Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 02, February-2025

A Comparative Study on AI-IDS Artificial Intelligence-Based Intrusion Detection System

Aathif Nizam
Department of Computer Science
College of Engineering Karunagappally
Kerala, India

Ananthu Prakash
Department of Computer Science
College of Engineering Karunagappally
Kerala, India

Aparna S
Department of Computer Science
College of Engineering Karunagappally
Kerala, India

Harishma Mohan
Department of Computer Science
College of Engineering Karunagappally
Kerala, India

Afrah Mehar
Department of Computer Science
College of Engineering Karunagappally
Kerala, India

Abstract*—This project aims to develop an Artificial Intelligence-based Intrusion Detection System (AI-IDS) for realtime web traffic monitoring. The system integrates deep learning techniques, specifically Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, to detect sophisticated web-based attacks. The AI-IDS processes network traffic in real time and identifies unknown, obfuscated, and variant attacks, making it adaptable for real-world large-scale traffic scenarios. The proposed system achieves high detection accuracy using publicly available datasets like FLNET 2023 and CICIDS2017, ensuring scalability and flexibility through Docker-based deployment.The paper describes the development and application of an AI-based Intrusion Detection System (AIIDS) designed to detect web attacks in real-time on HTTP traffic. Unlike previous deep learning applications limited to experimental conditions, this system integrates a CNN-LSTM model to efficiently process and analyze large-scale traffic for real-world use. By encoding HTTP data with normalized UTF-8 and calculating entropy and compression, the system identifies complex attack patterns, including obfuscated threats. The model is validated on public datasets (CSIC-2010, CICIDS2017) and live data, and can continuously improve through retraining based on labeled events. Additionally, the AI-IDS is containerized with Docker, enabling it to scale and dynamically update with new attack signatures, thus assisting traditional signature-based systems like Snort in handling unknown or sophisticated attacks more effectively.

I. INTRODUCTION

As technology advances, cybercriminals are continually enhancing their methods, tools, and techniques to target organizations. Public web services, which are accessible to anyone, are particularly vulnerable since many companies rely on open webpages to provide services. When these web services are compromised, it can damage a company's reputa- tion and affect revenue. Typically, security managers protect against external attacks by blocking unused services through firewall policies, but web services within the Internet De- militarized Zone (DMZ) remain open to public access and cannot be shielded by firewalls. Therefore, distinguishing between normal and malicious access is crucial in cybersecurity, especially as many security incidents stem from web attacks, such as information leaks, service disruptions, and malware infections. The HTTP protocol, a core application-level protocol for transferring information over the web, has evolved beyond web pages to include command exchanges and updates across various devices, including scripts and mobile applications. Web attacks frequently exploit vulnerabilities in applications within open web services rather than targeting host systems directly. Attackers may send exploitative code through a specific domain or file path, gain- ing control over the webserver or device. Intrusion detection is a critical area in network security, focusing on identifying abnormal access attempts. Network Intrusion Detection Systems (NIDS) monitor network packets to detect security threats by mirroring network traffic through devices like switches and routers. NIDS generally rely on signature-based detection using rules from tools like Snort, where analysts define patterns to detect attacks. However, while effective at recognizing known patterns, these systems often fail to detect unknown or obfuscated threats. To address this limitation, AI-IDS was developed, utiliz- ing advanced techniques to identify complex attacks that bypass traditional signature-based NIDS.

II. INTRUSION IN CYBERSECURITY

In cybersecurity, intrusion refers to unauthorized access or attempts to gain access to a computer system, network, or data. This can occur through various means, such as exploiting vulnerabilities, phishing attacks, malware deployment, or brute force methods. Intrusions pose significant risks, including data theft, system disruption, or unauthorized surveillance, and often serve as the precursor to more damaging cyberattacks. Effective intrusion detection and prevention systems are critical for identifying and mitigating such threats, ensuring the integrity, confidentiality, and availability of digital assets.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 02, February-2025

We classify intrusion in cybersecurity into eight main types.

