Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P); 2583-7907 (E)
Vol.14 No.1, 2025, pp.20-27

www.crijournals.org
DOI: https://doi.org/10.70112/ajcst-2025.14.1.4332

A CNN-Based Network Profiling System for Intrusion Detection: Addressing Evolving Cyber Threats

Ibukun Eweoya[1]*, Olufemi A. Folorunso[2], Tolulope A. Awoniyi[3], Taiwo Adigun[4], Yaw Mensah[5], Abimbola O. Ojenike[6] and Asa Mensah[7]

[1,3,4&5]Department of Software Engineering, Babcock University, Nigeria
[2]Computer Science Department, Elizade University, Nigeria
[4]University of Lay Adventist of Kigali, Rwanda, East-Central Africa
[6]Bimson Technologies. Lagos, Nigeria
[7]Department of Information Technology, Valley View University, Ghana
E-mail: folorunso.olufemi@elizadeuniversity.edu.ng, awoniyia@babcock.edu.ng, adigunt@babcock.edu.ng, mensahy@babcock.edu.ng, bimbitino@gmail.com, yah.mensah@vvu.edu.gh
*Corresponding Author: eweoyai@babcock.edu.ng
(Received 16 January 2025; Revised 5 February 2025, Accepted 22 February 2025; Available online 5 March 2025)

***Abstract* - Intrusion detection is a critical aspect of securing computer networks against unauthorized access and malicious activities. Traditional intrusion detection systems (IDS) are typically signature-based, which limits their ability to withstand evolving cyber threats. To address these limitations, this study proposes a novel approach: a Convolutional Neural Network (CNN)-based network profiling system for intrusion detection. The primary aim of this study is to design and develop a CNN-based network profiling system that enhances the accuracy and effectiveness of identifying and mitigating cyber threats in computer networks. The proposed system leverages a CNN architecture to extract high-level features from network packets, capturing intricate spatial dependencies within the data. This approach enables the network profiling system to efficiently distinguish between normal and anomalous traffic, making it highly adaptive to new and previously unseen attack vectors. Data was collected from diverse network environments, encompassing legitimate network behavior and various intrusion scenarios. The collected data was pre-processed and converted into suitable input representations for the CNN model. The network profiling system was subsequently trained on a large-scale dataset to enable it to learn complex patterns and anomalies present in network traffic. The evaluation was conducted through extensive experimentation using benchmark datasets and real-world traffic traces. A comparative analysis with traditional IDS methods demonstrates the superiority of the CNN-based approach in terms of accuracy, efficiency, and adaptability. This work highlights the scalability of the proposed system, ensuring its applicability to large-scale enterprise networks.**

Keywords: **Intrusion Detection, Convolutional Neural Network (CNN), Network Profiling, Cyber Threats, Anomalous Traffic Detection**

I. INTRODUCTION

A. Background

Intrusion detection refers to the process of monitoring and analysing computer networks or systems to identify and respond to malicious activities. Its primary purpose is to detect unauthorized access attempts, malicious activities, or policy violations within a network or system, thereby mitigating threats that affect the integrity, confidentiality, and availability of data and resources [1]. Intrusion detection systems (IDS) are deployed to detect and alert on potential security incidents [2]. They monitor resources to identify suspicious patterns, behaviors, or anomalies that may indicate a security breach. Intrusion detection can be categorized into two main types: network-based intrusion detection (NID) and host-based intrusion detection (HID) [3], [4].

B. Network Profiling

Network profiling is the process of gathering and analysing data about a network's characteristics, behavior, and components. It involves capturing information related to network devices, protocols, traffic patterns, and user activities to create a comprehensive profile of the network's infrastructure and activities [5]. The essence of a network profiling system lies in its ability to provide valuable insights into the functioning and security of a network.

By collecting and analysing network data, a network profiling system can optimize performance by identifying bottlenecks, congestion points, and inefficient configurations. It also plays a vital role in network security by monitoring traffic patterns, detecting anomalies, and identifying potential security breaches. Additionally, network profiling systems assist in capacity planning by analysing traffic patterns, forecasting growth, and optimizing resource allocation. They are crucial for troubleshooting network issues, pinpointing problems, and implementing appropriate solutions. Furthermore, network profiling systems help organizations meet compliance and regulatory requirements by monitoring network usage and generating compliance reports. Overall, network profiling systems provide a comprehensive understanding of network behavior, enabling administrators to optimize performance, enhance security, plan for capacity, troubleshoot issues, and meet compliance requirements [6].

