Securing Networks in the Digital Age: A Review of Intrusion Detection and Prevention Strategies

P.Hari Kishore
Computer Science and Engineering
Koneru Lakshmaiah Educational Foundation Guntur, India

Sk.Muzubar Rahiman
Computer Science and Engineering
Koneru Lakshmaiah Educational Foundation Guntur, India

P.Mahidhar
Computer Science and Engineering
Koneru Lakshmaiah Educational Foundation Guntur, India

Mohan Kumar Chandol
Computer Science and Engineering
Koneru Lakshmaiah Educational Foundation Guntur, India

T.Mahendra
Computer Science and Engineering
Koneru Lakshmaiah Educational Foundation Guntur, India

Abstract:- In today's interconnected world, billions of individuals rely on the internet for various activities, from communication and commerce to entertainment and education. However, this widespread connectivity also brings about an increased risk of cyber threats and malicious activities. In response to these challenges, intrusion detection technology has emerged as a vital component of modern cybersecurity strategies. This paper presents a comprehensive literature survey focusing on Internal Intrusion Detection Systems (IIDS) and traditional Intrusion Detection Systems (IDS). These systems utilize a diverse array of data mining and forensic techniques algorithms to monitor and analyze system activities in real-time, thereby detecting and preventing potential security breaches. Additionally, the paper explores the integration of data mining methods for cyber analytics, offering valuable insights into the development and enhancement of intrusion detection capabilities. Through a thorough examination of existing research and methodologies, this study aims to provide a deeper understanding of the evolving landscape of intrusion detection and contribute to the advancement of cybersecurity practices in an increasingly digitized world.

Keywords:- *Internal Intrusion Detection System (IIDS), Intrusion Detection System (IDS), System Call (SC), Denial of Service (DOS).*

I. INTRODUCTION

Intrusion Detection and Prevention Systems (IDPS) constitute integral components within the realm of contemporary cybersecurity, meticulously engineered to proactively identify and thwart unauthorized access, malicious activities, and potential threats lurking within networks or systems [1]. The distinct amalgamation of detection and prevention functionalities distinguishes IDPS from conventional security measures, endowing it with a holistic defense mechanism against a myriad of cyber threats. In today's interconnected digital milieu, the indispensability of IDPS looms large [2]. These systems assume the role of vigilant sentinels, continuously monitoring network activities to discern and respond to aberrant behaviors suggestive of potential intrusions. Their ability to perform real-time analysis and execute rapid responses is paramount in mitigating risks associated with malware, unauthorized access attempts, and sophisticated cyber assaults [2]. The proactive essence of IDPS, characterized by its fusion of detection and prevention capabilities, assumes pivotal significance in fortifying the security posture of organizations [3]. By preemptively intercepting, containing, or neutralizing potential threats, IDPS augments organizational resilience against the ever-evolving landscape of cyber threats. In an era, fraught with the perils of data breaches and cyberattacks, IDPS assumes a multifaceted role as both a vigilant detective and a proactive deterrent, thereby contributing to the ongoing refinement of security measures and the mitigation of risks [4]. The motivation underlying this review stems from the dynamic nature of cybersecurity threats and the incessantly evolving techniques employed by attackers. Thus, the aim here is to furnish a comprehensive analysis of prevailing intrusion detection and prevention strategies. By amalgamating recent research findings, industry best practices, and technological advancements, this endeavor seeks to deepen understanding and illuminate potential avenues for future development within the field. However, it is imperative to acknowledge the inherent scope and limitations associated with this review. While it aspires to encompass a broad spectrum of intrusion detection and prevention strategies, the dynamic nature of the cybersecurity landscape and the advent of new technologies may yield varying levels of maturity among these strategies [5]. Furthermore, owing to the vast expanse of the field, certain emerging technologies or approaches may not be exhaustively addressed within the confines of this review.

II. INTRUSION DETECTION STRATEGIES

A. *Overview of Signature Based Detection*

Signature-based detection relies on predefined patterns or signatures of known threats to identify malicious activities within a network or system. These signatures serve as unique fingerprints of known malware, enabling the system to recognize and block specific attack patterns efficiently [6]. This method offers several advantages, including high accuracy in identifying known threats, a low rate of false positives due to precise matching against known patterns, and quick and efficient identification of recognized threats.

However, signature-based detection also comes with limitations. It is inherently limited to known threats and is ineffective against novel or zero-day attacks that lack predefined signatures [7]. Maintaining the signature database requires regular updates to keep pace with evolving threats, presenting a challenge for real-time protection. Additionally, signature-based detection struggles to detect polymorphic malware, which dynamically changes its code to evade detection. Examples of signature-based IDPS include Intrusion Prevention Systems (IPS), where many commercial solutions utilize signature-based detection to identify, and block known threats. Similarly, traditional antivirus software relies on signature databases to recognize and eliminate known malware strains [8].

