IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

NETWORK INTRUSION DETECTION SYSTEM USING ML

[1]Anusha B, [2]L S Sai Harika, [3]Nikhil Kumar,[4]Diksha Manu

[1]Assistant Professor , [234]Student

Information Science and Engineering,

Cambridge Institute of Technology, Bengaluru, India

Abstract: In the face of increasingly complex cyber threats, the necessity for robust Network Intrusion Detection Systems (NIDS) has never been greater. Conventional rule-based systems often struggle to keep pace with evolving attack methodologies, necessitating the integration of machine learning (ML) techniques to bolster detection capabilities. This paper puts forward an innovative NIDS approach that leverages ML algorithms to effectively detect and mitigate network intrusions.

Our proposed system utilizes supervised learning algorithms trained on labelled network traffic data to differentiate incoming traffic as normal or malicious. By harnessing extensive labelled data, our system can discern intricate patterns and anomalies indicative of malicious activities, thereby enhancing detection accuracy and reducing false positives. Additionally, the system incorporates detection methods for anomalies in network traffic to uncover previously unseen threats by detecting deviations from established baseline behaviour.

Key features of our NIDS include real-time monitoring, scalability to accommodate large network infrastructures, and adaptability to dynamic environments. Through Ongoing adaptation through the incorporation of fresh data and refinement of detection algorithms, our system offers proactive defence against a wide spectrum of cyber threats, including known and zero-day attacks.

In our evaluation, we demonstrate the effectiveness of our ML-based NIDS through comprehensive experimentation on diverse datasets, demonstrating its enhanced effectiveness in comparison to traditional rule-based approaches. Our results underscore significant enhancements in both detection rates and false positive mitigation, underscoring the potential of ML in bolstering network security defences against evolving cyber threats.

I. INTRODUCTION

In today's interconnected digital landscape, ensuring the security of computer networks is paramount. With the rise of sophisticated cyber threats, traditional rule-based Network Intrusion Detection Systems (NIDS) often fall short in adequately safeguarding against evolving attack vectors. As a result, there has been a notable shift towards integrating machine learning (ML) techniques to bolster NIDS capabilities, empowering them to adapt dynamically to emerging threats.

The main goal of a network intrusion detection system is to monitor network traffic in real-time, identifying suspicious or malicious activities, and responding appropriately to mitigate potential security breaches. Traditional NIDS rely on predefined rules and signatures to detect known attack patterns, rendering them vulnerable to evasion tactics employed by adversaries who continually refine their techniques to evade detection.

In contrast, ML-based NIDS leverage advanced algorithms to analyze extensive volumes of network traffic data, uncover underlying patterns, and autonomously generate models capable of distinguishing between normal and anomalous behavior. By learning from historical data, ML algorithms can discern subtle deviations from expected network behavior, facilitating the detection of previously unseen and zero-day attacks.

This paper offers a comprehensive overview of ML-based approaches to network intrusion detection, highlighting their advantages over traditional rule-based systems and discussing various ML techniques and algorithms suitable for this purpose. We delve into

challenges and considerations involved in designing and implementing ML-based NIDS, encompassing data preparation, feature curation, model training, and evaluation methodologies.

Moreover, we underscore the significance of live monitoring and scalability in NIDS deployment, acknowledging the dynamic nature of network environments and the imperative for timely detection and response to emerging threats. Additionally, we explore the potential ramifications of ML-based NIDS in fortifying overall network security posture, encompassing the reduction of false positives, enhancement of detection accuracy, and facilitation of proactive threat mitigation strategies.

Through this investigation, our objective is to provide insights into the pivotal role of ML in propelling the field of network security and furnish guidance for researchers and practitioners keen on developing and deploying ML-based NIDS to effectively combat modern cyber threats.

II. LITERATURE SURVEY

The field of network intrusion detection systems (NIDS) has undergone remarkable progress in recent years, propelled by the escalating complexity of cyber threats and the burgeoning adoption of machine learning (ML) techniques. An extensive examination of the literature unveils a plethora of studies investigating various facets of ML-based NIDS, spanning algorithm selection, feature engineering, evaluation methodologies, and real-world deployment considerations.

One of the seminal works in ML-based NIDS dates back to the 1980s, with Denning pioneering the concept of anomaly detection to detect variances from typical network behavior. Since then, numerous studies have delved into anomaly detection techniques, encompassing statistical methods as well as more sophisticated ML algorithms.

