Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 4): pp. 4865-4879
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.04.521

Intrusion Detection System And Ddos Response System: A Comprehensive Review

Anil baburao Asstociate Professor, Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand India 248002

Abstract:

The upkeep and protection of the security of computer networks is of the highest significance in the linked world of today. Intrusion Detection Systems (IDS) and systems that can respond to Distributed Denial of Service (DDoS) attacks are an imperative requirement for defending network infrastructure from a wide range of cyberthreats. DDoS stands for "distributed denial of service," while IDS is for "intrusion detection system." This research study gives a complete assessment of intrusion detection and DDoS response systems, underlining the relevance of these systems as well as the underlying concepts and difficulties they bring. The study was carried out by a group of researchers. In addition to this, as part of our commitment to educate academics, practitioners, and policymakers on the subject of network security, we examine the most recent developments and trends in these systems.

Keywords. DDoS, Intrusion Detection System, classification.

I. Introduction

Ensuring the security of these networks has become a vital concern as a result of the growing reliance on computer networks and the rise of cyber threats. Network security infrastructure must include Intrusion Detection Systems (IDS) and Distributed Denial of Service (DDoS) response systems [1]. While DDoS response systems strive to lessen and stop the consequences of DDoS assaults, IDS are made to spot unauthorised activity and potential security breaches within a network and respond to them. To properly defend network assets and preserve operational integrity, one must have a thorough grasp of IDS and DDoS response systems due to the ongoing evolution of cyber threat [2]s. This study paper's main goal is to give an in-depth analysis of IDS and DDoS response systems. The purpose of the article is to examine these systems' importance, learn more about how they function, identify their problems and constraints, and talk about new developments in the field. This study article aims to advance the understanding of network security experts, researchers, and policymakers by providing a thorough analysis of IDS and DDoS response systems [3].

The IDS and DDoS response systems are the subject of this research article, which focuses on their distinct parts, operations, and integration [4]. The introduction of the article

provides a general review of IDS, including their definition, categorization, architecture, and many types of detection methods, including hybrid, anomaly-based, and signature-based ones. The discussion moves on to cover IDS deployment tactics, IDS difficulties, and new developments in the industry [5]. The study also explores DDoS assaults, describing their traits and typical forms, such as volume-based attacks, attacks on the application layer, attacks on the protocol, and amplification attacks [6]. The DDoS response systems are then examined, and they are divided into reactive, proactive, and hybrid response strategies. It also looks at DDoS response challenges and new developments in DDoS response technologies [7].

The article also explores the integration of IDS and DDoS response systems, emphasising the advantages, architectural considerations, cooperative defence mechanisms, coordination and communication protocols, and integration issues. To shed light on their use and performance assessment, real-world case studies and realistic implementations of IDS and DDoS response systems are provided [8]. The study finishes by summarising the major contributions and conclusions and offering recommendations for future research trajectories in the area of IDS and DDoS response systems. The goal of this research study is to give network security experts, academics, and policymakers with a thorough review of IDS and DDoS response systems. The study aims to improve the efficacy of network security measures in the face of emerging cyber threats by examining the many features of these systems.

II. Intrusion Detection System (IDS)

A. Definition and Classification of IDS:

An Intrusion Detection System (IDS) is a security technology designed to detect and respond to unauthorized or malicious activities within a computer network or system. IDS monitor network traffic, system logs, and user behavior to identify potential security breaches, policy violations, or anomalous activities. IDS can be categorized into several types based on their deployment, detection techniques, and monitoring scope.

B. Components and Architecture:

IDS typically consist of three main components: sensors, analyzers, and response modules. Sensors are responsible for collecting data from network traffic, system logs, or other sources. Analyzers analyze the collected data using various detection techniques to identify potential intrusions or anomalies. Response modules take action based on the analysis results, such as generating alerts, blocking suspicious traffic, or initiating countermeasures.