- Network Intrusion: Unauthorized access to a network, often achieved through exploiting vulnerabilities, weak passwords, or malware. Examples include sniffing, manin-the-middle attacks, and unauthorized port scanning.
- System Intrusion: Compromising individual systems by exploiting software vulnerabilities or executing malicious code to gain control or steal sensitive data.
- Application Intrusion: Attacks targeting specific applications, such as web applications, through techniques like SQL injection, cross-site scripting (XSS), or buffer overflow exploits.
- Physical Intrusion: Gaining unauthorized physical access to hardware or facilities to tamper with, steal, or compromise devices.
- Social Engineering Intrusion: Manipulating individuals into divulging confidential information or performing actions that compromise security, such as phishing or pretexting.
- Wireless Network Intrusion: Exploiting weaknesses in wireless networks, such as unprotected Wi-Fi or outdated encryption standards, to intercept data or gain unauthorized access.
- Insider Threats: Intrusions caused by individuals within an organization who misuse their access privileges, either maliciously or negligently.
- Distributed Denial of Service (DDoS) Attacks: Overloading systems or networks with traffic to disrupt services, which can act as a form of intrusion to destabilize the infrastructure.

III. DEEP LEARNING

Deep learning (DL) enhances intrusion detection systems (IDS) by leveraging its ability to automatically process and learn complex patterns in network traffic and system behavior.Traditional machine learning methods rely on manually crafted features, which may fail to capture the full complexity of network behaviors. Deep learning techniques, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), can automatically learn and extract intricate patterns from raw data, such as network packets or logs. This capability reduces the dependency on domain expertise for feature engineering and makes the models more adaptable to evolving attack patterns.Deep learning methods excel in identifying subtle and complex correlations within the data. Models like CNNs analyze spatial relationships, while RNNs process sequential data, making them well-suited for detecting anomalies or known attack signatures. These techniques have demonstrated superior accuracy in detecting intrusions compared to traditional methods like Support Vector Machines (SVMs) or Random Forest (RF), especially in multiclass and binary classifications.False alarms are a significant challenge in IDS, leading to inefficiencies in responding to potential threats. Studies have shown that deep learning models like CNNs can significantly reduce false alarm rates by learning nuanced traffic characteristics, distinguishing between normal behavior and actual threats with greater precision.The purpose of deep learning in intrusion detection systems is to enable more accurate, efficient, and adaptive security mechanisms by leveraging its powerful feature-learning capabilities. While it has shown significant promise in research, overcoming practical challenges like real-time applicability and deployment in diverse environments is essential for its broader adoption in cybersecurity.

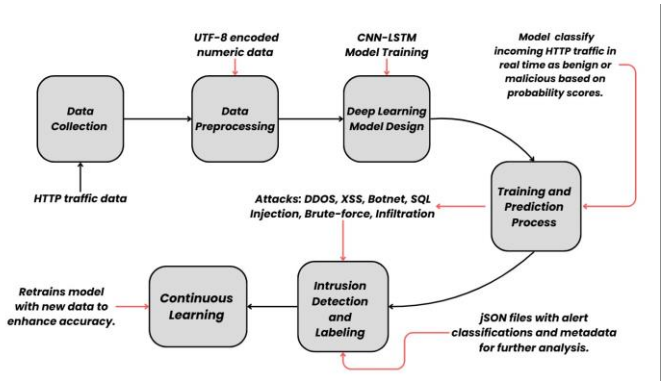

Fig. 1. Flow Chart

IV. LITERATURE REVIEW

Kijun Han et al. [1] proposed an AI technique for cyberthreats detection, based on artificial neural networks. The proposed technique converts multitude of collected security events to individual event profiles and use a deep learningbased detection method for enhanced cyber-threat detection. Notably, NSLKDD Dataset: FCNN achieved 95.8% accuracy, while CNN and LSTM achieved 95.2% and 93.2%, respectively. To evaluate the performance comparison with existing methods, we conducted experiments using the five conventional machine-learning methods (SVM, k-NN, RF, NB, and DT). Consequently, the experimental results of this study ensure that our proposed methods are capable of being employed as learning-based models for network intrusiondetection, and show that although it is employed in the real world, the performance outperforms the conventional machinelearning methods.

