IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 2, February 2024

Anomaly Detection System

Prof. K. G. Jagtap,
Professor, Department of AI & ML
AISSMS Polytechnic, Pune, India

Shreeram Shinde
Student, Department of AI & ML
AISSMS Polytechnic, Pune, India

Akshay Adhav
Student, Department of AI & ML
AISSMS Polytechnic, Pune, India

Sahil Kadambande
Student, Department of AI & ML
AISSMS Polytechnic, Pune, India

Abstract: *The "Network Anomaly Detection System" is a sophisticated software program designed to safeguard computer networks from malicious activities aimed at unauthorized access, data theft, or compromising network agreements. Existing Advanced Detection System (ADS) technologies, despite their effectiveness, face challenges in handling the dynamic and complex security attacks orchestrated by hackers in contemporary computer networks. The pivotal factor influencing the system's efficacy is accuracy, particularly in the context of login activities. With the exponential increase in the volume of data transmitted over the Internet due to the gradual expansion of technology utilization, the imperative to secure this data has become paramount. In response to this, the proposed anomaly detection system (ADS) emerges as a crucial solution by actively monitoring and analyzing data to detect virtual security threats. As intruders deploy diverse methods to infiltrate networks, the ADS is poised to identify anomalies within the system or network proactively. Significantly, the system leverages cutting-edge technology, specifically machine learning algorithms, to classify and detect assaults in real-time. The emphasis is on determining the most appropriate machine learning technique for recognizing the specific nature of the attack, highlighting an adaptive and forward-looking approach to network security. In essence, the "Network Anomaly Detection System" represents a proactive and adaptive defense mechanism, utilizing the power of machine learning to address the evolving landscape of cyber threats in computer networks. Positioned as the final safeguard following a series of preventive measures, anomaly detection plays a crucial role in identifying and thwarting attacks that may have evaded earlier security measures*

Keywords: Anomaly Detection System, Network Anomaly Detection System, Secure data, Cyber threats, Intruders, Secure data, Data theft, Accuracy

I. INTRODUCTION

In the contemporary digital landscape, the importance of network security has reached unprecedented levels due to the explosive rise of network-based services and the proliferation of sensitive data. As organizations rely more heavily on interconnected systems, safeguarding against potential threats becomes paramount. Network security is a multifaceted challenge, with various defense layers in place, including secure network architecture design, firewalls, passwords, encryptions, and personal screening. However, despite these preventive measures, the evolving sophistication of cyber threats necessitates a robust last line of defense, and this is where anomaly detection technology emerges as a crucial safeguard. Anomaly detection stands as the ultimate defense against computer attacks, complementing other security measures. It operates after the fortification provided by secure network architecture, firewalls, passwords, encryptions, and personal screening. The prevalence of anomaly prevention methods, however, does not eliminate the efficacy of attacks on computer systems. To counteract these threats effectively and ensure real-time network security, the integration of anomaly detection systems (ADSs) is indispensable. An anomaly, in the context of network security, is defined as any series of actions intended to corrupt or damage data. This includes deliberate unauthorized access to data, data manipulation, or instances of system unreliability. Anomaly detection systems are meticulously designed models created to identify attacks among different types of packets traversing a network. The process involves scrutinizing

DOI: 10.48175/568

computer system or network events and analyzing them to detect anomalies that may signify malicious intent.

Machine learning plays a pivotal role in anomaly detection, providing the capability to identify unusual behavior by attackers on a network or system. With illegal access to a computer system ranking among the most significant threats to network and computer security in the modern era, the need for adaptive mechanisms is evident. New varieties of network attacks are emerging as rapidly as network applications, necessitating continuous improvement in system capabilities to handle suspicious activity effectively.¬The network administrator plays a crucial role in this defense strategy, being notified when an assault is discovered or when strange conduct is detected. By identifying and rerouting attacks, access systems (ADS) follow the path determined by the network or host. However, these systems are not immune to vulnerabilities, as attack signatures can frequently reveal malicious or questionable motives. The patterns in network traffic, identified through the validation of an ID, are crucial in retrieving information when dealing with potential threats

II. MATERIALS AND METHODS

Building a robust anomaly detection system necessitates a comprehensive approach, integrating carefully chosen materials and methods to ensure accuracy and adaptability. One of the foundational considerations is the selection of appropriate data sources. The type of data, whether it be network traffic, sensor readings, or user behavior, forms the bedrock upon which the anomaly detection system operates. Ensuring data quality and consistency is paramount, as the system's efficacy hinges on the reliability of the information it processes.Feature selection plays a crucial role in shaping the system's ability to discern normal behavior from anomalies. Identifying and engineering relevant features that adequately represent the system's regular operations is essential. This step often involves domain expertise to determine which aspects of the data are most indicative of normalcy. Additionally, feature engineering may be necessary to extract meaningful patterns from raw data, enhancing the system's ability to discern subtle deviations.

Designing an effective anomaly detection system entails careful consideration of both materials and methods. The choice of materials involves selecting appropriate hardware components such as sensors, cameras, or other data acquisition devices capable of capturing relevant information from the environment being monitored. Additionally, the selection of materials may include the use of specialized equipment for data preprocessing or feature extraction, depending on the nature of the data being analyzed.

