ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

Comprehensive Review of Network Intrusion Detection and Prevention Systems

Ms. Hemangni Mehta, Ms. Anjali Nizama, Ms. Subhashini K

P P Savani University, India

DOI: https://doi.org/10.51583/IJLTEMAS.2025.140600087

Abstract— The global network infrastructure remains vulnerable and is susceptible to attacks from various sources. These attacks can take the form of denial-of-service (DoS) or other malicious threats. To safeguard such networks, Intrusion Detection and Prevention Systems (IDPS) are employed. These systems serve as critical security mechanisms designed to detect and prevent both internal and external threats.IDPS continuously monitor network traffic using a variety of techniques. When suspicious or malicious activity is detected, the system blocks the threat and generates alerts for further investigation. Intrusion remains a significant challenge, especially in hybrid computing environments.This paper explores key concepts including network intrusion, types of intrusions, intrusion detection systems, and a review of previous research related to IDPS. The software solutions implemented to counter such threats are referred to as intrusion prevention systems (IPS). Various types of prevention systems are discussed within this study.

Keywords— Intrusion detection system, Hybrid computing, Hybrid in Detection system, prevention system

I. Introduction

A growing number of organizations rely on information systems to carry out their primary business operations. Consequently, the occurrence and severity of intrusion incidents have risen considerably. These intrusion attacks can stem from various sources, such as malware (e.g., worms, spyware), unauthorized system access, and the misuse of privileges or attempts to escalate privileges. While certain incidents are intentionally harmful, others may not be. To minimize exposure to both types of intrusion threats, organizations require Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Network-based IDS focus on detecting network-level attacks originating both externally and internally within the organization. They utilize network adapters operating in promiscuous mode to observe network activity in real-time. This mode makes detection and localization by attackers particularly difficult. However, network-based IDS lack scalability.

AES encryption is employed to safeguard databases within network systems and also identifies and mitigates intrusion attacks such as SQL injection. It introduces an extra layer of protection in the Database Management System (DBMS). This approach is applicable to any type of database and addresses the shortcomings of current database security techniques [1]. Monitoring processes alone do not guarantee adequate assurance and protection [3]. A Hybrid Intrusion Detection System has been developed using the .Net framework as the front-end and SQL Server as the back-end for data storage. This system is implemented in a hybrid environment. Its dynamic nature is supported by a straightforward and user-friendly interface. The scalability and self-adaptive features of the Hybrid Intrusion Detection System are realized by deploying it across both the network and all hosts within the network [2].

Issue in Hybrid Computing System

A new hybrid intrusion detection system combines the advantages of low false-positive rate of a signature-based IDS and the ability of an anomaly-based IDS to "detect novel unknown attacks"[4].The hybrid system extracts signatures from the output of the anomaly-based system and adds them to the signature database for accurate and efficient intrusion detection .It was shown that the hybrid IDS had a 60 percent detection rate in comparison to 30 percent and 22 percent for SNORT and Bro systems, respectively. This was obtained with less than 3 percent false alarms. This method thus achieves a "higher detection accuracy, lower false alarms, and, thus, a raised level of "cyber trust" through the automated data mining and signature generation process over Internet connection episodes[4]. Hybrid Computing can also be called as On Demand Computing. Another interesting fact about Hybrid computing is that, Hybrid computing is like an elephant, for those who see this elephant in front will say it as snake, for those whose see in the side will say it as wall etc, yet few are able to say it is an elephant. There is no proper definition or none has defined Hybrid computing in a standardized manner [2].

Hybrid Intrusion Detection System

Nowadays, most services are delivered through the Internet. As a result, intrusion threats have become a major concern in hybrid computing networks. Intrusion can be simply defined as the unauthorized access or entry of a person or system into another system, potentially causing harm. Inadequate authentication mechanisms in networks allow attackers or hackers to compromise the system. To protect the network from such intrusions, it is essential to detect them promptly. Various systems are employed for intrusion detection. The proposed Hybrid Computing Intrusion Detection System offers reliable and standardized security against such threats. Intrusions refer to unauthorized access that can damage systems or steal sensitive data. Weak authentication mechanisms make networks vulnerable to such attacks. A Hybrid Computing Intrusion Detection System (HCIDS) provides a robust solution by detecting and preventing these threats in real time.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

Intrusion Detection Systems can be broadly categorized into three types:

- Anomaly-based Intrusion Detection Systems
- Pattern-matching (or Signature-based) Intrusion Detection Systems
- Hybrid Intrusion Detection Systems

Anomaly-based Intrusion Detection Systems

The statistical anomaly detection model identifies intrusions by observing activities that diverge from a user's typical behavior. It establishes a baseline of normal activity by profiling individual users or network connections, and then monitors for deviations from this baseline. Since the model focuses on unusual behavior, it has the capability to detect previously unknown attacks. However, due to the unpredictable nature of user and network behavior, it tends to produce a high number of false positives. Additionally, these systems often require extensive training data and detailed event logs to accurately define normal behavior patterns. Sophisticated attackers may also find ways to bypass or disable such detection mechanisms.

