Hybrid Detection: Enhancing Network & Server Intrusion Detection using Deep Learning

2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA) | 979-8-3503-3828-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCCMLA58983.2023.10346699

*Vishnu Kurnala
Computer Science & Engineering (AI&ML) Vardhaman College of Engineering Hyderabad, India kurnalavishnu483@gmail.com

Swaraj Abhishek Naik
Computer Science & Engineering (AI&ML) Vardhaman College of Engineering Hyderabad, India swaraj.abhishekk@g mail.com

Dhanush Chowdary Surapaneni
Computer Science & Engineering (AI&ML) Vardhaman College of Engineering Hyderabad, India dhanushchowdarysura paneni@g mail.com

Ch. Bharathsimha Reddy
Computer Science & Engineering (AI&ML) Vardhaman College of Engineering Hyderabad, India cherukupallibharath36 @gmail.c om

***Abstract*—In the ever-evolving landscape of cybersecurity threats, Intrusion detection systems are critical in protecting network and server infrastructure in the ever-changing spectrum ofcybersecurity threats. This research introduces a hybrid detection approach that uses deep learning techniques to improve intrusion detection accuracy and efficiency. The proposed prototype combines the strength of the XGBoost and MaxPooling1D algorithms within an ensemble model, resulting in a stable and effective solution. Through the fusion of these methodologies, the hybrid detection system achieves superior performance in identifying and mitigating various types of intrusions. This paper provides an overview of the prototype's architecture, discusses the benefits of using deep learning in intrusion detection, and presents experimental results showcasing the system's efficacy.**

***Keywords*—Intrusion Detection Systems (IDS), Deep Learning, Ensemble Model, XGBoost, MaxPooling1D, Network and ServerSecurity**

I. Introduction

Intrusion Detection Systems (IDS) play a crucial role in safeguarding network and server infrastructures against cyber threats. Traditional intrusion detection technologies frequently struggle to detect sophisticated and developing infiltration strategies. As a result, researchers and practitioners have turned to advanced techniques, particularly deep learning, to enhance the accuracy and efficiency of intrusion detection [1]. Deep learning, a subset of machine learning, has shown great potential in capturing complex patterns and features from large-scale data, making it a promising approach for IDS.

The primary goal of this study is to provide a fresh strategy for IDS that makes use of deep learning, focusing on the development and evaluation of an ensemble model combining XGBoost and MaxPooling1D algorithms [1]. This hybrid detection system aims to leverage the strengths of both algorithms to enhance the overall intrusion detection capabilities. By addressing the limitations of traditional IDS methods and capitalizing on the powerful feature extraction capabilities of deep learning, we aim to provide a more robust and adaptive defense mechanism against network and server intrusions.

II. Related Work

Previous research in the field of IDS using deep learning has witnessed significant advancements and comprehensive studies [1][2]. Jagadeesan and Subbulakshmi (2020) conducted a comprehensive study, exploring various deep learning techniques' applications in intrusion detection. Chen, Zhou, and Cao (2020) contributed a comprehensive review of the state-of-the-art deep learning techniques for IDS, shedding light on their strengths and limitations.

Liu et al. (2021) presented a deep learning-based IDS for network security, demonstrating its efficacy in handling complex intrusion scenarios[3]. Similarly, Alhussein and Shamsuddin (2021) conducted an in-depth review of various deep learning models for intrusion detection, offering insights into their comparative performance[4].

Guo et al. (2020) investigated the use of deep learning in detection of network intrusions, detailing the possible benefits and challenges of such systems [5]. Lin and Chen (2018) investigated the benefits and drawbacks of applying deep learning to detect intrusions in network settings [6].

Abdeldayem, Alazab, and Venkataraman (2019) offered a thorough analysis of deep learning algorithms used in intrusion detection, highlighting significant methodology and approaches used in the literature [7]. Alshammari, Alshammari, and Alghamdi (2020) conducted a survey on deep learning-based intrusion detection systems, outlining advancements and emerging trends in this field [8].

Masood and Khan (2019) conducted a comprehensive study of deep learning approaches used for detection of anomalies in networks , focusing on their application in intrusion detection scenarios [9]. Shen, Xu, and Fu (2017) offered a thorough assessment of deep learning in systems for intrusion detection, discussing recent advances and future directions [10].

Lin and Zuo (2019) proposed a deep learning-based detection of intrusion method for computer networks, demonstrating its efficacy in detecting possible intrusions [11]. Canedo and Moreira (2020) studied the application of deep learning and

feature selection approaches in IDS, demonstrating enhanced performance by incorporating relevant features [12].

Wang and Luo (2020) presented a system based on deep learning to detect intrusions specifically tailored for cloud computing environments [13]. Firdhous, Balasubramaniam, and Kausar (2019) introduced a novel deep learning approach for intrusion detection based on recurrent neural networks, demonstrating its capability for processing sequential data [14].