Tai-Hoon Kim and Rahul Saha et al. [3] conducted a study which discusses various models used for Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) based on machine learning (ML) and deep learning (DL) techniques. The paper does not focus on one specific model but provides a comparative analysis of several techniques used in the field. Impressively,Decision Trees achieve 99% accuracy (NSLKDD dataset), Random Forests achieves 99% accuracy on most datasets, CNN Close to 99.8% in hybrid frameworks and DNN achieved 99.14% on IoT datasets like BoT-IoT.

Hyunjin Kim, and Dowon Hong et al. [4] presents a model based on Generative Adversarial Networks (GANs).

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 02, February-2025

TABLE I RELATED WORKS ON INTRUSION DETECTION

DL Method and Ref.	Dataset Used	Pros	Cons	Performance Metrics
Artificial Neural Networks [1]	Custom Event Profiles Dataset	Effective event-based threat detection	Limited generalization to new threats	Accuracy: 98.5%, Precision: 97.2%, Recall: 96.8%
Deep Learning (CNNLSTM) [2]	NSL-KDD, UNSW-NB15	Real-time detection capa-bility	Computationally expensive	Accuracy: 99.3%, F1-Score: 98.9%
ML & DL (Survey) [3]	Various IoT datasets	Comprehensive comparison of methods	No novel implementa-tion	N/A
Generative Adversarial Networks [4]	CICIDS2017	Enhanced accuracy with adversarial training	High training complex-ity	Accuracy: 99.6%, Detection Rate: 98.8%
Multi-layer Perceptron (MLP) [5]	CICIDS2017	Explainable AI with LIME and SHAP	May not handle realtime requirements	Accuracy: 98.7%, Precision: 97.4%
Convolutional Neural Networks [6]	UNSW-NB15	High efficiency for largescale data	Limited to static fea-tures	Accuracy: 98.3%, F1-Score: 97.6%
Deep Learning (Hybrid) [7]	NSL-KDD, UNSW-NB15	Intelligent handling of diverse network threats	Limited scalability to extremely large datasets	Accuracy: 99.1%, Precision: 98.2%, Recall: 98.0%
Hierarchical SpatialTemporal [8]	NSL-KDD, UNSW-NB15	Captures spatial-temporal dependencies	Requires extensive tuning of hyperparameters	Accuracy: 98.9%, Detection Rate: 98.5%
CNN + BiGRU [9]	CICIDS2017	Combines spatial and sequential analysis for better detection	High memory and compute requirements	Accuracy: 99.4%, F1-Score: 99.0%
Long Short-Term Memory (LSTM) [10]	NSL-KDD, CICIDS2017	Enhanced detection of sequential patterns	May overfit with limited training data	Accuracy: 98.8%, Precision: 97.9%, Recall: 98.2%
Convolutional Neural Network (CNN) [11]	NSL-KDD, UNSW-NB15	Effective feature extraction and classification	Limited sequential pattern handling	Accuracy: 98.5%, Detection Rate: 98.0%

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 02, February-2025

The system uses GANs to address the data imbalance problem by generating synthetic data, particularly for minor attack traffic, which helps improve the detection rate of rare network intrusions. In this they focused on the reconstruction error and Wasserstein distance-based generative adversarial networks, and autoencoder-driven deep learning models. To demonstrate the effectiveness of our system, they performed comprehensive evalu- ations over various data sets and demonstrated that the proposed systems significantly outperformed the previous AIbased NIDS.The proposed system achieved up to 93.2% accuracy on the NSL-KDD dataset.On the UNSW-NB15 dataset, the system reached an accuracy of 87%.

