IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13333

DEEP NEURAL FUZZY SYSTEM FOR INTRUSION DETECTION

Vignesh A Palan[1], Rathika Ramesh Gaunskar[2], Prashanth[3], Pruthviraj[4], Dr. Amirthavalli.M[5]

Student, Dept. of Artificial Intelligence & Machine Learning, Mangalore Institute of Technology & Engineering, Moodabidri, India[1-4]

Professor, Dept. of Artificial Intelligence & Machine Learning, Mangalore Institute of Technology & Engineering, Moodabidri, India[5]

Abstract: This project presents an innovative intrusion detection approach that utilizes the combined capabilities of deep neural networks (DNN), multilayer perceptron (MLP), long short-term memory (LSTM), convolutional neural networks (CNN), and fuzzy logic within a unified deep neuro- fuzzy framework. The key differentiator of this system lies in its strategic integration with Principal Component Analysis (PCA) during the training phase, which aims to increase feature representation and overall model performance. A distinctive feature of this system is the incorporation of PCA, a critical pre-processing step that plays a key role in extracting significant features from the CICIDS2017 and CICIDS2019 dataset. By using PCA, the dimensionality of the data set is substantially reduced, allowing the system to focus on the essential information necessary for effective intrusion detection. This dimensionality reduction leads to a remarkable improvement in feature representation, resulting in excellent model performance. PCA integration acts as a catalyst in the training phase, facilitating the extraction of relevant information and optimizing the deep neuro-fuzzy system for increased accuracy and robust generalization capabilities. The results show that this innovative approach not only improves the accuracy of intrusion detection, but also improves the system's ability to adapt to diverse and dynamic threats. Overall, the strategic use of PCA coupled with a unified deep neuro-fuzzy framework sets this system apart, making it a promising advancement in intrusion detection.

Keywords: Intrusion detection, Deep neural networks (DNN), Principal Component Analysis (PCA) Deep neuro-fuzzy framework

I. INTRODUCTION

In today's rapidly evolving digital realm, intrusion detection is a critical defense mechanism necessary to protect networks from malicious activity. This importance is even more pronounced in light of the expanding attack surface represented by a number of interconnected devices. As technology advances, the proliferation of the Internet of Things (IoT) has skyrocketed, bringing a complex network of devices that require robust intrusion detection mechanisms. However, the effectiveness of intrusion detection systems faces numerous challenges, especially when it comes to face recognition and detection in IoT environments. The exponential growth of IoT devices contributes to an expanding attack surface, making detection and prevention of cyberattacks on IoT infrastructure increasingly challenging. This spread introduces a large number of devices, each of which is potentially vulnerable to security threats. In addition, the interconnected nature of IoT devices results in diverse and heterogeneous traffic traversing the Internet.

The challenge lies in distinguishing normal behavior from anomalous patterns in this complex network of interconnected devices, which complicates the identification and classification of potential security threats. Rapid detection in the IoT environment is paramount, given the potential for malicious hackers to exploit vulnerabilities in the rapidly evolving infrastructure. Early identification of attacks is critical to mitigating potential damage and securing sensitive information. To solve these problems, it becomes necessary to integrate different deep learning (DL) models into a separate intrusion detection ensemble. However, achieving high accuracy and low false-positive rates across different datasets and classification scenarios is a significant hurdle in building a reliable and efficient intrusion detection system. This project aims to overcome these challenges by introducing a comprehensive approach that combines deep neural networks, multilayer perceptrons. long short-term memory networks, convolutional neural networks, and fuzzy logic within a unified deep neuro-fuzzy framework. In addition, the strategic use of principal component analysis (PCA) in the training phase improves feature representation and optimizes the system for accurate and robust intrusion detection. This innovative methodology aims to provide a solution that not only addresses the challenges posed by the rapid growth of IoT devices, but also ensures rapid detection and high accuracy in the face of diverse and heterogeneous IoT traffic.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13333

II. LITERATURE SURVEY

In paper [1]A stacking ensemble of deep learning models for IoT intrusion detection proposes a method where Ensemble of DL models DIS-IoT is able to detect attacks in the IoT environment while maintaining a low FP combining different models into an integrated stacking ensemble offers an excellent solution as an IDS

In paper [2]Intrusion detection in networks using crow search optimization algorithm with adaptive neuro-fuzzy inference system proposed a method where we make use of ANFIS which is a fusion of a fuzzy inference system (FIS) and ANN which has the benefits of both ANN and FIS.