B. *Anomaly Based Detection*

Anomaly-based detection operates by establishing a baseline of normal network or system behavior and flagging any deviations from this baseline as potential threats [9]. It identifies activities that significantly differ from established patterns, indicating a potential intrusion. This method offers several advantages, including the detection of unknown threats by highlighting deviations from normal behavior, adaptability to changes in the network environment without relying on predefined signatures, and a low rate of false negatives, capable of detecting subtle, sophisticated attacks that may go unnoticed by other methods. However, anomaly-based detection also has limitations [10]. It is prone to generating false positives due to variations in normal behavior that may not necessarily indicate an intrusion. The initial establishment of a reliable baseline can be challenging and time-consuming. Additionally, continuous monitoring and analysis may demand significant computational resources. Examples of anomaly-based IDPS include Network Behavior Analysis (NBA) Systems, which analyze network traffic patterns and behaviors to identify deviations from the norm [11]. Similarly, User and Entity Behavior Analytics (UEBA) focuses on analyzing the behavior of users and entities to detect abnormal activities that may indicate a security threat.

C. *Behavior-based Detection*

Behavior-based detection involves real-time monitoring of the behavior of applications, users, or entities to identify suspicious or malicious activities. It focuses on understanding the sequence of actions or patterns associated with normal behavior and flagging deviations from this expected conduct. This method offers several advantages, including dynamic threat detection capable of identifying threats that exhibit abnormal behavior, even if the specific signature is unknown [12]. Additionally, it provides contextual analysis by considering the context in which activities occur, thereby enhancing the accuracy of threat identification. Behaviour-based detection also helps reduce false positives by considering the overall behavior rather than isolated events. Behaviour-based detection also comes with limitations. It requires an initial learning period to understand normal behavior, during which it may be less effective. Implementing behaviour-based detection systems can be complex, requiring careful tuning to avoid false positives. Furthermore, it may struggle with entirely novel attack techniques that deviate significantly from known behaviors. Examples of behaviour-based IDPS include Endpoint Detection and Response (EDR) Systems, which monitor the behavior of endpoints to detect and respond to suspicious activities. Similarly, Application Control Systems analyze the behavior of applications to identify deviations from expected norms.

D. *Heuristic Based Detection*

Heuristic-based detection employs rules or heuristics to identify potentially malicious activities based on predefined criteria. Unlike strict signatures, heuristics offer a more flexible approach, allowing the system to flag activities that exhibit suspicious traits [13]. This method provides several advantages, including flexibility to adapt to emerging threats by using general rules rather than specific signatures, early detection of some previously unseen threats by identifying patterns that match heuristic rules, and customization, allowing for the creation of custom rules based on specific organizational needs. However, heuristic-based detection also has limitations. It may generate false positives due to the generalized nature of heuristics. The flexibility of heuristics may result in lower precision compared to more specific detection methods. Additionally, depending on the complexity of the heuristics, implementation can be resource intensive. Examples of heuristic-based IDPS include Intrusion Detection Systems with Custom Rules, where some solutions allow the creation of custom heuristics to detect organization-specific threats. Similarly, email filtering systems often employ heuristic rules to identify potentially malicious content based on general traits [14].

III. INTRUSION PREVENTION STRATEGIES

Intrusion prevention encompasses the detection and halting of potential security breaches through intrusion detection systems. The primary objective is to identify incidents, log relevant information, and actively prevent their escalation. Intrusion prevention systems (IPSs) are designed to halt detected threats in real-time, employing proactive measures to thwart unauthorized access or malicious activities [15].

A. *Access Control*

Access control stands as a critical pillar in the realm of intrusion prevention systems (IPS), with the integration of Network Access Control (NAC) serving as a potent strategy to fortify network security. Implementation strategies, such as Role-Based Access Control (RBAC), play a pivotal role in this regard. RBAC facilitates the assignment of permissions based on job roles, ensuring individuals possess only the minimum necessary access for their respective responsibilities [16]. Regular review and updating of roles remain imperative to align with organizational changes, thus sustaining an optimal access control framework.