Diogo Gaspar et al. [5] explored the Machine learning-based systems in a wide variety of tasks. However, the problem with some state-of-the-art models is their lack of transparency, trustworthiness, and explainability. To address this problem, eXplainable Artificial Intelligence (XAI) appeared. It is a research field that aims to make black-box models more understandable to humans. The research on this topic has increased in recent years, and many methods, such as LIME (Local Interpretable Model-Agnostic Explanations) and SHAP (SHapley Additive exPlanations) have been proposed..The Model used is Multi-Layer Perceptron (MLP).DBNs: 96.1% accuracy for malware detection. KNN with ACO: 94.17% accuracy, with a false alarm rate of 5.82%. CNN: Accuracy of 98.44%, precision of 98.40%, and F-score of 0.984 in network intrusion detection.

Zuge Chen et al. [6] proposed a novel network intrusion detection model utilizing convolutional neural networks (CNNs). We use CNN to select traffic features from raw data set automatically, and we set the cost function weight coefficient of each class based on its numbers to solve the imbalanced data set problem. The model not only reduces the false alarm rate (FAR) but also improves the accuracy of the class with small numbers.The accuracy (AC) of the CNN model is 79.48% when tested on the NSL-KDD dataset, which is better than traditional machine learning models but slightly lower than RNN (by 1.81% to 3.96%)

R. Vinayakumar et al. [7] prposed a deep neural network (DNN), a type of deep learning model, is explored to develop a flexible and effective IDS to detect and classify unforeseen and unpredictable cyberattacks. The continuous change in network behavior and rapid evolution of attacks makes it necessary to evaluate various datasets which are generated over the years through static and dynamic approaches. This type of study facilitates to identify the best algorithm which can effectively work in detecting future cyberattacks.These model achieved good detection rates, particularly with 1,024 hidden units and a learning rate of 0.1.

Wei Wang et al. [8] proposed a novel IDS called the hierarchical spatial-temporal features-based intrusion detection system (HAST-IDS), which first learns the low-level spatial features of network traffic using deep convolutional neural networks (CNNs) and then learns high-level temporal features using long short-term memory networks. The entire process of feature learning is completed by the deep neural networks automatically; no feature engineering techniques are required.On the ISCX2012 dataset, the system achieved the following results:Detection Rate (DR): 98.76% False Alarm Rate (FAR): 0.11% Accuracy: 99.18%.

Chenghai Li et al. proposed a network intrusion detection model that combines the components like Hybrid Sampling Algorithm :Combines ADASYN (Adaptive Synthetic Sampling) and RENN (Repeated Edited Nearest Neighbors) to address the issues of imbalanced positive and negative samples in the original traffic data.Feature Selection uses a combination of the Random Forest algorithm and Pearson correlation analysis to reduce the dimensions of features and select the most relevant ones.This model aims to improve accuracy and reduce the false alarm rate compared to similar models, such as CNN-GRU. It is evaluated on the UNSW-NB15, NSLKDD, and CIC-IDS2017 datasets, showing improved accuracy of 85.55%, 99.81%, and 99.70%, respectively.

Awad AA and Ali AFv et al. [10] introduced an improved version of LSTM called "Improved LSTM" (ILSTM), which they designed to boost accuracy. ILSTM combines two optimization techniques: the Chaotic Butterfly Optimization Algorithm (CBOA) and Particle Swarm Optimization (PSO). These techniques are used to fine-tune LSTM's settings, making it more precise.The ILSTM achieved an accuracy of 93.09% and a precision of 96.86% while LSTM gave an accuracy of 82.74% and a precision of 76.49%.

Eunjung Choi et al. [11] used deep learning, a more advanced type of ML, and developed a model based on a Convolutional Neural Network (CNN), which is good at recognizing patterns in data. They tested this CNN model on the CSE-CIC-IDS 2018 dataset and compared it with another model called a Recurrent Neural Network (RNN), which is often used for analyzing sequences of data.The accuracies of SD-2, SD-3, SD-5, and SD-9 with CNN are about 10% to 60% higher than that of using RNN.

