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 6, June 2024

DOI: 10.17148/IJARCCE.2024.13674

IntrusiShield: Navigating Safely Through Cyber Tides

A Jayakar[1], Abhijeet Biradar[2], Basavaraj Sajjan[3], Darshan H[4]

Student, Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur, India [1]

Student, Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur, India [2]

Student, Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur, India [3]

Student, Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur, India [4]

Abstract: This paper presents INTRUSISHIELD, an intelligent, multi-layered Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) designed to navigate the evolving landscape of cyber threats. By integrating traditional rule-based methods with advanced machine learning algorithms, INTRUSISHIELD provides real-time monitoring and automated response capabilities to detect and mitigate both known and unknown threats. The system continuously updates its knowledge base to adapt to new attack patterns, ensuring robust network security. Additionally, INTRUSISHIELD incorporates a user-friendly Streamlit web application for easy monitoring and management of IDS functionalities. Extending this approach, a separate Streamlit app allows users to upload files for real-time detection of malicious content, enhancing the system's preventive capabilities. This comprehensive solution demonstrates significant improvements in threat detection, mitigation, and user accessibility, thereby strengthening overall cybersecurity defenses.

Keywords: Intrusion Detection System, Intrusion Prevention System, Machine Learning, Cybersecurity, Real-time Monitoring, Streamlit

I. INTRODUCTION

The rapid evolution of cyber threats poses significant challenges to existing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Traditional systems often struggle with high false alarm rates and are ineffective against sophisticated attack methods such as zero-day exploits and polymorphic malware. This paper introduces INTRUSISHIELD, a novel IDS and IPS solution that leverages machine learning to provide adaptive and accurate threat detection and prevention. By combining traditional rule-based methods with advanced analytics, INTRUSISHIELD aims to strengthen network security against an increasingly complex landscape of cyber attacks.

In addition to incorporating established detection mechanisms, our project integrates a user-friendly Streamlit web application, enhancing accessibility and usability for monitoring and managing IDS. Moreover, we extend our approach to create an IPS, utilizing the same machine learning models to detect and prevent malicious files. This IPS functionality is also accessible through a separate Streamlit app, where users can upload files and receive immediate feedback on potential threats. To build a robust framework, our research draws on various foundational studies in the field of cybersecurity and machine learning:

[1]Gascon, H., Orfila, A., Blasco, J. (2011): Analysis of update delays in signature-based network intrusion detection systems highlighted the latency issues in traditional IDS and underscored the need for more dynamic and real-time solutions.

[2]Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., Malli, M. (2020): Cyber-physical systems security research identified limitations and future trends, particularly emphasizing the role of machine learning in overcoming these challenges.

[3]Ammar, A., et al. (2015): Proposed a decision tree classifier for intrusion detection priority tagging, demonstrating the potential for machine learning algorithms to enhance detection accuracy and reduce false positives.

[4]Almutairi, A.H., Abdelmajeed, N.T. (2017): Developed an innovative signature-based intrusion detection system using parallel processing and minimized database techniques, which informed our approach to optimizing IDS performance.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024
DOI: 10.17148/IJARCCE.2024.13674

[5]Yang, L., Shami, A. (2022): Their work on a transfer learning and optimized CNN-based IDS for the Internet of Vehicles provided a blueprint for leveraging advanced neural network architectures and transfer learning in intrusion detection(2201.11812v1).

These studies collectively underscore the necessity of integrating machine learning techniques to enhance the detection capabilities of IDS and IPS, paving the way for our development of INTRUSISHIELD

II. METHODOLOGY

The methodology involves a multi-step process combining data acquisition, transformation, model training, optimization, and ensemble learning to build an effective system for detecting and preventing cyber intrusions. This process is divided into two main components: the Intrusion Detection System (IDS) and the Intrusion Prevention System (IPS).

A. Intrusion Detection System (IDS)

1) Data Collection : The IDS collects network traffic data from various sources, including simulated environments and real-world network setups. This dataset encompasses both normal and malicious traffic patterns to ensure comprehensive coverage.

2) IDS Data Transformation : The network traffic data is normalized or scaled to transform it into a uniform distribution, which significantly improves model performance, especially for Convolutional Neural Networks (CNNs). The normalized network data is converted into image formats, leveraging CNN models' capabilities in processing image data. Each image is labelled to indicate whether it represents normal behaviour or a specific type of attack. These labels are essential for training the CNN models in a supervised manner.

3) Model Training and Validation : The CNN models are trained using the labelled image data representing network traffic. Each model's performance is evaluated based on detection accuracy and false positive rates. Rigorous testing and validation are conducted for IDS models to ensure reliability and effectiveness.

