Vol 6, Issue 2, February 2026 www.ijesti.com E-ISSN: 2582-9734
International Journal of Engineering, Science, Technology and Innovation (IJESTI)

Advanced Intelligent Intrusion Detection and Prevention Systems for Real Time Network Security

Dogiparthy Sravankumar [1]

[1] Research Scholar, Department of Computer Science, Mansarovar Global University, Sehore, M.P., India.

Dr. G. Soma Sekhar [2]

[2] Supervisor, Department of Computer Science, Mansarovar Global University, Sehore, M.P., India.

ABSTRACT

An intrusion detection and prevention system (IDPS) is a tool that keeps an eye out for potential dangers on a network and then takes measures to thwart them. As an intrusion detection system (IDS), an IDPS is quite similar to an IDS. Although both systems are capable of detecting dangers and sending alarms, an IDPS goes a step further by trying to fix those threats. In order to improve the efficacy of intrusion detection and prevention in real-time network settings, this study introduces a sophisticated intelligent method. If implemented, the suggested system will increase detection accuracy while decreasing false alarms by integrating several detection approaches such as signature-based detection, anomaly-based detection, and stateful protocol analysis. The system can easily detect both known and undiscovered threats by analyzing network traffic patterns and recognizing odd behaviour.

Keywords: *Security, Attacks, Anomaly Detection, Signature, Traffic.*

I. Introduction

With more and more people using the Internet, there are more and more security risks. A holistic view of computer security is necessary for the implementation of intrusion detection systems on hosts and networks. Information technology infrastructures are becoming more complicated at an alarming rate, making it impossible for a single individual to comprehend them, much less manage them securely. A network's security measures are those put in place by the network administrator to keep the network and its resources safe from abuse, alteration, denial of service, and other forms of unauthorised access.

Criminal assaults on the internet are becoming more common, more sophisticated, and more destructive annually, according to a CERT report. Thanks to the expansion of high-speed internet connections, the World Wide Web has become a global community of interconnected individuals. In addition, criminals (hackers, crackers, and thieves) may attack your system from anywhere in the world since network connection is so inexpensive. In addition, desktop PCs and laptops are pricey. Criminals may quickly set up machines running several operating systems and then hunt for systems that are susceptible enough to begin an attack. Further complicating efforts to manage and regulate assaults on computer systems is the global and dispersed character of the Internet.

A key difficulty in stopping unauthorised activity is the automatic finding of breaches into computer systems. Firewalls play an important role in limiting who may access the computers within a protected network, but they aren't foolproof and won't keep bad actors out. Careful manual monitoring of user activity or access records is required for intrusion detection. Not to mention that they're really slow (with a lengthy response time).

The majority of intrusion detection systems and intrusion prevention systems rely on two main mechanisms: signature-based detection and misuse detection. It notifies users when the system exhibits one of the defined "unacceptable" behaviours. While easy to implement and run, these solutions are only foolproof against specific, pattern-based forms of attack. A popular intrusion detection system that leverages the abuse notion is SNORT [5]. And because it's hard to keep a database of approved behaviours current, this method can't protect you against attacks that are completely out of the ordinary. In contrast, anomaly detection techniques build a profile of a user's usual behaviour and then trigger an alarm if the user tries to do something that doesn't match the profile. While this method is usually quite comprehensive in its ability to identify hit patterns, it takes a lot of work to build algorithms that can accurately profile users.

Signature based intrusion detection systems may quickly identify typical attempts and give protection against them by matching string patterns or signatures. Current signature-based detection is useless in the current circumstance because to the high volume of reported fresh incursions and attempts. While there have been several suggested IDPS, none of them have been as accurate or comprehensive as would be ideal. For example, most rely on signatures to identify attacks; while signature-based approaches are easy to implement and quick, they cannot identify attacks that are not yet known. To make up for that, we need an IDS/IPS system that can protect us from intrusions and assaults quickly and efficiently in real time.

