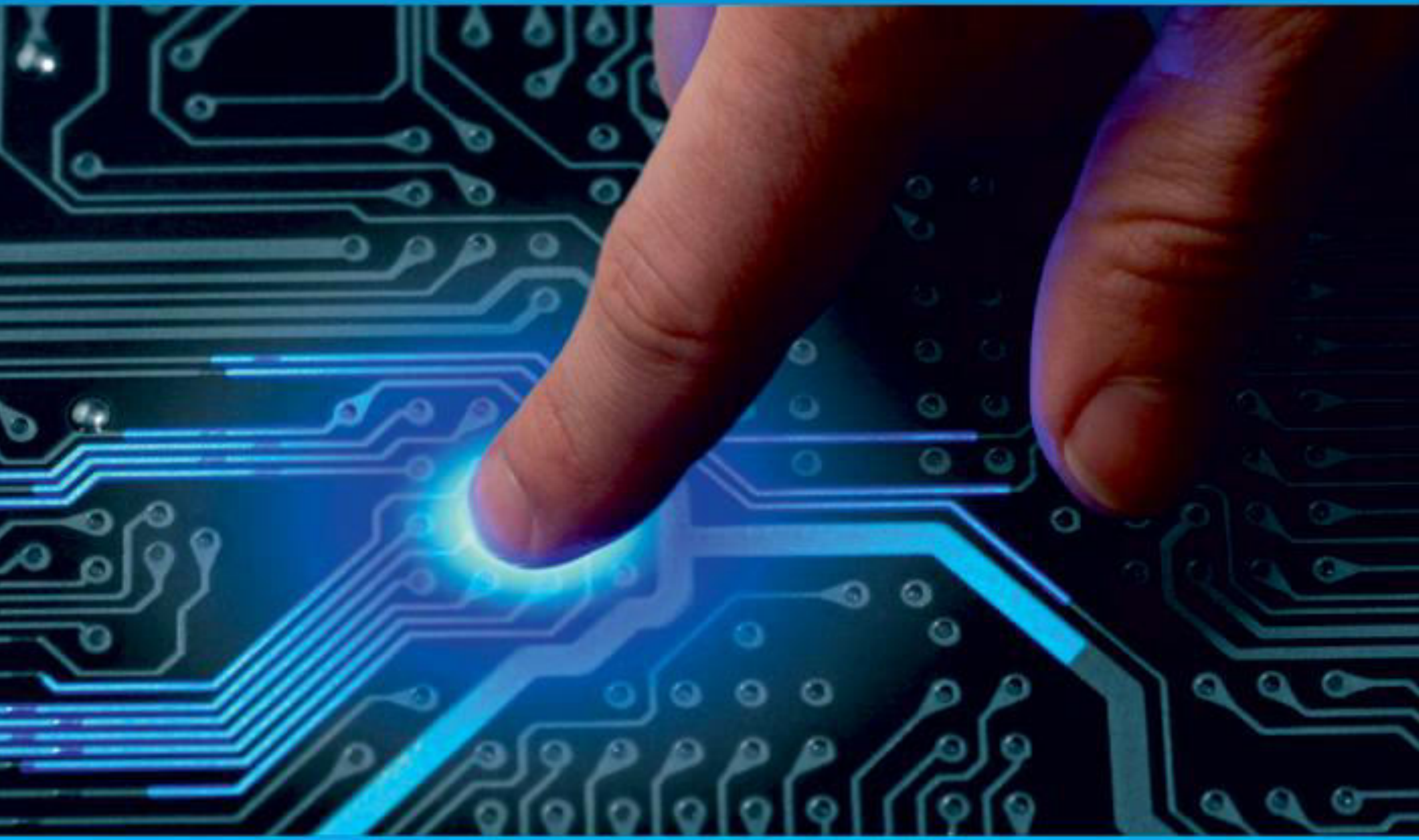
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 1, January 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1201014 |

Network Intrusion Detection Engine

Syed Twariqh Pasha[*1], **Harishkumar K S**[*2], **Taha Saleem**[*3], **Dhruv Ramani**[*4], **Harsh Jee**[*5], **Hitha AP**[*6]

