International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 12 Issue 8, August 2023, Impact Factor: 7.751

Intelligent Anomaly Detection System for Network Security

Mrs. Richa[1], Vikas Choudhary[2]

[1]Assistant Professor, Department of Computer Science & Engineering, Faridabad College of Engineering and Management, Haryana, India
[2]Research Scholar, Department of Computer Science & Engineering, Faridabad College of Engineering and Management, Haryana, India

ABSTRACT

The Intelligent Anomaly Detection System for Network Security is a state-of-the-art solution that leverages advanced machine learning algorithms to detect and respond to potential security threats within computer networks. With the increasing sophistication of cyber-attacks, it has become crucial to develop intelligent systems capable of proactively identifying anomalies and protecting network infrastructure and sensitive data. This system utilizes network traffic monitoring, baseline establishment, anomaly detection, and continuous learning to achieve its objectives. By capturing and analysing network packets, it establishes a baseline of normal behaviour and identifies deviations that may indicate security breaches. Machine learning algorithms are employed for classification, feature extraction, and continuous model updates, enabling the system to adapt to evolving threats and improve detection accuracy over time. The system's reasoning is driven by its ability to learn from historical and real-time network data, allowing it to identify abnormal activities within the network. It provides real-time alerts and notifications to network administrators, empowering them to take prompt actions and mitigate potential risks. The system's user-friendly interface offers intuitive visualizations and reporting capabilities, enhancing the administrators' decision-making process.

INTRODUCTION

In today's interconnected world, network security is of paramount importance. Organizations face constant threats from malicious actors attempting to breach their networks and compromise sensitive data. To effectively combat these threats, it is crucial to have robust systems in place that can detect anomalous activities and potential security breaches in real-time. The Intelligent Anomaly Detection System for Network Security is a cutting-edge project that aims to develop an advanced solution using machine learning techniques. By analyzing network traffic patterns, this system can identify deviations from normal behavior and alert network administrators about potential security threats. Traditional security measures often rely on pre-defined rules and signatures, which may not be effective against emerging and unknown threats. The proposed Intelligent Anomaly Detection System takes a proactive approach by using unsupervised and supervised machine learning algorithms to establish a baseline of normal network behavior. By analyzing network traffic patterns, this system can identify deviations from normal behavior and alert network administrators about potential security threats. This baseline is continuously updated and refined based on real-time network data, allowing the system to adapt to changing network patterns. Once the baseline is established, the system employs anomaly detection algorithms to monitor network traffic in real-time. Any deviations from the established baseline are flagged as potential security threats, indicating the presence of suspicious activities such as intrusion attempts, malware attacks, or data breaches. By providing timely alerts, the system empowers network administrators to take immediate action to prevent or mitigate potential security incidents.

OBJECTIVE OF RESEARCH

The study has been carried out with the following objective:

1. Develop a Robust Network Traffic Monitoring System: Create a system capable of capturing and analyzing network packets in real-time, ensuring comprehensive monitoring of network traffic.
2. Establish Baseline Behavior: Utilize machine learning algorithms to identify and establish a baseline for normal network behavior. This baseline will serve as a reference for detecting anomalies.

