Real-Time Network Intrusion Detection Using Convolutional Neural Networks and Behavioral Analytics

Dr. Abimbola Basiru Owolabi
National Open University of Nigeria

***Abstract*—The rapid expansion of interconnected digital systems has significantly increased exposure to cyber threats, making traditional security mechanisms insufficient for modern network protection. Network Intrusion Detection Systems (NIDS) are essential for identifying malicious activities; however, conventional approaches struggle with scalability, real-time processing, and detection of previously unseen attacks. This study presents a real-time intrusion detection framework that integrates Convolutional Neural Networks (CNNs) with behavioral analytics to enhance detection accuracy, adaptability, and responsiveness. The CNN component is employed for automated feature extraction from raw network traffic, while behavioral analytics models' user and system activity patterns to detect anomalies. The hybrid system combines deep learning-driven classification with behavioral deviation analysis to improve detection of both known and unknown attacks. Experimental evaluation demonstrates that the proposed model achieves high accuracy, improved precision-recall balance, reduced false positives, and efficient real-time performance, making it suitable for deployment in modern high-speed network environments.**

I. INTRODUCTION

The rapid evolution of information and communication technologies has fundamentally transformed how organizations and individuals interact, communicate, and conduct business. Modern society is increasingly dependent on interconnected digital infrastructures such as enterprise networks, cloud computing platforms, Internet of Things (IoT) devices, and distributed systems. While these technologies have significantly improved operational efficiency, scalability, and real-time data accessibility, they have also expanded the cyber threat landscape, exposing networks to a wide range of sophisticated and persistent attacks, (Wang, Hui & Cao, Zijian & Hong, Bo. 2020).

Cybersecurity has therefore become a critical concern in both public and private sectors, particularly as cyberattacks continue to grow in frequency, complexity, and impact. Malicious

actors now employ advanced techniques such as Distributed Denial of Service (DDoS), ransomware, phishing, port scanning, privilege escalation, and Advanced Persistent Threats (APTs) to exploit vulnerabilities in network infrastructures. These attacks are not only capable of disrupting services but can also lead to severe financial losses, data breaches, operational downtime, and in some cases, compromise of national critical infrastructure, (Wang, Hui & Cao, Zijian & Hong, Bo. 2020).

Network Intrusion Detection Systems (NIDS) play a central role in defending against such threats by continuously monitoring network traffic and identifying suspicious or malicious activities. Traditionally, intrusion detection systems have relied on signature-based and rule-based approaches, where predefined patterns of known attacks are used for detection. Although these methods are effective against previously identified threats, they are inherently limited in their ability to detect new, unknown, or evolving attack patterns. As cyber threats become more dynamic and adaptive, the limitations of these conventional systems have become increasingly apparent, (Zhang, H.; Li, J.L.; Liu, X.M.; Dong, C. 2021).

To address these shortcomings, researchers have turned to machine learning techniques, which enable systems to learn patterns from data and make predictive decisions. Machine learning-based intrusion detection systems have demonstrated improved performance over traditional methods; however, they still depend heavily on manual feature engineering and often struggle with high-dimensional, noisy, and rapidly changing network data. Additionally, their performance tends to degrade when deployed in real-time environments where data streams are continuous and large-scale, (Zhang, H.; Li, J.L.; Liu, X.M.; Dong, C. 2021).

In recent years, deep learning has emerged as a powerful paradigm for addressing complex pattern recognition problems in cybersecurity. Unlike traditional machine learning models, deep learning architectures are capable of automatically extracting hierarchical features from raw data without requiring extensive manual preprocessing. Among these architectures, Convolutional Neural Networks (CNNs) have shown remarkable success in capturing spatial relationships and hidden patterns within structured data, making them suitable for network traffic analysis. CNNs are particularly effective in identifying subtle anomalies that may indicate malicious activity within complex network environments, (Bengio Y., Boulanger-Lewandowski N., and Pascanu R., 2013).

However, network traffic analysis alone is often insufficient for comprehensive intrusion detection, as cyberattacks may also manifest through abnormal user or system behavior over time. This has led to the emergence of behavioral analytics as a complementary approach in cybersecurity. Behavioral analytics focuses on understanding normal patterns of user activity, system interactions, and network usage over time. By establishing a behavioral baseline, deviations from expected behavior can be detected as potential security threats, including insider attacks and stealthy intrusions that may not be easily identifiable through traffic analysis alone, (Tiwari Phd, Abhishek. 2019).

Despite the progress made in both deep learning and behavioral analytics, there remains a gap in integrating these approaches into a unified, real-time intrusion detection framework. Many

existing systems either focus solely on network traffic analysis or behavioral monitoring, limiting their overall detection capability and robustness. Furthermore, challenges such as computational efficiency, real-time processing requirements, and adaptability to evolving cyber threats remain unresolved.