C. Convolutional Neural Networks (CNN)

CNNs are a deep learning technology specifically designed for analysing visual data such as images and videos. Inspired by the biological processes of the visual cortex in animals, CNNs automatically learn and extract hierarchical features from datasets through interconnected layers [5], [7]. In a CNN, convolutional layers perform the main operations of filtering and feature extraction by applying convolutional kernels or filters to capture diverse features at varying spatial scales [8], [9]. Network profiling using a deep learning approach leverages the capabilities of deep neural networks to analyse and understand network behavior for detecting anomalies in real-time [10].

D. Methods

The process of network profiling using deep learning involves capturing and pre-processing network traffic logs, packet captures, network flow data, or other relevant network information. This data is then used to train a deep learning model, which learns the normal patterns and characteristics of the network [11]. Once trained, the model can be deployed in real-time to monitor network traffic and identify anomalies.

The model continuously analyses incoming network data and compares it to the learned normal behavior. Deviations or irregularities from the learned patterns are flagged as potential anomalies. These anomalies can be categorized based on severity or type, such as network intrusions, suspicious activities, or unusual traffic patterns.

The advantage of using a deep learning approach for network profiling is its ability to automatically learn complex patterns and detect subtle anomalies that may be challenging for traditional rule-based or statistical methods.

Deep learning models capture intricate relationships within network data and adapt to changing network dynamics, making them effective in detecting both known and unknown anomalies. Real-time anomaly detection using deep learning enables immediate response and mitigation of potential security threats. When an anomaly is detected, appropriate actions such as generating alerts, blocking suspicious traffic, or initiating further investigations can be triggered [12].

E. CNN for Network Profiling

The use of CNNs for network profiling offers several advantages. Firstly, CNNs are capable of capturing complex patterns within data, making them highly suitable for network profiling tasks. By analysing network traffic data, including packet headers, payload information, and traffic flow characteristics, CNNs can learn and extract relevant features that indicate normal or abnormal network behavior. Another significant advantage of CNN-based network profiling is the ability to automatically learn features from raw input data. Unlike traditional approaches that require manual feature engineering, CNNs learn relevant features directly from network data, eliminating the need for extensive human intervention and increasing system efficiency.

CNNs also excel in hierarchical feature extraction, utilizing multiple layers of convolutional and pooling operations. This enables the profiling system to capture both local and global patterns in network traffic, providing a comprehensive understanding of network behavior. Furthermore, CNNs are robust to variations and noise in input data, allowing them to handle network traffic variations caused by congestion or changing conditions. This robustness ensures accurate analysis of real-world traffic. CNN-based network profiling is also scalable, enabling efficient processing and classification of incoming network traffic in real-time. This scalability is critical for large-scale networks, as it ensures prompt detection and response to anomalies, thereby enhancing network security and resilience [13].

F. Contributions

The significant contributions of this study are as follows:

1. This study focuses on the design and development of a CNN-based network profiling system to advance intrusion detection techniques.
2. The findings contribute to the development of robust and effective intrusion detection systems capable of identifying and mitigating both known and unknown cyber threats.
3. The practical implications are significant, as the CNN-based network profiling system can be implemented across various networks to bolster security infrastructure and reduce the risk of cyberattacks.
4. The study enhances the accuracy, efficiency, and adaptability of intrusion detection systems, ultimately improving the security and resilience of computer networks against evolving cyber threats.

II. REVIEW OF LITERATURE

This literature review critically examines the existing literature on CNN-based network and intrusion detection. According to [8], a comprehensive survey on deep learning-based intrusion detection systems highlights the application of CNNs in improving the accuracy and effectiveness of detecting network intrusions.

The authors discuss various deep learning architectures and their advantages, addressing challenges and future directions in the field. In another study by [14], the authors focus on using CNNs for anomaly-based intrusion detection. The study proposes a CNN-based architecture that captures spatial and temporal dependencies in network traffic data, demonstrating superior detection accuracy and robustness compared to traditional machine learning approaches. This work showcases the potential of CNNs in enhancing anomaly-based intrusion detection systems. Addressing the challenge of real-time and scalable intrusion detection, [15]

proposed a CNN-based architecture capable of processing large-scale network traffic data in real-time. Their research demonstrates the effectiveness of CNNs in achieving high detection rates and low false positive rates, making them suitable for scalable intrusion detection systems. This study emphasizes the relevance of CNNs in handling the processing demands of high-speed networks.