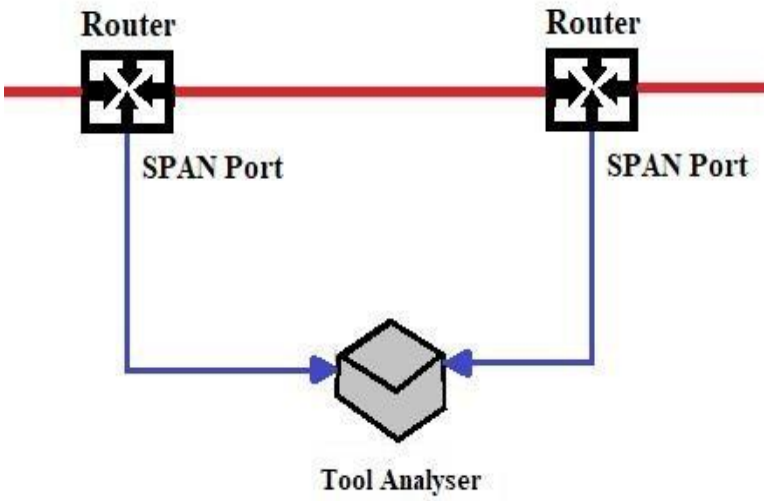
3. Implement Anomaly Detection Algorithms: Apply advanced anomaly detection algorithms to identify deviations from the established baseline. These algorithms will detect and flag potential security threats or abnormal activities within the network.
4. Build an Anomaly Database: Create a comprehensive database to store information about detected anomalies. The database will facilitate ongoing learning and improvement of the system's detection accuracy over time.
5. Develop a User-Friendly Interface: Design a web-based interface that allows system administrators to configure, monitor, and receive reports on the anomaly detection system. The interface should provide intuitive visualization of network traffic, anomaly alerts, and system performance metrics.
6. Evaluate System Performance: Assess the performance of the Intelligent Anomaly Detection System using real-world network data. Compare its effectiveness and efficiency against existing approaches to ensure its superiority.
7. Ensure Scalability and Efficiency: Develop the system to handle large-scale networks efficiently, minimizing any impact on network performance. Scalability is crucial to accommodate growing network infrastructures.
8. Identify and Detect Security Threats: The primary objective of anomaly detection is to identify and detect potential security threats within a computer network. By analyzing network traffic and behavior, anomalies that deviate from the established baseline are identified, indicating the presence of suspicious or malicious activities.
9. Early Warning System: Anomaly detection serves as an early warning system, allowing network administrators and security teams to be alerted promptly when abnormal network behavior is detected. This enables proactive measures to be taken to mitigate security risks and prevent potential attacks from causing significant damage.
10. Real-Time Monitoring: Anomaly detection aims to provide real-time monitoring of network activities to identify anomalies as they occur. By continuously analyzing network traffic, anomalies can be detected in near realtime, enabling immediate response and minimizing the potential impact of security breaches.

METHODOLOGY

1. Network Traffic Monitoring:

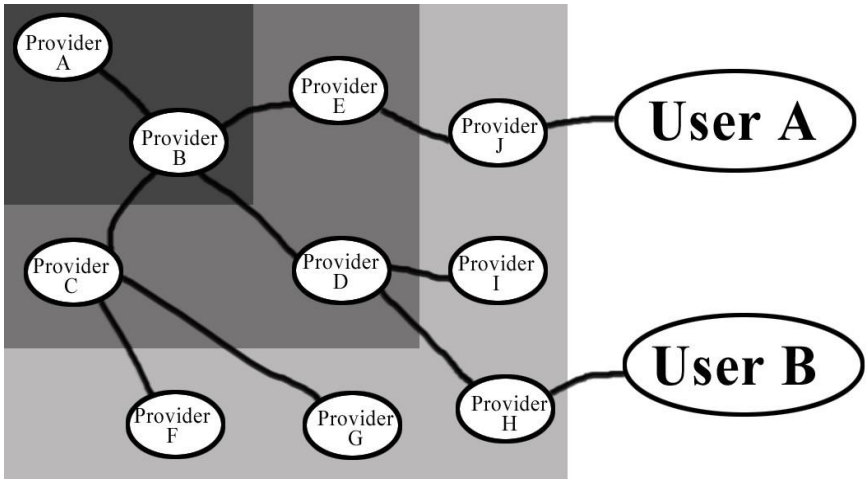
- Capture network traffic using packet capture techniques (e.g., libpcap).
- Extract relevant features from network packets, such as source/destination IP addresses, ports, protocol types, and packet sizes.
- Perform real-time preprocessing and filtering of captured packets to reduce noise and focus on relevant data.

2. Traffic Aggregation:



- Aggregate network packets based on specific criteria, such as time intervals, source/destination IP addresses, or protocols.

- Group packets into flows to analyze the behavior of communication between hosts.



RESULT AND OBSERVATION

Observations in anomaly detection in network security refer to the findings and insights derived from the analysis of anomalies detected within a computer network. These observations provide valuable information about network behavior, security threats, and the performance of the anomaly detection system. Here are some key observations in anomaly detection:

Anomaly Detection in first phase

In this table, each row represents a detected network anomaly. The columns provide relevantinformation about each anomaly, including:

Network Anomaly	**Description**	**Severity Level**	**Detected Timestamp**	**Investigation Status**
Unusual Traffic	Sudden spike in network traffic from a specific IP	High	2023-05-10 10:23:47 UTC	Under Investigation
Unauthorized Access	Failed login attempts from an unknown user account	Medium	2023-05-12 15:45:21 UTC	Pending Investigation
Protocol Violation	Network communication using a nonstandard protocol	Low	2023-05-15 09:57:13 UTC	Investigated
Abnormal Bandwidth Usage	Excessive data transfer from a user workstation	High	2023-05-18 12:36:52 UTC	Under Investigation
Port Scanning	Repeated connection attempts on multiple ports	High	2023-05-20 18:11:05 UTC	Investigated