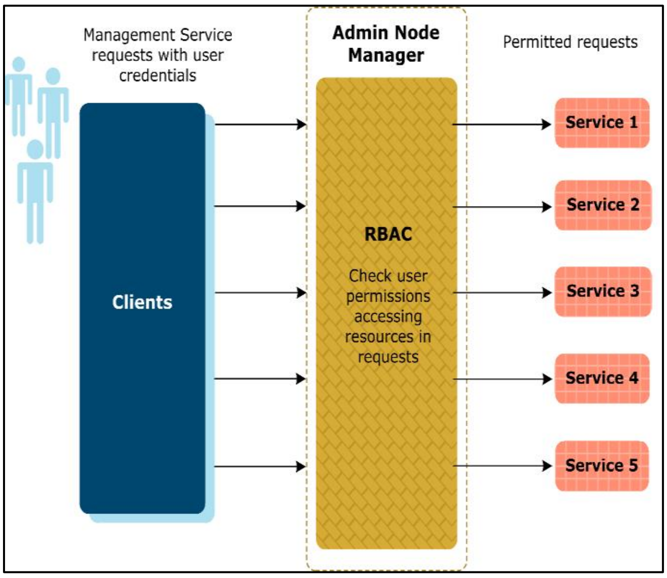
Management Service requests with user credentials
Admin Node Manager
Permitted requests
Clients
RBAC
Check user permissions accessing resources in requests
Service 1
Service 2
Service 3
Service 4
Service 5

Fig. 1. Access Control in IDPS

Authentication mechanisms constitute another crucial aspect in bolstering access control within IPS. Employing robust authentication methods like multi-factor authentication (MFA) fortifies the verification process, while the adoption of biometric authentication, particularly in sensitive areas or systems, further enhances security measures. Furthermore, the development of a comprehensive incident response plan assumes paramount importance. Such a plan should outline procedures for handling security incidents related to unauthorized access and be subjected to regular drills to validate its effectiveness [17].

Within the realm of intrusion detection and prevention systems (IDPS), access control manifests in various forms, each contributing to the overall security posture. Role-Based Access Control (RBAC) exemplifies a fundamental approach by assigning roles to users based on job functions and granting access to resources accordingly. This method simplifies user permission management and mitigates risks associated with human error. Network Access Control (NAC), on the other hand, restricts network access based on device identity and compliance status, preventing unauthorized or compromised devices from accessing the network or isolating them in separate segments [18]. Access policies serve as the bedrock of access control mechanisms within IDPS, defining rules dictating who or what can access specific resources or functionalities. These policies ensure only authorized entities interact with the IDPS and its components, thereby reinforcing security measures comprehensively.

B. *Fire Walls*

Network security is highly dependent on firewalls, which serve as interfaces between trusted internal networks and untrusted external networks, such as the internet. These devices oversee both incoming and outgoing network traffic, preventing unauthorized access and stopping cyber threats [19]. By monitoring and filtering the flow of traffic based on security rules, firewalls can proactively prevent unauthorized access and identify any malicious activity. Additionally, they can alert security departments of attempted intrusions, allowing for possible interventions to mitigate further damage and potentially capture the culprits. Sophisticated techniques like Stateful Inspecting Firewalls (SFIFs) and Next-Generation Firewalls (NGFWs) provide enhanced protection against advanced threats such as advanced persistent threats (APTs) and zero-day attacks [20].

Packet filtering is a basic form of firewall that examines packets of data as they pass through the network, filtering them based on predefined rules such as source and destination IP addresses, protocols (TCP, UDP, ICMP), and port numbers [21]. Packet filtering firewalls are commonly used in routers and switches to control traffic at the network layer. While efficient, they cannot inspect the contents of packets. Operating at the session layer of the OSI model, circuit-level gateways provide security by determining the legitimacy of communication sessions without inspecting the contents of the data. They focus on managing connections, making them suitable for applications requiring secure connections without analyzing the data payload.

Application-level gateways, also known as proxy firewalls, function at the application layer of the OSI model. They inspect and filter traffic based on specific applications or services, making decisions based on the content of the data being transmitted. This makes them useful for protecting against application-specific attacks, such as blocking malicious HTTP requests or SQL injection attempts. Stateful inspection firewalls monitor the state of active connections, considering not just individual packets but also the context of the traffic. By tracking the state of network connections, they ensure that only legitimate connections are allowed. These firewalls are used to prevent unauthorized access and detect and block certain types of attacks that exploit the state of network connections.

Next-Generation Firewalls (NGFWs) combine traditional firewall features with advanced functionalities such as deep packet inspection, intrusion prevention systems (IPS), and application awareness [22]. They often incorporate threat intelligence and may include cloud-based services for enhanced security. These firewalls are ideal for organizations seeking comprehensive solutions that offer advanced threat detection and prevention.

Cisco ASA (Adaptive Security Appliance) is widely used in enterprise environments, offering a comprehensive security solution with stateful inspection, VPN capabilities, and intrusion prevention features [23]. It is integrated into various network architectures, such as network perimeters, between network segments, or in virtualized environments.