Table 1 presents a thorough summary of the latest progress in the field of deep learning for intrusion detection system, which we have identified in our literature review.

V. CONCLUSIONS

The AI-IDS system demonstrates the practical application of deep learning techniques to real-time web intrusion detection, addressing the limitations of traditional signature based Intrusion Detection Systems (IDS). By leveraging a hybrid CNNLSTM architecture, the system effectively captures both spatial and sequential patterns in HTTP traffic, enabling the detection of sophisticated attacks, including unknown and obfuscated threats. This approach is validated through experiments on large-scale real-time data and public datasets like CSIC-2010 and CICIDS 2017, achieving high accuracy and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 02, February-2025

adaptability. Key innovations such as UTF-8-based preprocessing, Dockerbased modularization, and continuous retraining ensure scalability and precision, even in high-traffic environments. The integration of human analyst feedback further enhances the system's reliability by reducing false positives and refining detection rules. Ultimately, the AI-IDS system exemplifies the potential of AI in cybersecurity, offering a robust, scalable, and adaptable solution for protecting critical network infrastructure against evolving threats. Future developments aim to fully automate the detection and response cycle, making AI-IDS an indispensable tool in modern cybersecurity.

VI. FUTURE DIRECTIONS

In the field of AI based intrusion detection system focusing on real-world applicability by addressing scalability and adaptability challenges in dynamic network environments. Researchers should prioritize generating large, realistic datasets that reflect diverse and evolving attack patterns while avoiding overfitting. Advanced preprocessing and feature extraction techniques, such as exploring alternative encoding methods, can further enhance model robustness. Additionally, optimizing hybrid deep learning architectures (e.g., combining CNNs and LSTMs) and improving detection accuracy for obfuscated or novel attacks are key areas for improvement.

REFERENCES

[1] J. Lee, J. Kim, I. Kim, and K. Han, "Cyber threat detection based on artificial neural networks using event profiles," IEEE Access, vol. 7, pp. 165607–165626, 2019.

[2] A. Kim, M. Park, and D. H. Lee, "Ai-ids: Application of deep learning to real-time web intrusion detection," IEEE Access, vol. 8, pp. 70245–70261, 2020.

[3] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T.-H. Kim, "Machine and deep learning solutions for intrusion detection and prevention in iots: A survey," IEEE Access, vol. 10, pp. 121173–121192, 2022.

[4] C. Park, J. Lee, Y. Kim, J.-G. Park, H. Kim, and D. Hong, "An enhanced ai-based network intrusion detection system using generative adversarial networks," IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2330–2345, 2023.

[5] D. Gaspar, P. Silva, and C. Silva, "Explainable ai for intrusion detection systems: Lime and shap applicability on multi-layer perceptron," IEEE Access, vol. 12, pp. 30164–30175, 2024.

[6] K. Wu, Z. Chen, and W. Li, "A novel intrusion detection model for a massive network using convolutional neural networks," IEEE Access, vol. 6, pp. 50850–50859, 2018.

[7] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. AlNemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," IEEE Access, vol. 7, pp. 41525–41550, 2019.

[8] W. Wang, Y. Sheng, J. Wang, X. Zeng, X. Ye, Y. Huang, and M. Zhu, "Hast-ids: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection," IEEE Access, vol. 6, pp. 1792–1806, 2018.

[9] "Network intrusion detection technology based on convolutional neural network and bigru," Journal of Cybersecurity and Artificial Intelligence, vol. 10, no. 3, pp. 123–135, 2024.

[10] G. T. Awad AA, Ali AF, "An improved long short-term memory network for intrusion detection," Journal Name or Conference Proceedings, vol. XX, no. YY, pp. ZZZ–ZZZ, 2024.

[11] C. E. Kim Jiyeon, Shin Yulim, "An intrusion detection model based on a convolutional neural network," Journal Name, vol. XX, no. YY, pp. ZZZ–ZZZ, 2024.