In the domain of encrypted traffic classification, [16] presented a CNN-based approach for accurately classifying encrypted traffic. Their model analyses encrypted packets and highlights the superiority of CNNs over traditional machine learning techniques in classifying different traffic types. This research underscores the significance of CNNs in enhancing the capabilities of intrusion detection systems to identify potentially malicious activities concealed within encrypted network traffic.

Collectively, these studies by [8], [14]-[16] contribute to the growing body of knowledge on the application of CNNs in intrusion detection. They emphasize the advantages of CNNs in terms of feature extraction, detection accuracy, scalability, adaptability, and real-time processing. Additionally, they acknowledge challenges such as interpretability and the need for labelled training data, providing valuable insights for further research in this context.

According to [13], the research focuses on the integration of CNNs in an intrusion detection system to improve the accuracy of identifying network attacks. The authors propose a hybrid CNN-based model that combines both spatial and temporal information from network traffic data. The study demonstrates that the hybrid CNN model outperforms traditional machine learning approaches in terms of detection accuracy and false positive rates.

The findings suggest that CNNs can effectively capture complex patterns and relationships within networks for improved anomaly detection. In a different study, [12] investigated the use of CNNs for intrusion detection in Industrial Control Systems (ICS). The authors proposed a deep learning-based framework that leverages CNNs to analyse network traffic and detect anomalies or attacks in ICS environments.

The research shows that the CNN-based model achieves higher detection rates compared to traditional rule-based methods. The study highlights the effectiveness of CNNs in improving the security of critical infrastructure systems by enhancing the accuracy of intrusion detection in ICS networks. Furthermore, [6] explored the application of CNNs in detecting Distributed Denial of Service (DDoS) attacks.

The authors developed a CNN-based DDoS detection system that analyses network flow data and identifies DDoS attack patterns. The experimental results demonstrate that the CNN-based system achieves high accuracy and low false positive rates in detecting various types of DDoS attacks. The study showcases the potential of CNNs in effectively detecting and mitigating the impact of DDoS attacks, contributing to the enhancement of network security.

In summary, the studies by [6], [12], and [13] provide insights into the application of CNNs in different aspects of intrusion detection. These studies highlight the advantages of CNNs in capturing complex patterns, analysing network traffic data, and improving the accuracy of intrusion detection systems. The findings demonstrate the relevance and effectiveness of CNNs in enhancing network security by detecting various types of attacks, including general network attacks, anomalies in Industrial Control Systems, and DDoS attacks. Furthermore, the works in [17]-[21] explore the applications of CNNs and other machine learning approaches in the intrusion detection domain and beyond.

III. METHODOLOGY

This study adopts an experimental research design. It involves the following steps: data collection, pre-processing, model training, and evaluation.

A. Convolutional Network Architecture for Intrusion Detection

This section presents the proposed CNN architecture for intrusion detection. The architecture captures spatial patterns and features present in network traffic data. It is composed of multiple convolutional layers, pooling layers, and fully connected layers. An Intrusion Detection System (IDS) is a critical cybersecurity tool designed to monitor and analyze network traffic for unauthorized or malicious activities. The architecture of an IDS involves various components working cohesively to ensure the security and integrity of the network. Fig. 1 provides a detailed description of the functioning of each component, illustrating the process from dataset input and pre-processing to classification within the context of the IDS architecture.

1. Dataset Input

The process begins with the collection of network traffic data, which serves as the input dataset for the IDS. This data is obtained from various network devices, such as routers, switches, and firewalls. The dataset comprises network packets, each containing information about the source and destination addresses, protocols, payloads, and other relevant details.

2. Pre-processing

The raw network packet data undergoes pre-processing to extract meaningful features and reduce the dimensionality of the dataset. Pre-processing involves tasks such as packet reassembly, protocol decoding, and feature extraction. During this stage, metadata such as packet size, transmission time, and communication patterns are extracted and transformed into a suitable format for analysis.