In response to these challenges, this study proposes a real-time network intrusion detection system that integrates Convolutional Neural Networks with behavioral analytics. The objective is to develop an intelligent and adaptive security framework capable of accurately detecting both known and unknown cyber threats while maintaining real-time performance. By combining deep learning-based feature extraction with behavioral deviation analysis, the proposed system aims to enhance detection accuracy, reduce false positives, and improve overall network security resilience in modern digital environments, (Sekhar R., and K. Thangavel 2019).

II. PROBLEM STATEMENT

Despite significant advancements in cybersecurity technologies, modern network infrastructures continue to face persistent and increasingly sophisticated cyber threats. Traditional intrusion detection systems, which rely primarily on predefined rules and known attack signatures, are no longer sufficient in detecting emerging and evolving attacks. These systems struggle particularly with zero-day attacks, advanced persistent threats, and polymorphic malware, which are designed to evade conventional detection techniques, (Tae-Young Kim and Sung-Bae Cho 2019).

Furthermore, many existing machine learning-based intrusion detection approaches require extensive manual feature engineering and often fail to perform efficiently when dealing with high-dimensional, real-time network traffic data. As network environments become more complex and data-intensive, these limitations result in reduced detection accuracy, increased false alarm rates, and delayed response times. This makes it difficult to ensure timely identification and mitigation of cyber threats in critical systems, (Tae-Young Kim and Sung-Bae Cho 2019).

Another major challenge lies in the inability of most existing systems to incorporate behavioral context into intrusion detection. Without understanding normal user and system behavior patterns, it becomes difficult to distinguish between legitimate anomalies and malicious activities. This often leads to either missed detections or excessive false positives, both of which negatively impact system reliability and operational efficiency, (Nathan Shone, Ngoc Tran Nguyen, Phai Vu Dinh, and Qi Shi 2018).

Therefore, there is a critical need for an intelligent, adaptive, and real-time intrusion detection framework that can automatically learn from network data, identify complex attack patterns, and incorporate behavioral analysis to improve detection accuracy. This study addresses this gap by proposing a hybrid model that combines Convolutional Neural Networks with behavioral analytics to provide a more effective and scalable solution for modern cybersecurity challenges.

III. OBJECTIVES OF THE STUDY

The primary objective of this study is to design and develop an intelligent and real-time network intrusion detection system that leverages Convolutional Neural Networks (CNNs) in combination with behavioral analytics to enhance cybersecurity in modern network environments. The study aims to move beyond the limitations of traditional signature-based and rule-based intrusion detection systems by introducing a deep learning-driven approach capable of automatically learning complex patterns from network traffic data.

Specifically, the study seeks to develop a model that can accurately detect both known and unknown cyber threats by extracting meaningful features from raw network traffic using CNN architectures. Another key objective is to integrate behavioral analytics into the detection framework in order to capture deviations in user and system behavior that may indicate stealthy or insider attacks. The study also aims to ensure that the proposed system operates efficiently in real-time environments, where rapid detection and response are critical to minimizing potential damage from cyberattacks.

In addition, the research aims to evaluate the performance of the proposed model using standard metrics such as accuracy, precision, recall, F1-score, and false positive rate, and to compare its effectiveness against traditional machine learning-based intrusion detection systems. Ultimately, the study seeks to contribute to the development of a more robust, adaptive, and intelligent cybersecurity framework capable of protecting high-speed and large-scale network infrastructures.

IV. LITERATURE REVIEW

The field of network intrusion detection has evolved significantly over the past few decades, driven by the continuous advancement of networking technologies and the increasing sophistication of cyber threats. Early research in intrusion detection systems (IDS) was largely based on rule-based and signature-based approaches. These systems operated by comparing incoming network traffic against a database of known attack signatures or predefined rules. While this approach was effective in detecting previously identified threats, it was inherently limited in its ability to identify new, unknown, or modified attack patterns. As cybercriminals began to develop more adaptive and stealthy techniques, the inadequacy of these traditional systems became more evident, (Yifang Tang, Lize Gu, and Leiting Wang 2021).

In response to these limitations, anomaly-based intrusion detection methods were introduced. These approaches focused on establishing a baseline of normal network behavior and identifying deviations from this baseline as potential threats. Although anomaly-based systems improved detection of unknown attacks, they often suffered from high false positive rates due to the dynamic nature of network environments, where legitimate behavior can frequently change. This challenge highlighted the need for more intelligent and adaptive detection mechanisms capable of distinguishing between legitimate variations and malicious anomalies, (Yuchen Liu, Shengli

Liu, and Xing Zhao 2017).

