Grenze International Journal of Engineering and Technology, June Issue

Deploying an Advanced Intrusion Detection System (IDS) to Detect and Respond to Potential Breache and Malicious Activities

M. Senthil Kumar[1], B. Chidhambara Rajan[2], Harish P[3], Kishore Kumar R[4] and Vijayaraghavan N[5]
[1]Professor, Department of Cyber Security, SRM Valliammai Engineering College
Email: msen1982@gmail.com
[2]Director, SRM Valliammai Engineering College
Email: director@srmvalliammai.ac.in
[3-5]UG Scholar, Department of Cyber Security, SRM Valliammai Engineering College,
Email: h00146970@gmail.com, kishorerajendran2003@gmail.com, raghavcybe@gmail.com

Abstract*— The implementation of an advanced Intrusion Detection System (IDS) represents a pivotal step in fortifying cybersecurity, employing Machine Learning (ML) for heightened efficacy in identifying and countering a diverse array of potential breaches and activities. The random forest method is used as the heart of this system and an ensemble learning approach that amalgamates predictions from numerous decision trees, culminating in a more accurate and resilient predictive model. This algorithm's adaptability proves particularly advantageous in the intricate and noisy landscape of intrusion detection. The IDS undergoes comprehensive training on an extensive labeled internet traffic dataset that includes patterns from both malicious and legitimate sources. This strategic training equips the system with the ability to discern the nuanced patterns associated with malicious activities, enabling accurate detection of new and emerging threats. Upon detecting any suspicious activity, using a dedicated SMTP domain server, the IDS quickly creates alerts and sends them via email to the incident response team. This streamlined communication ensures the immediate notification of potential incidents, allowing the response team to act in a timely and appropriate manner. The random forest method and machine learning are combined to enable the IDS to attain an impressive degree of robustness and accuracy. This proficiency is further enhanced by its adaptive capabilities, enabling it to evolve and effectively counter new and emerging threats. The synergy of ML and the random forest algorithm, in addition to the email alerting system, markedly elevates the ability of the company to recognize and react to online threats. This all-encompassing strategy not only reduces the chance of data breaches but also strengthens cybersecurity posture and proactivity. In the dynamic landscape of digital security, this advanced IDS serves as a critical component in safeguarding organizations against the evolving and sophisticated nature of cyber threats.

***Index Terms*— Intrusion Detection System (IDS), Anomaly Detection, Behavioral Analysis, Threat Detection.**

I. INTRODUCTION

In today's digital world, network security must be protected for businesses in a variety of industries. Intrusion

Grenze ID: 01.GIJET.10.2.203

Detection System (IDS) development has become essential in the fight against contemporary cyberthreats. These watchful gatekeepers not only spot possible breaches but also quickly adjust to changing enemy strategies. Advanced intrusion detection systems set themselves apart by examining network traffic patterns and using AI and machine learning algorithms to correlate data points for quick detection of new threats. By integrating threat intelligence feeds, systems are kept up to date and are better able to identify unusual activity. Most importantly, they strengthen the network's resilience by working together in tandem with firewalls, antivirus programs, and SIEM systems as part of a comprehensive security architecture. While continuous monitoring proactively finds vulnerabilities, real-time threat mitigation reduces the amount of time attackers have to dwell on a target. Recognizing that there is a continual arms race, staying ahead of the changing threat scenario requires a commitment to regular updates and training.

II. Related Work

[1]. According to this research, Intrusion Detection Systems (IDS) are essential safeguards against hostile intrusion and unpredictable internet behaviors because of the exponential growth of digital information and the ever-changing danger environment in the IT industry. In order to overcome unbalance data in IDS based on Machine Learning (ML), This work merges the Enhanced Genetic Algorithm-Particle Swarm Optimization (EGA-PSO) and Improved Random Forest (IRF) approaches to create a novel Hybrid Network-based IDS (HNIDS) model. In order to maintain equilibrium across data samples and improve attribute learning accuracy for smaller sets, HNIDS first uses EGA-PSO. PSO and GA together improve feature selection, dimensionality reduction, True Positive Rate (TPR), and False Positive Rate (FPR). Subsequently, IRF eliminates insignificant characteristics, keeps track of classifier efficiency, and guards against overfitting.

