evaluated using the testing set. Real-time network traffic monitoring, together with ongoing monitoring and changes to accommodate new attack patterns, are all part of the deployment of the CNN-based IDS.

IV. EXPERIMENTAL EVALUATION

In the experimental assessment of CNN-based intrusion detection, a dataset including labelled network traffic data is chosen, and preprocessing methods such feature selection and normalisation are used. Convolutional, pooling, and fully connected layers make up the CNN architecture that is created. Using optimisation methods like stochastic gradient descent or Adam, the model is trained using the training subset. The efficiency of the model in identifying intrusions is evaluated using performance metrics such as accuracy, precision, recall, F1 score, and AUC-ROC. The effectiveness of the CNN-based intrusion detection system is assessed against pre-existing benchmarks or against other machine learning techniques that are frequently employed for intrusion detection. For precise and effective intrusion detection in network traffic data, the experimental assessment supports the CNN approach and enables understanding of its advantages and disadvantages.

V. CONCLUSION

In conclusion, CNN-based intrusion detection systems (IDS) have become a potent means of boosting network security. These IDS have a higher level of accuracy when automatically extracting features and detecting intrusions thanks to the use of convolutional neural networks. They are very resilient against new threats thanks to their capacity for handling high-dimensional data and adapting to changing assault patterns. The CNN-based IDS reduces human participation and speeds up response times by automating the detection and response process. These systems are well-suited to safeguard huge and intricate networks because of their scalability and real-time monitoring capabilities. In general, CNN-based IDS provides an effective and proactive approach to network security, ensuring the prompt identification and mitigation of cyber threats.

REFERENCES

[1] C.-D. Pham et al., "A Deep Learning Approach for Network Intrusion Detection System," in IEEE Access, vol. 6, pp. 32280-32289, 2018.
[2] A. Al-Shawabkeh et al., "Intrusion Detection in IoT Networks Using Deep Learning Techniques," in IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5245-5256, June 2020.
[3] C. Hong et al., "CNN-based Intrusion Detection System for Software-Defined Networking," in IEEE Transactions on Network and Service Management, vol. 15, no. 3, pp. 1241-1254, Sept. 2018.
[4] M. Alhussein et al., "Intrusion Detection System for Industrial Control Systems Using Deep Learning Approach," in IEEE Transactions on Industrial Informatics, vol. 15, no. 8, pp. 4518-4527, Aug. 2019.
[5] F. Hussain et al., "Deep Learning Approach for Network Intrusion Detection in Software-Defined Networking," in IEEE Communications Magazine, vol. 55, no. 2, pp. 126-133, Feb. 2017.
[6] M. R. Islam et al., "A CNN-Based Network Intrusion Detection System Using Particle Swarm Optimization," in IEEE Access, vol. 7, pp. 31288-31297, 2019.
[7] A. Azzouni et al., "Deep Learning for Network Intrusion Detection: A Survey," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 2025-2067, third quarter 2020.
[8] H. Nguyen et al., "A CNN-based Intrusion Detection System for Identifying Malicious Executables," in Proceedings of the 2019 International Joint Conference on Neural Networks (IJCNN), Budapest, Hungary, 2019, pp. 1-8.
[9] S. K. Garg et al. (2013). Scheduling methods for grid computing: State of the art and unresolved problems. 46(4), 47, ACM Computing Surveys.
[10] . D. Han et al. (2017). A thorough examination of software-defined networking architecture, security, and applications. IEEE Communications Surveys and Tutorials, vol. 19(1), pp. 1-23.
[11] K. Hwang et al. (2012). Networking and cloud computing. IEEE Network, vol. 26(4), pp. 4-5.
[12] A. K. Jeyarani et al. (2014). Analysis of virtual machine performance for cloud computing. Engineering Procedia, 97, 2207-2215.
[13] H. Kaur et al., 2016. Analysis of cloud computing service providers' performance. 855-864 in Procedia Computer Science.
[14] . H. Khazaei et al. (2011). A look at how to manage and leverage data deduplication in cloud storage

systems. 1347-1374 in Journal of Network and Computer Applications.
[15] H. Khazaei et al. (2013). An examination of data center network architectures. 520-533 in Computers and Electrical Engineering, 39(2).
[16] Li, L., and colleagues (2010). CloudCmp is a service that compares public cloud providers. 472-481 in the Proceedings of the 10th IEEE/ACM International Conference on Cluster, Cloud, and Grid Computing.
[17] Y. Liu et al. (2014). A thorough examination of network function virtualization. 409-426 in Computer Networks.
[18] Y. Lu et al. (2014). An overview of service-oriented network virtualization in the context of networking and cloud computing convergence. IEEE Communications Surveys & Tutorials, vol. 16, no. 2, pp. 1024-1042.
[19] P. Mell et al. (2011). The NIST defines cloud computing. 53(6), 50, National Institute of Standards and Technology.
[20] S. K. Garg et al. (2014). Load balancing in cloud computing environments that is energy conscious. Grid Computing, 12(1), pp. 111-138.