The introduction of machine learning into cybersecurity marked a significant turning point in intrusion detection research. Machine learning algorithms such as Support Vector Machines (SVM), Decision Trees, Random Forests, Naïve Bayes, and K-Nearest Neighbors were widely adopted for classifying network traffic. These models demonstrated improved accuracy compared to traditional methods, as they could learn patterns from data rather than relying solely on predefined rules. However, despite these advantages, machine learning-based systems still required extensive manual feature engineering, where domain experts had to select relevant features from raw network data. This process was not only time-consuming but also prone to human bias and inefficiency when dealing with large-scale datasets, (Yuchen Liu, Shengli Liu, and Xing Zhao 2017)

As network environments became more complex and data-rich, deep learning emerged as a more powerful alternative. Deep learning models, particularly neural networks, have the ability to automatically learn hierarchical feature representations from raw data without the need for manual feature extraction. Among these, Convolutional Neural Networks (CNNs) have gained significant attention due to their effectiveness in capturing spatial relationships and local patterns within structured datasets. Originally designed for image processing, CNNs have been successfully adapted for intrusion detection by treating network traffic data as structured input matrices. Research has shown that CNN-based models outperform traditional machine learning techniques in detecting complex and non-linear attack patterns, especially in high-dimensional datasets.,(Yang Yu, Jun Long, and Zhiping Cai 2017)

In addition to CNNs, other deep learning architectures such as Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks have also been explored for intrusion detection tasks. These models are particularly effective in capturing temporal dependencies in sequential network traffic data. However, RNN-based models often suffer from computational inefficiency and vanishing gradient issues, which can limit their scalability in real-time applications. CNNs, on the other hand, offer a more computationally efficient alternative while still maintaining strong feature extraction capabilities, (Rod, H., Darren, M., Hai, T. 1999).

Parallel to the development of deep learning-based intrusion detection systems, behavioral analytics has emerged as a complementary approach in cybersecurity. Behavioral analytics focuses on analyzing patterns of user activity, system behavior, and network usage over time to establish a baseline of normal behavior. Once this baseline is established, deviations from expected behavior can be flagged as potential security threats. This approach is particularly useful in detecting insider threats and low-and-slow attacks that may not generate obvious network anomalies. However, behavioral analytics alone is often insufficient, as it may generate false positives in dynamic environments where user behavior naturally changes over time, (Jayesh Surana, Jagrati Sharma, Ishika Saraf, Nishima Puri, and Bhavna Navin 2017).

Recent research has increasingly focused on hybrid intrusion detection systems that combine multiple techniques to improve overall performance. These hybrid models often integrate machine learning or deep learning algorithms with behavioral analytics or rule-based systems to

enhance detection accuracy and robustness. Studies have shown that such integrated approaches are more effective in identifying both known and unknown attacks while reducing false alarm rates. For example, combining CNN-based feature extraction with behavioral profiling has been found to improve the detection of subtle and complex attack patterns in network traffic, (Joseph, S., Rod, A., Tommy, G. 2003).

Despite these advancements, several challenges remain unresolved in the existing literature. One major limitation is the difficulty of achieving real-time performance while maintaining high detection accuracy. Deep learning models, while powerful, are often computationally intensive and may not be easily deployable in high-speed network environments without optimization. Another challenge is the lack of explainability in deep learning-based intrusion detection systems, which makes it difficult for security analysts to interpret model decisions and understand the reasoning behind detected anomalies, (Hou C. Y., Wang G. W., Wang C. J., 2019). Furthermore, many existing studies are evaluated using static datasets that may not fully represent real-world network conditions. This limits the generalizability of proposed models when deployed in dynamic and evolving environments. There is also a growing concern regarding adversarial attacks, where attackers deliberately manipulate input data to deceive machine learning models. This introduces an additional layer of complexity in designing robust intrusion detection systems, (Hou C. Y., Wang G. W., Wang C. J., 2019).

In summary, the literature reveals a clear progression from rule-based systems to machine learning and now to deep learning and hybrid approaches in intrusion detection. While significant improvements have been achieved, there remains a critical need for more adaptive, real-time, and behavior-aware systems. This study builds upon existing research by integrating Convolutional Neural Networks with behavioral analytics to address these gaps and provide a more robust and intelligent solution for modern network intrusion detection challenges, (Sahu S. K, Katiyar A, Kumari K. M, Kumar G., 2019).

V. INTRUSION DETECTION SYSTEM DETECTION MODELS

The effectiveness of an Intrusion Detection System (IDS) is commonly measured by its ability to accurately identify and respond to malicious activities within a network environment. The success of an IDS largely depends on its detection mechanism and its capability to distinguish legitimate network behavior from malicious actions. A robust intrusion detection framework should therefore maintain a high detection rate while minimizing false alarms. Broadly, IDS detection techniques can be categorized into two principal models: Signature-based Intrusion Detection Systems and Anomaly-based Intrusion Detection Systems. These categories were initially identified in earlier studies as misuse detection and anomaly detection approaches, (Sahu S., Mehtre B. M., 2023).