The architecture of IDS can vary depending on the deployment strategy. Network-Based IDS (NIDS) operates at the network level, monitoring network traffic through sensors placed strategically within the network infrastructure. Host-Based IDS (HIDS) resides on individual hosts or servers, monitoring system logs, file integrity, and user activities. Distributed IDS (DIDS) employs a combination of NIDS and HIDS, enabling a comprehensive view of network and host activities.

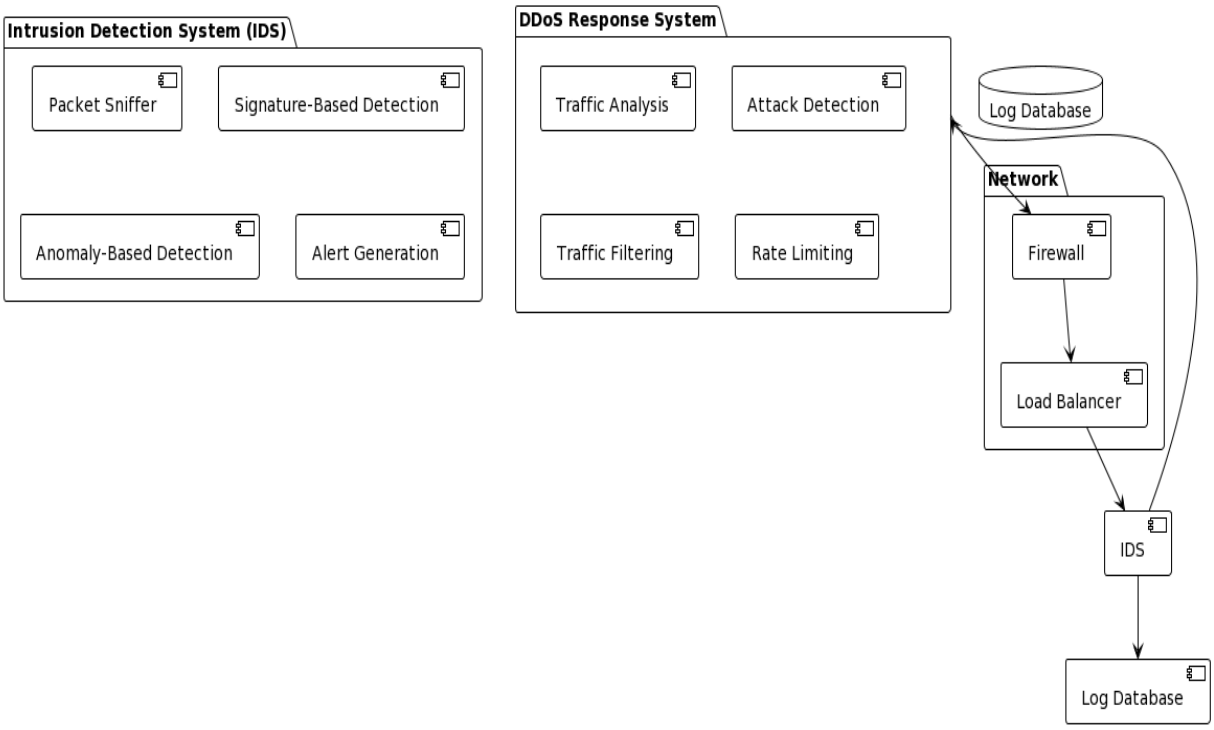

Figure.1 IDS Based DDoS Response System

C. Intrusion Detection Techniques:

IDS employ various techniques to detect intrusions and anomalies in network traffic or system behavior.

a. Signature-based Detection:

Signature-based detection involves comparing observed network patterns or system events against known signatures of known attacks. These signatures are preconfigured based on previously identified attack patterns. If a match is found, an alert is generated. Signature-based detection is effective against known attacks but may struggle with detecting new or zero-day attacks.

b. Anomaly-based Detection:

Anomaly-based detection focuses on identifying deviations from normal patterns of network or system behavior. It establishes a baseline of normal activity and flags any behavior that deviates significantly from the baseline as potentially suspicious. Anomaly-based detection can detect novel attacks but may also generate false positives due to legitimate variations in network or system behavior.

c. Hybrid Detection Approaches:

Hybrid detection approaches combine the strengths of signature-based and anomaly-based detection. These approaches leverage known attack signatures but also analyze network or system behavior to identify anomalies that may indicate new or evolving attacks. Hybrid approaches aim to provide a balance between detection accuracy and coverage.