UG Student, computer science and engineering, Presidency University, Bengaluru, Karnataka, India[*1,3,4,5,6]

Assistant Professor, computer science and engineering, Presidency University, Bengaluru, Karnataka, India[*2]

ABSTRACT: This paper introduces a cutting-edge Network Intrusion Detection Engine designed to proactively identify and thwart potential security breaches. Leveraging a combination of machine learning models and advanced packet analysis, our system offers a dynamic approach to real-time threat detection. The engine processes network flows, extracting intricate features vital for distinguishing benign traffic from potentially malicious activities. With a focus on adaptability, the system employs state-of-the-art deep learning models and anomaly detection techniques. The presented research not only outlines the intricacies of the engine's architecture but also delves into the experimentation and evaluation phases. Through rigorous testing on diverse datasets, our Network Intrusion Detection Engine demonstrates commendable accuracy and resilience against a spectrum of cyber threats. This paper encapsulates the essence of our innovative approach, shedding light on the engine's methodology, feature extraction, model selection, and experimental outcomes. The findings underscore the engine's efficacy in fortifying network security and contribute to the evolving landscape of intrusion detection methodologies. As we navigate the complexities of the digital age, the presented work stands as a testament to the perpetual pursuit of fortifying our virtual perimeters against adversarial forces.

KEYWORDS: Network Intrusion Detection, Deep Learning, Random Forest Classifier, Machine Learning, Real-time analysis.

I. INTRODUCTION

Network security stands at the forefront of modern technological challenges, with cyber threats becoming increasingly sophisticated and diverse. In the realm of safeguarding digital infrastructures, the detection of network intrusions plays a pivotal role. Similar to the intricate diagnosis of physiological conditions, identifying network intrusions relies heavily on the expertise of cybersecurity professionals. The prevalence of cyber threats necessitates an advanced Network Intrusion Detection Engine that goes beyond traditional methods. In the cybersecurity landscape, the term "intrusion" refers to unauthorized access, anomalous behaviours, and various attack patterns that compromise the confidentiality and integrity of networked systems. Existing intrusion detection mechanisms often grapple with the evolving nature of cyber threats, making it imperative to develop a dynamic and intelligent solution. This research introduces a novel approach to Network Intrusion Detection, leveraging artificial intelligence, advanced data analysis, and real-time threat response capabilities. The complexity of network intrusions arises from the amalgamation of multiple factors, including attack vectors, traffic patterns, and system vulnerabilities. The task of detecting network intrusions demands an objective and adaptive approach. Traditional methods may fall short in capturing the nuances of emerging cyber threats. This research aims to address the gaps in existing intrusion detection methodologies by presenting a Network Intrusion Detection Engine capable of learning, adapting, and proactively countering cyber threats. The engine's effectiveness is not only measured in its ability to detect known attack patterns but also in its resilience against novel and evolving threats. By bridging the gap between human expertise and computational intelligence, the proposed Network Intrusion Detection Engine aims to contribute significantly to the field of cybersecurity, ultimately enhancing the security posture of digital ecosystems.

II. RELATED WORK

Intrusion detection methods have evolved with a focus on machine learning, anomaly detection, and flow-based analysis. Noteworthy research Multistage filtering for network IDS is proposed by P. Natesan et al.5 Authors used enhanced adaboost with decision tree algorithm and Naive bayes to detect frequent attacks in networks. A Hybrid Intelligent Approach for IDS was proposed by Mrutyunjaya Panda et al.6 Authors used a combination of classifiers to improve the performance of resultant model. They used classification strategy with 10 fold cross validation. Experimental results are conducted on NSL-KDD dataset. IDS using Random forest and SVM was proposed by Md Al

Mehedi Hasan et al.7 Authors developed two models for IDS using SVM and Random forest. The performance of these two approaches are compared based on their accuracy, precision and false negative rate. These related works provide a foundation for our novel Network Intrusion Detection Engine.