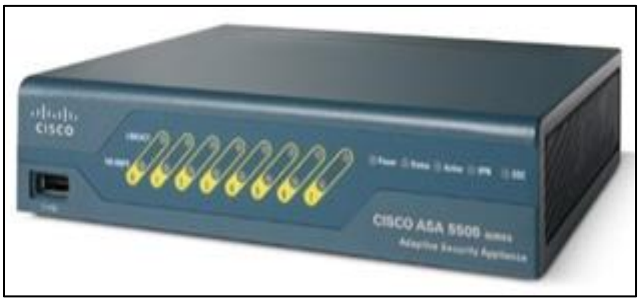

Fig. 2. Cisco ASA

Palo Alto Networks Next-Generation Firewalls provide advanced threat prevention capabilities by integrating intrusion prevention, application control, and URL filtering. They are often deployed at network perimeters and within data center environments, offering visibility and control over application and user activity [24].

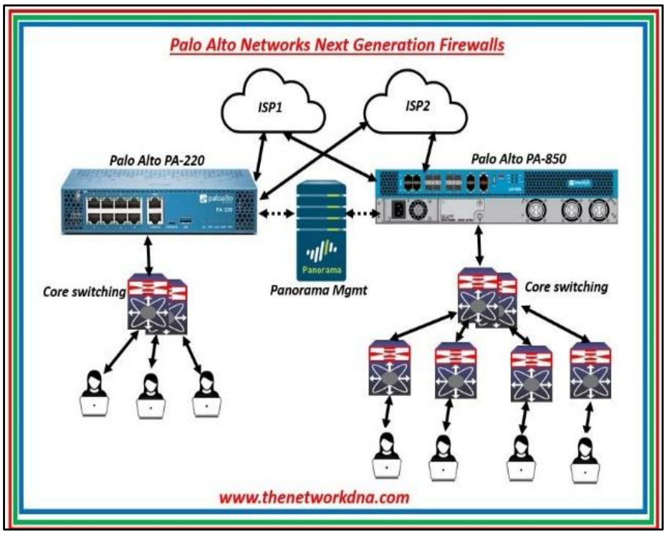

Fig. 3. Palo Alto Network Next Generation Firewalls

C. Encryption

The role of encryption in preventing intrusions is pivotal, serving as a critical component of a comprehensive cybersecurity strategy. Encryption ensures that sensitive information remains confidential by transforming plaintext data into ciphertext, making it extremely challenging for unauthorized entities to interpret intercepted data without the corresponding cryptographic keys [25]. It acts as a robust barrier against unauthorized access to data, both in transit and at rest. Even if an intruder gains access to encrypted data without the correct encryption keys, deciphering it becomes a formidable task, significantly reducing the risk of data breaches. In the context of web traffic, encryption protocols like SSL and TLS secure communication channels between users and websites, safeguarding sensitive information such as login credentials and financial details from eavesdroppers and man-in-the-middle attacks. This provides a secure online environment. Additionally, Virtual Private Networks (VPNs) utilize encryption to create secure tunnels for transmitting data over the internet. This is particularly crucial for remote workers and businesses, as it ensures the privacy and integrity of data even when traversing potentially insecure networks [26].

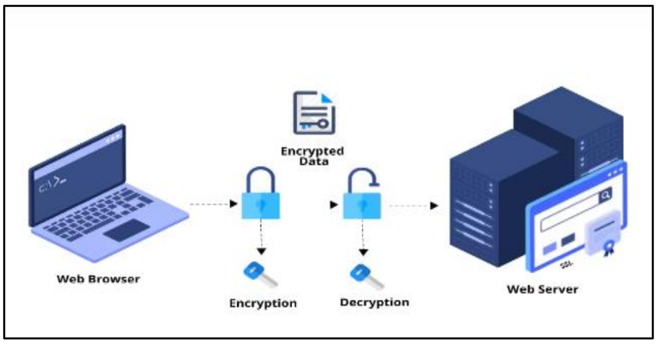

Fig. 4. Secure Communication Channels

Intrusion Prevention Systems (IPS) are crucial in identifying and mitigating potential security threats within a network, and encryption is an essential component that enhances the security posture of IPS implementations. One key use case is the protection of signatures and policies within the IPS database. Encrypting these signatures and policies prevents tampering and unauthorized modification, ensuring the integrity of IPS rules and configurations. This can be implemented by utilizing encryption algorithms to protect the database storing IPS signatures and policies, preventing attackers from manipulating the rules to exploit vulnerabilities [27]. Another important use case is the confidentiality of log data generated by the IPS. Encrypting this log data preserves the confidentiality of sensitive information, such as IP addresses, user details, and incident reports. Applying encryption to log files stored on the IPS device or transmitted to a central logging server safeguards the log data against unauthorized access and protects the privacy of individuals and entities involved. Additionally, IPS devices often communicate with central management servers for updates and commands. Encrypting this communication prevents attackers from intercepting and manipulating these commands. Implementing secure communication protocols, such as SSH or HTTPS, for interactions between the IPS and central management servers ensures the confidentiality and integrity of command-and-control communication.

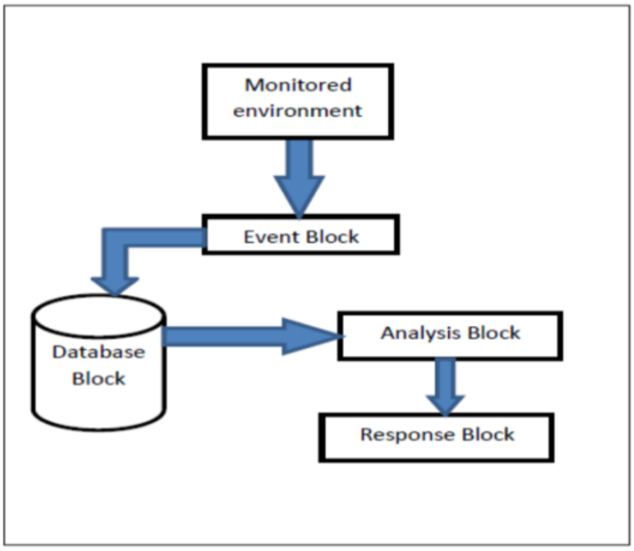

Fig. 5. Data Storage Protection

Encryption is also used to secure communication channels between different components of the Intrusion Detection and Prevention System (IDPS), such as sensors, management consoles, and logging servers. This ensures that sensitive information, including alerts and configuration data, is transmitted securely. Sensitive data collected by IDPS, such as event logs, user activity records, and intrusion alerts, is often stored in encrypted databases. This prevents unauthorized access, even if attackers breach the system. Overall, the strategic use of encryption significantly enhances the ability of IPS and IDPS to prevent and mitigate security intrusions, ensuring the confidentiality, integrity, and privacy of sensitive data.

IV. CLOUD NATIVE IDPS ARCHITECTURE

A. Microservices Based Designs

In cloud-native IDPS architectures, microservices-based designs are employed to break down the system into smaller, loosely coupled components. This approach allows individual IDPS components to be independently deployed, scaled, and managed [28]. By decoupling components, organizations gain agility and resilience, enabling IDPS functions to adapt quickly to changes in cloud environments without disrupting the entire system.

B. Containerization and Serverless Computing

Containers and serverless computing play pivotal roles in cloud-native IDPS architectures. Through containerization using technologies like Docker and Kubernetes, IDPS components are packaged with their dependencies into portable units, ensuring consistency across different cloud environments. Serverless computing further enhances scalability and cost efficiency by abstracting infrastructure management, allowing IDPS functions to be executed on-demand without the need to provision or manage servers [28].

C. Auto Scaling Capabilities

Auto-scaling capabilities are integral to cloud-native IDPS solutions, enabling them to automatically adjust resource allocation based on demand. This elasticity ensures optimal performance and cost efficiency, as IDPS components dynamically scale up or down in response to fluctuations in workload and network traffic [28]. By automatically scaling resources, organizations can maintain consistent performance levels without over-provisioning infrastructure.

D. Integration With Cloud-Native Security Services

Cloud-native IDPS architectures seamlessly integrate with cloud-native security services and features provided by major cloud providers. This integration allows organizations to leverage native security capabilities such as cloud access security brokers (CASBs), identity and access management (IAM) solutions, and native logging and monitoring services. By integrating with these services, organizations can enhance visibility and control over their cloud environments while leveraging the scalability and reliability of cloud-native infrastructure [28].

E. Enhanced Security Posture

cloud-native IDPS architectures offer organizations the flexibility, scalability, and efficiency needed to enhance their security posture in the cloud. By embracing cloud-native approaches to intrusion detection and prevention, organizations can effectively protect their assets in the cloud while mitigating the risks associated with cloud adoption. Through microservices-based designs, containerization, auto-scaling capabilities, and integration with cloud-native security services, organizations can build robust and resilient IDPS solutions tailored for the cloud environment [28].

V. USER-CENTRIC INTRUSION DETECTION AND PREVENTION

Traditionally, intrusion detection and prevention systems (IDPS) have focused on protecting network infrastructure and data assets from external threats. However, with the rise of insider threats and targeted attacks, there is a growing recognition of the importance of user-centric approaches to IDPS. User-centric IDPS solutions aim to detect and prevent malicious activities initiated by authorized users or compromised accounts within an organization [29].

A. Behavioural Analysis and User Profiling

User-centric IDPS solutions employ behavioral analysis techniques to establish baseline behavior profiles for individual users and entities within the network. By continuously monitoring user activities and interactions with digital resources, IDPS can detect deviations from established behavioral norms that may indicate unauthorized or malicious behavior [30].

B. Privilaged Access Monitoring

Monitoring and controlling privileged access is critical for preventing insider threats and data breaches. User-centric IDPS solutions monitor privileged user accounts, such as system administrators and IT personnel, to detect suspicious activities, unauthorized access attempts, and privilege escalation attempts.