Designing an effective anomaly detection system involves careful consideration of materials and methods to ensure accurate and reliable identification of abnormal behavior within datasets. The choice of materials encompasses both the data used for training and the computational resources necessary for analysis. High-quality datasets containing both normal and anomalous instances are essential for supervised learning approaches, while unsupervised methods can operate with unlabeled data but may require additional preprocessing. Common materials include labeled datasets, algorithms such as Support Vector Machines, Decision Trees, and One-Class SVM, and computing resources capable of handling large datasets efficiently. The methods employed vary based on the availability of labeled anomalies; supervised learning methods utilize labeled data to train models to recognize patterns of normal and abnormal behavior, while unsupervised methods rely on clustering algorithms to identify outliers within the data. Furthermore, hybrid approaches that combine both supervised and unsupervised techniques may be employed to leverage the strengths of each method. Overall, an effective anomaly detection system integrates appropriate materials and methods tailored to the specific requirements of the dataset and the desired level of anomaly detection accuracy

III. PROPOSED SYSTEM

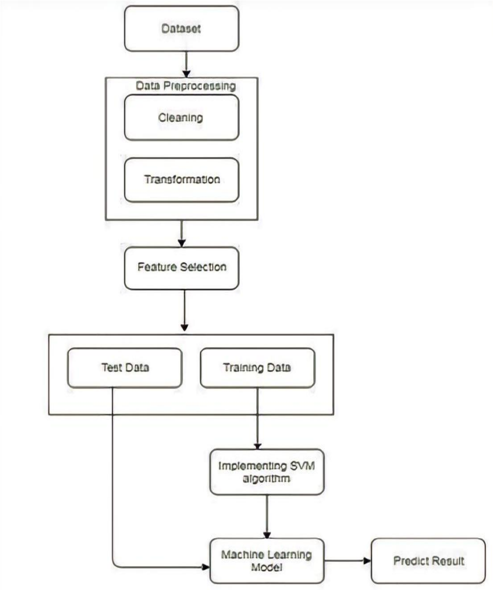

Fig: System Architecture

IV. CONCLUSION

The Anomaly Detection Problem Now Has a New Machine Learning Based Data Classification Algorithm Support Vector. To attain superior performance, improve accuracy rate, and accelerate running time. The Proposed ADS Framework's Performance Will Be Judged According to Its Detection Rate, Precision, F1 Score, Recall, And False-positive Rate. The proposed ADS Framework Will Be Tested Using the KDD CUP 1999

Results:

Anomaly detection systems play a crucial role in identifying irregular patterns, deviations, or outliers within a dataset, system, or network. These systems employ various techniques, including statistical analysis, machine learning algorithms, and pattern recognition, to establish a baseline of normal behavior and flag any deviations that may indicate potential anomalies or security threats. The results of an anomaly detection system are typically presented in the form of alerts or notifications, allowing users or administrators to investigate and address the identified anomalies. This proactive approach helps in early detection of unusual activities, minimizing the risk of security breaches, system failures, or other undesirable events. The effectiveness of an anomaly detection system relies on its ability to accurately distinguish between normal and anomalous behavior, adapt to evolving patterns, and provide timely and actionable insights for improved decision-making and threat mitigation.

REFERENCES

[1] Hurley, T.; Perdomo, J.E.; Perez-Pons, "A. HMM-Based Intrusion Detection System for Software Defined Networking. In Proceedings of the 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, 18–20 December 2016; pp. 617–621. 2.

[2] Shone, N.; Ngoc, T.N.; Phai, V.D.; Shi, "Q. A Deep Learning Approach to Network Intrusion Detection", IEEE Trans. Emerg. Top. Comput. Intell. 2018, 2, 41– 50. 3.

[3] Gomez, J.; Gil, C.; Banos, R.; Marquez, A.L.; Montoya, F.G.; Montoya, M.G. A,"Pareto-based multi-objective evolutionary algorithm for automatic rule generation in network intrusion detection systems", Soft Comput. 2013, 17, 255–263.

[4] Sangeetha, S.; Gayathri devi, B.; Ramya, R.; Dharani, M.K.; Sathya, P. Signature Based Semantic Intrusion Detection System on Cloud. In Information Systems Design and Intelligent Applications; Mandal, J.K., Satapathy, S.C., Kumar Sanyal, M., Sarkar, P.P., Mukhopadhyay, A., Eds.; Springer: New Delhi, India, 2015; pp. 657–666.

[5] Dey, S.K.; Rahman, M.M. , "Effects of Machine Learning Approach in Flow-Based Anomaly Detection on Software-Defined Networking", IEEE 2020

[6] Vipin, Das & Vijaya, Pathak & Sattvik, Sharma &Sreevathsan& MVVNS. Srikanth & Kumar T, Gireesh, "Network Intrusion Detection System Based On Machine Learning Algorithms , International Journal of Computer Science & Information Technology, 2010

[7] Choi, J & Choi, Chang & Ko, Byeongkyu& Choi, D & Kim, "Detecting web based Ddos attack using mapreduce operations in cloud computing environment " Journal of Internet Services and Information Security, 2013

[8] Baig, Zubair & Baqer, M & Khan, Asad, "A Pattern Recognition Scheme for Distributed Denial of Service (DDoS) Attacks in Wireless Sensor Networks", 2006

[9] Analyzing Log Files for Post-mortem Intrusion Detection Gamboa, Karen & Monroy, Raúl & Trejo, Luis & Aguirre Bermúdez, Eduardo & Mex-Perera, Carlos. (2012), IEEE Transactions on Systems Man and Cybernetics Part C (Applications and Reviews)

[10] Network Traffic Analysis and Intrusion Detection Using Packet Sniffer Qadeer, Mohammed & Iqbal, Arshad & Zahid, Mohammad & Siddiqui, Misbahur, Communication Software and Networks

DOI: 10.48175/568