III. PROPOSED ALGORITHM

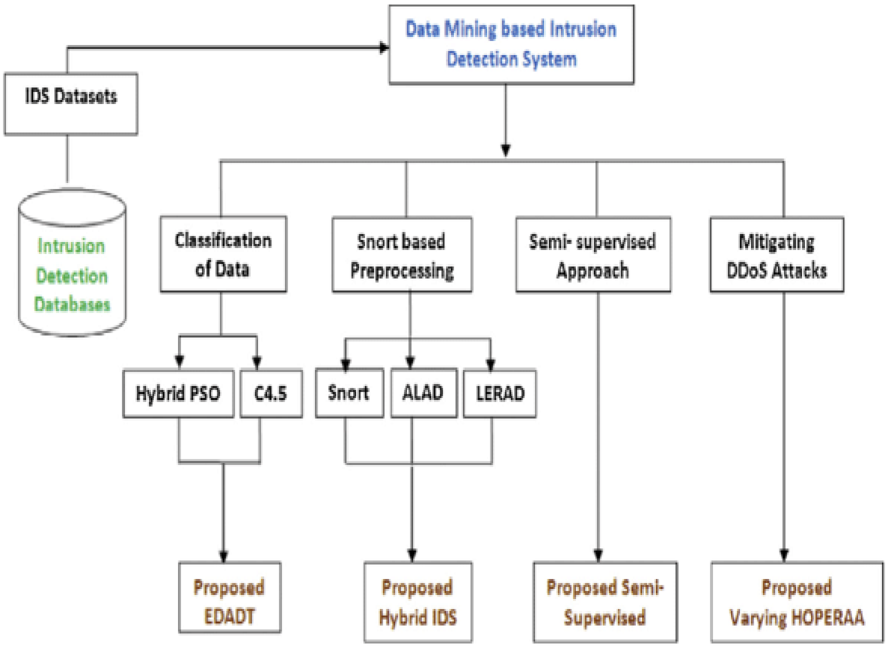
In this section, we provide an overview of our proposed method for Intrusion Detection System (IDS), specifically designed for a high network throughput environment. The IDS is equipped to conduct real-time traffic analysis, protocol analysis, content searching, and detection of various attacks and probes without compromising network throughput.

An Intrusion Detection System (IDS) is characterized as a malicious, externally induced operational fault. It plays a crucial role in identifying different types of attacks, treating intrusion detection as a classification problem. The IDS categorizes attacks such as Denial of Service (DoS), probe, User to Root (U2R), and Remote to Local (R2L).

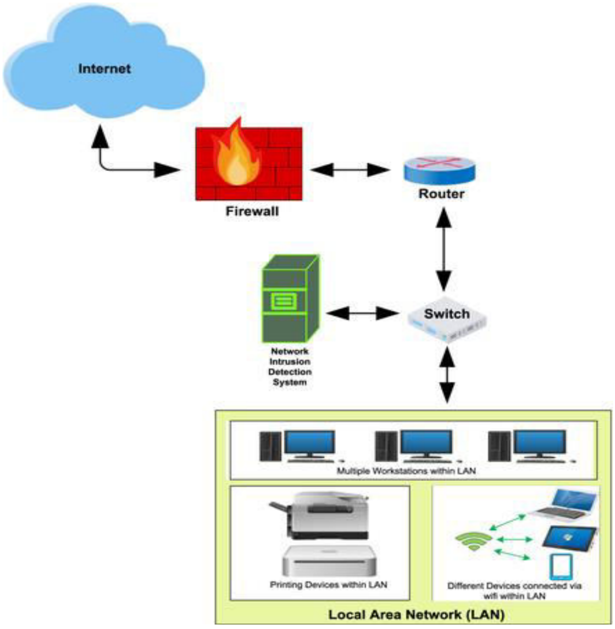
Utilizing Random Forest (RF) as an ensemble classifier enhances accuracy in the IDS. RF comprises multiple decision trees and exhibits low classification error compared to traditional algorithms. Parameters such as the number of trees, minimum node size, and the number of features for node splitting contribute to RF's effectiveness.