[2]. This paper proposed an exponential increase in the number of connected devices, with estimates indicating that this number would rise from 27 billion in 2017 to 125 billion by 2030. These applications include smart homes, smart cities, smart healthcare, and more. Because of its architecture, variety of device kinds, wireless connectivity, and volume of data moving across networks, security is a major concern in an ever-expanding Internet of Things environment. In response to these difficulties, we provide a brand-new intrusion detection system (DL-IDS) grounded in deep learning that is suited for Internet of Things settings. Our module, which differs from other IDSs, combines the Stacked-Deep Polynomial Network (SDPN) and Spider Monkey Optimization (SMO) algorithm for better feature selection and accurate classification. This allows us to detect anomalies like DoS, U2R, probing, and R2L assaults. A thorough research shows that our DL-IDS performs exceptionally well in terms of metrics of recall, accuracy, precision, and F-score provide a powerful means of enhancing IoT security.

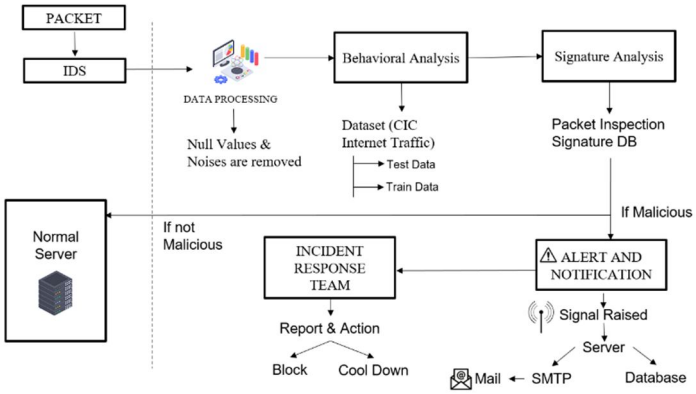
[3]. This paper narrates that Intrusion Detection Systems (IDS) are vital defenses, but it is still unclear how effective they are against unidentified threats such as zero-day attacks. To tackle this, we offer an exclusive intrusion detection technology called CoNN-IDS, that can recognize assaults rapidly that are unclear and adjust to new kinds of attacks. This system consists of a deep neural network-powered Malicious Behavior Parsing (MBP) module and an autoencoder-based Unknown Attack Detection (UAD) module. With an aggregation technique grounded in the DBSCAN algorithm and group decision system, our architecture guarantees ongoing educating and retraining, reinforced by a flexible system that retrains low-impact neurons to increase efficiency. Testing on two different datasets demonstrates better precision in identifying unidentified threats and quicker retraining periods, proving its dominance over traditional intrusion detection systems.

[4]. This paper proposed that the increasing dependence of vendors and customers on online communication underlines the necessity for enhanced efficacy and security protocols. In order to meet this requirement, this study presents a novel intrusion detection system made especially for Apache web servers. The Naive Bayes machine learning method is used in the procedure to provide extensive training, and it uses an IEEE dataset to enhance the system's learning capacity. The suggested solution notably demonstrates a 98.6% strong cross-validation accuracy, confirming its capacity to greatly improve these essential internet communication channels' security frameworks. Furthermore, the system effectiveness in identifying and thwarting such breaches indicates its ability to adjust to changing threats instantly, guaranteeing enhanced reliability and security in vendor-customer dealings in the ever-changing digital environment.