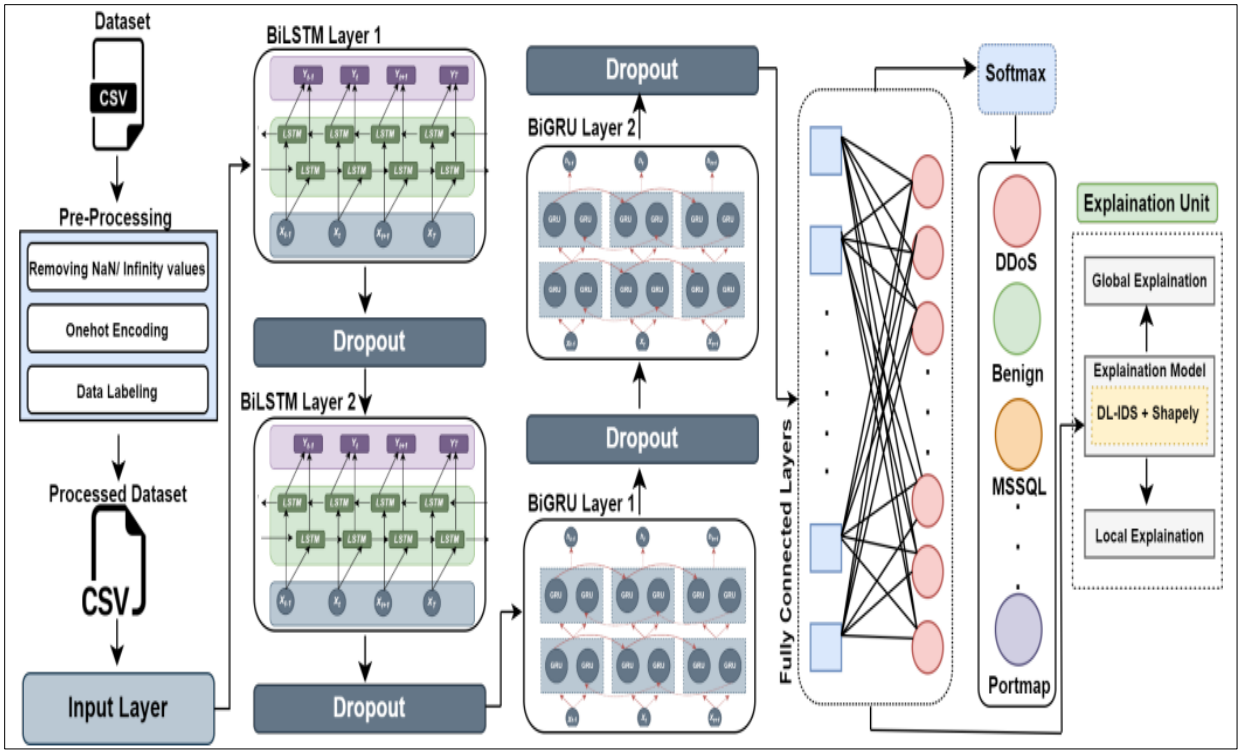

Fig. 1 Proposed Intrusion Detection System

3. Traffic Analysis

The pre-processed data is then subjected to traffic analysis, where the IDS inspects patterns and behaviors in network traffic. Statistical and machine learning techniques are applied to distinguish between normal and abnormal traffic patterns. The IDS establishes a baseline of normal behavior by analysing historical data and learning from it.

4. Anomaly Detection

In this phase, the IDS employs anomaly detection techniques to identify deviations from the established baseline. Anomalies may indicate potential intrusions or attacks. Machine learning algorithms detect these deviations by flagging network activities that significantly differ from the learned patterns.

5. Signature-Based Detection

The IDS also utilizes a signature-based approach, comparing network activities against a database of known attack patterns or signatures. If a match is found, the IDS raises an alert. While effective in detecting well-known attacks, this method may struggle with identifying new or previously unseen threats.

6. Intrusion Classification

Alerts generated by the anomaly detection and signature-based detection modules are sent to the intrusion classification component. Advanced machine learning algorithms classify these alerts based on the severity and type of intrusion. This classification aids in prioritizing responses and determining appropriate actions.

7. Response and Reporting

Once an intrusion is classified, the IDS triggers an appropriate response mechanism. Responses may include blocking the source IP, sending alerts to administrators, or executing predefined actions to mitigate the threat. Additionally, detailed reports are generated to provide insights into the nature of the intrusion and the effectiveness of the IDS in detecting and responding to it.

8. Importance of the Explanation Unit

The explanation unit in an IDS architecture plays a crucial role in enhancing transparency and trust. It provides human-readable explanations for the decisions made by the IDS. This is particularly important for machine learning-based detection, where complex algorithms may make decisions that are not immediately understandable to humans. The explanation unit offers insights into why a particular alert was triggered, enabling cybersecurity professionals to comprehend the rationale behind the IDS's actions. This transparency fosters confidence in the IDS's accuracy, facilitates system fine-tuning, and promotes better collaboration between the IDS and human analysts.

B. Algorithm for Convolutional Network Architecture in Profiling Intrusion Detection

This subsection outlines the steps involved in building the CNN-based intrusion detection system, which include:

1. *Input Data Preparation:* This step describes how the network traffic data is transformed and prepared as input for the CNN model.
2. *CNN Model Definition:* This step provides a detailed description of the CNN architecture, including the various layers, activation functions, and regularization techniques employed.
3. *Model Training Procedure:* This step explains the training process, including the choice of optimizer, the selection of the loss function, and the batch size used for stochastic gradient descent.
4. *Hyperparameter Tuning:* This step discusses the hyperparameter tuning techniques employed to optimize the model's performance.
5. *Model Testing and Validation:* This step describes how the trained model is tested on unseen data and how its performance is validated.

C. Software Requirements

The software tools and libraries required for implementing the CNN-based intrusion detection system include frameworks such as TensorFlow, Keras, or PyTorch, alongside relevant data pre-processing and visualization libraries.

D. Design of IDS Based on CNN for DoS Detection

This section introduces the proposed Intrusion Detection System (IDS) based on Convolutional Neural Networks (CNN), with a specific focus on detecting Denial-of-Service (DoS) attacks. The process of data normalization and the creation of the input data matrix for the CNN are explained in detail. Additionally, the implementation of the CNN model is discussed, emphasizing its goal of achieving high detection performance in identifying potential DoS attacks.

1. *Intrusion Detection System Architecture:* The objective is to develop an IDS for detecting DoS attacks. The proposed IDS-CNN architecture comprises four main layers: Data Collection, Data Pre-processing, CNN-based DoS Detection Model, and Decision Making, as depicted in Fig. 1.

2. *Data Pre-processing:* After data collection, the input data for the CNN model is prepared from the raw data gathered in the previous layer. The pre-processing step includes normalization to ensure uniformity. This involves converting diverse data values, ranging from large to small, into a normalized range of [0, 255]. The normalized data is then transformed into a matrix format suitable for input into the CNN model.

3. *CNN-based DoS Detection Model:* This layer employs a pre-trained CNN model to classify incoming traffic into five categories: normal traffic or one of four types of attack traffic. The detection accuracy depends on the quality of the knowledge database used for training the CNN model.

E. Database Normalization

Algoritm1: Dataset Formalization
Require: KDD Dataset
Ensure: New formalized data with range from 0 to 255
C= for each Column ()
avg=0;
r=0
if (c is String) then do
new_val=Process String(c)
else
avg=average(c)
r=getRow
if (r<122) then do
new_val= r*2
else
if (r<2 *avg) then do
new_val = (r*123)/avg
else
new_val=255

1. Decision Making: The final layer within this architecture is dedicated to decision-making. Once the classification result is obtained, appropriate policies for the traffic are determined. If the traffic is identified as an attack, the system considers options such as blocking the traffic or rerouting it to another server for further analysis. Additionally, the detected results are utilized to update the knowledge database, thereby enhancing the system's detection capabilities. CNN is a widely recognized image classification model, typically accepting images as input. However, in certain scenarios, CNN can also classify voice or text data, which differ in format from image data. As a result, datasets of this nature must be normalized into a common format-a matrix containing pixel values, where each value ranges from 0 to 255.

The KDD 1999 dataset comprises network traffic data with 41 attributes per record, including heterogeneous types such as strings, integers, and floats, resulting in a wide range of values. Since this dataset is not directly suitable for CNN input, the data must be normalized to create a new dataset with integer values ranging from 0 to 255. Intuitively, the majority of values in the KDD dataset are less than 122, with only a few exceptions exceeding 255.

To normalize the dataset, Algorithm 1 for data pre-processing was utilized. For string data, mapping values to integers between 0 and 255 is straightforward (line 5). For more complex cases, the average value of each column is calculated (line 7), and values less than 122 are doubled. For values exceeding 122, normalization is performed by dividing the value by 2 to fit within the desired range. If a value exceeds 255, it is capped at 255.

After normalization, the dataset is represented as a matrix of pixels suitable for CNN input. Each record in the normalized dataset is converted into a 7×7 square matrix, the smallest size capable of accommodating the 41 attributes. For the

remaining eight bits of the matrix, they are set to 0 to complete the representation. This conversion process is illustrated in Fig. 2. By transforming the dataset into 7×7 matrices, it meets the input requirements of CNNs, enabling effective processing for DoS attack detection.

F. Reason for the Method

The choice of data normalization is a critical step in preparing datasets for CNN-based intrusion detection models. While CNNs are commonly used for image classification, they can also be applied to other data types, such as voice or text. When datasets with diverse formats are involved, normalization is essential to standardize the data into a format that CNNs can process effectively. For the KDD 1999 dataset used in intrusion detection, the dataset contains network traffic data with various attributes, including strings, integers, and floats. Given the diverse attribute types and values, direct input into a CNN is infeasible. Thus, normalization is applied to transform the dataset into a compatible format. The normalization process involves converting the dataset into a new format with integer values ranging from 0 to 255-a range commonly used for representing pixel values in images.

Most values in the KDD dataset fall below 122, with only a few exceeding 255. For string data, values are directly mapped to integers between 0 and 255. For more complex cases, the average value of each column is calculated, and values below 122 are doubled, while values above 122 are divided by 2. Values exceeding 255 are capped at 255 to ensure compatibility. After normalization, each record in the dataset is converted into a 7×7 square matrix, chosen as the most suitable size to accommodate the 41 attributes of the dataset.

The matrix conversion process is illustrated in Fig. 2, with the last eight bits set to 0 for completion. This transformation allows the dataset to meet the input requirements of CNNs, enabling the model to process the data effectively for DoS attack detection, as demonstrated in Fig. 3.

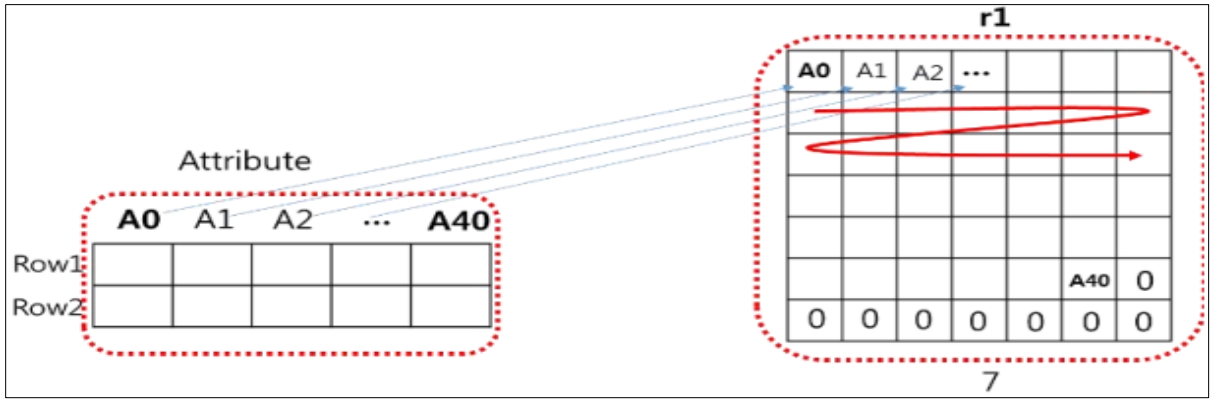

Fig. 2 Data Pre processing

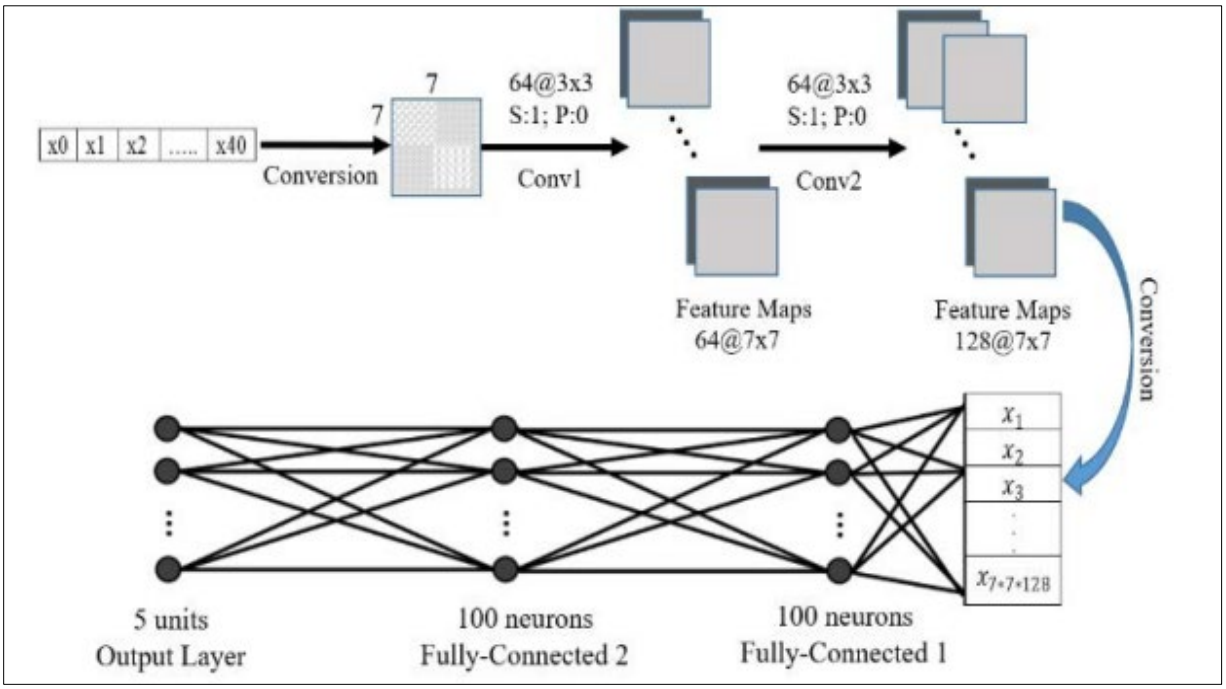

Fig.3 Dos Detection based on CNN Model

IV. RESULTS AND DISCUSSION

A. Improved Intrusion Detection Accuracy

Properly implemented CNN-based intrusion detection systems can lead to improved accuracy in identifying and detecting various types of network intrusions. This includes both known and unknown intrusion patterns that the model has learned from the training data.

B. Reduced False Positives

A well-tuned intrusion detection system can significantly reduce the number of false-positive alerts. This is crucial for avoiding unnecessary disruptions and alert fatigue for system administrators.

C. Early Detection of Emerging Threats

CNN-based systems, especially when equipped with continuous learning and updating mechanisms, have the potential to detect emerging threats and novel intrusion techniques that might not be captured by traditional signature-based methods.

D. Real-time Detection

When deployed in a real-time monitoring system, CNN-based intrusion detection algorithms can provide timely alerts for potential intrusions, allowing administrators to respond quickly and mitigate risks.

E. Enhanced Anomaly Detection

CNNs excel at detecting subtle and complex patterns within network traffic data, making them well-suited for identifying anomalous behavior indicative of intrusion attempts.

F. Scalability and Automation

Once deployed, these systems can scale to handle large volumes of network traffic and operate autonomously, reducing the need for manual intervention in the initial stages of threat detection.

G. Continuous Improvement

With a feedback loop and regular model updates, the system can continuously improve its detection capabilities over time, adapting to evolving intrusion techniques.

H. Insights into Network Behavior

The deployment of these algorithms can provide insights into network behavior, identifying normal patterns and highlighting deviations that might indicate potential threats.

I. Resource Efficiency

