International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Network Intrusion Detection System

Mr. Sahil Bhelkar, Mr. Amey Narvekar, Mr. Sahil Pimple, Mr. Prasad Salve, Ms. Shwetambari Borade

Dept. of Cyber Security, Shah & Anchor Kutchhi Engineering College
Mumbai, India
Sahil.bhelkar16443@sakec.ac.in
Amey.narvekar16854@sakec.ac.in
Sahil.pimple16862@sakec.ac.in
Prasad.salve16488@sakec.ac.in
Shwetambari.borade@sakec.ac.in

Abstract
Network intrusion detection systems (NIDS) play a crucial role in safeguarding network infrastructures against unauthorized access and malicious activities. This abstract explores the fundamental concepts, methodologies, and challenges associated with NIDS. It delves into the various techniques employed by NIDS, ranging from signature-based detection to anomaly detection, and highlights the importance of real-time monitoring and analysis for timely threat detection and response. Additionally, the abstract discusses the evolving landscape of cyber threats and the need for continuous adaptation and enhancement of NIDS to mitigate emerging risks effectively. Furthermore, it addresses the trade-offs between detection accuracy, resource utilization, and scalability, emphasizing the significance of striking a balance to ensure optimal NIDS performance in diverse network environments. Overall, this abstract provides a comprehensive overview of NIDS, underscoring its indispensable role in fortifying network security posture in the face of evolving cyber threats.

Keywords-
Network, intrusion, detection, NIDS, threat.

I. Introduction

In an era dominated by interconnected digital networks, the security of these systems is paramount. Network Intrusion Detection Systems (NIDS) stand as vigilant guardians, tasked with identifying and thwarting unauthorized access, malicious activities, and potential threats that jeopardize the integrity and confidentiality of network infrastructures. As organizations increasingly rely on networked environments to conduct critical operations and store sensitive data, the need for robust intrusion detection mechanisms becomes ever more pressing. NIDS operate as an integral component of a multi-layered security architecture, complementing other defensive measures such as firewalls and antivirus software. Unlike firewalls, which focus on regulating traffic based on predetermined rules, NIDS adopt a proactive approach by continuously monitoring network traffic for anomalous patterns and behaviours indicative of intrusion attempts or malicious activity. This proactive stance enables NIDS to detect both known threats, through signature-based detection techniques, and novel threats, through anomaly detection methodologies, thereby providing a comprehensive defence against a wide spectrum of cyber threats. However, the efficacy of NIDS hinges on their ability to strike a delicate balance between detection accuracy, resource utilization, and scalability. While high detection accuracy is desirable, it must be achieved without overwhelming network resources or impeding legitimate traffic flow. Moreover, NIDS must be capable of scaling seamlessly to accommodate the dynamic nature of modern network environments characterized by evolving threats, expanding infrastructures, and fluctuating traffic volumes. This introduction sets the stage for a deeper exploration of NIDS, encompassing their underlying principles, detection mechanisms, deployment considerations, and ongoing challenges in the relentless pursuit of network security excellence.

II. Objective

1. Threat Detection: The primary objective of a Network Intrusion Detection System (NIDS) is to accurately and promptly identify potential security breaches, unauthorized access attempts, and malicious activities within the network environment.

2. Real-time Monitoring: NIDS aims to provide continuous, real-time monitoring of network traffic, enabling swift detection and response to suspicious or anomalous behavior, thus minimizing the potential impact of security incidents.

3. Incident Response: NIDS plays a crucial role in facilitating incident response efforts by promptly alerting security personnel or automated systems to potential security breaches, allowing for timely investigation, containment, and mitigation of threats.

4. Enhanced Security Posture: By providing insights into the nature and scope of network threats, NIDS assists in bolstering the overall security posture of an organization, enabling proactive measures to strengthen network defenses and prevent future security incidents.

5. Comprehensive Coverage: NIDS aims to offer comprehensive coverage by employing a combination of signature-based detection, which identifies known attack patterns, and anomaly-based detection, which identifies

deviations from normal network behavior, thereby addressing a wide range of cyber threats.

6. Reduced False Positives: An important objective of NIDS is to minimize false positives, ensuring that security personnel can focus their attention and resources on genuine security threats rather than being inundated with irrelevant or erroneous alerts.

7. Scalability and Flexibility: NIDS should be designed to scale effectively with the growing size and complexity of network infrastructures, while also remaining flexible enough to adapt to evolving threats, technologies, and network configurations.

8. Regulatory Compliance: NIDS assists organizations in achieving regulatory compliance by helping them meet the security requirements stipulated by industry standards and regulatory frameworks, thereby avoiding penalties and reputational damage associated with non-compliance.

9. Continuous Improvement: NIDS should undergo regular evaluation and refinement to enhance its efficacy in detecting and mitigating emerging threats, leveraging advancements in technology, threat intelligence, and analytical techniques to stay ahead of evolving cyber threats.

10. User Awareness and Training: NIDS contributes to raising user awareness about network security threats and best practices by providing insights into the types of threats targeting the network, thereby fostering a culture of security awareness and proactive risk management within the organization.

III. Methodologies

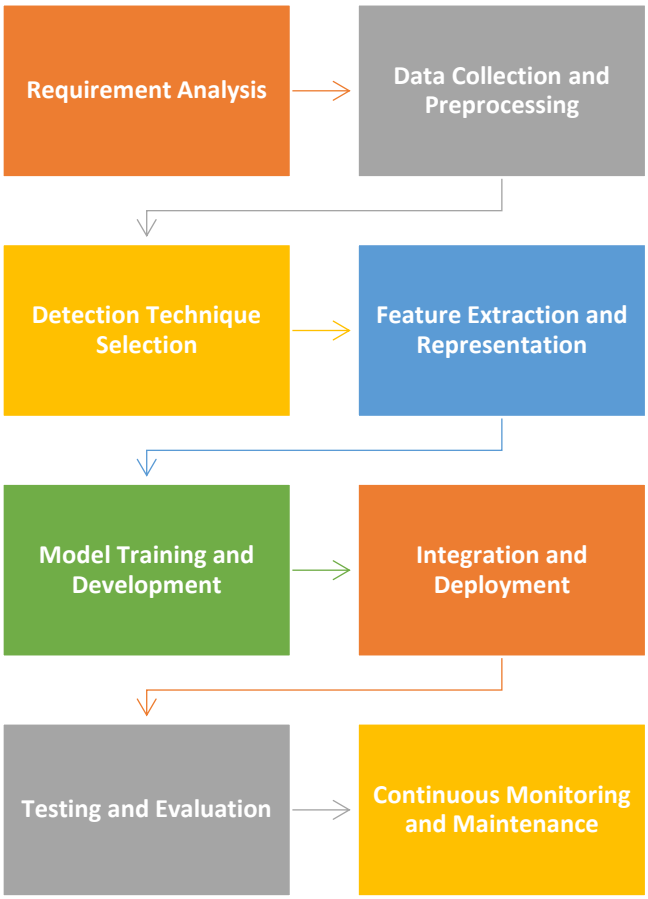

Fig 1

1. Requirement Analysis: Identifying the specific security needs and operational requirements of the network environment to tailor the intrusion detection system accordingly, ensuring alignment with organizational objectives and regulatory compliance.

2. Data Collection and Preprocessing: Gathering network traffic data from various sources, such as network sensors or packet captures, and preprocessing it to filter out irrelevant information, normalize data formats, and prepare it for analysis.

3. Detection Technique Selection: Choosing appropriate detection techniques based on the nature of threats, including signature-based detection for known attack patterns and anomaly-based detection for deviations from normal behavior, to maximize the system's ability to identify and mitigate threats.

4. Feature Extraction and Representation: Extracting relevant features from the preprocessed data, such as packet headers, payload content, or traffic flow characteristics, and

representing them in a suitable format for input into machine learning algorithms or rule-based detection engines.

5. Model Training and Development: Developing and training intrusion detection models using machine learning algorithms, rule sets, or statistical methods, utilizing labeled training data to learn patterns of normal and malicious behavior and improve detection accuracy.

6. Integration and Deployment: Integrating the developed detection models or rule sets into the network infrastructure and deploying the intrusion detection system in operational environments, ensuring compatibility with existing network components and minimal disruption to network operations.

7. Testing and Evaluation: Conducting thorough testing and evaluation of the intrusion detection system to assess its performance, detection accuracy, false positive rate, and scalability under different network conditions and attack scenarios.

8. Continuous Monitoring and Maintenance: Implementing ongoing monitoring of the intrusion detection system's performance and effectiveness, applying updates, patches, and configuration changes as needed, and adapting to evolving threats and network environments to ensure optimal security posture over time.

IV. Working of the Tool

Here's an overview of how NIDS typically works:

1.Traffic Monitoring: The NIDS passively monitors network traffic by capturing packets as they traverse the network. It can be deployed at various points within the network architecture, such as at network boundaries, within subnets, or even on individual hosts.[1][14]

2.Data Collection: Once network traffic is captured, the NIDS collects relevant data for analysis. This data includes packet headers, payload content, and other metadata that provide insights into the nature and characteristics of network communication.[1][14]

3.Preprocessing: Before analysis, the collected data undergoes preprocessing to filter out noise, normalize formats, and extract essential features. This step helps reduce the volume of data to be analyzed and ensures that only relevant information is passed on to the detection engine.[1][14]

4.Detection Engine: The core of the NIDS is its detection engine, which applies various detection techniques to identify potential security threats. These techniques can be categorized into signature-based detection and anomaly-based detection.[2][7]

- ***Signature-Based Detection:*** This technique involves comparing network traffic against a database of known attack signatures or patterns. If a match is found, indicating a known attack or malicious behaviour, the NIDS generates an alert.
- ***Anomaly-Based Detection:*** Anomaly detection focuses on identifying deviations from normal network behaviour. Machine learning algorithms or statistical models analyze network traffic patterns over time to establish a baseline of normal behavior. Any deviations from this baseline are flagged as potential anomalies**.**

5.Alert Generation: When the detection engine identifies suspicious activity or potential security breaches, it generates alerts to notify security personnel or automated response systems. These alerts typically include details about the detected threat, such as the type of attack, source and destination addresses, and severity level.

6.Logging and Reporting: The NIDS logs all detected events and activities for auditing and forensic analysis purposes. Detailed reports summarizing network security incidents, detection trends, and system performance are generated to facilitate ongoing monitoring, compliance reporting, and decision-making.

V. Implementation

The Steps involved in Implementation are as follows-

1. **Provide a csv/pcap file to NIDS**

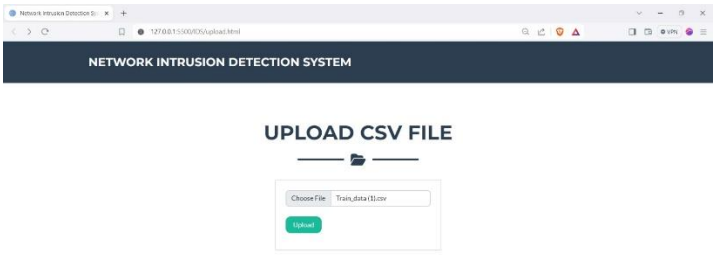

Fig.2. NIDS Dashboard (a)

2. **NIDS analyses the dataset and provides the reading of the data**

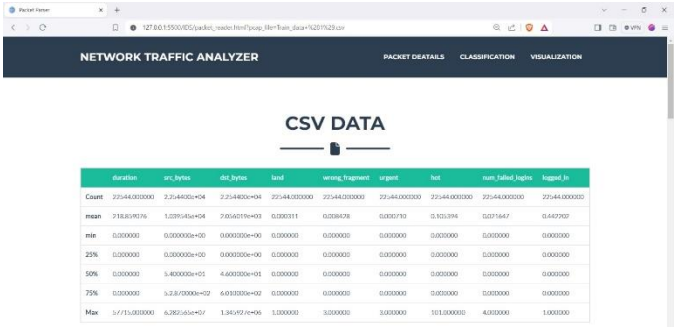

Fig.3. NIDS Dashboard (b)

3. **Classification of 3 algorithms is done to find which one gives the maximum accuracy**

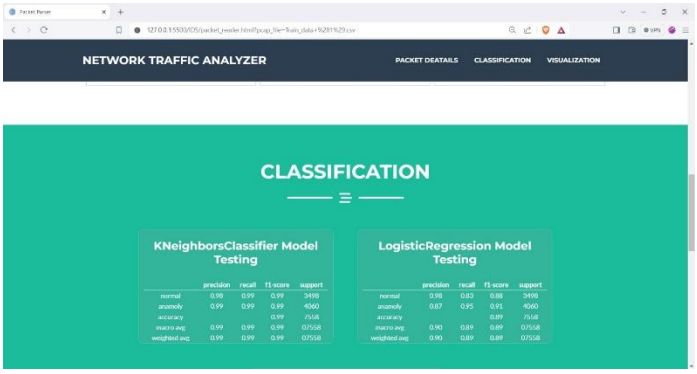

Fig.4. NIDS Dashboard (c)

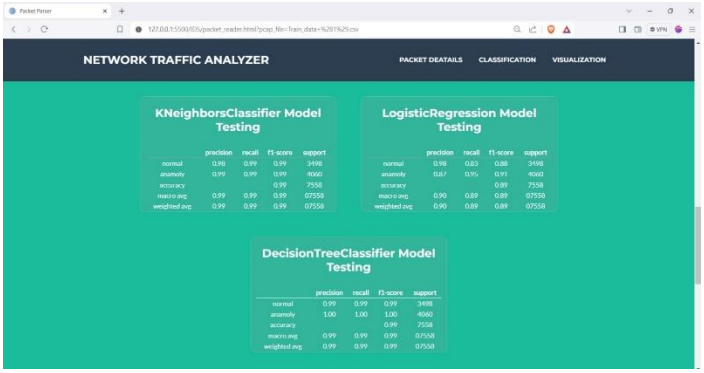

Fig.5. NIDS Dashboard (d)

4. Visualization of the Performance Data with Graphs

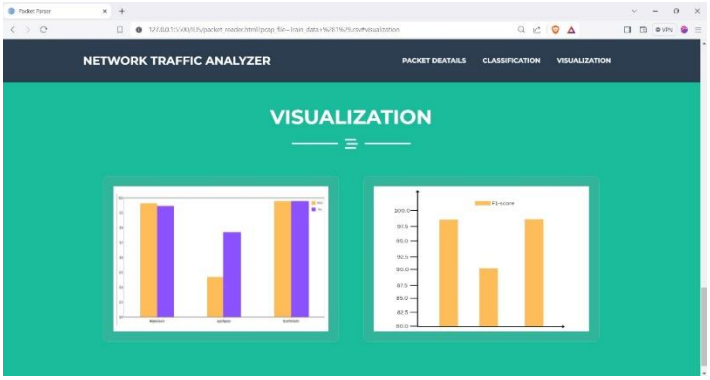

Fig.6. NIDS Dashboard (e)

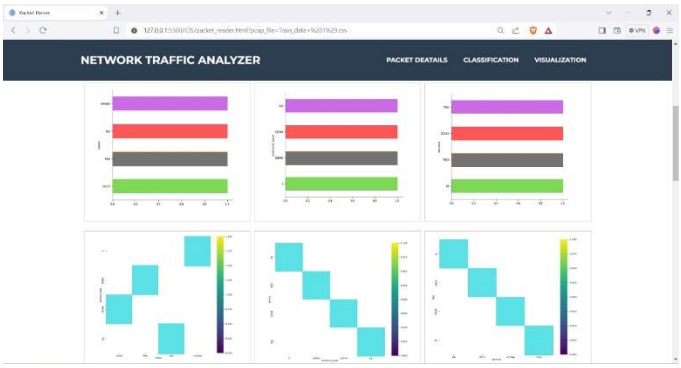

Fig.7. NIDS Dashboard (f)

VI. Limitations

1. Challenges with Encrypted Traffic: NIDS encounter difficulties when inspecting encrypted traffic due to the inherent secrecy of packet contents, hindering the system's ability to analyze and detect potential threats hidden within encrypted data streams.

2. Concerns with False Positives and Negatives: NIDS are susceptible to both false positives, where benign activities are mistakenly flagged as malicious, and false negatives, where actual intrusions evade detection. These occurrences can lead to alert fatigue among security personnel or, in more severe cases, overlook genuine security threats altogether.

3. Evasion Tactics Employed by Attackers: Advanced adversaries often employ evasion techniques to circumvent NIDS detection mechanisms. These tactics may include fragmenting packets, obfuscating payload data, encrypting communication channels, or employing traffic normalization methods to evade detection and launch successful attacks

4. Challenges in High-Speed Network Environments: NIDS face significant challenges in keeping pace with the rapid flow of data in high-speed network environments. Traditional architectures may struggle to handle the volume and velocity of network traffic, resulting in performance bottlenecks and diminished detection accuracy.

5. Resource Intensiveness of NIDS Deployments: Implementing comprehensive NIDS deployments necessitates significant resources, including robust hardware infrastructure, substantial processing power, and ample network bandwidth. The resource-intensive nature of NIDS deployments poses challenges in terms of scalability, maintenance, and operational costs.

VII. Conclusion

Network Intrusion Detection System (NIDS) stand as indispensable guardians of network security, playing a crucial role in identifying and mitigating potential threats in dynamic and interconnected environments. Despite their effectiveness in enhancing cybersecurity posture, NIDS face various challenges, including the inspection of encrypted traffic, concerns with false positives and negatives, evasion tactics employed by sophisticated adversaries, limitations in high-speed network environments, and the resource-intensive nature of deployments. However, advancements in technology, such as machine learning algorithms, behavioural analytics, and threat intelligence integration, hold promise in addressing these challenges and improving the efficacy of NIDS. Moreover, the collaborative efforts of cybersecurity professionals, researchers, and industry stakeholders are essential in developing innovative solutions and best practices to fortify NIDS against emerging threats and vulnerabilities. Ultimately, by continually evolving and adapting to the evolving threat landscape, NIDS play a vital role in safeguarding network infrastructures and ensuring the integrity, confidentiality, and availability of critical assets and resources.

References

[1] Z. Wang, T. Huang and S. Wen, "A File Integrity Monitoring System Based on Virtual Machine," 2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control, 2012, pp. 653-655, doi: 10.1109/IMCCC.2012.396.

[2] J. Kaczmarek and M. Wrobel, "Modern approaches to file system integrity checking," 2008 1st International Conference on Information Technology, 2008, pp. 1-4, doi: 10.1109/INFTECH.2008.4621669.

[3] F. Tomonori and O. Masanori, "Protecting the integrity of an entire file system," First IEEE International Workshop on Information Assurance, 2003. IWIAS 2003. Proceedings., 2003, pp. 95-105, doi: 10.1109/IWIAS.2003.1192462.

[4] G. Daci and M. Shyle, "Improving data integrity and performance of cryptographic structured log file systems," 2011 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011, pp. 1-5, doi: 10.15208/ati.2011.8.

[5] A. Pinheiro, E. D. Canedo, R. T. De Sousa and R. De Oliveira Albuquerque, "Monitoring File Integrity Using Blockchain and Smart Contracts," in IEEE Access, vol. 8, pp. 198548-198579, 2020, doi: 10.1109/ACCESS.2020.3035271.

[6] B. Wilbert and L. Chen, "Comparison of File Integrity Monitoring (FIM) techniques for small business networks," Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2014, pp. 1-7, doi: 10.1109/ICCCNT.2014.6963090.

[7] B. Shi, B. Li, L. Cui and L. Ouyang, "Vanguard: A Cache-Level Sensitive File Integrity Monitoring System in Virtual Machine Environment," in IEEE Access, vol. 6, pp. 38567-38577, 2018, doi: 10.1109/ACCESS.2018.2851192.

[8] Udzir, Nur & Samsudin, Khairulmizam. (2011). "Towards a Dynamic File Integrity Monitor through a Security Classification". International Journal of New Computer Architectures and their Applications (IJNCAA). 3. 789-802.