Signature-Based Intrusion Detection System

Signature-based IDS operates primarily on pattern recognition principles. In this detection

approach, attack characteristics, known as signatures, are encoded and stored in a repository or blacklist database. Incoming network traffic is continuously monitored and compared against these predefined signatures to identify potential intrusions, (Jiang F., Chun C. P., Zeng H. F., 2012).

The effectiveness of this model depends heavily on the comprehensiveness and regular updating of the signature database. Newly discovered attack patterns must be continuously added to maintain detection capability against emerging threats. Through pattern matching, the system identifies malicious behavior by comparing user or network activities with known attack profiles. This approach assumes that all network traffic is considered legitimate unless it matches predefined prohibited patterns, (Jiang F., Chun C. P., Zeng H. F., 2012).

Signature-based systems are highly effective in identifying previously known attacks with minimal false positives. However, their major limitation lies in their inability to detect unknown or zero-day attacks, since such attacks have no existing signatures within the database.

Anomaly-Based Intrusion Detection System

Anomaly-based Intrusion Detection Systems, commonly referred to as statistical anomaly detection systems, focus on identifying deviations from established normal behavior. Unlike signature-based approaches, anomaly detection systems do not depend on predefined attack patterns. Instead, they create a baseline model of normal system and network behavior and monitor for activities that significantly differ from this baseline, (Ahmim A., Maglaras L. A., Ferrag M. A., 2019).

This approach classifies system activities as either normal or anomalous based on behavioral rules and statistical patterns. Activities that deviate from expected operational behavior are flagged as suspicious and subjected to further analysis. In essence, anomaly detection identifies events that should normally occur but are absent, as well as events that appear unexpectedly within the system, (Ahmim A., Maglaras L. A., Ferrag M. A., 2019).

Anomaly-based IDS possesses the advantage of detecting novel and previously unseen attacks. Nevertheless, because it relies on behavioral assumptions, it may generate higher false positive rates compared to signature-based systems, (Ahmim A., Maglaras L. A., Ferrag M. A., 2019).

VI. DEEP LEARNING AND NEURAL NETWORKS

Deep learning is a specialized branch of machine learning characterized by the use of neural network architectures containing multiple hidden layers that enable hierarchical feature learning. Although a universally accepted definition remains elusive, existing scholarly interpretations converge on the concept that deep learning focuses on learning complex data representations through multiple abstraction levels, (Yun W. A, 2005).

Unlike traditional machine learning techniques that often require manual feature extraction, deep learning models automatically learn relevant features directly from input data. These architectures not only identify relationships among variables but also capture the underlying

knowledge governing such relationships.

Deep learning techniques can generally be classified into two broad categories: discriminative models and generative or unsupervised models, (Kamarudin M. H., Maple C., Watson T., Sofian T., 2015).

Discriminative models include:

- Deep Neural Networks (DNNs)
- Recurrent Neural Networks (RNNs)
- Convolutional Neural Networks (CNNs)

Generative and unsupervised models include:

- Restricted Boltzmann Machines (RBMs)
- Deep Belief Networks (DBNs)
- Deep Boltzmann Machines (DBMs)
- Deep Autoencoders (DA)

These techniques may further be categorized into:

1. Deep networks for supervised learning
2. Deep networks for unsupervised or generative learning
3. Hybrid deep learning networks

Deep learning approaches generally outperform traditional machine learning techniques due to their deep layered structures and their ability to automatically extract meaningful patterns from large datasets without human intervention. Through hierarchical representation learning, higher-level features are constructed from combinations of lower-level features, thereby enhancing model intelligence and adaptability, (Kamarudin M. H., Maple C., Watson T., Sofian T., 2015).

Deep learning architectures are fundamentally inspired by biological neural systems and mimic the structure and operational principles of the human brain using artificial neural networks. The ability to learn multi-level feature hierarchies has contributed significantly to their widespread adoption across cybersecurity applications, especially in intrusion detection, (Kamarudin M. H., Maple C., Watson T., Sofian T., 2015).

VII. CONVOLUTIONAL NEURAL NETWORKS

Convolutional Neural Networks (CNNs) represent a specialized category of deep neural networks designed to automatically learn feature representations directly from input data. CNNs are among the most widely used discriminative deep learning architectures because they eliminate the need for manual feature engineering, (Ioannou C, Vassiliou V., 2018).

The primary objective of CNN architecture is to learn meaningful representations of input characteristics through convolutional operations. Their capability to autonomously identify important features makes them more powerful than traditional neural network structures, (Ioannou C, Vassiliou V., 2018).

CNNs generally contain fewer trainable parameters than fully connected neural networks,

enabling efficient training and reducing the likelihood of overfitting. They are structured as feedforward neural networks composed of organized spatial layers, where each layer operates on multidimensional grid structures characterized by width, height, and depth, (Ioannou C, Vassiliou V., 2018).