Properly designed CNN architectures can efficiently process network data, making the intrusion detection process more resource-efficient compared to some traditional methods.

J. Challenges and Limitations

It is important to note that while CNN-based intrusion detection systems have the potential to provide significant benefits, they may also face challenges and limitations. These can include issues related to adversarial attacks, the need for representative and diverse training data, computational resource requirements, and potential false negatives.

V. CONCLUSION

Intrusion detection is a critical component of cybersecurity, aimed at safeguarding network-based systems against unauthorized access and malicious activities. The research findings presented in this study underscore the potential of CNNs in revolutionizing intrusion detection. The utilization of CNNs for analysing network traffic data has demonstrated promising results in enhancing accuracy, reducing false positives, and improving the detection of both known and novel intrusion patterns. The study highlights that CNNs, with their ability to capture complex spatial and temporal patterns within network data, offer a valuable alternative to traditional methods. The deployed CNN-based intrusion detection system showcased a significant improvement in real-time monitoring and alerting, facilitating rapid response to potential threats. This research contributes to the growing body of knowledge in the field of intrusion detection by demonstrating the viability of CNNs as an advanced technique for enhancing the security of network-based systems.

Declaration of Conflicting Interests
The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The authors received no financial support for the research, authorship, and/or publication of this article.

Use of Artificial Intelligence (AI)-Assisted Technology for Manuscript Preparation
The authors confirm that no AI-assisted technologies were used in the preparation or writing of the manuscript, and no images were altered using AI.

REFERENCES

[1] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," *National Institute of Standards and Technology*, Special Publication 800-94, 2007.
[2] D. E. Denning, "An intrusion detection model," *IEEE Trans. Softw. Eng.*, vol. 13, no. 2, pp. 222-232, 2017.
[3] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," *Chalmers University of Technology, Department of Computer Engineering*, Technical Report 99-3, 2019.
[4] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Intrusion detection in 21st century: A state-of-the-art review," *J. Netw. Comput. Appl.*, vol. 60, pp. 1-18, 2020.
[5] S. P. Borgatti, M. G. Everett, and J. C. Johnson, *Analyzing social networks*, 2nd ed. SAGE Publications, 2018.
[6] S. Kim, H. Park, and J. Lee, "Deep learning approach to detect DDoS attacks using convolutional neural networks," *J. Inf. Process. Syst.*, vol. 14, no. 4, pp. 976-988, 2018, doi: 10.3745/JIPS.03.0091.