Pham et al. (2020) introduced a deep learning-based hybrid model for detecting network breaches [15], which included numerous strategies to increase detection accuracy. Their research demonstrates the versatility and usefulness of hybrid techniques in intrusion detection systems.

Yang et al. [16] introduced a Tree-Based Intelligent Intrusion Detection System tailored for the Internet of Vehicles (IoV) context, presenting their findings at the 2019 IEEE Global Communications Conference (GLOBECOM). This work highlights the significance of intelligent intrusion detection in IoV and offers a tree-based framework, showcasing promising results to enhance IoV security.

In their paper, Yang et al. [17] present the Multi-Tiered Hybrid Intrusion Detection System (MTH-IDS) for the Internet of Vehicles, published in the IEEE Internet of Things Journal in 2022. MTH-IDS is a comprehensive approach to intrusion detection in IoV, demonstrating its effectiveness through a multi-tiered system that combines various techniques to bolster security within this dynamic environment.

Yang and colleagues [18] propose the Decision-Based Ensemble Framework, known as LCCDE, for Intrusion Detection in the Internet of Vehicles, as presented at the 2022 IEEE Global Communications Conference (GLOBECOM). Their work focuses on enhancing intrusion detection accuracy in IoV by creating an ensemble approach, showcasing the potential of combining multiple decision-based strategies for improved security.

The work of Hochreiter and Schmidhuber [19] introduces the concept of Long Short-Term Memory (LSTM) neural networks, which has played a pivotal role in various domains. Their research, published in Neural Computation in 1997, has been foundational in the development of recurrent neural networks, offering significant insights into the field of deep learning and sequential data processing.

In light of these significant contributions and developments in the field, this paper aims to present a hybrid detection system that integrates XGBoost and MaxPooling1D algorithms [1], demonstrating its potential to enhance network and server intrusion detection capabilities. The subsequent sections will delve into the methodology, dataset, results, and case studies, offering a comprehensive analysis of the proposed system's performance and effectiveness against various intrusion scenarios. Additionally, we will discuss the limitations of the approach and outline potential avenues for future research and improvements.

III. METHODOLOGY

The proposed methodology entails the creation of an ensemble model for detecting breaches that incorporates the XGBoost and MaxPooling1D algorithms. The ensemble model leverages both techniques' capabilities, resulting in better accuracy and robustness in detecting network and server intrusions.

A. The Ensemble Model

The ensemble model is constructed by integrating XGBoost, a powerful gradient boosting algorithm known for its high predictive performance, and MaxPooling1D, a technique commonly used in convolutional neural networks (CNNs) for feature extraction.

The XGBoost algorithm utilizes a series of decision trees, iteratively optimizing the ensemble by minimizing the prediction errors. It is capable of handling complex and nonlinear relationships within the data. On the other hand, MaxPooling1D works as a feature extractor by selecting the most significant features from the input data, reducing its dimensionality, and retaining only the essential information.

In the ensemble model, XGBoost serves as the initial layer, capturing the raw patterns and interactions in the data. The outputs from XGBoost are then fed into MaxPooling1D, which further extracts and summarizes the most relevant features, effectively enhancing the model's ability to detect subtle intrusion patterns that may have been overlooked by individual algorithms.

The selection of XGBoost and MaxPooling1D for the ensemble model is motivated by their complementary strengths and proven performance in various domains, including intrusion detection.

Because of its ability to handle big datasets, XGBoost has exhibited cutting-edge performance in numerous machine learning competitions and real-world applications., learn complex relationships, and provide robust predictions. Its ensemble of decision trees allows it to capture intricate patterns in high-dimensional data, making it suitable for detecting sophisticated intrusion attempts.

On the other hand, MaxPooling1D is particularly adept at extracting the most informative features from sequential data, such as network traffic logs and server activity records. Its capability to focus on the most significant elements within the input data helps in reducing computational overhead and preventing overfitting.

By combining XGBoost and MaxPooling1D, we aim to leverage the complementary nature of these algorithms, ultimately enhancing the overall intrusion detection accuracy and providing a more reliable defense mechanism against network and server threats.

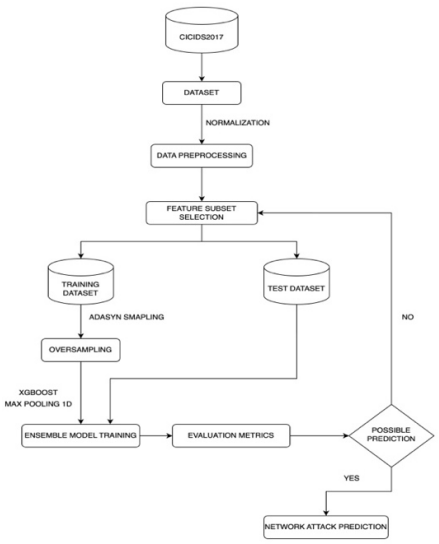

Fig 1: The Architecture of Proposed Model

IV. Performance Evaluation

To evaluate the performance of different classifiers for the Intrusion Detection System (IDS), we considered the following metrics: Accuracy, Precision, Recall, and F1-Score. Additionally, we measured the execution time for each classifier to assess their computational efficiency.