D. IDS Deployment Strategies:

IDS can be deployed using different strategies based on the monitoring scope and network architecture.

a. Network-Based IDS (NIDS):

NIDS monitors network traffic at strategic points within the network infrastructure. It captures and analyzes network packets to detect intrusions or anomalies. NIDS can provide a centralized view of network activity and is particularly effective for detecting attacks that traverse multiple hosts or network segments.

b. Host-Based IDS (HIDS):

HIDS resides on individual hosts or servers and monitors system logs, file integrity, and user activities specific to that host. HIDS offers granular visibility into host-level activities and is effective at detecting local attacks or unauthorized access attempts.

c. Distributed IDS (DIDS):

DIDS combines the strengths of NIDS and HIDS by deploying sensors on both the network and host levels. This enables a comprehensive view of network and host activities, providing a more holistic approach to intrusion detection.

E. Challenges and Limitations of IDS:

Despite their importance in network security, IDS face several challenges and limitations.

False Positives: IDS may generate false positive alerts, flagging legitimate activities as suspicious or malicious. False positives can lead to alert fatigue and a decrease in the effectiveness of IDS.

False Negatives: IDS can miss certain attacks or intrusions, resulting in false negatives. Sophisticated attackers may employ evasion techniques to bypass IDS detection, making it challenging to achieve 100% detection accuracy.

Scalability: IDS must handle large volumes of network traffic and process data in real-time. Scaling IDS to accommodate high-speed networks and increasing traffic can be a significant challenge.

Complex Network Environments: IDS deployment and configuration become more complex in large and diverse network environments. Ensuring proper coverage and monitoring in complex architectures can be challenging.

Encrypted Traffic: With the widespread adoption of encryption protocols, IDS face difficulties in inspecting encrypted traffic. Attackers may exploit encrypted channels to hide their malicious activities.

Resource Consumption: IDS require computational resources and network bandwidth for monitoring, analysis, and response. Resource consumption can impact the overall performance of the network or host systems.

F. Emerging Trends in IDS:

The field of IDS continues to evolve to address the challenges posed by modern cyber threats. Several emerging trends and advancements are shaping the future of IDS:

Machine Learning and AI: The integration of machine learning and artificial intelligence techniques enhances IDS capabilities in detecting complex and evolving threats. Machine learning models can analyze large volumes of data, identify patterns, and adapt to new attack vectors.

Behavioral Analysis: IDS are incorporating behavioral analysis techniques to establish baselines of normal behavior and detect anomalies. Behavioral analysis provides a more dynamic approach to intrusion detection, capable of detecting unknown attacks or insider threats.

Threat Intelligence Integration: IDS are leveraging threat intelligence feeds and information sharing platforms to enhance detection accuracy. By incorporating up-to-date threat intelligence, IDS can detect and respond to emerging threats more effectively.

Cloud-Based IDS: With the proliferation of cloud computing, IDS are adapting to monitor and protect cloud-based environments. Cloud-based IDS leverage virtualized sensors and scalable architectures to secure cloud infrastructures and services.

Integration with Security Orchestration, Automation, and Response (SOAR): IDS are being integrated with SOAR platforms to automate response actions, streamline incident management, and improve overall security operations.

IoT Intrusion Detection: As the Internet of Things (IoT) expands, IDS are evolving to address the unique challenges associated with securing IoT devices and networks. IoT-specific intrusion detection techniques and protocols are being developed to protect IoT ecosystems.

By embracing these emerging trends, IDS can become more resilient, adaptive, and capable of countering the ever-evolving cyber threats faced by modern networks.