[5]. This paper proposed that the intrusion detection system's (IDS) main objective is to keep an eye on network activities and recognize any potentially dangerous activity. When employing single classification models, anomaly-based intrusion detection systems (IDS) that are meant to identify anomalies inside network architectures frequently struggle with excessive fake alarm rates and inadequate detection rates. This work introduces a dual ensemble model that combines the methods of gradient boosting decision tree (GBDT) and bagging. This approach's efficacy for anomaly-based intrusion detection systems is shown by evaluating several techniques, such

as GBM, LightGBM, CatBoost, and XGBoost, across a variety of datasets, including NSL-KDD, UNSW-NB15, and HIKARI-2021. In particular, the mixture of Bagging and GBM performs better than other pairings, demonstrating more competitiveness when compared to the body of research already operating in the field. This unique dual ensemble provides a promising way to improve anomaly-based intrusion detection systems, as demonstrated by Bagging-GBM.

III. Architectural Diagram



IV. Proposed Work

A. *DATA COLLECTION AND PREPROCESSING*

Data collection involves gathering information related to user behavior, interactions, or activities from various sources such as sensors, logs, or surveys. Preprocessing includes cleaning, transforming, and organizing this data to make it suitable for analysis. This step ensures that the collected data is accurate, complete, and formatted appropriately for further analysis, which is crucial for behavioral insights. Data preprocessing is a critical phase in data analytics and machine learning. It initiates with the collection of data from diverse sources, encompassing databases, APIs, sensors, and surveys, followed by the essential step of data cleaning. During data cleaning, errors, missing values, and outliers are addressed, ensuring the integrity and quality of the dataset. The subsequent step, data transformation, involves feature engineering, scaling, and encoding, tailoring the data for efficient analysis and machine learning. Data integration may be required to consolidate data from multiple sources. Lastly, data reduction techniques can be employed to streamline large datasets, making them computationally efficient and eliminating redundancy. This meticulous process ultimately yields high-quality, organized data that computers can effectively interpret.

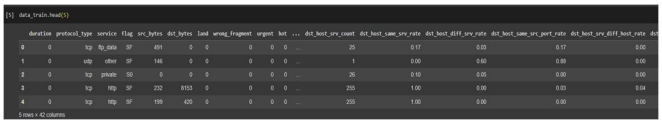


Figure 1. Data splitting

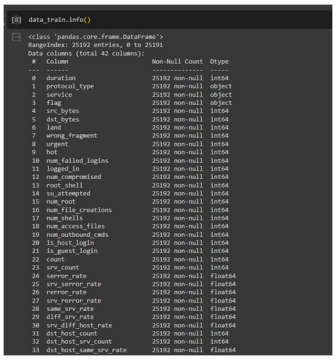


Figure 2: Null Value Removal

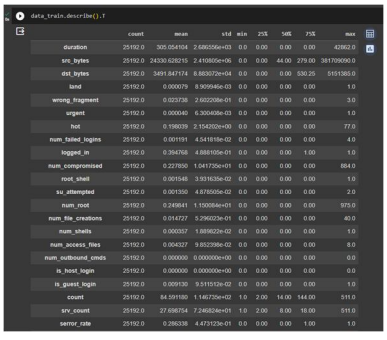


Figure 3: Dataset Training

B. BEHAVIORAL ANALYSIS

In Intrusion Detection Systems (IDS), behavioral analysis is a method used to identify and categorize network traffic according to its behavior. Unlike signature-based IDS, which depends on locating known attack signatures, this method is distinct. When it comes to identifying zero-day attacks that take use of vulnerabilities that intrusion detection systems are not yet aware of behavioral analysis is more successful. Establishing a baseline of typical network traffic and then identifying traffic that deviates from it are the two steps in the behavioral analysis process. Numerous methods, including statistical analysis, machine learning, and anomaly detection, can be used to do this. When an anomaly is found, the IDS can look into it more thoroughly to see if it's a malicious attack. Although it is an effective tool for identifying intrusions, it is not without drawbacks. One issue is that, particularly in intricate networks, it might be challenging to create a baseline of typical traffic. Behavioral analysis can sometimes produce false positives, or warnings that are set off by regular traffic.

