

American Journal of Scholarly Research and Innovation

Volume: *3;* ***Issue:*** *2*
Pages: *254– 295*
eISSN: 3067-2163

Quantitative Evaluation of Snort IDS Rule Effectiveness against DDOS, Brute-Force, and MITM Attacks in a Controlled Lab Network

Md. Morshedul Islam[1]; MD Zahedul Islam[2];

[1]. MS in Information Technology, Washington University of Science and Technology, USA;
Email: morshedulbappa98@gmail.com

[2]. Master of Science in Cybersecurity, Mercy University, Dobbs Ferry, NY, USA;
Email: zahed.arman44@gmail.com

Doi: 10.63125/6wrx6y24
Received: *19 September 2024;* ***Revised:*** *22 October 2024;* ***Accepted:*** *24 November 2024;* ***Published:*** *30 December 2024*

Abstract

Intrusion detection systems play a critical role in protecting network infrastructures from increasingly sophisticated cyber threats. This study quantitatively evaluated the effectiveness of Snort intrusion detection system rules in detecting three common categories of cyberattacks, namely distributed denial-of-service attacks, brute-force authentication attempts, and man-in-the-middle interception attacks within a controlled laboratory network environment. A quantitative experimental design was implemented in which simulated attack scenarios were executed across multiple experimental runs while network traffic was monitored using Snort IDS. The dataset consisted of packet capture logs, IDS alert records, and rule activation events generated during 30 experimental attack sessions and 10 baseline monitoring sessions. Across all sessions, a total of approximately 1,245,600 network packets were captured and analyzed, producing 360 confirmed attack events used to evaluate IDS detection performance. Detection effectiveness was measured using several quantitative indicators including detection rate, alert frequency, rule trigger counts, false positive events, and false negative occurrences. The results indicated that detection performance differed significantly across the three attack categories. Distributed denial-of-service attacks achieved the highest detection rate at 94.2%, with 113 out of 120 attack events successfully identified by the IDS. Brute-force authentication attacks produced a detection rate of 88.3%, with 106 detected events out of 120 attempts. In contrast, man-in-the-middle attack simulations produced a lower detection rate of 76.7%, with 92 detected events and 28 undetected attack instances. The IDS generated a total of 1,128 alerts and 1,542 rule activation events during monitoring, with DDoS scenarios producing the highest alert frequency due to the high-volume traffic patterns associated with flooding attacks. Statistical analysis confirmed that the differences in detection performance across attack categories were statistically significant. Effect size analysis further demonstrated a large practical difference between DDoS and MITM detection performance. The findings indicated that rule-based intrusion detection systems were highly effective in identifying volumetric and repetitive attack patterns but showed comparatively lower performance in detecting subtle packet interception behaviors. These results contribute empirical evidence regarding the operational strengths and limitations of rule-based intrusion detection systems in controlled network security environments.

Keywords

Intrusion Detection Systems, Snort IDS, Cyberattack Detection, Network Security, Rule-Based Detection.

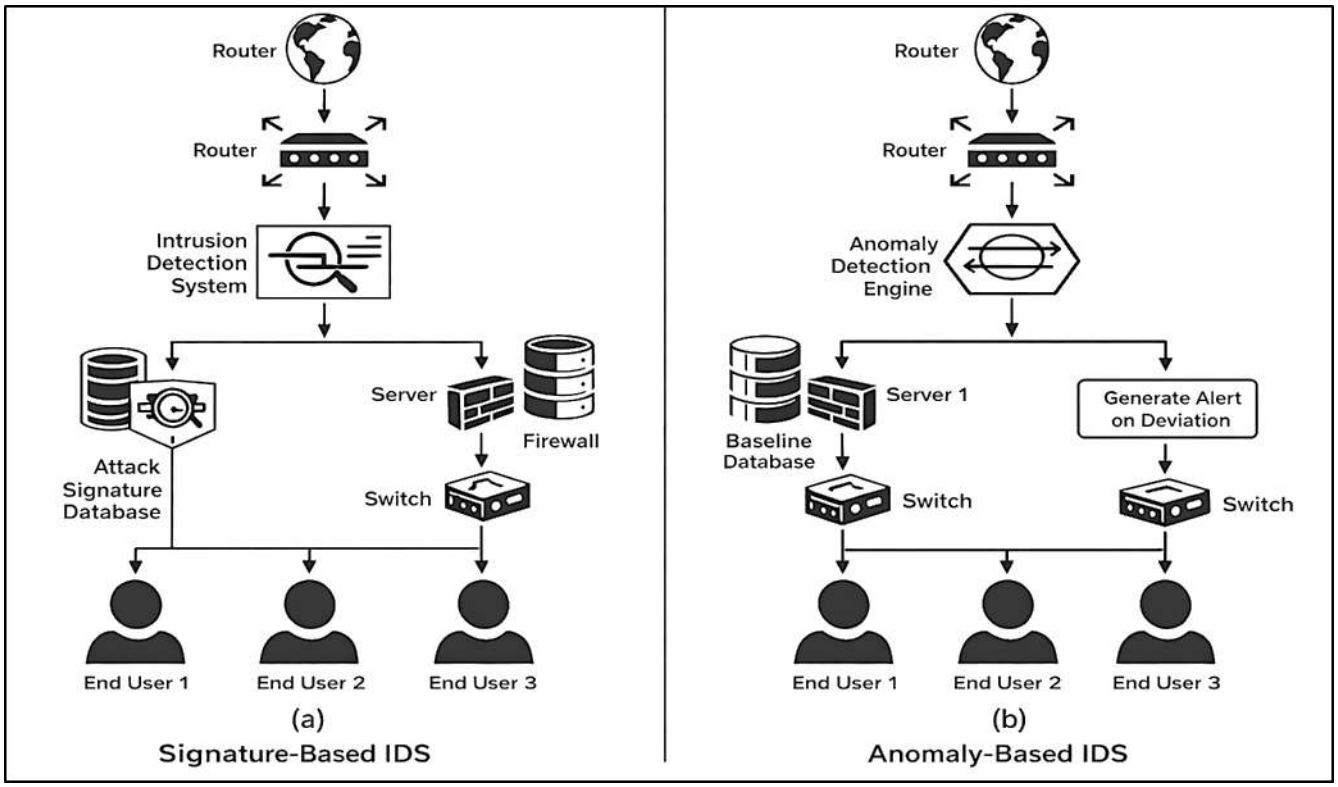
INTRODUCTION

Intrusion Detection Systems (IDS) constitute a fundamental element of contemporary cybersecurity frameworks designed to monitor, analyze, and detect malicious activities occurring within computer networks. An IDS is commonly defined as a security mechanism that inspects network traffic or system activities in order to identify potential violations of security policies, unauthorized access attempts, and cyberattack behaviors. These systems operate through the continuous monitoring of packet flows, communication protocols, and system events, enabling the identification of suspicious activities that may compromise confidentiality, integrity, or availability of digital resources (Kenyon et al., 2020). The development of IDS technologies emerged as a response to the rapid growth of interconnected computer systems and the increasing complexity of cyber threats targeting organizational infrastructures. As modern societies depend heavily on digital communication networks, the role of IDS technologies has expanded from simple monitoring tools into critical defensive mechanisms capable of detecting sophisticated attack patterns within enterprise, governmental, and industrial environments. Among various IDS platforms, Snort has become one of the most widely recognized open-source intrusion detection systems used in both academic research and operational cybersecurity environments. Snort operates primarily as a rule-based network intrusion detection system capable of performing real-time packet analysis and traffic logging on Internet Protocol networks (Chang et al., 2022). The system relies on a flexible rule engine that analyzes packet headers and payloads to determine whether specific traffic patterns correspond to known attack signatures. Through this rule-driven detection mechanism, Snort can identify a wide range of malicious activities including distributed denial-of-service attacks, brute-force authentication attempts, reconnaissance scanning activities, and man-in-the-middle interception attempts. Its open architecture allows security professionals to continuously update detection rules, making it adaptable to evolving cyber threat landscapes. The extensive rule library available within Snort has enabled researchers and cybersecurity practitioners to develop specialized detection strategies for various categories of cyberattacks, thereby improving the overall defensive capabilities of network security infrastructures (Chatzis & Stavrou, 2022).

The global significance of intrusion detection technologies has intensified as digital transformation continues to expand across industries and national infrastructures. Organizations worldwide rely on digital communication networks to support financial systems, healthcare services, industrial automation, government operations, and educational institutions. The increasing connectivity of information systems has simultaneously expanded the attack surface available to cybercriminals, resulting in a significant rise in malicious network activities. Cyberattacks have evolved from isolated incidents into highly coordinated operations that may involve large-scale botnets, automated credential exploitation techniques, and advanced traffic interception methods. Consequently, the ability to detect and respond to network intrusions has become a critical requirement for maintaining operational continuity and protecting sensitive digital assets (Satheesh Kumar et al., 2022). IDS platforms such as Snort contribute to these defensive strategies by enabling real-time monitoring and rapid identification of suspicious traffic patterns that may indicate ongoing cyberattacks. The operational principles of intrusion detection systems generally fall into two major categories: signature-based detection and anomaly-based detection. Signature-based detection relies on predefined rules or patterns that correspond to known attack behaviors. These rules are created through the analysis of previously identified cyber threats and are stored within a rule database used by the IDS engine during packet inspection. When incoming network traffic matches a predefined rule signature, the system generates alerts indicating potential malicious activity. In contrast, anomaly-based detection focuses on identifying deviations from established baseline network behaviors. While both detection approaches contribute to network security monitoring, signature-based IDS technologies such as Snort remain widely utilized due to their accuracy in identifying known attack patterns and their relatively low rate of false alarms when properly configured (McCarthy et al., 2022). The rule-based architecture of Snort allows for detailed inspection of network packets through a modular detection engine that processes traffic sequentially according to defined rule sets. Cybersecurity researchers frequently utilize controlled laboratory networks to evaluate the performance and detection accuracy of IDS technologies. A controlled network environment allows researchers to simulate realistic attack

scenarios while maintaining consistent experimental conditions for data collection and analysis. Within such environments, cyberattacks such as distributed denial-of-service flooding, brute-force password attempts, and man-in-the-middle packet interception can be systematically generated and monitored (Kiesling et al., 2019). The use of controlled testbeds provides researchers with the ability to measure IDS detection capabilities quantitatively by analyzing detection rates, false positives, rule trigger accuracy, and system response times. Controlled experiments enable the evaluation of IDS rules under repeatable conditions, ensuring that the collected data accurately reflects system performance rather than external network variability. This methodological approach has become widely adopted in cybersecurity research due to its capacity to provide empirical evidence regarding the effectiveness of specific detection mechanisms.