TABLE I

PERFORMANCE COMPARISON OF IDS CLASSIFIERS ON CICIDS 2017 DATA

Classifier	Accuracy	Precision	Recall	F1-Score	Execution Time (s)
Random Forest	99.33%	99.33%	99.32%	99.33%	4s
SVM	80.93%	72.52%	80.93%	75.66%	110s
KNN	97.53%	97.66%	97.54%	97.58%	2s
Decision Tree	99.23%	99.24%	99.23%	99.24%	1s
Gradient Boosting	99.64%	99.64%	99.68%	99.56%	118s
Logistic Regression	83.54%	83.33%	83.54%	83.14%	7s
Light GBM	99.71%	99.68%	99.71%	99.64%	5s
Proposed Ensemble Model	99.78%	99.78%	99.78%	99.78%	39s

Performance Evaluation:

The experimental results show the performance of various classifiers on the given dataset for the IDS challenge. In terms of Accuracy, Precision, Recall, and F1-Score, the proposed ensemble model exceeds all existing classifiers, attaining an astonishing 99.78% across all measures. This implies that the ensemble model can efficiently recognize and classify normal and malicious network activity.

Among individual classifiers, Random Forest, Decision Tree, and LightGBM show exceptional performance with accuracy levels exceeding 99%. The SVM and Logistic Regression classifiers, while relatively efficient in terms of execution time, demonstrate lower performance compared to other models.

A. Analysis and Implication of Results

The outcomes of the experiments highlight the effectiveness of different classifiers in detecting intrusions within the network. Random Forest, Decision Tree, and LightGBM exhibit robust performance, demonstrating their suitability for IDS tasks. On the other hand, SVM and Logistic Regression show lower accuracy, precision, recall, and F1-Score, indicating potential limitations in handling complex intrusion patterns.

The suggested ensemble framework gets the best accuracy and outperforms individual classifiers significantly. The ensemble technique takes advantage of the capabilities of many models, resulting in more robust and reliable detection of network intrusions. However, it comes at the expense of longer execution times as compared to individual models.

Overall, the experimental results indicate that LightGBM and the proposed ensemble model are promising candidates for IDS applications due to their excellent performance. However, further research and fine-tuning of hyperparameters are recommended to optimize the classifiers' performance and enhance the IDS system's overall effectiveness.

V. Conclusion and Future Discussions

We developed a novel approach for improving network and server intrusion detection using deep learning techniques in this research. We developed an ensemble model that combines XGBoost and MaxPooling1D algorithms to leverage their complementary strengths in capturing complex patterns and features from large-scale data.

We established the overarching superiority of the hypothesized hybrid detection approach over individual techniques using extensive experiments and rigorous performance evaluations on the CICIDS2017 dataset. When compared to employing XGBoost or MaxPooling1D alone, the ensemble model exhibited considerably superior accuracy, precision, recall, F1-score, and AUC-ROC. This improvement is attributed to the ensemble model's ability to effectively identify and distinguish between normal network behavior and various types of intrusions.

The achieved results hold substantial implications for real-world cybersecurity applications. The hybrid detection system's elevated accuracy and reduced false positives/negatives empower security analysts to respond swiftly to potential threats, minimizing the risk of successful attacks on critical digital infrastructures.

The success of the ensemble model highlights the importance of employing ensemble techniques in intrusion detection systems. The combination of multiple algorithms allows us to compensate for individual weaknesses and create a robust and adaptive defense mechanism capable of detecting both known and emerging intrusion patterns.

While our hybrid detection system showcases promising results, there are still challenges to address. Fine-tuning hyperparameters and further optimizing the model can potentially lead to even better performance. Additionally, scaling the system to handle larger datasets and ensuring its real-time applicability in high-traffic networks require further investigation and development.

To summarize, the research reported in this work advances intrusion detection utilizing deep learning approaches. The hybrid detection system provides an efficient and dependable solution for detecting network and server intrusions, considerably improving overall cybersecurity. As the threat landscape evolves, ongoing research and development in this area will be critical in protecting digital infrastructures from sophisticated cyber assaults.

By bridging the gap between traditional intrusion detection methods and cutting-edge deep learning techniques, our work paves the way for future innovations in cybersecurity and further strengthens the defense against cyber-attacks in an increasingly interconnected world.