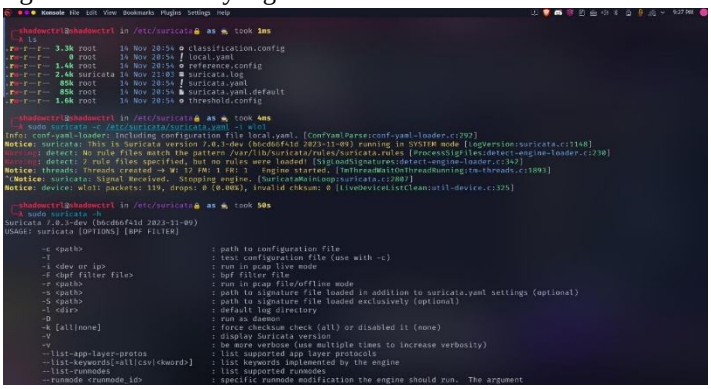


Figure 4. Behavourial Based Detection (Suricata Tool)

C. SIGNATURE-BASED ANALYSIS

Signature-based detection uses current data or network traffic to compare known malware patterns or signatures to identify malicious activities. Both intrusion detection systems (IDS) and antivirus software frequently employ this tactic. A database containing known signatures is consulted during the scanning process of a file or network packet. The file or packet is marked as suspicious and may be blocked or quarantined if a match is discovered. Detecting known threats is a very successful use of signature-based detection. It is ineffective, therefore, in identifying novel or zero-day threats—that is, threats without a signature because they have never been observed before.

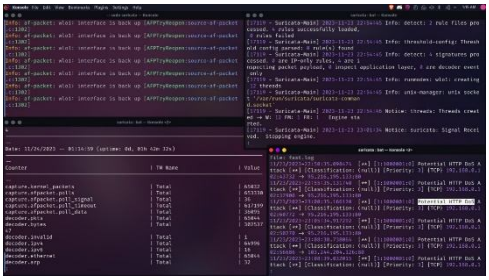


Figure 5: Detection of potential threat using Signature-Based

D. REAL-TIME MONITORING AND ALERT

The implementation of monitoring tools and practices that continuously track the health and performance of various components within a system. Real-time monitoring enables swift detection of anomalies, potential bottlenecks, or critical issues, allowing for immediate intervention before they escalate. It forms the foundation for maintaining system reliability, optimizing resource utilization, and ensuring a seamless user experience. Integration of alert mechanisms that provide timely notifications in response to predefined thresholds or unusual behavior. Alerts serve as the frontline defense, allowing administrators and stakeholders to respond promptly to emerging issues. These notifications can range from performance degradation and security breaches to resource exhaustion. A well-designed Real-time Monitoring and Alerts module contributes not only to the proactive

management of a system but also aids in preventing downtime, enhancing overall system efficiency, and improving the user satisfaction by addressing potential issues in their infancy.

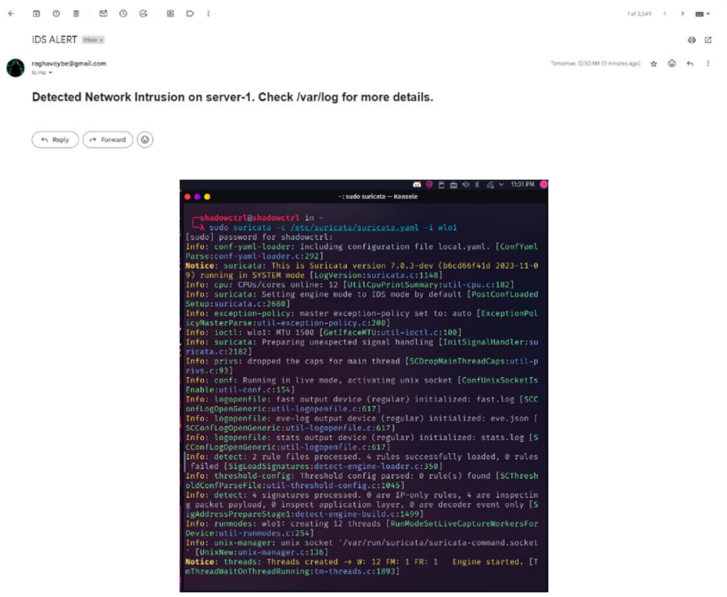


Figure 6: Monitoring the incoming packets via suricata tool.