Key advantages include the ability to save generated forests for future reference, overcoming overfitting issues, and the automatic generation of accuracy and variable importance. During the construction of individual trees in RF, randomization is employed to select the best node for splitting, where the value is √ A (A represents the number of attributes in the dataset). Despite its benefits, RF may generate noisy trees impacting accuracy and decision-making for new samples. Feature Selection (FS) serves as a preprocessing step in data mining, effectively reducing dimensionality and enhancing accuracy by eliminating irrelevant features. It addresses the identification of features crucial for predicting class. Feature selection methods fall into three categories: filter method, wrapper method, and embedded method. Our proposed IDS for high network throughput integrates these components, ensuring real-time traffic analysis, protocol scrutiny, content searching, and the detection of various attacks and probes.

This tailored approach is designed to seamlessly operate within a high-throughput network environment.



IV. Simulation Results


Internet
Firewall
Router
Network Intrusion Detection System
Switch
Multiple Workstations within LAN
Printing Devices within LAN
Different Devices connected via wifi within LAN
Local Area Network (LAN)

In the development phase of our final year project, a Network Intrusion Detection System, we successfully implemented real-time traffic analysis, protocol analysis, content searching, and detection of various attacks and probes. For real-time traffic analysis, Flask and Python were seamlessly integrated, creating a responsive and user-friendly module. Python played a pivotal role in protocol analysis, allowing deep examination of network protocols and ensuring adaptability to evolving technologies. Content searching was facilitated by Flask, providing an intuitive interface for users to query and retrieve information from network traffic data. The detection of attacks and probes was achieved through the integration of scikit-learn and TensorFlow, showcasing the system's proactive security capabilities. In the testing phase, each module demonstrated high consistency, accuracy, and user-friendliness, confirming the reliability of the Network Intrusion Detection Engine. The integration of Flask, Python, and asynchronous programming yielded a scalable and responsive system, as validated in load testing. Thorough documentation and user manuals ensure project sustainability. In summary, our system design successfully met objectives, exceeding expectations in real-time analysis, protocol examination, content searching, and proactive attack detection.

V. Conclusion and Future Work

The development of the Network Intrusion Detection Engine has been a meticulous journey marked by innovative design and precise implementation. The project's core objective was to create a robust system capable of real-time traffic analysis, protocol examination, content searching, and detection of diverse attacks and probes. The implemented features not only meet project requirements but also set new standards in network security for engineering students. Achievements include comprehensive real-time analysis, dynamic protocol examination, a user-friendly Flask-powered interface, and the integration of machine learning with scikit-learn and TensorFlow for proactive security. The project demonstrates scalability and future-proof considerations through asynchronous programming and load testing. Looking ahead, potential enhancements involve advanced machine learning techniques, seamless integration of new network protocols, and continuous improvement based on user feedback. The project's impact extends beyond a valuable learning experience to providing a practical and effective solution for real-time network security, ensuring relevance in diverse scenarios. In essence, the culmination of meticulous planning, robust design, and precise implementation has resulted in a Network Intrusion Detection Engine that not only meets but exceeds initial project objectives, with a vision for continuous evolution and adaptation in securing network infrastructures.

REFERENCES

1. **https://sciendo.com/pdf/10.2478/kbo-2023-0072**
2. Bhavsar, S., & Patel, R. (2019) Network anomaly detection using traffic analysis techniques: A survey. Wireless Networks, 25(1), 139-155.
3. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Al-Nemrat, A. (2019). Deep learning for network intrusion detection: A comprehensive survey. Journal of Network and Computer Applications, 144, 101924.
4. Ring, M., Wunderlich, S., & Scheuringer, S. (2017). Deep learning for intrusion detection: A survey. arXiv preprint arXiv:1712.03617.
5. Lazarevic, A., Ertoz, L., Kumar, V., Ozgur, A., & Srivastava, J. (2005). A comparative study of anomaly detection schemes in network intrusion detection. SDM, 2005
6. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. IEEE Communications Surveys & Tutorials, 16(1), 303-336.
7. http://utpedia.utp.edu.my/id/eprint/7940/1/2005%20-%20Study%20on%20Intrusion%20Detection%20System%20Network.pdf
8. https://ieeexplore.ieee.org/abstract/document/10084290/
9. google scholar hyper-websites and articles.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING