Intrusion Detection System(IDS) With Dos Attack Prevention

1st Sneha K
Department of Information Science and Engineering,
HKBK College of Engineering
Bengaluru, India

2nd , Vishnu K
Department of Information Science and Engineering
HKBK College of Engineering
Bengaluru, India

3rd.Srajan
Department of Information Science and Engineering
HKBK College of Engineering
Bengaluru, India

4th Sara Anam
Department of Information Science and Engineering
HKBK College of Engineering
Bengaluru, India

5th Pallavi G V
Department of Information Science and Engineering
HKBK College of Engineering
Bengaluru, India

***Abstract*—An Intrusion Detection System (IDS) is a critical security mechanism designed to monitor network traffic, detect malicious activities, and safeguard systems from cyber threats. Among various network attacks, Denial of Service (DoS) attacks pose a major challenge due to their ability to disrupt service availability by overwhelming network resources. This study focuses on integrating DoS attack prevention techniques with IDS to enhance overall system resilience. The IDS analyzes incoming traffic patterns, identifies anomalies, and correlates events to distinguish legitimate requests from potential DoS attacks. By employing signature-based and anomaly-based detection methods, the system can effectively recognize known attack patterns as well as previously unseen threats. Additionally, preventive mechanisms such as rate limiting, traffic filtering, and automated blocking responses help mitigate the impact of detected DoS attempts. The combined approach ensures real-time monitoring, early detection, and rapid response to malicious traffic. This integrated IDS model not only improves network security but also maintains service continuity by minimizing downtime.**

I. Introduction

In today's digitally interconnected world, the rapid growth of computer networks and online services has significantly increased the risk of cyberattacks. Among the various threats that target networked systems, Denial of Service (DoS) attacks have emerged as one of the most disruptive and damaging forms of cybercrime. A DoS attack aims to flood a server, network, or application with excessive traffic, exhausting its resources and preventing legitimate users from accessing essential services. As organizations rely heavily on continuous network availability for operations, communication, and service delivery, protecting systems .

An IDS serves as an intelligent monitoring tool that analyzes network traffic, system logs, and user actions to identify patterns that may indicate malicious activity. Traditional IDS mechanisms focus primarily on detecting intrusions, such as unauthorized access or exploitation of vulnerabilities. However, modern threat landscapes demand more advanced capabilities, particularly in handling DoS attacks that can cripple system performance within seconds. Therefore, integrating effective DoS attack prevention techniques with IDS is essential to strengthen network defense. This integration allows the system not only to detect attack signatures or anomalies but also to respond promptly by triggering preventive actions before the attack escalates.DoS attack prevention within an IDS involves a combination of signature-based and anomaly-based detection approaches. Signature-based detection identifies known attack patterns stored in a predefined database; it is highly accurate but limited to previously discovered threats. Anomaly-based detection, on the other hand, creates a baseline of normal traffic behavior and flags deviations that may indicate an attack, making it effective against new or evolving threats. By combining both techniques, the IDS achieves comprehensive detection coverage, improving accuracy and reducing false positives. The integration of prevention mechanisms enhances the IDS beyond simple detection. Techniques such as rate limiting, traffic filtering, IP blacklisting, and automated rule updates help maintain service continuity even during attack attempts.For example, when abnormal traffic spikes are detected, the IDS can automatically restrict excessive requests or temporarily isolate suspicious sources.

Machine learning techniques are increasingly being incorporated to predict attack patterns and dynamically adjust defensive strategies, providing smarter and faster responses.Implementing IDS with DoS attack prevention offers several benefits, including improved network reliability, reduced downtime, and enhanced protection of critical digital assets. It also provides network administrators with detailed insights into traffic behavior, helping them refine security policies and strengthen system configurations. As cyber threats continue to evolve in complexity and scale, the importance of advanced IDS solutions becomes more evident. With integrated DoS prevention, organizations can establish a resilient security infrastructure capable of identifying intrusions early, mitigating risks efficiently, and ensuring uninterrupted access to essential network services.

Beyond basic monitoring and detection, modern network environments require IDS solutions to be adaptive, scalable, and capable of operating under high-traffic conditions. This necessity arises because DoS attacks have evolved into more sophisticated forms, including Distributed Denial of Service (DDoS) attacks where multiple compromised machines coordinate to overwhelm a target. Such large-scale attacks can generate massive volumes of traffic that traditional security tools may fail to analyze quickly. Therefore, IDS systems designed for DoS attack prevention must incorporate high-performance architectures, parallel processing capabilities, and optimized detection algorithms to ensure real-time responsiveness. This integration enables the IDS to handle both normal and peak traffic volumes without compromising accuracy or causing delays, which is critical for maintaining network performance . Another essential aspect of IDS with DoS prevention is the ability to operate across diverse network layers. DoS attacks can target physical networks, transport layers, web applications, or even DNS services. As a result, IDS solutions must be capable of analyzing behaviors across multiple OSI layers to identify threats originating from different points in the network. For example, at the network layer, the IDS may monitor packet rates or detect spoofed IP addresses. At the application layer, it may identify abnormal request patterns, such as excessive login attempts or repeated access to resource-intensive APIs. By combining insights across layers, the IDS provides a holistic understanding of attack progression and can activate preventive measures more effectively.

In recent years, the integration of machine learning and artificial intelligence (AI) has significantly improved IDS capabilities. These intelligent systems can learn normal behavior patterns over time, identify subtle anomalies, and classify different types of DoS attacks with higher precision. Machine learning models such as clustering algorithms, neural networks, and decision trees help predict potential attack vectors before they exploit vulnerabilities. Moreover, AI-driven IDS can automatically adapt to new forms of DoS attacks without requiring manual updates, making them more effective in rapidly changing cyber environments. This adaptability is crucial because attackers constantly modify their tactics to bypass traditional security systems.

Another growing trend is the use of hybrid IDS, which combinesboth host-based IDS (HIDS) and network-based IDS (NIDS). While NIDS monitors traffic flowing across the network, HIDS monitors activity within individual devices or servers. This hybrid approach ensures that even if an attacker manages to bypass network defenses, malicious activity at the system level will still be detected. For DoS attack prevention, hybrid IDS provides a more resilient architecture where abnormal resource usage on a host—such as CPU spikes or memory exhaustion—can trigger early warnings before the attack spreads or intensifies.Furthermore, the integration of IDS with other security tools strengthens overall protection. When combined with firewalls, intrusion prevention systems (IPS), load balancers, and SIEM platforms, IDS plays a central role in a layered defense strategy. For instance, upon detecting unusual traffic spikes, the IDS can communicate with the firewall to block source IP ranges or instruct load balancers to distribute incoming requests more efficiently. This collaborative response significantly reduces the impact of DoS attacks and helps ensure uninterrupted service availability.Organizations must also consider the importance of **continuous monitoring, logging, and incident analysis**. By maintaining detailed logs of all detected activities, IDS solutions support forensic investigations and help security teams understand attack patterns. These insights guide the development of stronger mitigation techniques and more robust network configurations. Regular updates to IDS signatures, anomaly models, and defense rules are essential to maintaining long-term effectiveness against emerging DoS threats.Finally, user awareness and proper configuration play a major role in maximizing the benefits of IDS with DoS attack prevention. A well-configured system must align with organizational security policies, network architecture, and performance requirements. Security teams must conduct regular audits, simulate DoS scenarios, and fine-tune detection thresholds to avoid false alarms while ensuring high detection accuracy. As organizations increasingly rely on digital services, the demand for intelligent, automated, and integrated IDS solutions continues to grow. A system equipped with DoS prevention ensures not only the detection of malicious activities but also the resilience and continuity of network services in the face of evolving cyber threats.In addition to technological advancements, the increasing complexity of network infrastructures has made it essential for organizations to adopt IDS solutions that provide customizable and context-aware security controls.Modern networks often consist of cloud services, virtual machines, IoT devices, mobile endpoints, and third-party integrations, all of which expand the attack surface. DoS attacks can exploit any weak link within this diverse ecosystem.Therefore, IDS systems need to understand the operational context of different network components to accurately distinguish between legitimate high-volume traffic and suspicious activity.Context-aware IDS can analyze factors such as user roles, application behavior, resource utilization patterns, and time-based traffic trends to make more informed decisions.