Support vector machines (SVMs) have emerged as a cornerstone in ML-based NIDS, extensively researched due to their ability to classify data in high-dimensional spaces. Tax and Duin's seminal work in 1999 showcased the efficacy of SVMs in detecting network intrusions, laying the groundwork for subsequent research endeavors in this domain.

Ensemble learning stands out as another prominent approach in ML-based NIDS, leveraging the amalgamation of combining multiple models to improve detection accuracy and resilience. Research by Zhi-Hua Zhou et al. in 2002 applied ensemble methods such as AdaBoost and random forests to NIDS, yielding outperforming individual performance individual classifiers.

Deep learning methods, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), are widely recognized for their garnered significant attention in recent times due to their ability to autonomously extract hierarchical features from raw network traffic data. Studies by researchers like Zhang et al. in 2019 showcased the efficacy of deep learning techniques architectures in NIDS, achieving state-of-the-art performance in detecting complex intrusions.

Feature selection and representation play a pivotal role in enhancing the effectiveness of ML-based NIDS. Investigations have investigated various feature sets, including packet header attributes, flow statistics, payload content, and behavioral patterns. For instance, Mahapatra et al. in 2018 proposed a feature selection method based on information gain to optimize NIDS performance.

Evaluation of ML-based NIDS presents unique challenges owing to the dynamic nature of network traffic and the scarcity of labeled intrusion data. Researchers have proposed innovative evaluation frameworks and metrics to accurately assess NIDS performance. For example, Alazab et al. in 2019 introduced dynamic weighting to adaptively adjust evaluation metrics based on the severity of detected intrusions.

The real-world deployment of ML-based NIDS necessitates considerations such as scalability, resource constraints, and interoperability with existing security infrastructure. Studies by researchers like Li et al. in 2020 have addressed these challenges by developing lightweight and scalable ML models tailored for deployment in edge networks and resource-constrained environments.

III. RESEARCH QUESTIONNAIRES FOR NETWORK INTRUSION DETECTION SYSTEMS AND THEIR CHALLENGES:

1. How do network intrusion detection systems (NIDS) distinguish and categorize various types of network traffic?
2. What are the predominant challenges encountered by NIDS in identifying diverse cyber threats and intrusions?
3. To what extent do NIDS demonstrate efficacy in detecting and thwarting large-scale cyber attacks and data breaches?
4. What are the scalability and adaptability constraints affecting NIDS performance concerning evolving cyber threats?
5. How do NIDS uphold the confidentiality and integrity of sensitive data while monitoring network traffic?
6. What are the comparative performance merits between different NIDS variants, such as signature-based and anomaly-based detection systems?
7. How do NIDS address the scalability prerequisites for monitoring network traffic within expansive enterprise environments?

---

8. What are the recommended strategies for optimizing NIDS configuration and deployment to augment their proficiency in identifying and mitigating cyber threats?

By addressing these research questions, researchers and cybersecurity practitioners can acquire valuable insights regarding into the inherent challenges and constraints confronting network intrusion detection systems, facilitating the development of more resilient and efficient cybersecurity solutions.

IV. ADVANTAGES OF NETWORK INTRUSION DETECTION SYSTEM METHODOLOGY

Network intrusion detection systems (NIDS) serve as vital components in fortifying networks against unauthorized access and malicious activities. Here are several notable benefits of NIDS methodology:

- Comprehensive Monitoring: NIDS continually observe network traffic for any signs of suspicious patterns or anomalies, ensuring thorough coverage of network activity.
- Real-time Detection: NIDS possess the capability to detect intrusions and security breaches as they occur in real-time, facilitating prompt response and implementation of mitigation measures.
- Signature-based Detection: Many NIDS employ signature-based detection techniques, which involve cross-referencing network traffic patterns against a repository of known attack signatures. This enables swift identification of recognized threats.
- Anomaly-based Detection: Alongside signature-based detection, NIDS may utilize anomaly-based detection methods to flag unusual patterns or behaviors in network traffic that diverge from established baseline activity.
- Scalability: NIDS demonstrate scalability, allowing them to effectively monitor networks of varying sizes, from small local networks to expansive enterprise environments, thereby ensuring consistent protection across diverse network infrastructures.
- Customizable Policies: NIDS afford administrators the flexibility to define and tailor security policies and rules according to their organization's specific security requirements and compliance standards.
- Intrusion Prevention: Advanced NIDS possess the capability not only to detect intrusions but also to proactively prevent them by obstructing or mitigating malicious traffic in real-time.
- Forensic Analysis: NIDS furnish valuable forensic data and logs that can be subjected to analysis to investigate security incidents, pinpoint the root cause of breaches, and enhance overall network security posture.