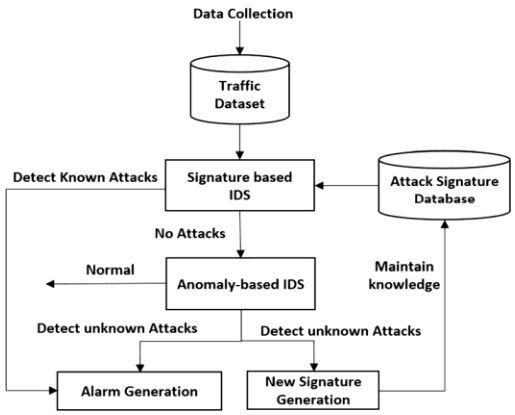
Pattern-matching (Signature-based) Intrusion Detection Systems

Pattern-matching (or signature-based) IDS examine network traffic and look for documented patters of attack. The system examines "every packet on the network segment for a defined pattern of activity that indicates an attempt to access a vulnerable script on a web server". Implementation of patter- matching IDS takes a shorter period of time than anomaly IDS, provided that there is a pattern-matching engine It is easy to implement, deploy, update and understand pattern- matching IDS.They produce less false positives than do anomaly-based IDS. They are vulnerable to hacking. They cannot detect unknown attacks. Constant updating is required in this type of Detection system. They are easier to "fool by sending fragmented packets across the network"[3].

Hybrid Intrusion Detection Systems

This section includes the design of hybrid intrusion prevention approach, and describes its basic concepts from previously research work. Hybrid Detection and prevention system overcome the Problem of above both intrusion detection system. Hybrid approaches have been proposal to combine this advantage of both signature-based and anomaly-based. Both systems have advantages and disadvantages. Hybrid Intrusion detection system overcome the problem of both system [2]. Hybrid IDS consists of six components viz., i) Data acquisition module, ii) Signature database, iii) Analyser, iv) Anomaly detector, v) Signature generator, and vi) Counter-measure module [9].

Figure1. Systematic Diagram of Hybrid IDS



Related Works

Intrusion Detection Systems (IDS), Hasina A. Razzak

[2] proposed a methodological approach for implementing IDS in hybrid networks. This work primarily addresses key challenges related to hybrid detection within network environments.

Rana Aamir Raza and Xi-Zhao Wang [3] introduced a fuzziness-based semi-supervised learning method for IDS. In their implementation, a hybrid intrusion detection system was developed using the .NET framework as the front-end and SQL Server as the back- end for data storage. The system utilizes both anomaly- based and misuse-based techniques to detect intrusions within the network.

Komal Dhok [4] focused on implementing a pattern- matching algorithm to prevent SQL injection attacks. The proposed solution includes the use of graphical passwords during login to enhance authentication and minimize the risk of attacks, thereby providing stronger security.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

Nilesh B. Nanda [7] contributed work on classification methods in IDS. The study discusses the limitations of anomaly-based systems and categorizes hybrid NIDS, which include alert mechanisms to notify administrators of detected threats.

Kanubhai K. Patel [9] also worked on the implementation of IDS. His paper presents the architecture of a hybrid intrusion detection system, emphasizing its integration with hybrid computing environments to enhance security management.

Architecture of our Hybrid IDS

The Data Acquisition Module incorporates multiple sensors, which are deployed either on individual hosts or specific network segments. Sensors placed on individual hosts monitor packets as they enter and leave the host, whereas those on network segments analyze packets moving through the segment. For optimal detection, sensors should be positioned to capture all incoming and outgoing packets. However, segment-based sensors may fail to capture all traffic under high loads. Although installing sensors on each host may require significant effort, it improves detection accuracy. Ensuring full packet capture is essential to prevent any intrusion from bypassing the IDS. In our implementation, Snort is utilized on a Windows operating system with WinPcap for packet capture.