C. Integration With Identity and Access Management Systems

Integrating IDPS with IAM systems enables organizations to enforce access controls and authentication mechanisms based on user identities and roles. By correlating user identity information with security events and network activities, IDPS can accurately identify and respond to suspicious behavior associated with specific user accounts [31].

D. Real-Time Alerting Response

User-centric IDPS solutions provide real-time alerting and response capabilities to quickly detect and mitigate security incidents involving user behavior. Automated response mechanisms, such as user account lockdowns, session termination, and access revocation, can be triggered in response to suspicious activities to prevent further damage or unauthorized access.

E. Insider Threat Detection

Detecting insider threats, including malicious insiders and unintentional insiders (e.g., employees who inadvertently compromise security), is a key focus area for user-centric IDPS solutions. By analyzing user behavior patterns and identifying anomalous activities indicative of insider threats, IDPS can help organizations proactively identify and mitigate internal security risks.

F. Compilance Monitoring and Repeating

User-centric IDPS solutions assist organizations in meeting regulatory compliance requirements by providing visibility into user activities and access permissions. Detailed audit logs, compliance reports, and user activity monitoring capabilities enable organizations to demonstrate compliance with industry regulations and standards [32].

VI. INTEGRATED INTRUSION PREVENTION AND DETECTION

Integrated Intrusion Detection and Prevention Systems (IDPS) combine both intrusion detection and prevention functionalities into a single cohesive solution, leveraging the capabilities of both intrusion detection systems (IDS) and intrusion prevention systems (IPS). This offers a comprehensive approach to network security, providing several benefits as well as presenting certain challenges.

A. Benefits of Integrated IDPS

By integrating detection and prevention capabilities, IDPS can provide real-time threat identification and immediate response, thereby minimizing the impact of security incidents. This integration also simplifies management tasks such as configuration, monitoring, and reporting, leading to greater operational efficiency. IDPS can proactively identify and mitigate both known and unknown threats, leveraging signature-based detection for known attacks and anomaly-based detection for previously unseen threats. Furthermore, with prevention capabilities, IDPS can automatically block or mitigate threats as they are detected, reducing the time required for manual intervention and minimizing potential damage.

B. Challenges of Integrated IDPS

However, the integration of detection and prevention features may lead to an increase in false positives, as preventive actions might inadvertently block legitimate traffic or activities. Implementing both functionalities within a single system can be resource-intensive, requiring significant computational resources and potentially impacting performance. Additionally, integrated IDPS solutions may be more complex to deploy and maintain compared to standalone detection or prevention systems, necessitating expertise in both areas of cybersecurity. Moreover, to remain effective, IDPS must continuously evolve to address new and emerging threats, requiring regular updates to detection signatures and prevention rules.

VII. TECHNOLOGICAL ADVANCEMENTS IN IDPS

A. Emerging Technologies in Intrusion Detection

In recent years, advancements in technology have significantly transformed the landscape of intrusion detection and prevention systems (IDPS). One of the most notable advancements is the integration of machine learning and artificial intelligence (AI) into IDPS architectures. These technologies enable IDPS to analyze vast amounts of data in real-time and identify patterns indicative of malicious activity more accurately than traditional rule-based approaches. Additionally, the adoption of cloud computing and the proliferation of Internet of Things (IoT) devices have expanded the attack surface, making it crucial for IDPS to evolve to detect and mitigate threats across diverse environments. As a result, IDPS vendors are increasingly incorporating cloud-native architectures and IoT-specific threat intelligence to effectively protect modern networks.

Moreover, advancements in hardware acceleration technologies, such as Graphics Processing Units (GPUs) and Field-Programmable Gate Arrays (FPGAs), have enhanced the performance and scalability of IDPS solutions. These technologies enable faster packet processing and more efficient analysis of network traffic, allowing IDPS to keep pace with the growing volume and complexity of cyber threats.

B. Impact of Machine Learning and AI on IDPS

Machine learning and AI have revolutionized the field of intrusion detection and prevention by enabling IDPS to adapt and learn from experience. Traditional signature-based detection methods are limited in their ability to detect previously unknown threats, but machine learning algorithms can analyze patterns in network traffic and identify anomalies indicative of malicious activity without relying on predefined signatures.

Furthermore, AI-powered IDPS can continuously improve their detection capabilities over time as they encounter new threats and learn from past incidents. By leveraging large datasets and sophisticated algorithms, AI-driven IDPS can detect sophisticated attack techniques, such as polymorphic malware and zero-day exploits, with higher accuracy and lower false positive rates than traditional approaches.