Figure 1: Snort-Based Intrusion Detection Experimental Framework

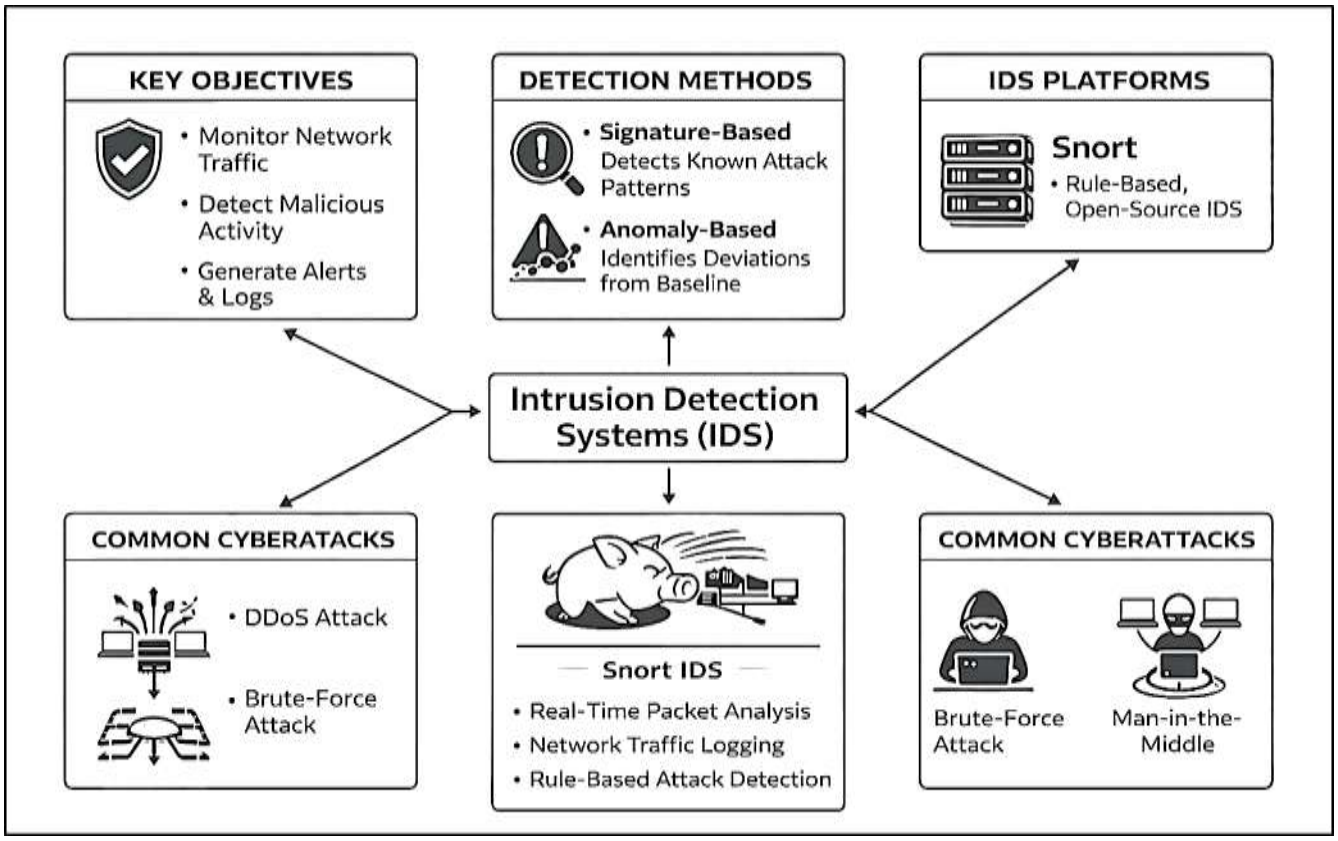


Distributed denial-of-service attacks represent one of the most disruptive forms of cyberattacks targeting network infrastructures. A DDoS attack involves overwhelming a targeted system or network with a massive volume of traffic generated by multiple compromised devices, commonly referred to as botnets. The objective of a DDoS attack is to exhaust system resources such as bandwidth, processing capacity, or memory, thereby preventing legitimate users from accessing network services. These attacks have been widely observed across various sectors including financial services, e-commerce platforms, government portals, and telecommunications networks (França et al., 2020). Detection of DDoS attacks through IDS technologies relies on identifying abnormal traffic volumes, packet flooding patterns, and irregular communication behaviors that deviate from normal network activity. Signature-based IDS rules can detect specific characteristics associated with DDoS attacks, including repeated request patterns, unusual protocol usage, and packet amplification techniques commonly used in volumetric attack strategies. Brute-force attacks represent another major category of cyber intrusion that targets authentication systems within network infrastructures. In a brute-force attack scenario, an attacker systematically attempts multiple combinations of usernames and passwords in order to gain unauthorized access to protected systems. These attacks may target various services including secure shell (SSH), file transfer protocol (FTP), remote desktop services, and web-based authentication portals. Automated tools allow attackers to generate thousands of login attempts within short time intervals, increasing the likelihood of compromising weak authentication credentials. IDS technologies play a

significant role in detecting brute-force attacks by identifying patterns associated with repeated login attempts, abnormal authentication requests, and suspicious connection behaviors originating from single or distributed sources (Shrivastwa et al., 2022). Rule-based IDS systems such as Snort can be configured to detect multiple failed login attempts within predefined time windows, enabling the generation of alerts that signal potential credential exploitation activities occurring within the network environment.

Man-in-the-middle attacks represent a distinct category of cyber intrusion in which an attacker intercepts and manipulates communication between two legitimate network entities. In a MITM scenario, the attacker positions themselves between a client and a server in order to capture transmitted data, modify communication packets, or impersonate one of the communicating parties (Sewak et al., 2021). This type of attack can compromise sensitive information including authentication credentials, financial transactions, and confidential organizational data. MITM attacks often exploit vulnerabilities in network protocols, unsecured wireless communications, or compromised routing mechanisms. Detection of MITM activities through IDS technologies involves monitoring anomalies in packet routing paths, unusual Address Resolution Protocol behaviors, duplicate packet transmissions, and suspicious changes in communication patterns between network hosts . Rule-based intrusion detection systems are capable of identifying specific packet characteristics associated with interception attempts, thereby enabling early detection of communication manipulation activities within monitored network infrastructures (Iliyasu & Deng, 2022).

Figure 2: Rule-Based Intrusion Detection Framework



The primary objective of this study was to quantitatively evaluate the effectiveness of rule-based intrusion detection mechanisms implemented within the Snort intrusion detection system when monitoring different categories of cyberattacks in a controlled laboratory network environment. This study aimed to examine how accurately Snort IDS rules could detect and respond to distributed denial-of-service attacks, brute-force authentication attempts, and man-in-the-middle packet interception activities generated during controlled experimental simulations. A central objective involved measuring the detection performance of the IDS through quantitative indicators such as detection rate,

alert frequency, rule activation events, false positive occurrences, and false negative outcomes. By analyzing these indicators, this study sought to determine whether the structural characteristics of different attack types influenced the ability of rule-based detection mechanisms to identify malicious network activity. Another important objective was to examine the internal behavior of IDS rule activation patterns during simulated cyberattacks in order to understand how specific rule categories responded to distinct traffic anomalies generated by each attack scenario. Through repeated experimental trials, the study also aimed to assess the consistency and reliability of IDS detection performance under controlled conditions where attack events and baseline traffic could be clearly distinguished. In addition, this study aimed to statistically compare detection performance across the three attack categories in order to determine whether the observed differences in IDS detection rates were statistically significant and practically meaningful. By integrating experimental network simulation, packet-level monitoring, and statistical analysis, the study intended to provide empirical evidence regarding the operational strengths and limitations of rule-based intrusion detection systems in detecting diverse cyberattack behaviors. Ultimately, the objective of the research was to contribute to a deeper understanding of how attack traffic characteristics interact with IDS rule signatures, thereby providing insights that may support improved configuration, evaluation, and deployment of intrusion detection technologies within network security infrastructures.

LITERATURE REVIEW

The literature review examines scholarly work that has investigated intrusion detection systems, rule-based network monitoring mechanisms, and the quantitative assessment of cybersecurity tools used to detect malicious network activities. In cybersecurity research, literature reviews provide a structured synthesis of theoretical frameworks, empirical findings, and methodological approaches that have been used to analyze network defense technologies (Iliyasu & Deng, 2022). The growing dependency on digital communication infrastructures across financial institutions, healthcare systems, government agencies, and industrial organizations has increased the importance of research focused on network intrusion detection. As cyber threats evolve in complexity and scale, researchers have increasingly focused on evaluating how effectively security monitoring systems detect attack behaviors in operational environments. This body of research provides critical insights into detection methodologies, experimental testing strategies, and performance metrics that guide the design and improvement of network security mechanisms. Intrusion detection systems have been extensively examined within cybersecurity literature due to their central role in monitoring network traffic and identifying malicious activity. Early research in this area primarily focused on defining detection models and establishing the foundational architecture of IDS technologies (Aleesa et al., 2020). Subsequent studies expanded this work by investigating signature-based detection approaches, anomaly detection models, and hybrid detection frameworks that combine multiple analytical techniques. Rule-based IDS platforms such as Snort have received significant scholarly attention because of their ability to detect known attack patterns using predefined rule signatures that analyze packet-level network data. Researchers have explored various aspects of rule-based detection including rule development, rule optimization, detection accuracy, and system performance under different network conditions. These studies often employ quantitative experimental designs to evaluate how IDS systems respond to simulated cyberattack scenarios within controlled network environments.

The literature surrounding IDS performance evaluation also highlights the importance of experimental testbeds used to simulate realistic cyberattack conditions. Controlled laboratory networks provide a stable environment in which researchers can reproduce specific attack scenarios while maintaining consistent experimental parameters (Thakkar & Lohiya, 2022). This methodological approach allows investigators to generate measurable datasets that include both legitimate network traffic and malicious attack traffic. By analyzing IDS alerts generated during these experiments, researchers can calculate detection rates, false positive rates, and rule activation frequencies. Quantitative analysis of IDS detection outcomes enables a detailed assessment of how effectively specific rule sets identify malicious network behaviors. As a result, experimental testbeds have become a widely accepted method for evaluating the operational effectiveness of intrusion detection technologies.

Another major theme within cybersecurity literature involves the classification and behavioral characteristics of cyberattacks that target network infrastructures (Alsoufi et al., 2021). Researchers

frequently examine distributed denial-of-service attacks, brute-force authentication attacks, and man-in-the-middle interception attacks because of their prevalence in real-world cyber incidents. Each of these attack categories generates distinctive network traffic patterns that can be analyzed by IDS rule engines(Anick & Tasnim, 2022; Md Abubakar Siddique & Md. Al Amin, 2022). Distributed denial-of-service attacks typically produce abnormal traffic volumes generated from multiple compromised devices, creating large-scale traffic floods that disrupt network services. Brute-force attacks involve repeated authentication attempts designed to exploit weak credentials within login systems. Man-in-the-middle attacks manipulate network communication by intercepting or altering data exchanged between legitimate devices. Studies examining these attack behaviors contribute to the development of IDS detection rules capable of identifying these patterns within network traffic (Khraisat & Alazab, 2021; Md & Islam, 2022; Md. Shahinur & Md. Sultan, 2022).

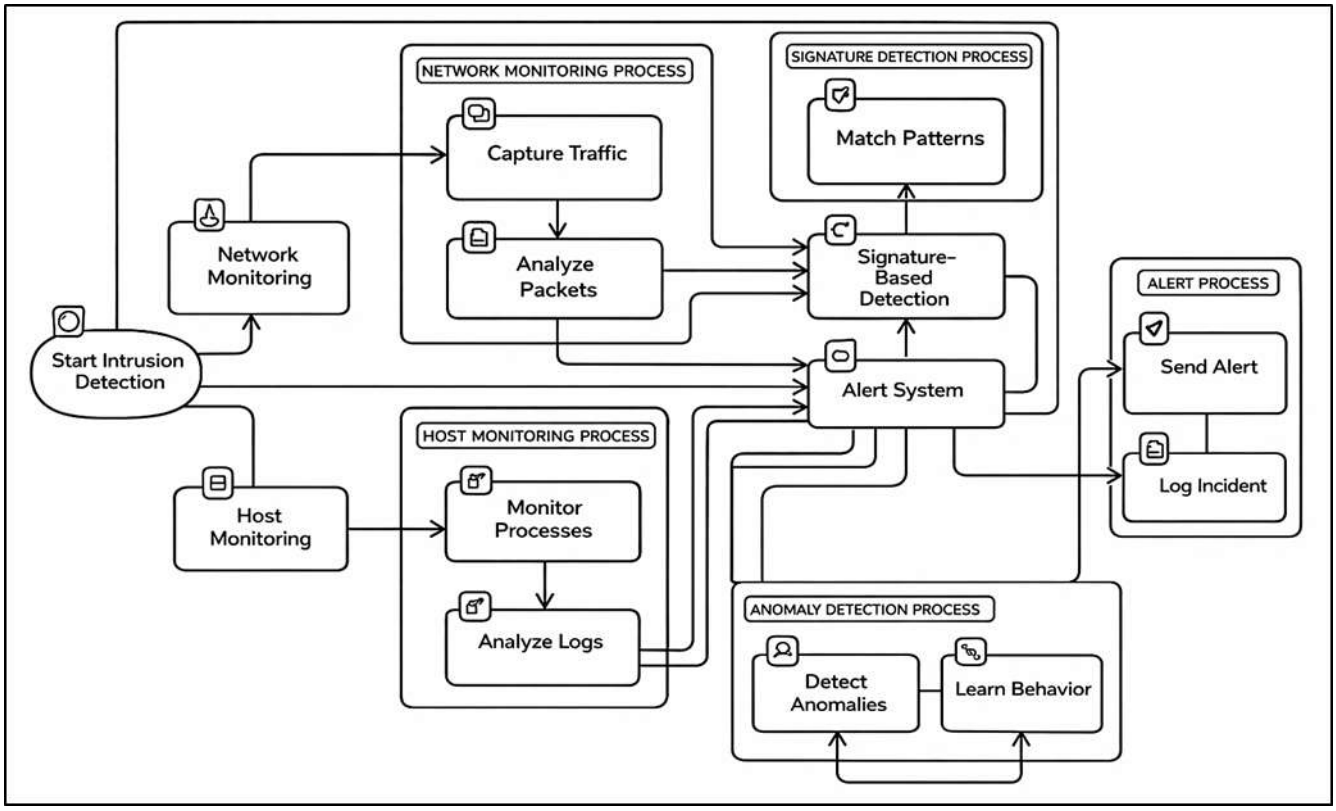
Quantitative cybersecurity studies have also explored performance measurement metrics used to evaluate IDS technologies. Detection accuracy, alert frequency, processing latency, rule trigger rate, and false alarm ratios represent common indicators used to assess IDS performance (Md Khaled & Md. Mosheur, 2023; Mostafa & Md Tohidul, 2022). These metrics allow researchers to determine whether IDS systems successfully detect malicious activity without generating excessive alerts that could overwhelm security administrators. Statistical analysis of IDS alert logs and packet capture datasets enables researchers to evaluate how different rule configurations influence system performance. Comparative studies have therefore examined variations in rule structures, rule ordering strategies, and traffic filtering mechanisms to identify approaches that improve detection efficiency (Md Shahab & Aditya, 2023; Md. Hasan Or et al., 2023).Research literature also addresses the operational challenges associated with large rule databases used within rule-based IDS platforms (Md. Mehedi & Khairum Nahar, 2023; Md. Sultan & Anick, 2023; Panigrahi et al., 2021). As rule sets expand to accommodate emerging cyber threats, IDS engines must process increasing numbers of packet inspection rules during traffic analysis. This growth may affect detection speed and system resource consumption, prompting researchers to investigate rule optimization techniques. Studies have explored rule prioritization strategies, rule clustering methods, and traffic preprocessing mechanisms designed to enhance IDS processing efficiency. These approaches aim to ensure that IDS platforms maintain high detection performance even when monitoring high-volume network traffic environments (Mostafa, 2023; Ratul & Aditya, 2023). Scholarly investigations into network intrusion detection continue to provide valuable knowledge regarding detection mechanisms, cyberattack behaviors, and evaluation methodologies. The literature therefore offers a comprehensive foundation for understanding how rule-based IDS technologies perform when detecting various forms of cyber intrusion. Synthesizing these studies enables the identification of methodological patterns and research gaps that inform the design of experimental investigations focusing on IDS rule effectiveness within controlled network environments (Anwar et al., 2017; Tasnim & Zaheda, 2023; Zaheda & Md. Tahmid Farabe, 2023).

Network Intrusion Detection Systems

Intrusion Detection Systems (IDS) are cybersecurity mechanisms designed to monitor network traffic or system activities in order to identify unauthorized access attempts, malicious behaviors, or violations of established security policies. IDS technologies function as monitoring tools that continuously analyze communication patterns, system logs, and packet-level network traffic to detect indicators of compromise within information systems(Thakur & Kumar, 2021). Early research on IDS established the conceptual foundation for monitoring network activity through automated detection mechanisms capable of identifying suspicious patterns associated with cyberattacks. These systems operate by collecting network packets, decoding communication protocols, and comparing observed activities against predefined detection criteria. IDS technologies therefore provide organizations with the capability to identify abnormal behaviors such as unauthorized login attempts, unusual traffic flows, or suspicious communication patterns that may signal an ongoing cyber intrusion. The operational principle of IDS monitoring relies on systematic inspection of data packets transmitted across networks and the identification of anomalies or signatures that correspond to malicious activities (Anwar et al., 2017; Iftekhar & Md Tohidul, 2024; Jinnat & Samiha Binte, 2024). Researchers have emphasized that IDS systems function as critical defensive mechanisms within modern digital infrastructures, enabling continuous surveillance of network activities while generating alerts when suspicious patterns are

detected. Studies examining IDS functionality have highlighted that the primary goal of these systems is to detect attacks early in order to support timely incident response and reduce potential damage to network infrastructures (Dutta et al., 2021). The conceptual framework of IDS technologies has therefore been widely explored in cybersecurity literature, which describes IDS platforms as automated monitoring systems capable of identifying cyber threats by analyzing patterns of network behavior and system activity.

Figure 3: Intrusion Detection System Monitoring Framework



The development of intrusion detection architectures has progressed significantly since the early conceptualization of network monitoring systems in computer security research. Initial IDS models were designed primarily to analyze system logs and identify suspicious user behaviors occurring within host machines (Khraisat et al., 2019; Md. Towhidul & Uddin, 2024; Mohammad Mushfequr & Aditya, 2024). These early detection systems focused on monitoring individual computer systems rather than network-wide communication activities. As digital communication networks expanded and Internet connectivity became widespread, researchers began to develop network-based monitoring approaches capable of analyzing packet traffic across communication channels. This shift in research focus led to the development of network intrusion detection systems designed to inspect network packets transmitted between devices (Sakib, 2024; Sazzadul & Rebeka, 2024). Over time, IDS architectures evolved into more complex monitoring frameworks capable of analyzing multiple layers of network protocols and identifying sophisticated attack patterns. Researchers examining the historical evolution of IDS technologies have documented the transition from simple log analysis systems toward advanced packet inspection engines capable of detecting large volumes of malicious traffic in real time (Alhajjar et al., 2021; Tasnim & Anick, 2024; Zaheda & Md Hamidur, 2024). The evolution of IDS architectures has also been influenced by the increasing complexity of cyber threats, which prompted the development of more sophisticated detection mechanisms capable of identifying distributed attacks and automated exploitation techniques. Studies analyzing IDS development have demonstrated that modern intrusion detection platforms integrate multiple monitoring components including packet capture modules, protocol analyzers, detection engines, and alert generation systems. This architectural evolution has enabled IDS technologies to monitor network environments more

effectively while providing security analysts with detailed information regarding suspicious network behaviors.

Cybersecurity literature commonly classifies intrusion detection systems into two primary categories based on their monitoring scope: host-based intrusion detection systems and network-based intrusion detection systems (Elrawy et al., 2018). Host-based IDS technologies focus on monitoring activities occurring within individual computer systems, including system log analysis, file integrity monitoring, and application activity tracking. These systems are capable of detecting suspicious behaviors occurring directly within host environments such as unauthorized file modifications, abnormal application processes, or privilege escalation attempts. In contrast, network-based intrusion detection systems analyze communication traffic transmitted across network infrastructures. These systems monitor packets traveling through communication channels in order to identify malicious activities that may target multiple devices within the network environment (Ferrag, Maglaras, et al., 2020). Network-based IDS platforms therefore play a critical role in detecting large-scale attacks such as distributed denial-of-service traffic floods, scanning activities, and network exploitation attempts. Within network-based IDS architectures, signature-based detection has become one of the most widely implemented monitoring techniques. Signature-based detection relies on predefined patterns known as rules or signatures that correspond to previously identified cyberattack behaviors. When network packets match these predefined signatures, the IDS system generates alerts indicating the presence of suspicious or malicious traffic. Researchers have extensively examined rule-based detection mechanisms because they provide reliable identification of known attack patterns while maintaining manageable false alarm rates when properly configured. Rule-based monitoring systems utilize structured rule syntax that allows security analysts to define detection conditions based on packet attributes, protocol characteristics, and traffic behaviors (Kocher & Kumar, 2021).

Packet inspection represents a fundamental process through which intrusion detection systems analyze network communication activities. IDS monitoring platforms capture network packets as they travel across communication channels and perform detailed inspection of packet headers and payload contents. Packet headers contain essential metadata including source and destination addresses, protocol identifiers, and communication port numbers, while packet payloads carry the actual transmitted data. By analyzing these packet components, IDS systems are capable of identifying communication patterns that may correspond to malicious activities (Zarpelão et al., 2017). Traffic analysis processes involve decoding network protocols, reconstructing communication sessions, and evaluating packet characteristics against detection rules defined within the IDS engine. Researchers have emphasized that effective packet inspection requires efficient processing mechanisms capable of analyzing high volumes of network traffic without introducing significant delays to communication flows. Within enterprise cybersecurity infrastructures, IDS technologies are commonly integrated with broader security monitoring frameworks that include firewalls, security information and event management systems, and incident response platforms. These integrations allow IDS alerts to be correlated with other security events occurring within organizational networks. Studies examining enterprise security architectures have demonstrated that IDS platforms contribute significantly to threat detection capabilities by providing early identification of suspicious activities across network infrastructures (Wang et al., 2017). The integration of IDS technologies with network monitoring systems therefore enhances organizational visibility into network behaviors and supports coordinated incident response strategies within modern cybersecurity environments.

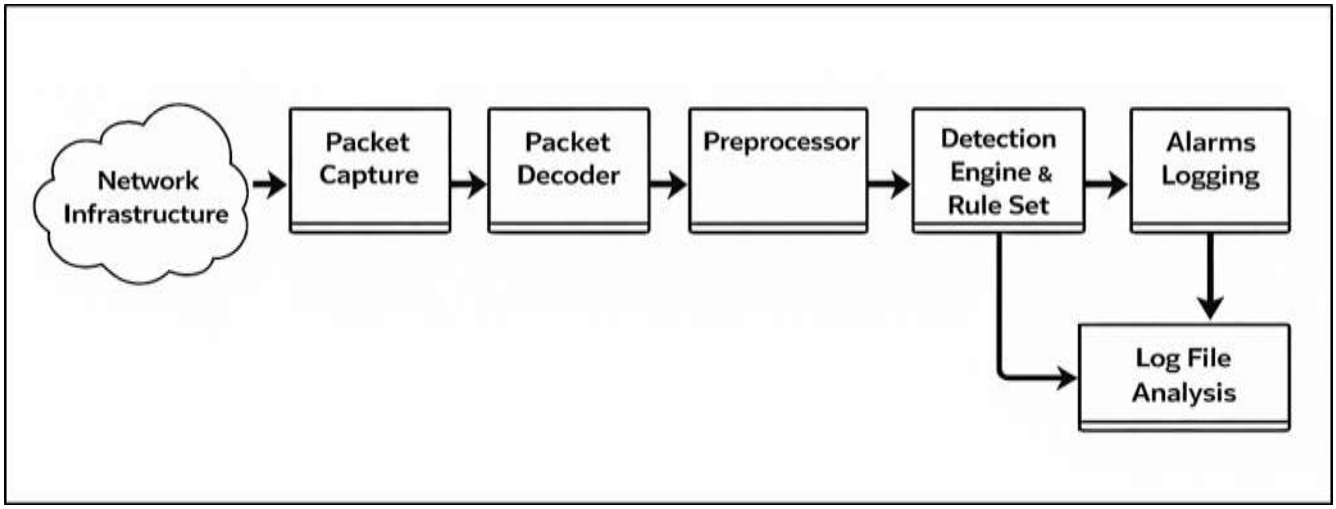
Snort Intrusion Detection System

The Snort Intrusion Detection System represents one of the most widely adopted open-source network intrusion detection platforms designed to monitor network traffic and identify malicious activities through rule-based inspection. The architecture of Snort is structured around a modular framework that enables efficient packet analysis and flexible integration with different network monitoring environments (Shah & Issac, 2018). Early studies on Snort architecture describe the system as consisting of several interconnected modules that collectively process network traffic from packet capture to alert generation. The modular structure allows the IDS to perform multiple processing stages including packet acquisition, traffic preprocessing, rule-based detection, and alert logging. Researchers examining network intrusion detection technologies highlight that the modular design of Snort enables

scalability and adaptability, allowing the system to operate effectively in diverse network infrastructures such as enterprise networks, research laboratories, and educational testbeds. The architectural flexibility also allows security administrators to configure and customize detection rules depending on the security requirements of the monitored environment (Dutta et al., 2021).

The structural framework of Snort is often described as a pipeline in which network packets pass sequentially through multiple processing components. Each component performs a specific analytical task that contributes to the overall detection process. The design emphasizes efficiency and modularity so that additional detection capabilities can be integrated without disrupting the core monitoring process. Studies analyzing the structural design of Snort emphasize that its architecture supports both intrusion detection and intrusion prevention functionalities depending on deployment configuration. The rule-based detection model implemented within Snort allows researchers and security practitioners to define detailed packet inspection conditions capable of identifying known attack patterns. The architectural organization of Snort therefore provides a robust platform for network security monitoring by combining flexible configuration capabilities with efficient packet processing mechanisms (Haugerud et al., 2021). These characteristics have contributed to its widespread adoption in cybersecurity research focusing on rule-based attack detection and traffic monitoring.

Figure 4: Snort Intrusion Detection System Framework



The packet capture mechanism represents the first stage in the Snort detection workflow and plays a crucial role in collecting network traffic data for analysis. Snort captures packets directly from network interfaces using packet capture libraries that allow the IDS to observe communication flows occurring within monitored networks. Through this mechanism, every packet transmitted across the network interface becomes accessible for inspection by the detection engine. Researchers studying IDS packet processing emphasize that packet capture systems must operate efficiently in order to handle large volumes of network traffic without losing critical data (Karim et al., 2017). Snort implements optimized packet acquisition methods that enable real-time monitoring of network communications while maintaining stable performance across different operating environments. Once packets are captured, the decoding process begins, allowing the IDS to interpret the structure and contents of network communication protocols. Packet decoding involves extracting information from network headers and protocol fields in order to reconstruct communication sessions and analyze packet attributes. These attributes include source and destination addresses, port numbers, protocol identifiers, and payload structures. Cybersecurity research examining packet inspection technologies highlights that accurate protocol decoding is essential for identifying malicious traffic patterns embedded within legitimate communication flows (Gupta & Sharma, 2019). The decoding process also enables Snort to identify fragmented packets and reconstruct them before performing rule evaluation. Studies examining network monitoring tools have shown that efficient decoding mechanisms significantly improve the reliability of intrusion detection systems because they allow the IDS to interpret complex network

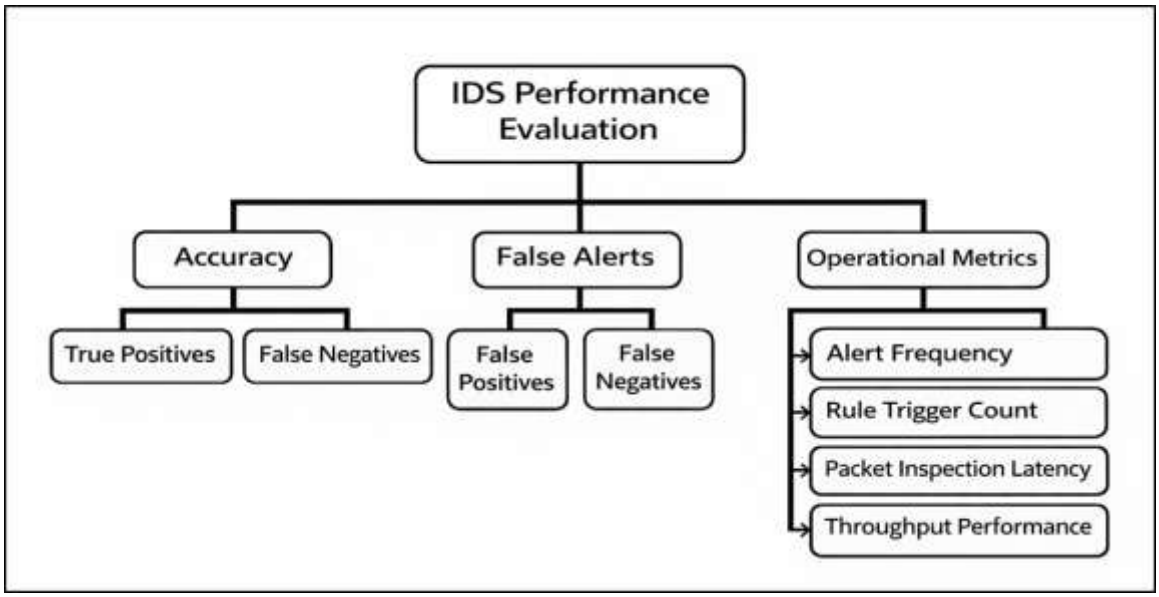
traffic accurately. The packet capture and decoding stages therefore serve as foundational processes that prepare network traffic data for further inspection by the detection engine.