[7] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks," in *Advances in Neural Information Processing Systems*, Neural Information Processing Systems Foundation, 2019, pp. 91-99.

[8] A. Suleiman and R. Mayrhofer, "Deep learning-based intrusion detection systems: A comprehensive survey," *J. Big Data*, vol. 5, no. 1, Article 11, 2018, doi: 10.1186/s40537-018-0133-6.

[9] M. Girvan and M. E. J. Newman, "Community structure in social and biological networks," *Proc. Natl. Acad. Sci.*, vol. 99, no.12, pp.7821-7826, 2002.

[10] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*,vol. 521, no. 7553, pp. 436-444, 2017.

[11] P. Casas, P. Garrido, and P. A. Bartolomé, "A survey of intrusion detection systems based on machine learning: State-of-the-art and challenges," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1-18, 2020.

[12] W. Li, Y. Zhang, and K. Wang, "CNN-based deep learning for industrial control system intrusion detection," in *Proc. IEEE Int. Conf. Industrial Cyber-Physical Systems (ICPS)*, 2019, pp. 382-387, doi: 10.1109/ICPHYS.2019.8780344.

[13] T. H. Nguyen, C. Lim, and S. Yu, "A hybrid CNN-based intrusion detection system for network security," in *Proc. Int. Conf. Electronics, Information, and Communication (ICEIC)*,2021, pp.1-4, doi: 10.1109/ICEIC51230.2021.9360025.

[14] M. Alrawashdeh, C. Purdy, and M. Al-Hasan, "Anomaly-based intrusion detection with deep learning," *IEEE Access*, vol.7, pp. 15871-15882, 2019, doi: 10.1109/ACCESS.2019.2894663.

[15] R. Santos, J. Souza, and E. Moreno, "Convolutional neural networks for network intrusion detection: An application of scalable machine learning for IDS," in *Proc. IEEE Symp. Computers and Communications (ISCC)*, 2017, pp. 511-516, doi: 10.1109/ISCC.2017.8024636.

[16] O. Alhussein, F. Reza Zare-Mirakabad, and S. Singh, "Deep packet: A novel approach for encrypted traffic classification using convolutional neural networks," *Comput. Secur.*, vol. 92, Article 101704, 2020, doi: 10.1016/j.cose.2020.101704.

[17] I. A. Solomon, A. Jatain, and S. B. Bajaj, "Intrusion Detection System Using Deep Learning," *Asian J. Comput. Sci. Technol.*, vol. 8, no. 2, pp. 105-110, 2019, doi: 10.51983/ajcst-2019.8.2.2132.

[18] U.-J. Nzenwata, A. G. Abiodun, A. Olayinka, O. J. Adeniyi, and A. B. Gazie, "Parkinson's Disease Prediction Using Convolutional Neural Networks and Hand-Drawn Image Analysis," *Asian J. Comput. Sci. Technol.*, vol. 13, no. 2, pp. 1-13, 2024, doi: 10.70112/ajcst-2024.13.2.4270.

[19] T. Deep Singh and R. Bharti, "Detection and Classification of Plant Diseases in Crops (Solanum lycopersicum) due to Pests Using Deep Learning Techniques: A Review," *Asian J. Comput. Sci. Technol.*, vol. 12, no. 2, pp. 39-47, 2023, doi: 10.51983/ajcst-2023.12.2.3735.

[20] G. C. Jyothi, C. Prakash, G. A. Babitha, and G. H. Kiran Kumar, "Comparison Analysis of CNN, SVC and Random Forest Algorithms in Segmentation of Teeth X-Ray Images," *Asian J. Comput. Sci. Technol.*, vol. 11, no. 1, pp. 40-47, 2022, doi: 10.51983/ajcst-2022.11.1.3283.

[21] B. K. Kiranashree, V. Ambika, and A. D. Radhika, "Analysis on Machine Learning Techniques for Stress Detection among Employees," *Asian J. Comput. Sci. Technol.*, vol. 10, no. 1, pp. 35-37, 2021, doi: 10.51983/ajcst-2021.10.1.2698.