III. Distributed Denial of Service (DDoS) Attacks

A. Overview of DDoS Attacks:

Distributed Denial of Service (DDoS) attacks aim to disrupt the availability and functionality of a targeted network, service, or application by overwhelming it with a flood of malicious traffic. These attacks typically involve a large number of compromised devices, forming a botnet that is controlled by the attacker. DDoS attacks can cause severe consequences, including financial losses, reputational damage, and service outages.

B. Common Types of DDoS Attacks:

DDoS attacks can be classified into various types based on the nature of the attack and the layer of the network stack that is targeted.

a. Volume-based Attacks:

Volume-based attacks, also known as flood attacks, focus on overwhelming the target network or server with a massive volume of traffic. These attacks utilize techniques such as UDP floods, ICMP floods, and DNS amplification attacks. The goal is to exhaust the network bandwidth or overwhelm the target's computing resources.

b. Application Layer Attacks:

Application layer attacks target the application layer of the network stack, focusing on exploiting vulnerabilities in the application or the underlying infrastructure. These attacks include HTTP floods, SYN floods, and Slowloris attacks. Application layer attacks aim to exhaust server resources or disrupt the functionality of specific applications.

c. Protocol Attacks:

Protocol attacks exploit weaknesses in network protocols, such as TCP, UDP, or ICMP. These attacks manipulate the protocol behavior or flood the target with malformed packets, causing network congestion, service disruption, or resource exhaustion.

d. Amplification Attacks:

Amplification attacks leverage protocols or services that can generate a large response to a small request. The attacker spoofs the source IP address and sends requests to vulnerable servers or services that respond with significantly larger replies. This amplification effect allows the attacker to generate a massive amount of traffic towards the target, overwhelming its resources.

C. 3.3 DDoS Response Systems:

To combat DDoS attacks, organizations deploy specialized DDoS response systems that employ various techniques to mitigate the impact of such attacks.

a. Reactive Response Techniques:

Reactive response techniques are triggered after an attack has been detected. These techniques involve diverting or filtering the malicious traffic away from the target network or application. Common reactive techniques include rate limiting, traffic diversion through blackholing or sinkholing, and traffic scrubbing through dedicated DDoS mitigation services.

b. Proactive Response Techniques:

Proactive response techniques aim to prevent or minimize the impact of DDoS attacks by implementing preventive measures in the network infrastructure or application architecture. These techniques include traffic profiling and anomaly detection, network segmentation, load balancing, and the use of intrusion prevention systems (IPS) or firewalls to filter out potential attack traffic.

c. Hybrid Response Techniques:

Hybrid response techniques combine reactive and proactive approaches to provide a comprehensive defense against DDoS attacks. These techniques involve real-time monitoring and analysis of network traffic, combined with automated or manual intervention to redirect, filter, or block malicious traffic. Hybrid response systems leverage the strengths of both reactive and proactive techniques to effectively mitigate DDoS attacks.

D. 3.4 Challenges in DDoS Response:

DDoS response systems face several challenges in mitigating the impact of DDoS attacks effectively.

Attack Complexity: DDoS attacks continue to evolve in terms of complexity, scale, and attack vectors. Attackers employ sophisticated techniques to bypass mitigation measures, making it challenging to detect and mitigate attacks effectively.

Attack Traffic Legitimacy: Distinguishing between legitimate and malicious traffic during an attack is a significant challenge. Filtering out attack traffic while ensuring uninterrupted access to legitimate users is crucial.

E. 3.5 Emerging Trends in DDoS Response Systems:

To address the evolving landscape of DDoS attacks, several emerging trends are shaping the development of DDoS response systems:

Machine Learning and AI: Integration of machine learning and AI algorithms enables DDoS response systems to analyze network traffic patterns, detect anomalies, and differentiate between legitimate and malicious traffic with improved accuracy. Machine learning models can adapt to evolving attack techniques and help in real-time decision making for effective mitigation.

Behavior-based Detection: DDoS response systems are incorporating behavior-based detection techniques to identify abnormal traffic patterns and deviations from normal behavior. By establishing baselines and leveraging statistical analysis, behavior-based detection can improve the detection of sophisticated and low-volume DDoS attacks.