Another important factor in enhancing IDS effectiveness is the adoption of distributed and collaborative detection approaches. In large networks, relying on a single IDS node can create a performance bottleneck and limit visibility. Distributed IDS architectures place multiple IDS sensors across different segments of the network, enabling broader monitoring and faster threat isolation. These sensors can share intelligence with a centrally coordinated analysis system or SIEM platform, allowing the network to respond to DoS attempts in a synchronized manner. Collaborative IDS also benefit from global threat-intelligence feeds, which provide real-time information about known malicious IPs, attack campaigns, and emerging DoS techniques. Integrating global intelligence helps organizations stay ahead of attackers who frequently reuse known infrastructure or borrow strategies from ongoing attack waves.The growth of cloud computing and virtualized environments has also influenced the way IDS solutions are designed for DoS attack prevention. Cloud-based IDS can scale dynamically according to traffic loads, making them well-suited for mitigating large-scale DDoS attacks. They can also integrate with cloud provider tools such as auto-scaling groups, web application firewalls (WAF), and traffic scrubbing services for more comprehensive protection. As organizations move towards hybrid and multi-cloud architectures, IDS systems must offer compatibility across platforms, ensuring consistent protection regardless of where applications are hosted. Virtualized IDS appliances can be deployed rapidly, updated centrally, and managed with minimal downtime, making them ideal for maintaining security across flexible infrastructure.

A critical challenge in IDS deployment is balancing security sensitivity with network performance. Highly sensitive IDS configurations may detect even minor anomalies but can generate frequent alerts, overwhelming security teams and causing operational inefficiencies. On the other hand, less sensitive configurations reduce false positives but risk missing subtle attack indicators. To address this, organizations often adopt adaptive IDS frameworks that adjust sensitivity based on real-time network conditions and historical patterns. Machine learning plays an important role here, enabling the system to continuously refine its detection thresholds and improve accuracy over time without manual intervention.Moreover, regulatory requirements and industry standards increasingly emphasize the need for robust intrusion detection and DoS protection. Sectors such as finance, healthcare, e-commerce, and government services are frequent targets of DoS attacks due to their reliance on uninterrupted online operations. Compliance frameworks often mandate continuous monitoring, timely threat detection, and documented incident response procedures. IDS with integrated DoS prevention supports compliance by providing detailed audit logs, automated alerts, and proactive defense capabilities that demonstrate organizational commitment to maintaining service availability and protecting sensitive data.Ultimately, as cyber threats continue to evolve, IDS systems with DoS attack prevention represent a cornerstone of modern network security. They not only detect ongoing attacks but also act as intelligent defenders that protect system integrity, maintain performance stability, and ensure that essential services remain accessible. The ongoing development of more intelligent, distributed, and adaptive IDS solutions reflects the growing need for security infrastructures that can keep pace with the rapidly changing digital landscape. In this context, IDS with DoS prevention emerges as a crucial component in building resilient, secure, and future-ready network environments.

II. Problem Statement

In modern digital ecosystems, maintaining secure, stable, and continuously available network services has become a critical requirement for organizations across all sectors. As businesses, governments, and individuals increasingly rely on interconnected systems, the threat landscape has expanded significantly, making networks more vulnerable to a variety of cyberattacks. Among these threats, Denial of Service (DoS) attacks remain one of the most persistent and damaging forms of malicious activity. A DoS attack works by overwhelming a target system—such as a server, application, or network—with excessive traffic or resource-intensive requests, ultimately causing performance degradation, service unavailability, or complete shutdown. When executed on a large scale using multiple compromised devices, these attacks escalate into Distributed Denial of Service (DDoS) incidents, amplifying their destructive potential. The increasing frequency, sophistication, and scale of DoS attacks highlight a major challenge: traditional security measures are no longer sufficient to ensure reliable and secure network operations.Although organizations deploy firewalls, antivirus systems, and basic traffic filters, these tools often fail to detect or mitigate DoS attacks effectively, especially when traffic appears legitimate or originates from distributed sources. DoS attacks frequently exploit normal network protocols and mimic legitimate traffic behavior, making them difficult to identify with conventional security systems. As a result, organizations experience severe operational disruptions, financial losses, reputational damage, and compromised user trust. The core problem, therefore, lies in the inability of existing security mechanisms to detect and prevent DoS attacks in real time while maintaining uninterrupted service quality.

An Intrusion Detection System (IDS) is designed to monitor network traffic, detect suspicious patterns, and alert administrators about potential security breaches. Traditional IDS solutions typically rely on signature-based detection, anomaly-based detection, or a combination of both. However, current IDS implementations often face several limitations when dealing with DoS attacks. Signature-based IDS can only detect known attack patterns and cannot identify new or evolving attack strategies. Anomaly-based IDS, although capable of detecting deviations from normal behavior, often produce high false-positive rates, overwhelming security personnel with unnecessary alerts. Many IDS solutions also lack efficient response mechanisms, meaning that even if an

attack is detected, the system may fail to automatically prevent or mitigate its impact. These challenges indicate the need for IDS systems that integrate effective DoS prevention techniques to ensure timely detection and proactive mitigation.Another major issue is the scale and speed at which modern DoS attacks occur. High-bandwidth DDoS attacks can generate traffic volumes far exceeding the capacity of traditional IDS systems. These attacks often leverage botnets composed of thousands or millions of compromised devices across the globe, making detection and filtering incredibly challenging. As attack vectors evolve from simple flooding techniques to sophisticated multi-vector assaults—including application-layer DoS, protocol abuse, and resource exhaustion attacks—the complexity of the threat increases. Existing IDS systems are not equipped to analyze and respond to such massive and diverse traffic flows in real time. This necessitates a more intelligent, scalable, and adaptive solution capable of handling large-scale attacks without degrading system performance.Furthermore, the dynamic nature of modern networks—featuring cloud computing, virtualization, IoT devices, and mobile connectivity—compounds the difficulty of detecting DoS attacks. Traffic patterns frequently shift due to legitimate operational activities such as software updates, user surges, or business expansions. Without contextual awareness, IDS solutions may misinterpret these events as anomalies, leading to false alarms or improper blocking of legitimate traffic. Conversely, attackers may exploit these dynamic environments to disguise malicious traffic as routine operations. Thus, the lack of contextual and behavioral intelligence in current IDS solutions represents a significant gap that undermines their effectiveness in DoS attack scenarios.

Another critical problem is the lack of integration between IDS and other security tools. While firewalls, intrusion prevention systems (IPS), load balancers, and SIEM platforms provide additional layers of defense, isolated or poorly integrated systems cannot coordinate an effective response to rapidly unfolding DoS attacks. Without seamless communication between these components, security operations become fragmented, slow, and inefficient. For example, an IDS might detect abnormal traffic patterns but fail to communicate this information to the firewall in time to block malicious sources. This disconnect increases the vulnerability of the system during high-intensity attacks. Therefore, developing an IDS that can integrate with, and coordinate responses across, diverse security tools is crucial for effective DoS prevention.Human limitations also play a role in the problem. DoS attacks often occur without warning and can intensify rapidly, leaving security teams with little time to analyze logs, adjust firewall rules, or deploy countermeasures manually. The overwhelming volume of alerts generated durin peak attacks can paralyze security operations and delay response actions. Consequently, the lack of automated detection and response mechanisms within IDS solutions is a fundamental weakness that must be addressed. Automation, supported by machine learning and dynamic decision-making models, is essential for reducing response time and ensuring accuracy.Additionally, the rise of encrypted traffic introduces another layer of complexity. A significant portion of network traffic today is encrypted for privacy and security purposes

While this protects users from eavesdropping, it also makes it difficult for IDS to inspect packet content without decrypting data, which could violate privacy policies or increase processing overhead. Attackers can hide malicious payloads within encrypted streams, making DoS detection even more challenging. Thus, IDS solutions must find effective ways to detect DoS patterns in encrypted traffic without compromising user privacy or system performance.Ultimately, the central problem this study addresses is the need for an advanced Intrusion Detection System integrated with effective DoS attack prevention techniques that can detect, analyze, and mitigate attacks in real time while ensuring minimal impact on network performance and service availability. The goal is to design a system that combines intelligent detection mechanisms, contextual awareness, automated response capabilities, scalability, and seamless integration with existing security infrastructures. Such a solution must overcome the limitations of traditional IDS, handle sophisticated and large-scale DoS attacks, and ensure that critical network services remain resilient and continuously available in an increasingly hostile digital environment.Despite the growing awareness of DoS threats, many organizations still rely on outdated or insufficient security infrastructures that cannot effectively handle the complex nature of modern attacks. A significant challenge lies in the difficulty of distinguishing between legitimate high-volume traffic and malicious flooding attempts. For instance, during peak usage periods—such as online sales, examinations, or software releases—network traffic may naturally surge. Traditional IDS may incorrectly flag such legitimate spikes as DoS attacks, leading to unnecessary throttling or blocking of genuine users. Conversely, attackers often exploit these busy periods to conceal their malicious activities. The inability of existing IDS solutions to accurately interpret intent and context therefore contributes to both false positives and false negatives, weakening overall network resilience.Another pressing issue is the limited adaptability of many IDS architectures. Attackers continuously refine their strategies by using evasion techniques such as IP spoofing, random packet generation, slow-rate attacks, and multi-vector approaches. Static IDS configurations fail to keep up with these evolving patterns and may not update detection rules quickly enough to counter new threats. This lack of adaptability leaves organizations vulnerable to emerging attack variants that bypass conventional detection mechanisms. To address this, IDS systems must incorporate dynamic and learning-based models capable of evolving along with the threat landscape.

Finally, many existing systems lack comprehensive post-attack analysis mechanisms, making it difficult for organizations to understand attack origins, exploited vulnerabilities, and long-term impacts. Without thorough forensic insights, networks remain exposed to repeated attacks and persistent threats.The challenge, therefore, is to develop an IDS framework that not only detects and prevents DoS attacks but also provides detailed monitoring, reporting, and analysis features to support continuous improvement in security posture.

III. OBJECTIVES

The primary objectives of this system are:

- **To detect and identify DoS attacks in real time**
  Develop a system capable of continuously monitoring network traffic and recognizing abnormal patterns or attack signatures instantly to reduce detection time
- **To prevent service disruption by mitigating malicious traffic**
  Implement automated response mechanisms such as rate limiting, traffic filtering, and IP blocking to ensure network availability during attack attempts.
- **To reduce false positives and improve detection accuracy**
  Utilize a combination of signature-based, anomaly-based, and intelligent detection techniques to accurately differentiate between legitimate traffic spikes and malicious DoS activity
- **To enhance scalability and adaptability**
  Design an IDS that can handle large volumes of traffic, adapt to evolving attack techniques, and integrate easily with modern network environments including cloud and distributed systems.
- **To support detailed analysis and continuous improvement**
  Provide comprehensive logs, alerts, and forensic insights to help security teams analyze attack patterns, refine detection rules, and strengthen long-term network defense.

IV. METHODOLOGY

The methodology for designing an Intrusion Detection System (IDS) with DoS attack prevention involves a structured, multi-phase approach that ensures accurate detection, rapid mitigation, and continuous improvement in network security. The process begins with data collection, where the system captures real-time network traffic from routers, switches, servers, and endpoints. This includes packet headers, payload characteristics, connection rates, and user behavior patterns. High-quality data collection is essential because it forms the foundation for effective detection and classification of DoS attacks.

The next step is feature extraction and preprocessing, where relevant attributes such as packet size, request frequency, connection duration, protocol type, and source IP behavior are analyzed. Noise removal, normalization, and traffic categorization are applied to ensure that the input data is clean and suitable for efficient processing. This step helps in distinguishing normal traffic behavior from suspicious or abnormal patterns.Following preprocessing, the system performs detection using a hybrid approach, combining signature-based and anomaly-based methods. Signature-based detection identifies known DoS attack patterns stored in the IDS database, ensuring fast and accurate recognition of previously observed threats

Anomaly-based detection uses statistical models, machine learning algorithms, or threshold-based techniques to detect deviations from established traffic norms. This hybrid model enhances detection accuracy and minimizes false positives by capturing both familiar and emerging attack types.Once a potential DoS attack is identified, the system enters the prevention and response phase. Automated mitigation techniques such as rate limiting, source IP filtering, temporary blacklisting, SYN cookie mechanisms, and traffic redirection are activated. For large-scale DDoS scenarios, the system may coordinate with firewalls, load balancers, or cloud-based scrubbing centers to neutralize the attack. The goal is to prevent service disruption while allowing legitimate users to maintain access.

