International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

An Analysis of AI-Driven, Anomaly Detection, and Signature-Based Intrusion Detection and Prevention Systems in Modern Cyber-security

Dr.Hemanth Kumar K G [1], Shubha B G [2]

[1,2] Lecturer, Department of Computer Science, SJR College of Science, Arts and Commerce, Race Course Road, Bengaluru - 560 009, India

Abstract: Security systems termed intrusion detection and prevention systems are designed to monitor or scan computer networks and systems for the presence of security threats. Intrusion detection and prevention systems are programmed to detect and prevent the occurrence of security threats to computer networks. The IDPS automatically detects and prevents computer network security problems. These systems achieve their objectives by reducing vulnerabilities in the computer networks that are being monitored. To detect and prevent security threats, the intrusion detection and prevention systems use various methods such as signature based, anomaly based, stateful protocol analysis and hybrid that combines the first three methods to detect and prevent security threats. Hybrid systems incorporate one or more of the three methods mentioned above to detect and prevent security threats. The choice of methods is not always straight-forward due to various systems using multiple methods. This study looks at core detection methods, including signature-based, anomaly-based, stateful protocol analysis and hybrid models, to clarify how they work and help users choose the right system.

Keywords: Intrusion detection, Protocols, Monitoring, Network, Anomaly, Resistance

1. INTRODUCTION

1.1 Intrusion Detection Systems

An Intrusion Detection System (IDS) is a cybersecurity mechanism that observes network traffic, host activity, or endpoint events to identify indications of malicious behavior, unauthorized access, or violations of security policy. Depending on its implementation, an IDS can identify activities associated with malware, reconnaissance, repeated authentication failures, command-and-control communication, and other suspicious events. Detection can be performed through known attack signatures or by identifying behavior that differs significantly from an established normal pattern. The principal role of an IDS is to generate an alert so that security personnel can investigate the event and initiate an appropriate response.

1.2 Importance of Intrusion Detection

Organizations generate large volumes of security-related events every day, making it difficult for analysts to distinguish ordinary activity from genuine attacks. IDS technologies provide continuous visibility into network and host behavior and can highlight events that may indicate compromise. This capability is especially important in environments that combine cloud services, software-as-a-service applications, remote connectivity, mobile devices, and encrypted communications. Such environments require behavioral and contextual analysis in addition to conventional signature matching.1.3 IDS and IDPS: Key Difference

An IDS is primarily concerned with identifying suspicious activity and notifying security personnel. An Intrusion Detection and Prevention System (IDPS) extends this function by allowing predefined or automated actions to be

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

taken after a threat is identified. Depending on policy and confidence level, an IDPS may block traffic, isolate a host, modify a security control, or otherwise contain the activity. Thus, detection provides visibility, while prevention adds an active response capability.

1.4 Major Types of IDS/IDPS

- Network-based IDS (NIDS): examines network packets and communication flows to identify suspicious traffic.
- Host-based IDS (HIDS): monitors activity within individual systems, including operating-system and application logs.
- Signature-based IDS: compares observed activity with previously documented attack patterns.
- Anomaly-based IDS: establishes a model or baseline of expected behavior and identifies significant deviations from it.

1.5 Attacks and Suspicious Activities Detectable by IDS

An IDS can identify a broad range of events that may indicate an attempted or successful compromise, including:

- Port scanning used to discover accessible services and potentially vulnerable hosts.
- Repeated or automated brute-force authentication attempts against accounts or administrative services.
- Communication between compromised systems and command-and-control infrastructure.
- Denial-of-service activity characterized by abnormal traffic volumes or patterns.
- Network reconnaissance intended to discover hosts, applications, services, or open ports.
- Unauthorized connections, privilege misuse, or other violations of established security policy.
- Suspicious DNS behavior, including tunneling or communication with known or suspected malicious domains.