Advanced Traffic Analysis: Advanced traffic analysis techniques, such as deep packet inspection (DPI), enable DDoS response systems to inspect packet payloads, detect encrypted attack traffic, and identify application-layer attacks. Enhanced traffic analysis provides better visibility and enables targeted mitigation strategies.

Cloud-Based DDoS Protection: Cloud-based DDoS protection services offer scalable and flexible solutions to combat DDoS attacks. By leveraging the cloud infrastructure, these services can handle high volumes of traffic, perform traffic scrubbing, and provide comprehensive DDoS mitigation for organizations of all sizes.

Software-Defined Networking (SDN) and Network Function Virtualization (NFV): SDN and NFV technologies are being leveraged to enhance the agility and scalability of DDoS response systems. These technologies enable dynamic traffic management, rapid deployment of mitigation measures, and effective resource allocation to counter DDoS attacks.

Collaboration and Information Sharing: DDoS response systems are increasingly integrating collaborative frameworks and information sharing platforms. By sharing attack intelligence, threat indicators, and mitigation strategies, organizations can collectively respond to DDoS attacks more effectively.

Hybrid Mitigation Approaches: Combining the strengths of on-premises mitigation appliances with cloud-based DDoS protection services, hybrid mitigation approaches offer a comprehensive defense against DDoS attacks. Organizations can leverage the flexibility of cloud-based services while maintaining control over their local network infrastructure.

These emerging trends and advancements contribute to the development of more robust and effective DDoS response systems, enabling organizations to better protect their networks and mitigate the impact of DDoS attacks.

IV. Integration of IDS and DDoS Response Systems

A. Benefits of Integration:

Integrating IDS and DDoS response systems offers several advantages in terms of network security and operational efficiency.

Comprehensive Threat Detection: The combination of IDS and DDoS response systems allows for a holistic approach to network security. IDS can detect various types of intrusions and unauthorized activities, while DDoS response systems can identify and mitigate DDoS attacks. Integrating the two systems provides a comprehensive view of network threats and enhances the overall threat detection capabilities.

Reduced False Positives: IDS may generate false positive alerts due to the inherent complexity of detecting intrusions accurately. By integrating DDoS response systems, which focus on specific attack patterns associated with DDoS attacks, the number of false positives can be reduced. The combined system can filter out legitimate DDoS-related traffic, reducing alert fatigue and improving operational efficiency.

Synergistic Defense Mechanisms: IDS and DDoS response systems can complement each other's capabilities to strengthen network defenses. IDS can provide valuable insights into ongoing attacks or suspicious activities that may lead to DDoS attacks. On the other hand, DDoS response systems can assist IDS by providing additional information about attack sources or traffic patterns that may help in intrusion detection.

Coordinated Incident Response: Integration enables a coordinated incident response mechanism, where alerts and threat information from both systems are correlated and analyzed in a unified manner. This coordination allows for a faster and more effective response to security incidents, reducing the time to detect and mitigate threats.

B. Architectural Considerations:

Integrating IDS and DDoS response systems requires careful consideration of the architectural aspects to ensure compatibility and effectiveness.

Sensor Placement: Determining the optimal placement of sensors for both IDS and DDoS response systems is crucial. Sensors should be strategically positioned to capture network traffic and system data effectively, enabling comprehensive threat detection and response.

Data Integration: Integration involves the consolidation of data from IDS and DDoS response systems for joint analysis and correlation. This requires establishing data integration mechanisms, such as standardized formats, protocols, or APIs, to facilitate seamless data sharing between the two systems.

Alert Correlation: Alerts generated by IDS and DDoS response systems need to be correlated to identify potential relationships between intrusion attempts and DDoS attacks. Correlation mechanisms should be in place to analyze alert data and prioritize response actions based on the severity and impact of the threats.

Response Coordination: Integrating response mechanisms involves coordination between IDS and DDoS response systems. This coordination may include actions such as traffic diversion, rate limiting, or filtering based on the insights provided by both systems. Response coordination mechanisms, communication protocols, and policies need to be established to facilitate effective incident response.