II. Basic Functions of an IDPS

An intrusion detection and prevention system offers the following features:

Figure 1: Basic Functions of an IDPS

Guards Technology Infrastructure and Sensitive Data

Nowadays, data-driven companies make it impossible for any system to function independently. Since data is always moving over the network, hiding in the data itself is the simplest approach to attack or get access to a system. As soon as the intrusion detection system detects suspicious activity, it notifies the appropriate security personnel. The intrusion prevention system (IPS) component is proactive, enabling security personnel to lessen the impact of these assaults that might harm the company's finances and image.

Reviews Existing User and Security Policies

User rules and access-related policies for apps and systems are unique to every security-driven company. By limiting access to vital resources to a small number of trusted user groups and systems, these policies drastically lower the attack surface. Administrators can quickly identify any vulnerabilities in these policy frameworks thanks to intrusion detection and prevention systems' continuous monitoring. Furthermore, administrators may fine-tune regulations to ensure optimum efficiency and security.

Gathers Information About Network Resources

A bird's-eye view of the traffic streaming across its networks may also be provided by an IDS-IPS to the security team. They may then adjust a system in the event of server underutilisation or traffic congestion thanks to this improved visibility into network resources.

Helps Meet Compliance Regulations

More and more rules are being put in place to make sure that customer data is safe and secure for all kinds of organisations. In most cases, implementing an intrusion detection and prevention system is the initial stage in meeting these requirements.

An intrusion detection system (IDPS) checks processes for malicious patterns, compares system files, and keeps an eye on user and system activity. IPS achieves incident prevention by utilising web application firewalls and traffic filtering techniques.

III. IDPS Detection Methodologies

In order to identify assaults, IDPS systems employ a wide variety of methods. Stateful protocol analysis, signature-based analysis, and anomaly-based analysis are the main techniques. Below, you can find detailed descriptions of these approaches.

Signature-Based Detection

In order to identify potential threats, a signature-based intrusion detection system (IDS) looks through data flow for patterns that correspond to recognised signatures. An assault's signature is a pattern that is recognised to correlate to a specific sort of attack. By matching signatures with observed events, signature-based detection can uncover potential threats. Signatures can take the form of:

- A telnet attempt with a username of “root”, which is a violation of an organization’s security policy.
- An e-mail with a subject of “Free pictures!” and an attachment filename of “freepics.exe”, which are characteristics of a known form of malware.
- An operating system log entry with a status code value of 645, which indicates that the host’s auditing has been disabled.

Due to the fact that many assaults have discernible fingerprints, signature-based intrusion detection systems are extensively utilised. One drawback of signature-based approaches is the constant need to update the signature database of intrusion detection systems (IDSs) in response to newly discovered attack techniques.

Anomaly-Based Detection

By comparing predefined standards of behaviour with actual occurrences, anomaly-based detection can spot out-of-the-ordinary changes. Profiles in an anomaly-based detection intrusion detection system depict the typical actions of various entities, including users, hosts, connections to the network, and applications. The profiles are created by tracking the features of regular behaviour over time.

The ability of anomaly-based detection systems to effectively identify previously unseen threats is its primary advantage. Consider the following scenario: a computer becomes infected with a new kind of virus. Malware can divert system resources, send an overwhelming amount of emails, establish an excessive number of network connections, and engage in other actions that are not in line with the computer's predefined profiles.

Typical issues with anomaly-based detection include creating profiles that do not accurately represent real-world computer activity, producing an excessive number of false positives, and unintentionally include harmful activity inside a profile.

Stateful Protocol Analysis

Stateful protocol analysis involves comparing observed events with predefined profiles of benign protocol activity for each protocol state in order to detect deviations from these criteria. Stateful protocol analysis differs from anomaly-based detection in that it employs vendor-developed universal profiles to dictate the proper and improper usage of individual protocols, as opposed to host-or network-specific profiles. Network, transport, and application protocols that include a sense of state are able to be understood and tracked by the IDPS, thanks to the "stateful" part of stateful protocol analysis.

Unexpected command sequences, such as continually issuing the same command or a command that is dependent on another command not being issued before, can be identified by stateful protocol analysis. The IDPS can record the authenticator used for suspicious behaviour and maintain track of the authenticator used for each session thanks to stateful protocol analysis, which also allows for state tracking. Additionally, certain IDPSs can make use of the authenticator data to set varying standards for acceptable user behaviour across different user classes or even for individual users.