By harnessing these advantages, NIDS empower organizations to preemptively identify and address cyber threats, thereby bolstering their overall cybersecurity posture and shielding sensitive data assets from unauthorized access and exploitation.

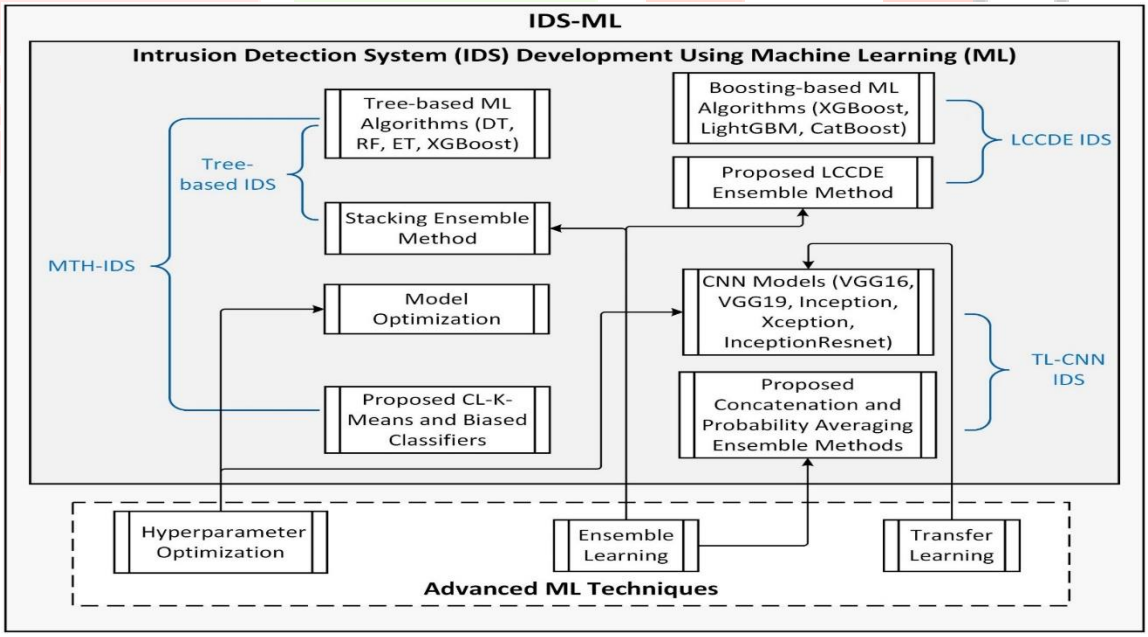

Fig: 1 A high-level overview of IDS-ML is illustrated

V. INFERENCE ON NETWORK INTRUSION DETECTION SYSTEMS

The synthesis of various sources yields insightful perspectives on the capabilities and limitations inherent in traditional network intrusion detection systems (NIDS). One source accentuates the efficacy of signature-based detection methods in promptly identifying established attack patterns, underscoring their reliability in detecting well-known threats. Nevertheless, it also underscores the constraints of signature-based approaches in identifying novel and intricate attacks that may evade predefined signatures.

Another source delves into the significance of anomaly-based detection methods, which prioritize the identification of deviations from typical network behavior. While anomaly detection holds promise in uncovering previously unseen attacks, it encounters hurdles in discerning between malicious activities and legitimate network behavior, potentially leading to false positives.

Moreover, hybrid approaches amalgamating both signature and anomaly detection techniques are becoming increasingly prevalent prominence, proffering a balanced strategy that harnesses the strengths of each method. Furthermore, the advancement of machine learning and artificial intelligence has facilitated the emergence of more adaptive and intelligent NIDS, capable of learning and adapting to evolving threats.