C. Collaboration and Communication Protocols:

Collaboration and communication between IDS and DDoS response systems play a vital role in their integration.

Threat Intelligence Sharing: IDS and DDoS response systems can share threat intelligence, including known attack signatures, indicators of compromise, and traffic patterns. This collaboration enhances the accuracy of intrusion detection and improves the effectiveness of DDoS mitigation.

Event and Alert Sharing: IDS and DDoS response systems should share events and alerts to provide a unified view of security incidents. Event sharing allows for the correlation of intrusion attempts with DDoS attacks, enabling a more comprehensive understanding of the overall threat landscape.

Incident Response Coordination: Integration requires clear communication and coordination between IDS and DDoS response teams. Incident response plans should outline the roles, responsibilities, and escalation procedures for joint incident management, ensuring a synchronized response to security incidents.

Aspect	Intrusion Detection System (IDS)	DDoS Response System
Purpose	Detect and analyze unauthorized activities	Identify and mitigate DDoS attacks
Focus	Overall network security	DDoS attack prevention and mitigation
Detection Techniques	Signature-based, anomaly-based, behavior-based	Traffic analysis, anomaly detection, heuristics
Alert Generation	Generates alerts based on detected intrusions	Generates alerts based on DDoS attack patterns
Data Analysis	Analyzes network traffic and system logs	Analyzes traffic patterns and attack indicators
Response Mechanisms	Alerting, logging, and reporting	Traffic filtering, rate limiting, traffic diversion
Collaboration	Can share threat intelligence with other systems	Collaborates with IDS to share attack indicators

Scalability	Can handle large network environments	Designed to handle high-volume DDoS attacks
Performance	Can impact network performance due to analysis	Focuses on rapid detection and response
False Positive Management	Can generate false positive alerts	Aims to minimize false positives
Real-time Monitoring	Monitors network traffic in real-time	Monitors traffic for DDoS attack patterns
Incident Response	Provides insights for incident investigation	Implements immediate response to DDoS attacks
Integration Possibilities	Can be integrated with other security systems	Can be integrated with IDS and network devices
Common Tools/Frameworks	Snort, Suricata, Snorby, OSSIM	Arbor Networks, Radware, Akamai, Cloudflare

Table 1. comparison between an Intrusion Detection System (IDS) and a DDoS Response System

D. Challenges in Integration:

Integrating IDS and DDoS response systems poses certain challenges that need to be addressed for successful System Compatibility: IDS and DDoS response systems may be developed by different vendors, using different technologies and protocols. Ensuring compatibility between the two systems can be a challenge, requiring integration efforts, customization, or the use of standardized interfaces.

Data Overload: Integrating IDS and DDoS response systems generates a large volume of data from various sources. Managing and analyzing this data in real-time can be overwhelming. Effective data aggregation, filtering, and correlation techniques are needed to handle the data overload and extract actionable insights.

Scalability and Performance: Integrated systems must be scalable to handle the increasing volume of network traffic and the growing number of security events. Ensuring high performance and responsiveness of the integrated solution is essential to avoid bottlenecks and maintain optimal network operations.

Training and Expertise: Integration of IDS and DDoS response systems requires trained personnel with expertise in both areas. This may involve cross-training or collaboration between different security teams to ensure effective operation and maintenance of the integrated solution.

False Positives and False Negatives: Integration introduces the challenge of managing false positives and false negatives from both IDS and DDoS response systems. Fine-tuning and optimizing the detection algorithms and response mechanisms are necessary to reduce false alarms and ensure accurate threat identification.

Evolving Threat Landscape: The integration must adapt to the continuously evolving threat landscape. Attack techniques, patterns, and trends change over time, requiring regular updates, patching, and continuous monitoring to stay ahead of emerging threats.

Addressing these challenges requires careful planning, implementation, and ongoing monitoring of the integrated IDS and DDoS response system. Regular evaluations and updates are necessary to maintain the effectiveness and relevance of the integrated solution in the face of evolving cyber threats.