IV. Benefits of Using IDPS

Among the many benefits that may be gained by implementing intrusion detection and prevention system technologies are:

Early Threat Detection

The capacity to constantly watch network activity is a major benefit of IDPS. You may detect suspicious activity before it escalates into a major cyber disaster thanks to this real-time monitoring, which allows early detection of potential hazards. The best way to stop hackers from getting into your systems is to move swiftly.

Improved Incident Response

Quick notifications and information about the type of danger are provided by IDPS if an incursion is found. Your security staff must have this information in order to react quickly and efficiently. With better incident response, your organization may lessen the blow of a cyberattack by reducing the likelihood of harm.

Protecting Sensitive Data

When it comes to protecting confidential data, IDPS is crucial. These solutions prevent your data from getting into the wrong hands by detecting attempts at unauthorised access. Data breaches may have devastating effects for organisations that deal with customers' personal or financial information, thus this is of the utmost importance for them.

Enhanced Security Visibility

IDPS provides helpful information on system and network activity. With this level of transparency, your security team may identify and assess possible system vulnerabilities. Improving your entire security posture and fortifying your defences begins with pinpointing their weak spots.

Support for Compliance

Intruder detection systems are a need for many businesses due to rules and laws. If your business is concerned about penalties or legal issues stemming from noncompliance, IDPS may help it achieve these compliance duties.

Reduced Risk of Data Breaches

Identify and prevent security incidents (IDPS) aids in the prevention of attacker access to critical data by continually monitoring and alerting on suspicious actions. Data breaches, which may lead to major consequences including damaged reputations, lost trust from customers, and expensive legal battles, are made far less likely by this measure.

Increased Security Awareness

Improving your company's security awareness may be as simple as using an IDPS. A culture of alertness is fostered among employees by the alerts and reports generated by these systems, which highlight possible security threats. The organization may take more proactive security steps if more people are aware of the issue.

V. IDPS Security Capabilities

IDPS systems usually have a wide range of detecting capabilities. More precise detection and more tuning and customisation options are typically supported by solutions that employ a mix of detection approaches. Depending on the IDPS technology, the kinds of events that may be recognised and the usual accuracy of such detections can differ substantially. When it comes to improving the detection accuracy, usability, and efficacy of most IDPSs, tweaking and customisation are usually necessary. Following are some examples of the capabilities for adjusting and customisation.

Information Gathering Capabilities

Collecting host or network information from observed behaviour is one example of the information gathering capabilities offered by some IDPS platforms. A few examples are figuring out what the network is generally like and figuring out what hosts utilise in terms of operating systems and apps.

Logging Capabilities

IDPSs usually keep a lot of records on the incidents they find. This information may be utilised to verify the accuracy of warnings, probe occurrences, and establish connections between events recorded by the IDPS and other sources of logging. Date and time of the incident, event type, important rating (e.g., priority, severity, impact, confidence), and any preventative action taken are data variables that IDPSs often employ. For example, host-based IDPSs record user IDs while network-based IDPSs collect packets. These types of IDPSs log extra data fields. Security information and event management software, or syslog, are examples of centralised logging servers that managers may get log copies of via IDPS technology. For data availability and integrity, it's best to save logs in two places: one locally and one centrally. If an attacker were to hack the IDPS, for example, they might change or delete the logs. It is important to keep the clocks of IDPSs synchronised with each other or with the Network Time Protocol (NTP) in order to ensure that the timestamps in their log entries are accurate.

Detection Capabilities

Typically, intrusion detection system technologies have wide-ranging detecting capabilities. More precise detection and more tuning and customisation options are typically supported by solutions that employ a mix of detection approaches. Depending on the IDPS technology, the kinds of events that may be recognized and the usual accuracy of such detections can differ substantially. Improving the detection accuracy, usability, and efficacy of most IDPSs requires some tweaking and customization. This includes specifying the preventative actions to be executed for certain warnings, among other things. The degree to which technologies may be adjusted and personalized varies greatly. The degree to which a product's detection accuracy may be enhanced from its default configuration is directly proportional to the strength of its tweaking and customization options. When assessing products, organizations should give serious thought to the IDPS technologies' ability for tweaking and customization.