However, these advanced approaches necessitate ample training data and may confront challenges in accurately interpreting intricate network patterns. In summary, while traditional NIDS excel in detecting known threats and abnormal network behavior, they confront difficulties in addressing novel and sophisticated attacks, underscoring the imperative for continuous innovation and integration of advanced detection techniques.

VI. CONCLUSION

The integration of machine learning (ML) techniques into network intrusion detection systems (NIDS) marks a significant leap forward in cybersecurity. By leveraging ML algorithms, NIDS can dynamically adapt to the evolving cyber threat landscape, enhancing their detection capabilities and fortifying proactive defense mechanisms.

The literature survey conducted underscores the vast array of research in ML-based NIDS, showcasing diverse approaches, algorithms, and methodologies. From traditional machine learning methods like support vector machines and ensemble learning to cutting-edge deep learning models such as convolutional neural networks, along with and recurrent neural networks, researchers have explored multifaceted avenues to enhance NIDS efficacy.

Crucial considerations in ML-based NIDS development include feature selection, evaluation methodologies, and real-world deployment challenges. Addressing these factors enables researchers to optimize NIDS performance, scalability, and usability across varied network environments.

Continued research endeavors are imperative to tackle lingering challenges and propel ML-based NIDS to the forefront. This entails devising innovative algorithms for extracting features, anomaly detection, and model optimization, alongside establishing robust evaluation frameworks to gauge NIDS effectiveness under practical conditions.

Furthermore, collaborative endeavors involving academia, industry, and government entities are essential to foster knowledge
exchange, data sharing, and technology transfer in the realm of ML-based NIDS. Through interdisciplinary collaboration and advocacy for open standards and interoperability, the adoption of ML-based NIDS can be accelerated, bolstering cybersecurity defenses against emergent cyber threats.

In essence, ML-based NIDS hold immense potential in fortifying network security and safeguarding critical assets from cyber threats. By harnessing the capabilities of machine learning, organizations can proactively mitigate risks and uphold the resilience and integrity of their digital infrastructure.

VII. REFERENCES

[1]. Hossain, Md. Alamgir. (2023). Ensuring network security with a robust intrusion detection system using ensemble-based machine learning. Array. 19. 10.1016/j.array.2023.100306.

[2]. S. Mirlekar and K. P. Kanojia, "A Comprehensive Study on Machine Learning Algorithms for Intrusion Detection System," 2022 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22), Nagpur, India, 2022, pp. 01-06, doi: 10.1109/ICETET-SIP-2254415.2022.9791586.

[3]. Mohammed Ishaque, Md Gapar Md Johar, Ali Khatibi, Muhammed Yamin,A novel hybrid technique using fuzzy logic, neural networks and genetic algorithm for intrusion detection system, doi.org/10.1016/j.measen.2023.100933.

[4]. Rathee, P. Malik and M. Kumar Parida, "Network Intrusion Detection System using Deep Learning Techniques," 2023 International Conference on Communication, Circuits, and Systems(IC3S), BHUBANESWAR, India, 2023, pp. 1-6, doi: 10.1109/IC3S57698.2023.10169122.

[5]. Singh, A., Amutha, J., Nagar, J. et al. AutoML-ID: automated machine learning model for intrusion detection using wireless sensor network. Sci Rep 12, 9074 (2022). https://doi.org/10.1038/s41598-022-13061-z.

[6]. Vanin, P.; Newe, T.; Dhirani, L.L.; O'Connell, E.; O'Shea, D.; Lee, B.; Rao, M. A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning. Appl. Sci. 2022, 12, 11752. https://doi.org/10.3390/app122211752

[7]. Akhtar, M.A., Qadri, S.M.O., Siddiqui, M.A. et al. Robust genetic machine learning ensemble model for intrusion detection in network traffic. Sci Rep 13, 17227 (2023). https://doi.org/10.1038/s41598-023-43816-1

[8]. Talukder, M.A., Islam, M.M., Uddin, M.A. et al. Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. J Big Data 11, 33 (2024). https://doi.org/10.1186/s40537-024-00886-w

[9]. U. S. Musa, S. Chakraborty, M. M. Abdullahi and T. Maini, "A Review on Intrusion Detection System using Machine Learning Techniques," 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2021, pp. 541-549, doi: 10.1109/ICCCIS51004.2021.9397121.