E. INCIDENT RESPONSE AND REPORTING

The main goal is to create a methodical and effective framework for handling cybersecurity events. Creating procedures for prompt detection, containment, elimination, and recovery from security breaches is part of this. The module places a strong emphasis on writing thorough incident reports that outline the occurrence's extent, consequences, and steps taken. The organization wants to minimize damage, improve resilience against future threats, and guarantee reporting obligations are followed by putting in place a strong incident response plan. The study underscores the significance of promptly and comprehensively responding to incidents to maintain the security and integrity of digital assets. The training also highlights post-incident analysis and lessons learned sessions as means of ongoing improvement. The project intends to strengthen incident response capabilities overall, by conducting thorough analyses of incidents and reactions, pinpoint areas that require improvement and implement preventative steps to lower the likelihood of similar problems in the future. Using an iterative methodology enhances the cybersecurity posture of the business by cultivating a culture of adaptation and resilience in the face of dynamic threats.

V. CONCLUSION

An advanced intrusion detection system (IDS) must be put into practice in order to improve a network environment's overall security posture. An intrusion detection system (IDS) keeps an eye on network activity all the time, looking for possible breaches and malicious activities. This enables it to offer threat detection and response capabilities in real time. This diligent approach to attack prevention lessens the damage caused by security breaches. Furthermore, an advanced intrusion detection system enhances incident response by providing thorough understanding of the characteristics and sources of threats, facilitating prompt and effective remediation. By identifying and addressing threats of all kinds, an intrusion detection system (IDS) improves the network's overall security. Users and data are placed in a more secure environment as a result.

REFERENCE

[1] James, E., & Rabbi, F. (2023). Fortifying the IoT Landscape: Strategies to Counter Security Risks in Connected Systems. Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries, 6(1), 32-46.

[2] Chandana, P., & Gulzar, C. M. (2023). Securing Cyberspace: A Comprehensive Journey through AI's Impact on Cyber Security. Tuijin Jishu/Journal of Propulsion Technology, 44(2).

[3] Ilca, L. F., Lucian, O. P., & Balan, T. C. (2023). Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response. Sensors, 23(15), 6757.

[4] Ishaq, K., & Javed, H. A. (2023). Implementing Snort Intrusion Prevention System (IPS) for Network Forensic Analysis. arXiv preprint arXiv:2308.13589.
[5] Islam, M. A. (2023). Application of artificial intelligence and machine learning in security operations center (Doctoral dissertation, Georgia State University).
[6] Alsumaini, A. Y. M. (2023). Two-Stage Ensemble Learning for NIDS Multiclass Classification (Doctoral dissertation, Hamad Bin Khalifa University (Qatar)).
[7] Albibrahim, T., & Hendaoui, S. (2023). Double level Code Scanning Leveraging network virtualization to decrease risks of memory starvation and insecure programming.
[8] Ahmed, Y. (2022). Data-driven framework and experimental validation for security monitoring of networked systems (Doctoral dissertation, Birmingham City University).
[9] Mpungu, C., George, C., & Mapp, G. (2023, January). Developing a novel digital forensics readiness framework for wireless medical networks using specialised logging. In Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022 (pp. 203-226). Cham: Springer International Publishing.
[10] Airlangga, G., & Liu, A. (2023). A Study of the Data Security Attack and Defense Pattern in a Centralized UAV–Cloud Architecture. Drones, 7(5), 289.