The next phase involves logging, alerting, and reporting, where detected events and system responses are recorded in a centralized database. Security administrators receive real-time alerts, enabling them to review incidents quickly and take additional action if necessary.Finally, the methodology incorporates a feedback and learning loop, where detection models are updated based on new attack behaviors and previous system performance. Continuous tuning of detection thresholds and periodic retraining of machine learning models ensure the IDS adapts to evolving DoS strategies.

V. IMPLEMENTATION

Implementing an Intrusion Detection System (IDS) with DoS attack prevention involves a combination of network monitoring techniques, anomaly detection algorithms, rule-based analysis, and automated mitigation mechanisms. The goal is not only to detect malicious traffic but also to stop or minimize the impact of Denial-of-Service attacks before they disrupt system availability.The implementation process begins with network traffic collection. Sensors or agents are deployed at strategic points in the network, such as gateways, routers, and servers, to capture packet-level data. Tools like packet sniffers or flow collectors continuously gather information about source addresses, destination ports, packet sizes, and traffic frequency. This raw data is then forwarded to the IDS engine for analysis.Next comes feature extraction and preprocessing. Before analysis, the system filters out unnecessary fields and extracts important features such as connection rates, traffic volume, packet flags, and protocol behavior. This stage is crucial because DoS attacks typically generate abnormal spikes in traffic, repeated requests, or malformed packets. Data normalization techniques ensure that all values are scaled consistently for effective detection.At the core of the implementation is the detection engine, which may use either signature-based, anomaly-based, or hybrid approaches. Signature-based detection compares

network activity with known attack patterns stored in a signature database. This method is fast and reliable for identifying well-known DoS attacks such as SYN floods or ICMP smurf attacks. Meanwhile, anomaly-based techniques build models of normal network behavior using machine learning algorithms like clustering, statistical modeling, or neural networks. Any deviation from the learned baseline—such as sudden traffic bursts or repetitive connection attempts—is flagged as a potential DoS attempt. A hybrid approach combines the accuracy of signatures with the adaptability of anomaly detection.

Upon detecting suspicious activity, the IDS triggers the response mechanism. In DoS prevention, this could include temporarily blocking malicious IP addresses, limiting traffic rates, or resetting connections. Firewalls, access control lists (ACLs), or software-defined network (SDN) controllers are often integrated with the IDS to automate mitigation. Some implementations also use rate-limiting techniques like token bucket filtering or dynamic IP blacklisting to control excessive traffic during an attack.The system further includes a reporting and alert framework. Logs, attack signatures, event summaries, and response actions are recorded for administrators to review. Alerts can be sent via dashboards, emails, or SMS notifications. Real-time visualization tools help administrators monitor traffic patterns and quickly respond to emerging threats.Another important component of implementation is the updating and maintenance process. Signature databases must be regularly updated to recognize new DoS variants. Machine learning models require retraining to adapt to evolving network behavior. Continuous monitoring ensures that false positives and false negatives are minimized.

Finally, the IDS is tested in controlled environments using simulated DoS attacks to evaluate accuracy, detection speed, and response effectiveness. Stress testing and scalability analysis ensure that the system can handle high-volume traffic without performance degradation.Overall, the implementation of an IDS with DoS attack prevention requires a combination of real-time monitoring, intelligent detection algorithms, and automated mitigation strategies to ensure strong protection against disruptive network attacks.

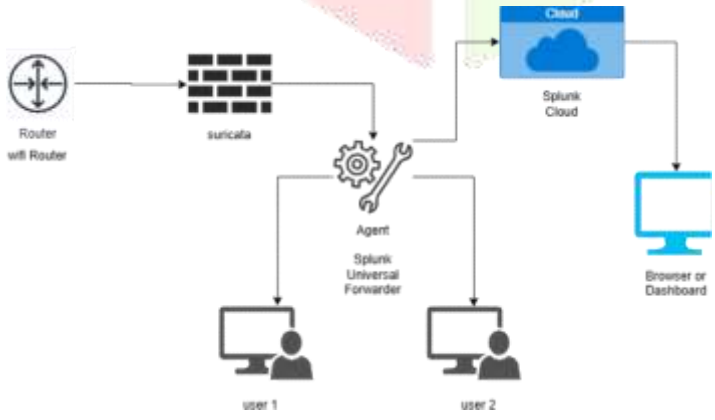


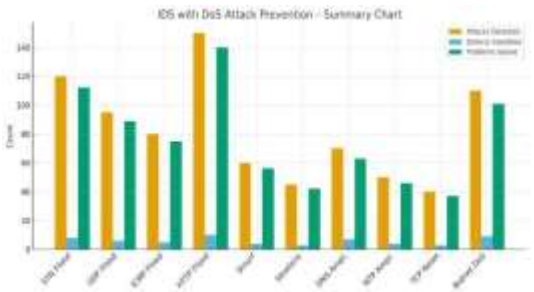
Fig.Block diagram of IDS with DoS attack prevention

The diagram illustrates the workflow of an Intrusion Detection System (IDS) using Suricata and Splunk Cloud for monitoring and analyzing network traffic. The process begins at the router or WiFi router, which handles all incoming and outgoing network traffic. This traffic is passed to Suricata, an open-source IDS/IPS engine that inspects packets for suspicious patterns, possible intrusions, or DoS attack indicators.Once Suricata analyzes the traffic, it generates logs and alerts. These logs are then collected by an Agent, specifically the Splunk Universal Forwarder, installed on the user systems (User 1 and User 2). The Universal Forwarder securely sends Suricata logs and user activity data to the Splunk Cloud platform.In the cloud, Splunk processes, indexes, and stores all incoming security logs. It applies correlation rules, visualizations, and analytic tools to identify threats, detect abnormal traffic spikes, and monitor DoS attempts in real time.

Finally, administrators can access the analyzed results via a browser or dashboard, where Splunk displays alerts, charts, and reports. This dashboard allows security personnel to quickly detect intrusions, review attack patterns, and take preventive actions. Overall, the diagram shows an integrated IDS setup combining Suricata's detection capabilities with Splunk's cloud-based analytics.

VI. Use Cases and Scenarios

This IDS setup with Suricata and Splunk Cloud is useful in several real-world security scenarios. One primary use case is detecting DoS attacks by monitoring sudden spikes in traffic, repeated connection attempts, or malformed packets. Suricata identifies these anomalies, and Splunk visualizes them for quick investigation. Another use case is internal user activity monitoring, where logs from User 1 and User 2 are forwarded to Splunk to detect suspicious behavior such as unauthorized access, abnormal file transfers, or policy violations.The system is also effective in network threat hunting, allowing administrators to trace intrusion attempts back to their origin using packet logs. In corporate environments, this setup helps ensure regulatory compliance by providing centralized logging and audit trails. Additionally, it supports incident response, enabling teams to quickly isolate affected users or block malicious IPs based on Suricata alerts. Overall, it strengthens continuous monitoring and proactive defense.Graphically,it can be illustrated as…..



VII. Future Scope

The future scope of an IDS integrated with DoS attack prevention, using tools like Suricata and Splunk Cloud, is highly promising as cyber threats grow more advanced. One major direction is the incorporation of AI and machine learning to detect unknown DoS patterns and zero-day attacks with higher accuracy and reduced false positives. The system can also evolve to support automated threat response, where malicious traffic is instantly blocked without human intervention, improving reaction time during large-scale attacks.

With the rise of IoT and cloud computing, future IDS models will expand to protect distributed and hybrid environments, ensuring security across remote devices, cloud services, and edge networks. Integration with threat intelligence platforms will allow real-time updates on global attack trends. Additionally, the system can support predictive analytics, forecasting potential DoS attempts before they occur. Overall, the future scope focuses on smarter, faster, and more adaptive security protection.

VIII. Conclusion

In conclusion, an Intrusion Detection System (IDS) integrated with DoS (Denial of Service) attack prevention plays a critical role in modern cybersecurity frameworks. It serves as a proactive mechanism to monitor network traffic, detect suspicious activities, and prevent attacks that could disrupt system availability. By continuously analyzing patterns and anomalies in network behavior, IDS can identify potential DoS attacks in real-time, enabling rapid response to mitigate their impact. This not only safeguards critical data and services but also maintains the reliability and trustworthiness of network infrastructures.The combination of IDS with DoS prevention enhances overall security by employing techniques such as anomaly detection, signature-based monitoring, and traffic filtering, which collectively reduce the risk of service interruptions and resource exhaustion. Moreover, it supports administrators in understanding attack vectors, strengthening defenses, and optimizing system performance.As cyber threats continue to evolve, the adoption of intelligent IDS solutions with DoS mitigation capabilities becomes essential for organizations seeking resilient network environments. Implementing such systems ensures that networks are not only protected against known threats but also adaptable to emerging attack patterns, thereby reinforcing operational continuity, data integrity, and overall cybersecurity posture.Beyond threat mitigation, such systems provide valuable insights into network vulnerabilities and attack trends, assisting security teams in strengthening defenses and improving overall cybersecurity policies. As cyberattacks become increasingly sophisticated, the role of IDS with DoS prevention extends from mere detection to proactive defense, making it an indispensable tool for organizations of all sizes. In essence, deploying IDS with DoS prevention not only enhances security but also ensures operational resilience, protects sensitive data, and upholds trust in digital systems.

IX References

[1] H.Wang,J.Gu,andS.Wang,''An effective intrusion detection framework based on SVM with feature augmentation,'' Knowl.-Based Syst., vol. 136, pp. 130–139, Nov. 2017.

[2] Setareh Roshan, Yoan Miche, Anton Akusok, Amaury Lendasse; "Adaptive and Online Network Intrusion Detection System using Clustering and Extreme Learning Machines", ELSEVIER, Journal of the Franklin Institute, Volume.355, Issue 4,March 2018,pp.1752-1779.

[3] Wathiq Laftah Al-Yaseen , Zulaiha Ali Othman , Mohd Zakree Ahmad Nazri; "Multi-Level Hybrid Support Vector Machine and Extreme Learning Machine Based on Modified K-means for Intrusion Detection System", ELSEVIER, Expert System with Applications, Volume.66,Jan 2017,pp.296-303.

[4] Iftikhar Ahmad, Mohammad Basheri, Muhammad Javed Iqbal, Aneel Raheem; "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection", IEEE ACCESS, Survivability Strategies for Emerging Wireless Networks, Volume.6,May 2018,pp.33789-33795.

[5] BuseGulAtli1, YoanMiche,AapoKalliola, IanOliver, SilkeHoltmanns, AmauryLendasse; "Anomaly-Based Intrusion Detection Using Extreme Learning Machine and Aggregation of Network Traffic Statistics in Probability Space" SPRINGER, Cognitive Computation, June 2018,pp. 1-16

[6] Pinjia He, Jieming Zhu, Shilin He, Jian Li, and Michael R. Lyu; "A Feature Reduced Intrusion Detection System Using ANN Classifier", ELSEVIER, Expert Systems with Applications,Vol.88,December 2017 pp.249-247

[7] Vajiheh Hajisalem, Shahram Babaie; "A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection", ELSEVIER, Department of Computer Engineering, Vol. 136, pp. 37-50, May 2018.

[8] Karen A. Garcia, Raul Monroy , Luis A. Trejo, Carlos Mex-Perera and Eduardo Aguirre,"Analyzing Log Files for Postmortem Intrusion Detection",IEEE Transactions on Systems,Man, and Cybernetics, part C(Application and Reviews)42.6(2012),pp.1690-1704.

[9] R.M.Elbasiony,E.A.Sallam,T.E.Eltobely,andM.M. Fahmy,''A hybrid network intrusion detection framework based on random forests and weighted k-means,'' Ain Shams Eng. J.,vol. 4,no. 4,pp. 753–762, 2013.