C. Advanced Threat Detection Mechnanisms and Their Effectiveness

In response to the evolving threat landscape, IDPS vendors are developing and deploying advanced threat detection mechanisms that go beyond traditional signature-based detection. These mechanisms include behavior-based analysis, anomaly detection, and predictive modeling techniques. Behavior-based analysis focuses on identifying deviations from normal behavior patterns within a network, allowing IDPS to detect insider threats and sophisticated attacks that evade traditional detection methods. Anomaly detection techniques analyze network traffic for unusual patterns or deviations from baseline behavior, enabling IDPS to detect previously unknown threats and zero-day attacks.

Predictive modeling techniques leverage historical data and machine learning algorithms to anticipate and prevent future security incidents before they occur. By analyzing past attack patterns and identifying emerging threats, predictive IDPS can proactively mitigate risks and enhance the overall security posture of an organization.

In conclusion, technological advances in IDPS, particularly in the areas of machine learning, AI, and advanced threat detection mechanisms, are reshaping the way organizations detect and prevent cyber threats. By leveraging these emerging technologies, IDPS can improve detection accuracy, reduce response times, and mitigate the impact of security incidents in an increasingly complex and dynamic threat landscape.

VIII. FUTURE ENHANCEMENTS IN IDPS

As technology continues to evolve and cyber threats become more sophisticated, intrusion detection and prevention systems (IDPS) must adapt to effectively mitigate emerging security risks. Here are some potential future enhancements in IDPS.

A. Artificial Intelligence And Machine Learning

Further integration of artificial intelligence (AI) and machine learning (ML) algorithms can enhance IDPS capabilities in detecting and responding to evolving threats. Advanced ML models can analyze large datasets and identify complex patterns indicative of malicious activities with greater accuracy.

B. Predictive Analysis

IDPS can leverage predictive analytics to anticipate and prevent security incidents before they occur. By analyzing historical data, user behavior patterns, and threat intelligence feeds, IDPS can proactively identify potential security threats and vulnerabilities, allowing organizations to take preventive measures to mitigate risks.

C. Behavioural Biometrics

Incorporating behavioral biometrics, such as keystroke dynamics, mouse movement patterns, and voice recognition, into IDPS can enhance user authentication and access control mechanisms. Behavioral biometrics provide an additional layer of security by verifying the identity of users based on their unique behavioral traits.

D. Deception Techniques

Integration of deception technologies, such as honeypots and decoy systems, into IDPS can enhance threat detection capabilities by luring attackers into simulated environments and gathering intelligence about their tactics, techniques, and procedures (TTPs). Deception technologies can help organizations proactively identify and respond to advanced threats.

IX. CONCLUSION

In conclusion, intrusion detection and prevention systems (IDPS) play a critical role in safeguarding organizations against a wide range of cyber threats. By continuously monitoring network traffic, analyzing security events, and enforcing access controls, IDPS can detect and mitigate security incidents in real-time, thereby minimizing the impact of cyber-attacks. As technology advances and cyber threats evolve, IDPS must evolve to keep pace with the changing threat landscape. Future enhancements in IDPS, such as the integration of artificial intelligence, predictive analytics, behavioral biometrics, deception technologies, and quantum-safe cryptography, will further strengthen their effectiveness in protecting organizations against emerging security risks. By embracing these future enhancements and adopting a proactive approach to cybersecurity, organizations can enhance their resilience to cyber threats and ensure the confidentiality, integrity, and availability of their digital assets in an increasingly interconnected and dynamic threat environment.

REFERENCES

[1]. Muneer, Salman, et al. "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis." Journal of Engineering 2024.1 (2024): 3909173.

[2]. He, Ke, Dan Dongseong Kim, and Muhammad Rizwan Asghar. "Adversarial machine learning for network intrusion detection systems: A comprehensive survey." IEEE Communications Surveys & Tutorials 25.1 (2023): 538-566.

[3]. Lampe, Brooke, and Weizhi Meng. "Intrusion detection in the automotive domain: A comprehensive review." IEEE Communications Surveys & Tutorials (2023).

[4]. Talukder, Md Alamin, et al. "A dependable hybrid machine learning model for network intrusion detection." Journal of Information Security and Applications 72 (2023): 103405.

[5]. Qazi, Emad Ul Haq, Muhammad Hamza Faheem, and Tanveer Zia. "HDLNIDS: hybrid deep-learning-based network intrusion detection system." Applied Sciences 13.8 (2023): 4921.

[6]. Kaur, Harmandeep, and Munish Kumar. "Signature identification and verification techniques: state-of-the-art work." Journal of Ambient Intelligence and Humanized Computing 14.2 (2023): 1027-1045.

[7]. Asadi, Majid, Marzieh Hashemi, and Narayanaswamy Balakrishnan. "An overview of some classical models and discussion of the signature-based models of preventive maintenance." Applied Stochastic Models in Business and Industry 39.1 (2023): 4-53.