2. LITERATURE SURVEY AND WORKING OF IDS/IDPS

Modern IDS/IDPS implementations commonly combine more than one analytical technique. Signature matching provides reliable recognition of established threats, while anomaly analysis helps identify activity that does not correspond to known attack patterns. In more advanced deployments, machine learning and behavioral analytics can be used to examine relationships among users, devices, identities, applications, and cloud resources.

2.1 Signature-Based Detection

In signature-based detection, observed network packets or system events are compared with a repository of known malicious patterns. A signature may represent characteristics of a previously analyzed exploit, malware communication pattern, or other attack behavior. When sufficient similarity is found, the system generates an alert and, in an IDPS deployment, may initiate a predefined response. The method is generally fast and precise for threats that are already represented in the signature database, but its effectiveness depends on timely updates.

2.2 Anomaly-Based Detection

Anomaly-based detection first establishes a representation of expected network or system behavior. This baseline can be derived from historical observations, statistical characteristics, or learned models. New activity is then evaluated against the baseline, and substantial deviations are treated as potentially suspicious. Because the approach does not

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

require an exact signature for every attack, it can provide useful visibility into novel or modified threats. Its major challenge is distinguishing genuinely malicious deviations from legitimate but unusual behavior.

2.3 Real-Time Monitoring

IDPS technologies continuously process network and host events so that suspicious activity can be recognized as close as possible to the time it occurs. Monitoring engines search for matches to known signatures as well as deviations from expected behavior. Continuous analysis improves the opportunity for early detection and rapid containment.

2.4 Alerting and Reporting

When suspicious activity is identified, the system creates an alert containing relevant information such as the event type, severity, affected host or network segment, and supporting observations. Alerts may be delivered directly to security personnel or forwarded to Security Information and Event Management (SIEM) platforms, where events can be correlated with other security data for investigation.

2.5 Prevention and Response

An IDPS can supplement detection with automated containment. Depending on the organization's security policy and the confidence associated with the detection, the system may block a connection, quarantine an endpoint, modify a control, or perform another predefined mitigation. This reduces the time between detection and response and can limit the damage caused by an active attack.

3. Detecting Modern Cyberattacks

Conventional intrusion detection remains useful for recognizable events such as scanning, repeated authentication failures, malware communication, denial-of-service activity, and attacks associated with established signatures. However, modern adversaries increasingly employ techniques that provide limited or no direct signature evidence. Examples include encrypted communications, misuse of legitimate credentials, living-off-the-land techniques, lateral movement, insider activity, and exploitation of previously unknown vulnerabilities. Consequently, organizations increasingly combine traditional detection with behavioral analytics and AI-assisted methods that can examine activity across users, devices, identities, applications, and cloud resources.

4. COMPARATIVE EVALUATION OF IDPS METHODS

Feature	Signature-Based IDPS	Anomaly-Based IDPS	AI-Driven IDPS
Operating principle	Compares observed activity with a repository of known attack signatures.	Learns or defines normal behavior and identifies significant departures from that baseline.	Uses machine-learning techniques to identify complex relationships and evolving threat patterns.
Detection of new threats	Limited when the attack has no corresponding signature.	Strong potential because previously unseen behavior can be flagged as anomalous.	Strong potential, particularly when models are trained on representative and current data.
False positives	Generally low for accurately defined signatures.	Can be higher because legitimate unusual behavior may resemble an anomaly.	Can range from low to moderate and may improve through model tuning and feedback.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Deployment and setup	Relatively straightforward; requires maintenance of signature databases.	Requires sufficient observations to establish reliable normal-behavior profiles.	Typically more complex because model development, training data, validation, and monitoring are required.
Computational demand	Usually low because matching known patterns is efficient.	Moderate, depending on the complexity and frequency of baseline comparisons.	Often higher because model training and advanced inference may require substantial computing resources.

5. BENEFITS OF IDS/IDPS

1. Threat detection and early warning: IDS/IDPS technologies can identify suspicious events at an early stage, providing security teams with an opportunity to investigate and contain attacks before their impact increases.