A typical CNN architecture consists of several interconnected layers:

- Convolutional layers for feature extraction
- Activation layers for introducing non-linearity
- Pooling layers for dimensionality reduction
- Fully connected layers for classification tasks

Convolutional Neural Networks have demonstrated exceptional performance in image classification and computer vision applications. Beyond image processing, CNNs have also been successfully applied in object detection, speech recognition, natural language processing, action recognition, facial expression analysis, text classification, and cybersecurity systems, (Krizhevsky A., Sutskever I., Hinton G. E, 2012).

Within intrusion detection environments, CNNs provide significant advantages because they can automatically discover hidden traffic patterns and complex relationships in network data. As cyber threats evolve continuously, relying solely on traditional intrusion detection mechanisms becomes insufficient. Consequently, recent studies have shown that deep learning approaches, particularly CNN-based methods, produce superior results in terms of detection accuracy, precision, recall, false alarm reduction, and overall system performance, (Krizhevsky A., Sutskever I., Hinton G. E, 2012).

Methodology

The methodology adopted in this study focuses on the development and implementation of a real-time hybrid intrusion detection system that combines Convolutional Neural Networks with behavioral analytics to improve cybersecurity effectiveness. The proposed architecture adopts a multilayered framework comprising data acquisition, preprocessing, feature transformation, CNN-based detection, behavioral analytics, decision fusion, and real-time deployment, (Zhang Y., Dong Y., Liu C., Sun H., Lei K., 2018).

This structured approach enables the system to process high-speed network traffic efficiently while ensuring scalability, adaptability, and improved detection performance.

Algorithm for CNN-Based Intrusion Detection System

The CNN-IDS implementation process follows the steps below:

1: Convert preprocessed network data into image-like structures with defined dimensions suitable for CNN processing.

2: Import and reshape the transformed dataset to fit CNN input requirements, including the number of samples, image height, image width, and channel dimensions.

3: Initialize parameters for convolutional layers, pooling layers, filters, and layer weights for grayscale image inputs.

4: Apply activation functions across layers except the fully connected output layer.
5: Introduce regularization methods when overfitting occurs during testing.
6: Utilize optimization techniques to minimize training time and prediction errors.
7: Evaluate model performance using loss functions and prediction error calculations.

The methodology begins with network traffic acquisition from public datasets, simulation environments, and real operational networks. Both normal and malicious traffic samples are collected to expose the learning model to diverse attack conditions.

Following acquisition, preprocessing techniques are applied to remove inconsistencies, noise, and irrelevant records. Missing values are handled appropriately, numerical features are normalized, and categorical variables are encoded into numerical representations, (Javaid A. N., Sun Q., Alam W. A, 2016) .

Subsequently, network traffic features are transformed into multidimensional matrices to support CNN-based feature extraction. Correlation and statistical analyses are further applied to eliminate redundant attributes.

The CNN model serves as the primary feature extraction and classification engine. Convolutional layers identify local traffic patterns, activation functions learn complex relationships, and pooling layers reduce computational overhead. Fully connected layers perform final intrusion classification, (Javaid A. N., Sun Q., Alam W. A, 2016) .

Parallel to CNN processing, a behavioral analytics module continuously learns user and system activity patterns. Parameters including login frequency, session duration, access behaviors, and communication trends are monitored to establish behavioral baselines.

A decision fusion mechanism subsequently combines outputs from both modules using weighted decision strategies. Integrating traffic analysis with behavioral profiling improves detection reliability and reduces false classifications.

For deployment, the system operates continuously within a real-time streaming environment. Incoming traffic is processed with minimal latency, enabling immediate threat identification and rapid response actions such as alert generation, IP blocking, traffic rerouting, or node isolation.

The model training procedure involves partitioning datasets into training, validation, and testing subsets to facilitate proper performance evaluation and prevent overfitting. Training is achieved through backpropagation using optimization algorithms such as Adam, while loss functions such as cross-entropy guide learning, (Wei W, Sheng Y, Wang J, Zheng Y., Ye Y. ,2018).

Regularization mechanisms including dropout techniques are introduced to improve model generalization within complex environments.

Finally, system performance is evaluated using standard metrics such as accuracy, precision, recall, F1-score, detection rate, and false positive rate. Comparative analyses against traditional machine learning-based intrusion detection approaches are conducted to demonstrate the effectiveness of the proposed hybrid CNN-behavioral analytics framework in achieving superior detection accuracy and real-time cybersecurity performance, (Ma Z., Jin Li, Lu Y., Chen C. 2021).

Deep Learning-Based Intrusion Detection System Architecture and Implementation

The proposed Intrusion Detection System (IDS) adopts a real-time hybrid architecture that combines the strengths of Convolutional Neural Networks (CNNs) with behavioral analytics to improve cyber threat detection accuracy. The framework is designed to identify both known and emerging attack patterns through automated feature extraction and anomaly-based behavioral monitoring. The overall system architecture consists of seven major stages: data acquisition, data preprocessing, feature representation, CNN-based detection, behavioral analytics, decision fusion, and real-time deployment, (Liu J., sun X., Jin J., 2020).

1. Data Acquisition

The first stage involves collecting network traffic information from both simulated environments and real-world network infrastructures. The dataset comprises packet-level details, flow statistics, system logs, and communication protocol metadata. To ensure robust model training and evaluation, the collected dataset includes both benign and malicious traffic instances. The attack scenarios considered encompass Denial-of-Service (DoS) attacks, port scanning, brute-force login attempts, malware communication patterns, and unauthorized access activities. The inclusion of diverse attack categories enhances the system's ability to generalize across varying cyber threat conditions, (Liu J., sun X., Jin J., 2020).

2. Data Preprocessing

Network traffic data often contains inconsistencies, missing values, redundant entries, and noise that can negatively affect model performance. Consequently, preprocessing procedures are applied to improve data quality and suitability for machine learning implementation. Data cleaning involves eliminating duplicate records and handling incomplete values. Numerical attributes are normalized to ensure uniform feature scales and improve convergence during model training. Additionally, categorical variables such as protocol types, services, and communication labels are transformed into numerical representations through encoding techniques, making them compatible with deep learning algorithms, (Zhou P., Zhou Z., Wang Li, Zhao W., 2020).

3. Feature Representation and Transformation

Traditional IDS models often rely heavily on manual feature engineering; however, the proposed framework utilizes deep learning techniques for automated feature extraction. Prior to CNN processing, network traffic features undergo structural transformation into matrix representations suitable for image-based analysis. Specifically, network attributes are converted into a $9 \times 9 \times 1$ feature matrix, enabling multidimensional data processing through convolution operations. Feature correlation analysis is further employed to identify and remove redundant attributes, thereby reducing computational complexity and improving efficiency, (Yan B. H., Han G. D., 2018) .

4. CNN-Based Intrusion Detection Model

The core detection mechanism is implemented using a Convolutional Neural Network architecture designed to identify complex patterns in network traffic data. The CNN model consists of three two-dimensional convolutional layers operating on the transformed $9 \times 9 \times 1$ input matrices.

Each convolutional layer utilizes the Rectified Linear Unit (ReLU) activation function to introduce non-linearity and enhance learning capabilities. To preserve spatial dimensions and prevent information loss during convolution, zero-padding is uniformly applied across the input dimensions. The convolutional layers automatically extract local features from network traffic patterns, such as suspicious packet sequences and irregular communication behaviors, (He H, Bai Y, Garcia E. A, Li S., 2008).

Following feature extraction, a flatten layer is introduced to convert multidimensional feature maps into:

a one-dimensional vector representation. This transition facilitates information transfer from convolutional operations to the fully connected network layer.

The output stage consists of a dense fully connected layer responsible for traffic classification. A Softmax activation function is employed in the final layer to support multi-class classification tasks by generating probability distributions across different attack categories. Depending on the system configuration, the model can perform either binary classification (normal versus malicious traffic) or multiclass categorization of attack types.

Model implementation and classification procedures were conducted within the Jupyter Notebook environment using Python libraries including Pandas for data manipulation, NumPy for numerical processing, and Scikit-learn for preprocessing and evaluation tasks.

5. Behavioral Analytics Module

To complement CNN-based traffic analysis, a behavioral analytics module operates concurrently to monitor user and system activities over time. Unlike signature-based approaches, this module focuses on understanding normal behavioral patterns and identifying deviations that may indicate malicious activity.

Behavioral profiles are generated using historical network activity records and include parameters such as login frequency, session duration, communication patterns, resource utilization, and access behaviors. Any substantial deviation from established behavioral baselines is considered anomalous and flagged for further inspection. This capability improves detection of insider threats, stealth attacks, and sophisticated intrusions that may evade traditional traffic-based analysis mechanisms, (He H, Bai Y, Garcia E. A, Li S., 2008).

6. Decision Fusion Mechanism

To improve detection reliability and minimize false positives, outputs from the CNN detection model and behavioral analytics module are integrated through a decision fusion strategy. The

hybrid decision-making framework evaluates both network traffic characteristics and behavioral anomalies simultaneously.

A weighted scoring mechanism is employed to combine outputs from both components and determine the final intrusion classification. This fusion process leverages complementary information from each subsystem, resulting in improved detection accuracy and enhanced system robustness, (Guan H. J. 2020).

7. Real-Time Deployment Framework

The proposed IDS architecture is designed for real-time deployment within operational environments. Incoming network traffic is continuously monitored through a streaming data processing pipeline optimized for low-latency analysis. The system performs rapid evaluation of network events and immediately generates alerts upon detection of suspicious activities, (Guan H. J. 2020).