In paper [3]Hybrid optimization enabled deep learning technique for multi-level intrusion detection proposed a intrusion detection technique on the basis of a hybrid optimization-based Deep learning algorithm.The proposed technique did not analyze the robustness of the classifiers against adversarial attacks, noise or missing data, which may affect the accuracy and reliability of the intrusion detection system

III. SCOPE AND METHODOLOGY

Aim of the project:In the dynamic field of cybersecurity, intrusion detection is critical against sophisticated cyber threats. This project introduces DNFS (Deep Neural-Fuzzy Stacking), a state-of-the-art ensemble model combining four DL architectures – MLP, DNN, CNN and LSTM. DNFS takes advantage of their strengths and ensures high accuracy and a low false positive rate. Extensive evaluations using the CICIDS2017 and CICIDS2019 dataset verify the reliability of DNFS in various network environments. Its focus on accuracy and low FPR is demonstrated through rigorous evaluations, representing a significant advance in intrusion detection.

The proposed system, named DNFS (Deep Neural-Fuzzy System), is an advanced intrusion detection solution that integrates deep learning and fuzzy logic. It uses a unique combination of neural network architectures, including multilayer perceptron (MLP), deep neural network (DNN), convolutional neural network (CNN), and long-term memory (LSTM). External activities such as data preprocessing and principal component analysis (PCA) increase the system's ability to adapt to different network environments. The DNFS model is strategically designed to detect and classify intrusions with high accuracy and low false positive rates, demonstrating adaptability to evolving cyber threats.