2. Support for compliance: Organizations operating under regulatory or industry security requirements may use monitoring and prevention capabilities as part of their broader control framework.

3. Incident response: Detection records provide evidence about the nature, source, timing, and scope of an event, supporting investigation and containment activities.

4. Reduced operational impact: Rapid detection and automated containment can reduce the duration of an attack and limit associated downtime or damage.

5. Improved network visibility: Monitoring reveals patterns in communication and system activity, helping organizations identify abnormal behavior and potential weaknesses.

6. Proactive protection: An IDPS can take automated preventive actions, such as blocking or quarantining suspicious activity, instead of relying exclusively on manual intervention.

6. LIMITATIONS AND EVASION CHALLENGES

Attackers can deliberately design their activity to avoid detection. Five important evasion areas are signature avoidance, encrypted communication, perimeter bypass, internal movement, and credential theft.

6.1 Signature Evasion

Signature-based controls are less effective when malicious traffic is modified so that it no longer resembles a stored pattern. At a simple level, an attacker may change infrastructure such as domains or addresses. More sophisticated adversaries can exploit previously unknown vulnerabilities, for which a conventional signature may not yet exist.

6.2 Encrypted Traffic

Encryption can conceal malicious content from systems that depend on inspection of packet payloads. Decrypting traffic at security boundaries can provide additional visibility, but it introduces performance, operational, privacy, and management considerations. Consequently, security teams increasingly need approaches that can derive useful signals from encrypted flows without necessarily storing or inspecting complete payloads.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

6.3 Perimeter Avoidance

Modern users and devices frequently operate outside traditional enterprise boundaries. A compromised home device, mobile endpoint, or other externally connected system can provide an alternative path into organizational resources. This reduces the effectiveness of security architectures that depend primarily on a fixed network perimeter.

6.4 Internal Movement

After obtaining an initial foothold, attackers may conduct reconnaissance inside the environment and move laterally toward valuable resources. Visibility can be particularly difficult in distributed, hybrid, and multi-cloud architectures, where communication between workloads, storage systems, and services may cross several control boundaries.

6.5 Credential Harvesting

Attackers who gain access to a system may attempt to obtain usernames, passwords, authentication tokens, or credential material stored in memory or other locations. Valid credentials can then be used to access additional systems without relying on obvious malware or exploit activity, making behavior-based monitoring especially important.

7. PREVENTIVE ACTIONS PERFORMED BY IDPS

The response selected by an IDPS depends on the detected event, confidence in the detection, and the organization's security policy. Common actions include:

- Alerting administrators so that a human analyst can investigate events where automated blocking may be inappropriate or where false-positive risk is significant.
- Blocking or isolating suspicious sources, users, or connections to prevent continued malicious activity.
- Changing the security configuration, such as dynamically modifying firewall rules or other access controls.
- Removing or neutralizing malicious components from content when the deployed security architecture supports such an action.

8. FIREWALL AND IDPS: VARIATIONS AND EXTRA RESPONSIBILITIES

A firewall primarily controls network access using information such as source and destination addresses, ports, protocols, and configured access policies. An IDPS adds deeper security monitoring by examining traffic and system activity for evidence of malicious behavior, and some implementations perform deep inspection of application-layer content. In modern security products, firewall and IDPS functions may be integrated, particularly in next-generation firewall platforms. Nevertheless, the two capabilities remain complementary: the firewall can serve as an initial access-control layer, while the IDPS provides additional analysis and can trigger containment when suspicious activity is identified.