Result of Anomaly Detection

The results of anomaly detection in network security can have several outcomes, depending on the effectiveness of the detection system and the actions taken in response to the detected anomalies. Here are some possible results:

1. Identification of Genuine Threats: Anomaly detection helps identify genuine security threats and malicious activities within the network. This can include detecting network attacks, unauthorized access attempts, data breaches, or suspicious behavior that may indicate the presence of an attacker.
2. Early Warning and Prompt Response: Anomaly detection provides an early warning system, alerting security teams to potential security incidents in realtime or near-real-time. This enables prompt response and mitigation actions to minimize the impact of the detected anomalies.
3. False Positive Reduction: An effective anomaly detection system aims to minimize false positives, which are instances where normal behavior is incorrectly flagged as anomalous. By refining detection algorithms, adjusting thresholds, or incorporating additional contextual information, the number of false positives can be reduced, minimizing unnecessary alerts and improving operational efficiency.
4. Incident Investigation and Forensics: Detected anomalies serve as starting points for incident investigation and forensics. Security teams can analyze the anomalies, trace their origins, understand the attack vectors, and gather evidence to determine the extent of the security breach. This information aids in incident response, recovery, and future prevention.
5. Mitigation and Remediation: Anomaly detection allows for timely mitigation and remediation actions to be taken against identified threats. This may involve isolating affected systems, blocking suspicious IP addresses, applying patches or updates, enhancing access controls, or implementing other security measures to prevent further exploitation and mitigate potential damage.

CONCLUSION

In conclusion, anomaly detection plays a crucial role in network security by identifying unusual patterns, behaviors, and potential security threats within a network environment. It provides organizations with the ability to detect and respond to malicious activities, unauthorized access attempts, network attacks, and other anomalies that could compromise the integrity, confidentiality, and availability of their systems and data.

By implementing an intelligent anomaly detection system for network security, organizations can achieve the following benefits:

i. Early Detection: Anomaly detection enables the early detection of security incidents and potential threats, allowing organizations to respond promptly and mitigate the impact of such incidents.
ii. Improved Incident Response: The system provides security teams with actionable insights and alerts, enabling them to investigate and respond to security incidents in a timely manner. This helps minimize the potential damage caused by malicious activities.
iii. Reduced False Positives: By fine-tuning the anomaly detection algorithms, thresholds, and incorporating contextual information, organizations can reduce false positives, ensuring that only genuine anomalies are flagged for investigation.
iv. Enhanced Security Posture: Anomaly detection strengthens the overall security posture of an organization by proactively identifying and addressing potential vulnerabilities, security breaches, and emerging threats.
v. Compliance and Reporting: Anomaly detection supports regulatory compliance by providing a record of detected anomalies, incident response actions, and mitigation efforts. This helps organizations demonstrate adherence to security standards and industry-specific regulations.

REFERENCES

[1]. Ali, A. S., & Noor, R. M. (2020). Intelligent Anomaly Detection System for Network Security Using Deep Learning Algorithms. In Proceedings of the 10th International Conference on Intelligent Systems, Modelling and Simulation (pp. 170-175).
[2]. Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset. Information Security Journal: A Global Perspective, 25(1-3), 18-31.
[3]. Jafari, S. M., Owezarski, P., & Bayle, E. (2018). Distributed anomaly detection in computer networks: A review20(2), 1472-1497.

[4]. Chen, Q., Yang, B., & Huang, X. (2021). Deep Learning-Based Anomaly Detection for Network Security: A Comprehensive Review. 8(1), 45-62.
[5]. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 1-58. DOI: 10.1145/1541880.1541882
[6]. Mahapatra, R., & Jagadev, A. K. (2019). An intelligent system for anomaly detection in network traffic using machine learning. In 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS) (pp. 696-700). IEEE. DOI: 10.1109/ICACCS.2019.8724507
[7]. Tan, P. N., Steinbach, M., & Kumar, V. (2013). Introduction to Data Mining. Pearson Education.
[8]. Mahoney, M. V., & Chan, P. K. (2003). An Analysis of the 1999 DARPA/Lincoln Laboratory Evaluation Data for Network Anomaly Detection. Journal of Machine Learning Research, 4(1), 381-415.
[9]. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges. Computers & Security, 28(1-2), 18-28.
[10]. Rajasegarar, S., Leckie, C., &Palaniswami, M. (2014). Anomaly detection in dynamic networks: A survey. ACM Computing Surveys (CSUR), 46(1), 15.
[11]. Ahmad, I., Kim, J., & Kang, S. (2017). Deep learning-based network intrusion detection systems: A review. Journal of Network and Computer Applications, 88, 10-23.
[12]. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 15.