In addition to alert generation, automated response mechanisms can be integrated into the deployment framework. These actions may include blocking suspicious IP addresses, terminate malicious sessions, or isolating compromised nodes from the network infrastructure. Such automated responses significantly reduce incident response time and strengthen the overall cybersecurity posture of the protected environment.

Overall, the integration of deep CNN-based feature extraction with behavioral analytics provides a comprehensive and adaptive intrusion detection solution capable of addressing evolving cyber threats in modern network environments, (Tiwari Phd, Abhishek. 2019).

VIII. RESULTS AND DISCUSSION

The performance of the proposed system was evaluated using standard evaluation metrics, including accuracy, precision, recall, F1-score, and false positive rate. The CNN-based model demonstrated strong capability in identifying both known and unknown intrusion patterns.

The integration of behavioral analytics significantly improved detection reliability by providing contextual understanding of user activity. This combination reduced false positives and enhanced the system’s ability to detect subtle and stealthy attacks.

Comparative analysis with traditional machine learning models such as SVM, Random Forest, and KNN showed that the proposed hybrid system consistently outperformed them in all evaluation metrics. The CNN component effectively captured complex spatial relationships in network traffic, while behavioral analytics enhanced anomaly detection through temporal behavior modeling.

The system also demonstrated suitability for real-time deployment, with minimal detection delay. This is critical in cybersecurity environments where rapid response is essential to prevent damage. However, the model’s computational requirements remain a challenge, particularly in high-throughput network environmentsx, (Yifang Tang, Lize Gu, and Leiting Wang 2021).

IX. CONCLUSION

This study presents a comprehensive real-time network intrusion detection framework that combines Convolutional Neural Networks with behavioral analytics to enhance cybersecurity effectiveness. The proposed system addresses the limitations of traditional intrusion detection methods by leveraging deep learning for automated feature extraction and behavioral modeling for contextual anomaly detection.

The results demonstrate that the hybrid approach significantly improves detection accuracy, reduces false positives, and supports real-time analysis of network traffic. The integration of CNN and behavioral analytics provides a robust and adaptive solution capable of detecting both known and unknown cyber threats.

Despite its advantages, the system requires optimization in terms of computational efficiency and scalability. Future research should focus on developing lightweight deep learning models, improving interpretability, and integrating federated learning approaches for distributed network environments.

REFERENCES

[1] Wang, Hui & Cao, Zijian & Hong, Bo. (2020). A network intrusion detection system based on convolutional neural network. Journal of Intelligent & Fuzzy Systems. 38. 1-15. 10.3233/JIFS-179833.

[2] Zhang, H.; Li, J.L.; Liu, X.M.; Dong, C. (2021) Multidimensional feature fusion and stacking ensemble mechanism for network intrusion detection. Future Gener. Compute. Syst. 122, 130–143.

[3] Bengio Y., Boulanger-Lewandowski N., and Pascanu R., (2013). Advances in optimizing recurrent networks in 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 8624–8628.

[4] Tiwari Phd, Abhishek. (2019). Real-Time Intrusion Detection System Using Computational Intelligence and Neural Network: Review, Analysis and Anticipated Solution of Machine Learning. 10.1007/978-981-10-7590-2_11.

[5] Sekhar R., and K. Thangavel (2019). Intrusion Detection System using Deep Neural Network and Regularization of Hyper Parameters with Adam Optimizer. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249–8958, Volume-8, Issue5S.

[6] Tae-Young Kim and Sung-Bae Cho (2019). CNNLSTM Neural Networks for Anomalous Database Intrusion Detection in RBAC-Administered. DOI:10.1007/978-3-030-36808-1_15.

[7] Nathan Shone, Ngoc Tran Nguyen, Phai Vu Dinh, and Qi Shi (2018). A Deep Learning Approach to Network Intrusion Detection. IEEE Transactions on Emerging Topics in Computational Intelligence 2(1):41-50 DOI:10.1109/TETCI.2017.2 772792.

[8] Yifang Tang, Lize Gu, and Leiting Wang (2021). Deep Stacking Network for Intrusion Detection. Sensors 2022, 22(1), 25. DOI: 10.3390/s2 2010025.

[9] Yuchen Liu, Shengli Liu, and Xing Zhao (2017). Intrusion Detection Algorithm Based on Convolutional Neural Network. DEStech Transactions on Engineering and Technology Research. DOI:10.12783/dtetr/iceta2017/19916.

[10] Yang Yu, Jun Long, and Zhiping Cai (2017). SessionBased Network Intrusion Detection Using a Deep Learning Architecture. Lecture Notes in Computer Science DOI:10.1007/978-3-319-67422-3_13.