[8]. Cuchiero, Christa, Guido Gazzani, and Sara Svaluto-Ferro. "Signature-based models: Theory and calibration." SIAM journal on financial mathematics 14.3 (2023): 910-957.

[9]. Bhavsar, Mansi, et al. "Anomaly-based intrusion detection system for IoT application." Discover Internet of Things 3.1 (2023): 5.

[10]. Idrissi, Meryem Janati, et al. "Fed-anids: Federated learning for anomaly-based network intrusion detection systems." Expert Systems with Applications 234 (2023): 121000.

[11]. Thanh, Nguyen Huu, et al. "On Profiling, Benchmarking and Behavioral Analysis of SDN Architecture Under DDoS Attacks." Journal of Network and Systems Management 31.2 (2023): 43.

[12]. Akhtar, Muhammad Shoaib, and Tao Feng. "Evaluation of machine learning algorithms for malware detection." Sensors 23.2 (2023): 946.

[13]. Dey, Arun Kumar, Govind P. Gupta, and Satya Prakash Sahu. "Hybrid Meta-Heuristic based feature selection mechanism for cyber-attack detection in IoT-enabled networks." Procedia Computer Science 218 (2023): 318-327.

[14]. Djenna, Amir, et al. "Artificial intelligence-based malware detection, analysis, and mitigation." Symmetry 15.3 (2023): 677.

[15]. Kizza, Joseph Migga. "System intrusion detection and prevention." Guide to computer network security. Cham: Springer international publishing, 2024. 295-323.

[16]. Omotunde, Habeeb, and Maryam Ahmed. "A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond." Mesopotamian Journal of CyberSecurity 2023 (2023): 115-133.

[17]. Saviour, Mariya Princy Antony, and Dhandapani Samiappan. "IPFS based storage Authentication and access control model with optimization enabled deep learning for intrusion detection." Advances in Engineering Software 176 (2023): 103369.

[18]. Javadpour, Amir, et al. "DMAIDPS: a distributed multi-agent intrusion detection and prevention system for cloud IoT environments." Cluster Computing 26.1 (2023): 367-384.

[19]. Ahmadi, Sina. "Next Generation AI-Based Firewalls: A Comparative Study." International Journal of Computer (IJC) 49.1 (2023): 245-262.

[20]. Bauböck, Rainer, and Julia Mourão Permoser. "Sanctuary, firewalls, regularisation: three inclusive responses to the presence of irregular migrants." Journal of Ethnic and Migration Studies 49.14 (2023): 3671-3688.

[21]. Tian, Yue, et al. "Methodology for optimally designing firewalls in hydrogen refueling stations." International Journal of Hydrogen Energy 49 (2024): 1196-1209.

[22]. Singh, Lakhvir, and Ram Singh. "Comparative Analysis of Traditional Firewalls and Next-Generation Firewalls: A Review." Latest Trends in Engineering and Technology: Proceedings of the 2nd International Conference on Latest Trends in Engineering and Technology (ICLTET 2023), July 13-14, 2023, Mohali, India. CRC Press, 2024.

[23]. Benadjila, Ryad, and Arnaud Ebalard. "Randomness of random in Cisco ASA." Cryptology ePrint Archive (2023).

[24]. Choi, Brendan, and Erwin Medina. "Creating IPSec Tunnels on Palo Alto Firewalls." Introduction to Ansible Network Automation: A Practical Primer. Berkeley, CA: Apress, 2023. 847-865.

[25]. Singh, Monu, and Amit Kumar Singh. "A comprehensive survey on encryption techniques for digital images." Multimedia Tools and Applications 82.8 (2023): 11155-11187.

[26]. Akinsanya, Michael Oladipo, Cynthia Chizoba Ekechi, and Chukwuekem David Okeke. "Virtual private networks (vpn): a conceptual review of security protocols and their application in modern networks." Engineering Science & Technology Journal 5.4 (2024): 1452-1472.

[27]. Wang, Chunhua, et al. "High-dimensional memristive neural network and its application in commercial data encryption communication." Expert Systems with Applications 242 (2024): 122513.

[28]. Koskinen, Jonne. "Cloud Security Architecture." (2023).

[29]. Rivadeneira, Jorge Eduardo, et al. "User-centric privacy preserving models for a new era of the Internet of Things." Journal of Network and Computer Applications (2023): 103695.

[30]. Anderson, Laura K. "Autistic experiences of applied behavior analysis." Autism 27.3 (2023): 737-750.

[31]. Olabanji, Samuel Oladiipo, et al. "AI for Identity and Access Management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems." Authorization, and Access Control within Cloud-Based Systems (January 25, 2024) (2024).

[32]. Henriques, João, et al. "A forensics and compliance auditing framework for critical infrastructure protection." International Journal of Critical Infrastructure Protection 42 (2023): 100613.