Firewall	IDPS
Controls access and sets network boundaries by filtering traffic.	Monitors, detects, and/or prevents malicious behavior, intrusions, and policy violations inside network streams.
Looks mostly at surface-level packet headers like IP addresses, ports, and protocols or stateful connections.	Performs Deep Packet Inspection (DPI) to look inside the payload for signatures and anomalous patterns.
Drops or allows traffic strictly based on pre-defined access control rule-sets.	An IDS (Detection) generates passive logs and alerts, while an IPS (Prevention) acts inline to drop packets

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

	or reset connections immediately.
Positioned right at the network perimeter as the first line of defense.	Positioned inline just behind the firewall or at strategic internal segments for deeper analysis.
Optimized for fast throughput and low latency. [Throughput - the actual rate at which successfully delivered data is transmitted over a communication channel or network within a specific timeframe]	Can introduce mild latency due to intensive real-time packet payload analysis. [Latency - the time delay between a user action or request and the system's response, typically measured in milliseconds]
Allow, deny, or reject packets .	Passive alerts (Intrusion Detection System) or active block/drop (Intrusion Protection System)

9. OVERALL BENEFITS OF IDPS

- Automated monitoring and response can reduce the time required to react to routine security events.
- Anomaly-oriented analysis can reveal suspicious behavior that may not be obvious to human analysts during manual monitoring.
- Consistent enforcement of predefined detection and response policies can strengthen security operations.
- Continuous visibility helps security teams prioritize investigations and identify recurring patterns.

10. FUTURE TRENDS IN IDPS TECHNOLOGY

IDPS technology is moving beyond traditional, appliance-oriented signature detection toward cloud-native monitoring and analytics suitable for distributed and multi-cloud infrastructures. Integration with Extended Detection and Response (XDR) platforms and Security Orchestration, Automation and Response (SOAR) systems enables security events to be correlated, prioritized, investigated, and contained through increasingly automated workflows.

Current developments also emphasize AI-assisted investigation, analysis of encrypted traffic, and lightweight monitoring within cloud workloads. Agentic or autonomous AI techniques are being explored for investigating anomalies and reducing analyst alert fatigue. Encrypted Traffic Analysis seeks to identify suspicious communication characteristics without requiring unrestricted inspection of complete plaintext content. Kernel-level technologies such as extended Berkeley Packet Filter (eBPF) can provide efficient telemetry and filtering within Linux-based workloads.

Regulatory developments and privacy requirements are also influencing monitoring architectures. Security frameworks and regulations can increase the need for timely detection, reporting, and prevention, while privacy considerations encourage organizations to minimize unnecessary collection of full packet payloads and to use metadata or flow-level information where appropriate.

11. CONCLUSION

No single IDPS approach is sufficient for every modern threat environment. Signature-based techniques remain highly valuable for efficiently recognizing established attacks, while anomaly-based methods provide a mechanism for identifying behavior that differs from expected patterns. AI-driven techniques can further strengthen detection by learning complex relationships and adapting to changing activity, although they introduce additional requirements for data quality, model management, computational resources, and operational validation. A layered architecture that combines these approaches with firewalls, endpoint controls, Security Information and Event Management (SIEM), Extended Detection and Response (XDR), Security Orchestration, Automation, and Response (SOAR), identity security, and appropriate human analysis can provide broader and more resilient protection. The continued evolution of cloud computing, encryption, automation, and adversarial techniques makes adaptive and context-aware intrusion detection increasingly important.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

REFERENCES

[1] D. Mudzingwa and R. Agrawal, "A study of methodologies used in intrusion detection and prevention systems (IDPS)," Proceedings of IEEE SoutheastCon, Orlando, FL, USA, 2012, pp. 1–6, doi: 10.1109/SECon.2012.6197080.

[2] Jain, A., & Singh, P. (2024). Artificial Intelligence Applications in Next-Generation Cyber Security Systems. International Journal of Advanced Computing Research, 18(2), 87–102.

[3] Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.

[4] Animesh Patcha and Jung-Min Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Computer Networks, vol. 51, no. 12, 2007, pp. 3448–3470.

[5] Rebecca Bace, An Introduction to Intrusion Detection and Assessment for System and Network Security Management, ICSA Intrusion Detection Systems Consortium Technical Report, 1999.

[6] James P. Anderson, "Computer security threat monitoring and surveillance," James P. Anderson Co., Fort Washington, Pennsylvania, Technical Report, April 1980.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)