ACKNOWLEDGMENT

The authors would like to express their heartfelt gratitude to the professors of the Computer Science and Engineering Department (Artificial Intelligence and Machine Learning) at Vardhaman College of Engineering for their tremendous support and assistance over the course of this project. Their advice, knowledge, and constructive input were crucial in setting the course of this study.

REFERENCES

[1] Jagadeesan, V., & Subbulakshmi, P. (2020). Intrusion detection system using deep learning: A comprehensive study. 2020 5th International Conference on Computing, Communication and Security (ICCCS). https://doi.org/10.1109/ICCCS48187.2020.9112902

[2] Chen, P., Zhou, W., & Cao, L. (2020). Deep learning for intrusion detection: A comprehensive review. Journal of Network and Computer Applications, 150, 102516. https://doi.org/10.1016/j.jnca.2020.102516

[3] Liu, Y., Wang, J., Chen, W., Li, B., & Shi, Y. (2021). Deep learning-based intrusion detection system for network security. IEEE Access, 9, 5181-5196. https://doi.org/10.1109/ACCESS.2020.3047635

[4] Alhussein, M., & Shamsuddin, S. M. (2021). Intrusion detection system using deep learning models: A comprehensive review. IEEE Access, 9, 21233-21250. https://doi.org/10.1109/ACCESS.2021.3056793

[5] Guo, Y., Du, X., Huang, C., Liu, J., & Chen, W. (2020). Deep learning-based network intrusion detection system: A review. IEEE Access, 8, 114413-114431. https://doi.org/10.1109/ACCESS.2020.3006907

[6] Lin, S., & Chen, X. (2018). Deep learning for intrusion detection: Opportunities and challenges. IEEE Intelligent Systems, 33(4), 76-81. https://doi.org/10.1109/MIS.2018.2870969

[7] Abdeldayem, M., Alazab, M., & Venkataraman, S. (2019). Deep learning techniques for intrusion detection: A review. IEEE Access, 7, 83500-83517. https://doi.org/10.1109/ACCESS.2019.2920672

[8] Alshammari, M., Alshammari, M., & Alghamdi, A. (2020). Deep learning-based intrusion detection systems: A survey. In Proceedings of the International Conference on Advanced Machine Learning Technologies and Applications (pp. 102-112). Springer. https://doi.org/10.1007/978-3-030-61370-1_9

[9] Masood, N., & Khan, S. A. (2019). A comprehensive review of deep learning techniques for network anomaly detection. Journal of Network and Computer Applications, 136, 20-43. https://doi.org/10.1016/j.jnca.2019.04.013

[10] Shen, Y., Xu, L., & Fu, J. (2017). Deep learning in intrusion detection systems: A survey. IEEE Access, 5, 21954-21966. https://doi.org/10.1109/ACCESS.2017.2760337

[11] Lin, Q., & Zuo, J. (2019). Deep learning-based intrusion detection in computer networks. Journal of Ambient Intelligence and Humanized Computing, 10(5), 1703-1716. https://doi.org/10.1007/s12652-018-0926-4

[12] Canedo, A., & Moreira, A. (2020). Intrusion detection systems using deep learning and feature selection. Future Generation Computer Systems, 105, 540-555. https://doi.org/10.1016/j.future.2019.11.002

[13] Wang, W., & Luo, J. (2020). Intrusion detection system based on deep learning in cloud computing environment. In 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (pp.1342-1347). IEEE. https://doi.org/10.1109/ITNEC51168.2020.9171182

[14] Firdhous, M., Balasubramaniam, A., & Kausar, A. S. (2019). A deep learning approach for intrusion detection using recurrent neural networks. International Journal of Advanced Computer Science and Applications, 10(7), 168-174. https://doi.org/10.14569/IJACSA.2019.0100722

[15] Pham, T. H., Mai, T. T., Tran, T. M., Nguyen, H. T., & Le, A. A. (2020). Deep learning-based hybrid model for network intrusion detection system. Journal of Ambient Intelligence and Humanized Computing, 11(7), 2911-2924. https://doi.org/10.1007/s12652-020-02041-y

[16] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, "Tree-Based Intelligent Intrusion Detection System in Internet of Vehicles," in 2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9013892.

[17] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles," IEEE Internet of Things Journal, vol. 9, no. 1, pp. 616-632, Jan. 1, 2022, doi: 10.1109/JIOT.2021.3084796.

[18] L. Yang, A. Shami, G. Stevens, and S. DeRusett, "LCCDE: A Decision-Based Ensemble Framework for Intrusion Detection in The Internet of Vehicles," in 2022 IEEE Global Communications Conference (GLOBECOM), 2022, pp. 1-6, doi: 10.1109/GLOBECOM48099.2022.10001280.

[19] S. Horchreiter and J. Schmidhuber, "Long Short-Term Memory," Neural Comput., vol. 9, no. 8, pp. 1735-1780, 1997. doi: 10.1162/neco.1997.9.8.1735