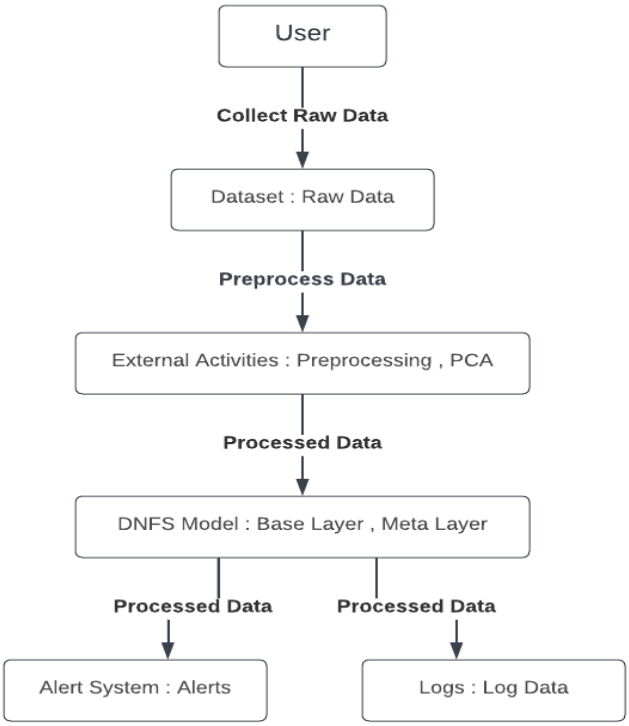

fig 1. Proposed System

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13333

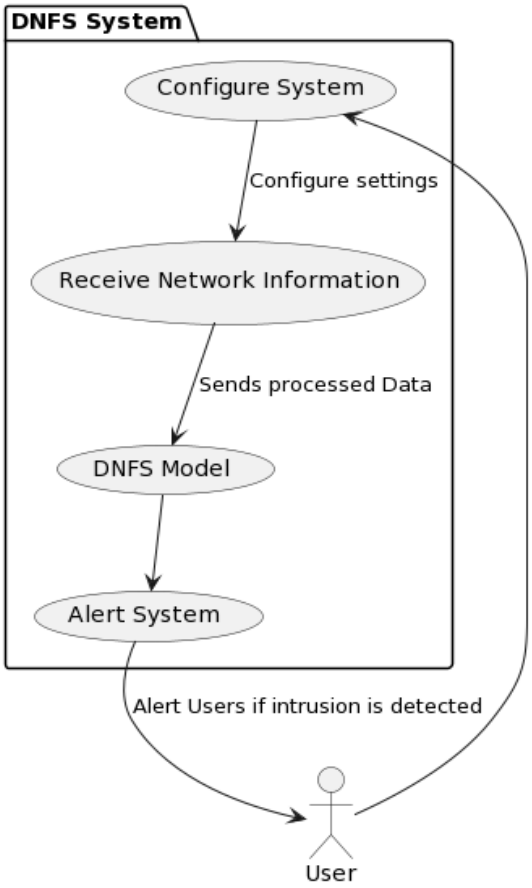

fig 2. Use Case Diagram

The use case diagram for the DNFS system outlines the key interactions between actors and system functions. Users and security professionals interact with the system through use cases such as configuring the system, monitoring intrusions, and receiving alerts. These use cases are directly linked to the DNFS model and alerting system, highlighting the user-centric design of the system. This use-case approach ensures that the system meets the practical needs and expectations of users and increases its usability and effectiveness.

IV. CONCLUSIONS

In conclusion, the DNFS model represents a significant milestone in the field of intrusion detection and offers a robust solution to combat the evolving cyber threat landscape. By leveraging the collective performance of multiple DL architectures within a stack ensemble, DNFS achieves the high accuracy and low false positive rate necessary for effective threat detection.

Through extensive evaluations on the CICIDS2017 dataset, DNFS demonstrates its reliability and adaptability in various network environments, surpassing stringent performance standards. With its focus on accuracy and excellence in distinguishing between normal and malicious activities, DNFS heralds a new era in intrusion detection and promises improved security measures for digital ecosystems.

REFERENCES

[1].Lazzarini, R., Tianfield, H. and Charissis, V., 2023. A stacking ensemble of deep learning models for IoT intrusion detection. Knowledge-Based Systems, 279, p.110941..

[2].Manimurugan, S., Majdi, A.Q., Mohmmed, M., Narmatha, C. and Varatharajan, R., 2020. Intrusion detection in networks using crow search optimization algorithm with adaptive neuro-fuzzy inference system. *Microprocessors and Microsystems*, *79*, p.103261.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13333

[3].GSR, Emil Selvan, et al. "Hybrid optimization enabled deep learning techniques for multi-level intrusion detection." Advances in Engineering Software 173 (2022): 103197.

[4].Basak, S., Jia, R. and Lei, C., 2018, August. Face recognition using fuzzy logic. In 2018 IEEE International Conference on Information and Automation (ICIA) (pp. 1317-1322). IEEE.

[5].Chacon-Murguia, M.I. and Gonzalez-Duarte, S., 2011. An adaptive neural-fuzzy approach for object detection in dynamic backgrounds for surveillance systems. IEEE Transactions on Industrial Electronics, 59(8), pp.3286-3298.

[6].Talpur, N., Abdulkadir, S.J., Alhussian, H., Hasan, M.H., Aziz, N. and Bamhdi, A., 2023. Deep Neuro-Fuzzy System application trends, challenges, and future perspectives: A systematic survey. Artificial intelligence review, 56(2), pp.865-913.

[7].Matthew Vincent Mahoney. A machine learning approach to detecting attacks by identifying anomalies in network traffic. TRCS-2003-13, Melbourne, Florida; 2003.

[8].Venkateswaran, N. and Prabaharan, S.P., 2022. An Efficient Neuro Deep Learning Intrusion Detection System for Mobile Adhoc Networks. EAI Endorsed Transactions on Scalable Information Systems, 9(6), pp.e7-e7.

[9].Manju, A., Revathi, A., Arivukkarasu, M., Hariharan, S., Umarani, V., Chen, S.Y. and Wang, J., 2023. Fuzzy Rule-Based Model to Train Videos in Video Surveillance System. Intelligent Automation & Soft Computing, 37(1).

[10].Nawaratne, R., Alahakoon, D., De Silva, D. and Yu, X., 2019. Spatiotemporal anomaly detection using deep learning for real-time video surveillance. *IEEE Transactions on Industrial Informatics*, *16*(1), pp.393-402.