Prevention Capabilities

The particular capabilities offered by different types of IDPS technology differ, however most of them offer numerous preventative capabilities. The setup of the preventive capabilities for each sort of warning may often be specified by administrators in IDPSs. It is common practice to enable or disable prevention and to indicate the sort of preventive capability to be utilised in this context. A learning or simulation mode is available on some IDPS sensors; in this mode, the sensors will not conduct any preventative steps but will instead show when they would have. By allowing administrators to carefully observe and adjust the setup of the prevention capabilities prior to activating preventive measures, the likelihood of unintentionally blocking legitimate activity is reduced.

VI. Conclusion

Network security is a major issue for both consumers and organisations due to the growing reliance on computer networks and internet-based services. The ability to continuously monitor and guard against harmful activity is provided by Intrusion Detection and Prevention Systems, which are an integral part of current cybersecurity frameworks. The suggested method improves the efficiency and accuracy of threat identification by integrating several detection approaches, such as signature-based detection, anomaly-based detection, and stateful protocol analysis. The technology can improve the security of network infrastructures by detecting both common and unusual attack behaviours. Better security management and quicker incident response are both made possible by features like real-time warnings, logging procedures, and automatic preventative measures. Secure critical information, keep network operations running reliably, and lessen the likelihood of cyber assaults using advanced intrusion detection and prevention systems.

References

1. M. Mehta, M. Nizama, and M. K, “Comprehensive Review of Network Intrusion Detection and Prevention Systems,” *International Journal of Latest Technology in Engineering Management and Applied Science*, vol. 14, no. 6, pp. 804–807, 2025.
2. A. Singh, J. Prakash, G. Kumar, P. Jain, and L. Ambati, “Intrusion Detection System,” *Journal of Database Management*, vol. 35, no. 1, pp. 1–25, 2024.
3. S. Abbas, W. Naser, and A. Abbas, “Subject review Intrusion Detection System and Intrusion Prevention System,” *Global Journal of Engineering and Technology Advances*, vol. 14, no. 2, pp. 155–158, 2023.
4. T. Sowmya and M. A. Mary, “A Comprehensive Review of AI Based Intrusion Detection System,” *Measurement Sensors*, vol. 28, no. 4, pp. 1–13, 2023.

5. A. N. Prasad, V. Kumar, K. Rachith, and S. Rokhade, "Intrusion Detection and Prevention Systems A Comparative Analysis of Techniques and Approaches," vol. 12, no. 2, pp. 59–62, 2023.
6. M. Ni, "A Review on Machine Learning Methods for Intrusion Detection System," *Applied and Computational Engineering*, vol. 27, no. 1, pp. 57–64, 2023.
7. A. Tasneem, A. Kumar, and S. Sharma, "Intrusion Detection Prevention System Using SNORT," *International Journal of Computer Applications*, vol. 181, no. 32, pp. 21–24, 2018,
8. A. Sharifi, F. Zad, F. Farokhmanesh, A. Noorollahi, and J. Sharif, "An Overview of Intrusion Detection and Prevention Systems and Security Issues," *IOSR Journal of Computer Engineering*, vol. 16, no. 1, pp. 47–52, 2014.
9. M. Korcak, J. Lamer, and F. Jakab, "Intrusion Prevention Intrusion Detection System for WiFi Networks," *International Journal of Computer Networks and Communications*, vol. 6, no. 4, pp. 77–89, 2014, doi: 10.5121/ijcnc.2014.6407.
10. A. Patel, M. Taghavi, K. Bakhtiyari, and J. C. Junior, "An Intrusion Detection and Prevention System in Cloud Computing A Systematic Review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 1–33, 2012.
11. Y. Farhaoui and A. Asimi, "Performance Method of Assessment of the Intrusion Detection and Prevention Systems," vol. 3, no. 7, pp. 5916–5928, 2012.
12. I. Mukhopadhyay, M. Chakraborty, and S. Chakrabarti, "A Comparative Study of Related Technologies of Intrusion Detection and Prevention Systems," *Journal of Information Security*, vol. 2, no. 1, pp. 28–38, 2011.