[11] Rod, H., Darren, M., Hai, T. (1999). An introduction to automated intrusion detection approaches. Information Management and Computer Security.Information Management and Computer Security 7(2):76-82.

[12] Jayesh Surana, Jagrati Sharma, Ishika Saraf, Nishima Puri, and Bhavna Navin (2017). A Survey on Intrusion Detection System. International Journal of Engineering Development and Research, Volume 5, Issue 2 | ISSN: 2321-9939.

[13] Joseph, S., Rod, A., Tommy, G. (2003). Intrusion detection: methods and systems. Part II. http://www.emeraldinsight.com/0968-5227.htm (Acc ess Date: 6 June 2023).

[14] Hou C. Y., Wang G. W., Wang C. J., (2019) Intrusion detection method based on improved genetic algorithm to optimize SVM. Journal of Ordnance Equipment Engineering. 2019;40(6):15–24.

[15] Sahu S. K, Katiyar A, Kumari K. M, Kumar G., (2019) Mohapatra D. P. An SVM-based ensemble approach for intrusion detection. International Journal of Information Technology and Web Engineering. 2019;14(1):66–84. doi: 10.4018/ijitwe.2019010104.

[16] (Sahu S., Mehtre B. M., 2023) Network intrusion detection system using J48 Decision Tree[C]. Proceedings of the International Conference on Advances in Computing; 10-13 Aug. 2015; Kochi, India. ICACCI); pp. 2023–2026.

[17] Jiang F., Chun C. P., Zeng H. F., (2012) Relative decision entropy-based decision tree algorithm and its application in intrusion detection. Computer Science. 2012;39(4):223–226.

[18] Ahmim A., Maglaras L. A., Ferrag M. A., (2019) Derdour M., Janicke H. A novel hierarchical intrusion detection system based on decision tree and rules-based models. Proceedings of the International Conference on Distributed Computing in Sensor Systems (DCOSS); 29-31 May 2019; antorini, Greece. pp. 228–233.w

[19] (Yun W. A, 2005) “Multinomial logistic regression modeling approach for anomaly intrusion detection. Computers & Security” . 2005;24(8):662–674.

[20] Kamarudin M. H., Maple C., Watson T., Sofian T., (2015) “Packet header intrusion detection with binary logistic regression approach in detecting” R2L and U2R attacks. Proceedings of the International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec); 29-31 Oct. 2015; Jakarta, Indonesia. pp. 101–106.

[21] Ioannou C, Vassiliou V., (2018) “An intrusion detection system for constrained WSN and IoT nodes based on binary logistic regression”. Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems; October 28 - November 2, 2018; Montreal, Canada. pp. 259–263.

[22] Krizhevsky A., Sutskever I., Hinton G. E, (2012) ImageNet classification with deep

convolutional neural networks. Proceedings of the Annual Conference on Neural Information Processing Systems; 2012; NIPS); pp. 1106–1114.

[23] Zhang Y., Dong Y., Liu C., Sun H., Lei K., (2018) "Trends and prospects of deep learning applied to cyberspace security. Journal of Computer Research and Development". 2018;55(6):1117–1142.

[24] Javaid A. N., Sun Q., Alam W. A, (2016) Deep Learning Approach for Network Intrusion Detection system. Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies; 2016; New York, USA. ACM Press; pp. 21–26.

[25] Wei W, Sheng Y, Wang J, Zheng Y., Ye Y.,(2018) HAST-IDS: learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. IEEE Access. 2018;6(99):1792–1806. doi: 10.1109/ACCESS.2017.2780250.

[26] Ma Z., Jin Li, Lu Y., Chen C. (2021) A network intrusion detection approach by fusing WaveNet and BiGRU. Systems Engineering and Electronics Technology. 2021;1(12) http://kns.cnki.net/kcms/detail/11.2422.TN.20211115.1620.002.html

[27] Liu J., sun X., Jin J., (2020) Intrusion detection model based on principal component analysis and cyclic neural network. Chinese Journal of information technology. 2020;34(10):105–112.

[28] Zhou P., Zhou Z., Wang Li, Zhao W., (2020) Network intrusion detection method based on autoencoder and RESNET. Computer application research. 2020;37(S2):224–226.

[29] Yan B. H., Han G. D., (2018) Combinatorial intrusion detection model based on deep recurrent neural network and improved SMOTE algorithm. Chinese Journal of Network and Information Security. 2018;4(7):48–59.

[30] He H, Bai Y, Garcia E. A, Li S., (2008) Adaptive Synthetic Sampling Approach for Imbalanced Learning. Proceedings of the 2008 IEEE International Joint Conference on Neural Networks; 1-8 June 2008; Piscataway, NJ. IEEE World Congress on Computational Intelligence); p. p. 1322.

[31] Guan H. J. (2020) Research on Classification Methods for Complex Distribution Features of Unbalanced Data. Harbin: Harbin Institute of Technology; 2020.