The Signature Database stores a collection of known signatures, rules, or criteria used to compare against packets captured by the sensors. This database must be installed alongside the IDS software and hardware. Once set up, the sensors collect packet data from the network and reassemble them, accounting for issues such as out-of- order delivery, duplication, or high-speed arrival. Therefore, data storage is required to temporarily store packets for accurate analysis [9].

The Analyzer Module processes these packets by matching them against known patterns in the Signature Database using a pattern-matching algorithm, specifically the Aho-Corasick algorithm [1]. If a match is found, it identifies a known attack and sends an alert to the Countermeasure Module, while also logging the event. If no match is detected, the data is forwarded to the Anomaly Detector, which applies pattern mining techniques to identify unusual activity.

If the Anomaly Detector detects suspicious behavior, it notifies the Signature Generator, which then formulates a new rule or signature and updates the Signature Database accordingly.

Upon receiving an alert, the Countermeasure Module notifies the system administrator through pre-configured methods such as pop-up alerts or email notifications. In addition to these notifications, the module can be configured to execute automatic responses when alerts are triggered.

This module is also used by network administrator to evaluate the alert message and to take proper actions such as dropping a packet or closing a connection. The administrator can anticipate having to fine-tune the signature database to account for situations that seem to the IDS to be intrusions but that are actually legitimate traffic. For example, an adjustment might be made to enable traffic that might otherwise be seen by the firewall as suspicious, such as a vulnerability scan performed by a scanning device located at a particular IP address. The IDS could be configured to add a rule that changes the action performed by the IDS in response to traffic from that IP address from Alarm to Drop.

Conclusion

The proposed of Hybrid model is Detect malicious packets within network traffic and stop intrusions dead, blocking the aberrant traffic automatically before it does any damage in Hybrid network rather than simply giving an alert as, the malicious load has been delivered. It were invented independently to resolve ambiguities in network monitoring by placing prevention.

Future Scope

The proposed model can be implemented in very low cost and within short time.

References

1. Yashashree Dawle, Manasi Naik,Sumedha Vande,Nikita Zarkar ,"Reserch of Database Security Using Intrusion Detection System" International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137 Volume – 02, Issue – 03, March – 2017, PP – 01-06.
2. Janu Gupta, Jasbir Singh" Detecting Anomaly Based Network Intrusion Using Feature Extraction and Classification Techniques" International Journal of Advanced Research in Computer Science,volume 8, No. 5, May – June 2017.
3. Atmaja Sahasrabuddhe, Sonali Naikade, Akshaya Ramaswamy, Burhan Sadliwala , Prof.Dr.Pravin Futane," Survey on Intrusion Detection System using Data Mining Techniques, International Research Journal of Engineering and Technology (IRJET)Volume:04 Issue: 05 May -2017 .
4. Kanubhai K. Patel, Bharat V. Buddhadev"Research of An Architecture of Hybrid Intrusion Detection System" International Journal of Information & Network Security (IJINS) Vol.2, No.2, April 2013, pp. 197~202.
5. Amaan Anwar & Syed Imtiyaz Hassan," Applying Artificial Intelligence Techniques to Prevent Cyber Assaults "International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 5 (2017), pp.
6. Ghosh, A. Shinde, and N. Pissinou, "A Survey on Network Intrusion Detection using Deep Learning Techniques," IEEE Access, vol. 9, pp. 21932–21957, 2021. DOI: 10.1109/ACCESS.2021.3056066
7. B. Subba, S. Biswas, and S. K. Das, "A Neural Network- Based System for Intrusion Detection and Attack Classification,"

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

Computer Communications, vol. 145, pp. 167–175, Nov. 2019.
8. DOI: 10.1016/j.comcom.2019.07.006
9. M. Usama et al., "Unsupervised Machine Learning for Networking: Techniques, Applications and Research Challenges," IEEE Access, vol. 7, pp. 65579–65615, 2019. DOI: 10.1109/ACCESS.2019.2916648
10. S. Shone and Q. N. Ng, "A Deep Learning Approach to Network Intrusion Detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, Feb. 2018.DOI: 10.1109/TETCI.2017.2772792
11. S. B. Jadhav and A. R. Thakare, "Anomaly Detection for Network Intrusion Prevention: A Hybrid Approach," Procedia Computer Science, vol. 167, pp. 719–728, 2020. DOI: 10.1016/j.procs.2020.03.387