4) Streamlit-based GUI for IDS : A user-friendly graphical interface is developed using Streamlit, allowing users to monitor network traffic and analyse detected threats in real-time. The IDS outputs the classification of the network traffic as either "Attack-free" or one of several attack types (e.g., DoS, Fuzzy, Gear Spoofing, RMP spoofing).

B. Intrusion Prevention System (IPS)

1) Data Collection : The IPS focuses on collecting datasets of benign and malicious files. These datasets are sourced from publicly available repositories and proprietary databases to ensure diversity and comprehensiveness.

2) IPS Data Transformation : Relevant features that distinguish between benign and malicious files are extracted. This step includes metadata, file structure, and behaviour analysis. Similar to IDS, the extracted features of files are transformed into image formats to utilize CNNs effectively.

3) Model Training : The same CNN models used for IDS are retrained using the transformed file data to detect malicious files. This approach leverages the robustness of the pre-trained models and adapts them to the file-based intrusion prevention context.

4) Streamlit-based GUI for IPS : A separate Streamlit application is developed for the IPS, enabling users to upload files and perform real-time malware analysis. The interface is designed to be accessible to users with varying levels of technical expertise. Users can upload files through the IPS GUI for analysis.

The uploaded files are processed by the machine learning models to determine their legitimacy, providing immediate feedback on potential threats. The IPS outputs the classification of files as either "Benign" or "Malicious," along with details of the type of threat detected.

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 6, June 2024

DOI: 10.17148/IJARCCE.2024.13674

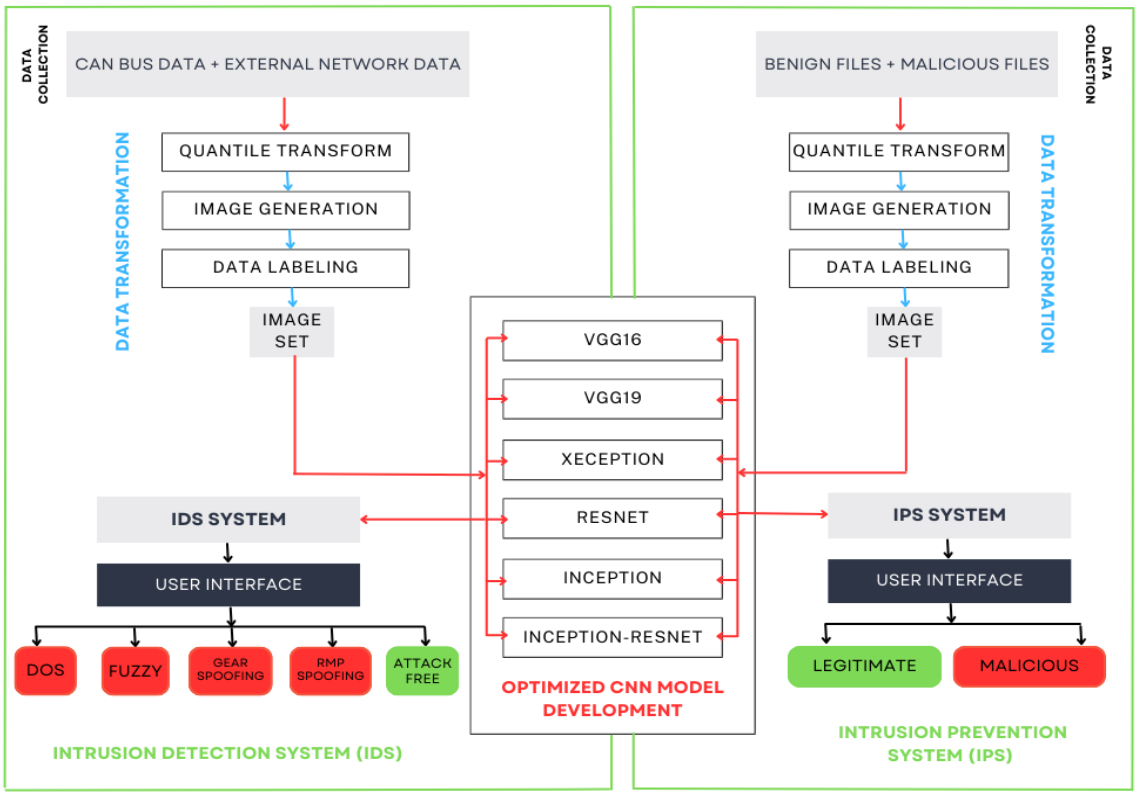

Fig. 1 Comprehensive Workflow Diagram Illustrating the Development of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)

III. RESULT ANALYSIS

In comparison to other models used in Intrusion Detection Systems (IDS), Inception stands out due to its unique architecture that incorporates parallel convolutional operations and multi-scale feature extraction. While achieving a training accuracy of 98.86% and a prediction accuracy of 86.00%, Inception surpasses simpler architectures like VGG16 and VGG19, which typically exhibit strong performance but may not capture as nuanced patterns in network traffic data.