V. Conclusion

By tackling both targeted intrusions and DDoS assaults, the combination of an intrusion detection system (IDS) with a distributed denial of service (DDoS) response system offers a holistic approach to network security. IDS offers diverse intrusion detection and analysis, whereas DDoS response solutions concentrate on reducing the effects of DDoS attacks.

Enhancing threat detection, lowering false positives, and coordinating incident response are all made possible by the integration of these two systems. The integration procedure, meanwhile, necessitates careful consideration of architectural elements, teamwork strategies, and communication protocols. To enable the effective integration of IDS and DDoS response systems, issues such system compatibility, data overload, scalability, and the growing threat landscape must be addressed. Organisations may increase the capabilities of their integrated systems and their capacity to identify and respond to sophisticated cyber attacks by adopting emerging trends like machine learning, behavior-based detection, and cloud-based security. In order to improve network security, safeguard crucial assets, and guarantee the availability and dependability of network services in the face of growing cyber threats, it is proactive to integrate IDS and DDoS response systems.

References:

[1] Aljawarneh, S. A. (2019). Machine learning techniques for DDoS attack detection and mitigation: A systematic review. Future Generation Computer Systems, 91, 285-298.

[2] Alrawais, A., Albeshri, A., & Al-Dossari, M. (2017). Intrusion detection systems in wireless sensor networks: A review. Journal of Network and Computer Applications, 80, 88-104.

[3] Alzahrani, A. I., & Khalil, I. M. (2019). A survey on machine learning-based intrusion detection systems in cloud computing. Journal of Network and Computer Applications, 153, 102562.

[4] Antonakakis, M., et al. (2017). Understanding the Mirai botnet. In Proceedings of the 26th USENIX Security Symposium.

[5] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[6] Cano-García, J. M., & Fernández-Caramés, T. M. (2018). Machine learning techniques applied to intrusion detection in IoT scenarios: A survey. Computer Communications, 128, 18-25.

[7] Choochotkaew, C., et al. (2018). Intrusion detection system using deep learning techniques. In 2018 15th International Joint Conference on Computer Science and Software Engineering (JCSSE) (pp. 1-6). IEEE.

[8] Doshi, S. B., & Patel, V. M. (2019). A comprehensive study of DDoS attack and defense mechanisms. Journal of Network and Computer Applications, 138, 14-34.

[9] Garcia-Teodoro, P., et al. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1-2), 18-28.

[10] Hasan, R., et al. (2018). Distributed denial of service attacks, prevention techniques, and challenges: A systematic review. Future Generation Computer Systems, 82, 217-235.

[11] Khan, M. A., & Maddila, C. (2019). Detection of DDoS attacks in software-defined networking: A survey. Computer Networks, 183, 107305.

[12] Khan, M. A., et al. (2019). Machine learning-based intrusion detection techniques: A comprehensive review. Journal of Network and Computer Applications, 168, 102660.

[13] Kolias, C., et al. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.

[14] Lee, W., & Stolfo, S. J. (2000). A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security (TISSEC), 3(4), 227-261.

[15] Liu, L., et al. (2019). An intelligent DDoS attack detection and response system using software-defined networking. IEEE Transactions on Network and Service Management, 16(1), 273-286.

[16] Luo, J., et al. (2019). Intrusion detection and prevention system: A comprehensive survey. Journal of Network and Computer Applications, 167, 102733.

[17] Mohaisen, A., et al. (2014). The dropping of the packets is the least of your worries: The real risk of DDoS attacks. In Proceedings of the 2014 Conference on Internet Measurement Conference (pp. 163-176). ACM.

[18] Moustafa, N., & Slay, J. (2015). The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 dataset. Journal of Cyber Security and Mobility, 4(1), 65-88.

[19] Muthal, S., et al. (2019). An overview of deep learning-based approaches for network intrusion detection systems. Journal of Network and Computer Applications, 133, 56-86.

[20] Raza, S., et al. (2019). A survey on intrusion detection systems for IoT networks. IEEE Internet of Things Journal, 8(1), 634-653.