[9] NARAYAN KULKARNI, Neha; KUMAR A. JAIN, Shital; Survey on Data Integrity, Recovery, and Proof of Retrievability Techniques in Cloud Storage. International Journal of Engineering & Technology, [S.l.], v. 7, n. 3.6, p. 55-58, july 2018. ISSN 2227-524X.

[10] Anusha Priya.G, Mrs. Esther Daniel: A Literature Survey on Integrity Verification

[11] Techniques, International Journal of Engineering Research & Technology (IJERT)ISSN: 2278-0181 Vol. 4 Issue 05, May-2015.

[12] F. Li, F. Xiong, C. Li, L. Yin, G. Shi and B. Tian, "SRAM: A State-Aware Risk Assessment Model for Intrusion Response," 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), 2017, pp. 232-237, doi: 10.1109/DSC.2017.9.

[13] R. R. Jueneman, "Integrity controls for military and commercial applications," [Proceedings 1988] Fourth Aerospace Computer Security Applications, 1988, pp. 298-322, doi: 10.1109/ACSAC.1988.113351.

[14] C. Zeidler and M. R. Asghar, "CloudEFS: Efficient and secure file system for cloud storage," 2016 14th Annual Conference on Privacy, Security and Trust (PST), 2016, pp. 239-246, doi: 10.1109/PST.2016.7906969.

[15] Nguyen Anh Quynh and Y. Takefuji, "A Real-time Integrity Monitor for Xen Virtual Machine," International conference on Networking and Services (ICNS'06), 2006, pp. 90-90, doi: 10.1109/ICNS.2006.13.

[16] I. F. A. Shaikhli, A. M. Zeki, R. H. Makarim and A. -S. K. Pathan, "Protection of Integrity and Ownership of PDF Documents Using Invisible Signature," 2012 UKSim 14th International Conference on Computer Modelling and Simulation, 2012, pp. 533-537, doi: 10.1109/UKSim.2012.81.

[17] S. Deepika and P. Pandiaraja, "Ensuring CIA triad for user data using collaborative filtering mechanism," 2013 International Conference on Information Communication and Embedded Systems (ICICES), 2013, pp. 925-928, doi: 10.1109/ICICES.2013.6508262.

[18] Y. Wang, B. Zhang, W. Lin and T. Zhang, "Smart grid information security - a research on standards," 2011 International Conference on Advanced Power System Automation and Protection, 2011, pp. 1188-1194, doi: 10.1109/APAP.2011.6180558.

[19] I. V. Mashkina, M. B. Guzairov, V. I. Vasilyev, L. R. Tuliganova and A. S. Konovalov, "Issues of information security control in virtualization segment of company information system," 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM), 2016, pp. 161-163, doi: 10.1109/SCM.2016.7519715.

[20] M. Tvrdikova, "Information system integrated security," 2008 7th Computer Information Systems and Industrial Management Applications, 2008, pp. 153-154, doi: 10.1109/CISIM.2008.41.

[21] J. Kim, I. Kim and Y. I. Eom, "NOPFIT: File System Integrity Tool for Virtual Machine Using Multi-byte NOP Injection," 2010 International Conference on Computational Science and Its Applications, 2010, pp. 335-338, doi: 10.1109/ICCSA.2010.79.

[22] zettaset's "Data Integrity Attacks: Is Data Manipulation More Dangerous Than Theft?" https://www.zettaset.com/blog/data-integrity-attacks-data-manipulation-more-dangerous

[23] "Data Integrity Attacks: Welcome to the next level in Cyber Security arena." by cyware : https://cyware.com/news/data-integrity-attacks-welcome-to-the-next-level-in-cyber-security-ar ena-0136466d

[24] A protocol Article " A 'nightmare scenario': Data-tampering attacks are hard to detect, with devastating consequences" :

[25] https://www.protocol.com/enterprise/data-integrity-security-cyberattacks-threat

[26] The dash module in python : https://dash.plotly.com/introduction

[27] The plotly module for graphs : https://plotly.com/python/