Moreover, Inception-ResNet-v2, another advanced architecture, may offer similar or slightly improved performance due to its hybrid nature combining Inception and ResNet features, yet it often requires more computational resources. ResNet, known for its depth and resilience to vanishing gradients, excels in capturing complex dependencies but may not match Inception's ability to handle multi-scale features in IDS applications. Overall, Inception's balance between computational efficiency and accuracy makes it a compelling choice for IDS, particularly in detecting diverse and evolving network threats with high fidelity.

For the Intrusion Prevention System (IPS), which focuses on detecting malicious files, the same optimized CNN models used for IDS were retrained and adapted. The IPS achieved a detection accuracy of 96% and a recall rate of 98%, effectively identifying malicious files. In comparison to simpler models like VGG16 and VGG19, which may not perform as well in file analysis due to their architecture's limitations in handling varied file attributes, Inception excels by leveraging its multi-scale feature extraction capabilities.

While Inception-ResNet-v2 and ResNet provide strong performance, their higher computational demands can be a limiting factor in real-time file analysis scenarios. The use of Inception in the IPS context strikes a balance between performance and computational efficiency, making it a robust solution for real-time detection of malware in files. The Streamlit-based GUI for IPS further enhances usability, providing users with immediate analysis results and maintaining system scalability and performance during simultaneous analyses.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024
DOI: 10.17148/IJARCCE.2024.13674

IV. CONCLUSION

INTRUSISHIELD is a significant advancement in cybersecurity, integrating traditional rule-based methods with advanced machine learning to create a robust Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). This system effectively addresses modern cyber threats, including zero-day exploits and polymorphic malware, which often bypass conventional defences. The IDS leverages advanced CNN architectures like Inception for precise detection of malicious network traffic, while the IPS focuses on identifying and preventing malicious files. Both systems feature a Streamlit-based user interface, making real-time monitoring and threat mitigation accessible to all users.

INTRUSISHIELD continuously adapts to new attack patterns, enhancing its detection capabilities over time. Its real-time monitoring and automated response features provide swift threat mitigation, strengthening overall network security. By combining advanced machine learning with practical usability, INTRUSISHIELD offers a powerful, comprehensive solution for modern cybersecurity challenges, ensuring robust protection against a complex and evolving threat landscape.

ACKNOWLEDGMENT

We express our sincere gratitude to the Department of Computer Science and Engineering at SSIT, Tumakuru, for their support and guidance throughout this project. Special thanks to our project advisor, **Dr.Channakrishna Raju**, for their invaluable insights and encouragement. We also acknowledge the contributions of our colleagues and peers, whose feedback and collaboration were instrumental in the development and refinement of INTRUSISHIELD. Our thanks extend to the creators of the datasets and tools that facilitated our research and experimentation. Finally, we are grateful to our families and friends for their unwavering support and understanding during the course of this project. Their encouragement has been a constant source of motivation. Thank you to everyone who has contributed to making this project a success.

REFERENCES

[1]. Gascon, H., Orfila, A., Blasco, Analysis of update delays in signature-based network intrusion detection systems. Computers Security 30, 613–624 [2011].
[2]. J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli . Cyberphysical systems security:Limitations, issues and future trends.[2020].
[3]. Ammar, A., et al., A decision tree classifier for intrusion detection priority tagging. Journal of Computer and Communications 3, 52. [2015].
[4]. Almutairi, A.H., Abdelmajeed, N.T., Innovative signature based intrusion detection system: Parallel processing and minimized database, in: 2017 International Conference on the Frontiers and Advances in Data Science (FADS), IEEE. pp. 114–119. [2017].
[5]. K. Hattasin, S. Kaewvichit, W. Niwatananun, and C. Ruengorn, "Modification and evaluation of tools for pharmaceutical care of patients with schizophrenia in non-psychiatric hospitals," *Songklanakarin Journal of Science and Technology*, vol. 40, no. 3, pp. 550-554, May-Jun. 2018.
[6]. S. Walker-Roberts, M. Hammoudeh, O.Aldabbas, M. Aydin, and A. Dehghantanha , Threats on the horizon:Understanding cyber-physical systems. Heliyon 5, e01802. [2018].
[7]. J. Preden, "Generating situation awareness in cyberphysical systems: Creation and exchange of situational information,IEEE [2020].
[8]. Q. V. Le and T. Mikolov, Distributed representations of sentences and documents,IEEE, pp. 152-156 [2007].
[9]. Friedman, J.H.,Greedy function approximation: a gradient boosting machine. Annals of statistics, 1189–1232 [2001].