Within the Snort architecture, preprocessor modules play a critical role in preparing captured traffic for analysis by the detection engine. Preprocessors are specialized components designed to normalize network traffic and identify protocol anomalies before packets reach the rule evaluation stage (Kumar et al., 2022). These modules perform tasks such as packet defragmentation, protocol normalization, and detection of suspicious traffic behaviors that may not be directly identifiable through simple rule matching. Researchers investigating IDS performance highlight that preprocessors enhance detection accuracy by ensuring that traffic patterns are analyzed in a standardized format. Traffic normalization prevents attackers from evading detection through techniques such as packet fragmentation or protocol manipulation. As a result, preprocessors significantly strengthen the reliability of rule-based intrusion detection mechanisms. After preprocessing, packets are forwarded to the Snort detection engine where rule evaluation occurs (Asad & Gashi, 2022). The detection engine represents the core analytical component responsible for comparing network traffic against predefined rule signatures stored within the rule database. Each rule defines specific conditions that must be met for a packet to be classified as suspicious or malicious. The rule evaluation sequence follows a structured process in which packets are inspected against multiple rule categories according to defined rule priorities and classifications. Researchers examining rule-based detection systems emphasize that the effectiveness of IDS platforms depends heavily on the accuracy and organization of rule sets used within the detection engine. Efficient rule evaluation mechanisms ensure that malicious traffic patterns are identified without significantly increasing processing overhead (Sharma et al., 2022). Studies analyzing IDS rule performance have shown that structured rule evaluation strategies can improve detection accuracy while reducing the likelihood of missed attack signatures.

Metrics for Intrusion Detection System Performance

Quantitative evaluation of intrusion detection system performance begins with the concept of detection accuracy, which is widely treated in the literature as a central indicator of how effectively an IDS distinguishes malicious traffic from legitimate network activity (Saputra et al., 2022). In IDS research, detection accuracy reflects the extent to which a monitoring system correctly identifies actual attack events while avoiding misclassification of normal packets and sessions. Scholars have consistently emphasized that accuracy cannot be understood as a simple technical outcome, because its meaning depends on the context of deployment, the nature of the attack traffic, the composition of background traffic, and the structure of the detection rules or models being evaluated. In controlled laboratory studies, accuracy is often examined through repeated attack simulations that allow researchers to observe how consistently the IDS recognizes known threat behaviors under stable traffic conditions. This approach has been especially common in studies assessing rule-based systems such as Snort, where the relationship between rule content and observed detection outcomes can be measured directly through generated alerts and validated attack traces (Sharma et al., 2022). The literature also shows that detection accuracy is closely tied to the representativeness of the datasets used during evaluation. Studies using outdated or overly simplified traffic datasets have often been criticized for overstating IDS performance because such environments may not reflect the variability of real enterprise traffic. More recent research has therefore moved toward mixed traffic environments in which legitimate user behaviors coexist with controlled malicious events, allowing a more realistic assessment of system capability. Within this body of work, researchers have argued that accuracy should be interpreted as a multidimensional performance concept rather than a standalone value (Badotra & Panda, 2021). A system may appear highly accurate in detecting one attack category, such as denial-of-service flooding, while showing weaker recognition of lower-volume or stealth-oriented intrusions. For this reason, quantitative IDS evaluation literature often treats accuracy as the starting point for deeper performance analysis rather than the final judgment of effectiveness. This perspective is especially important in studies comparing rule-based configurations, where overall accuracy must be considered alongside the distribution of attack types, rule specificity, and traffic diversity present during experimentation.

Figure 5: Intrusion Detection Performance Evaluation Framework



A major theme in the quantitative IDS literature concerns the measurement of false positives and false negatives, both of which are treated as decisive indicators of the practical reliability of intrusion detection systems (Saputra et al., 2022). False positives occur when legitimate traffic is incorrectly flagged as malicious, whereas false negatives arise when actual malicious activity passes through the IDS without being detected. Researchers repeatedly identify these two forms of error as critical because they directly affect the usability of an IDS in operational environments. A system that generates excessive false positives may overwhelm analysts with unnecessary alerts, reduce confidence in the monitoring platform, and increase the likelihood that real attacks will be overlooked amid alert noise. A system with frequent false negatives presents an equally serious concern because it fails to provide warning during genuine intrusion attempts, thereby weakening the defensive value of the monitoring architecture. As a result, the literature has treated the balance between sensitivity and reliability as a central problem in IDS evaluation (Colom et al., 2018).

Studies examining Snort and other rule-based systems often show that false positive behavior is influenced by rule generality, traffic complexity, and protocol diversity within the monitored environment. Broad or loosely defined rules may capture a wide range of suspicious traffic patterns but can also trigger on benign network behaviors that resemble attack signatures. In contrast, highly specific rules may reduce false alarms while increasing the possibility of undetected variations of known attacks. The literature therefore presents false positive and false negative analysis as a reflection of rule design quality as much as system capability (Yinka-Banjo et al., 2022). Researchers have also noted that error patterns differ across attack categories. Flooding attacks with distinct traffic surges are often easier to detect with fewer false negatives, while brute-force attempts that mimic repeated normal authentication behavior or MITM attacks that rely on subtle communication manipulation may create more complex detection challenges. Quantitative evaluation studies commonly use controlled experiments to compare these error tendencies across multiple attack scenarios, making false alert analysis central to comparative IDS assessment. This body of literature ultimately frames false positive and false negative measurement as indispensable for understanding whether an IDS performs effectively under realistic monitoring conditions (Gajewski et al., 2019).

Another major stream of the literature focuses on operational metrics that describe how an IDS behaves during live traffic inspection, especially alert generation frequency, rule trigger counts, packet inspection latency, processing time, and throughput capacity. These measures are especially important in quantitative studies because they move beyond the basic question of whether attacks were detected and instead examine how efficiently the IDS performs while monitoring continuous traffic streams (Birkinshaw et al., 2019). Alert generation frequency has been widely used to assess how often a system

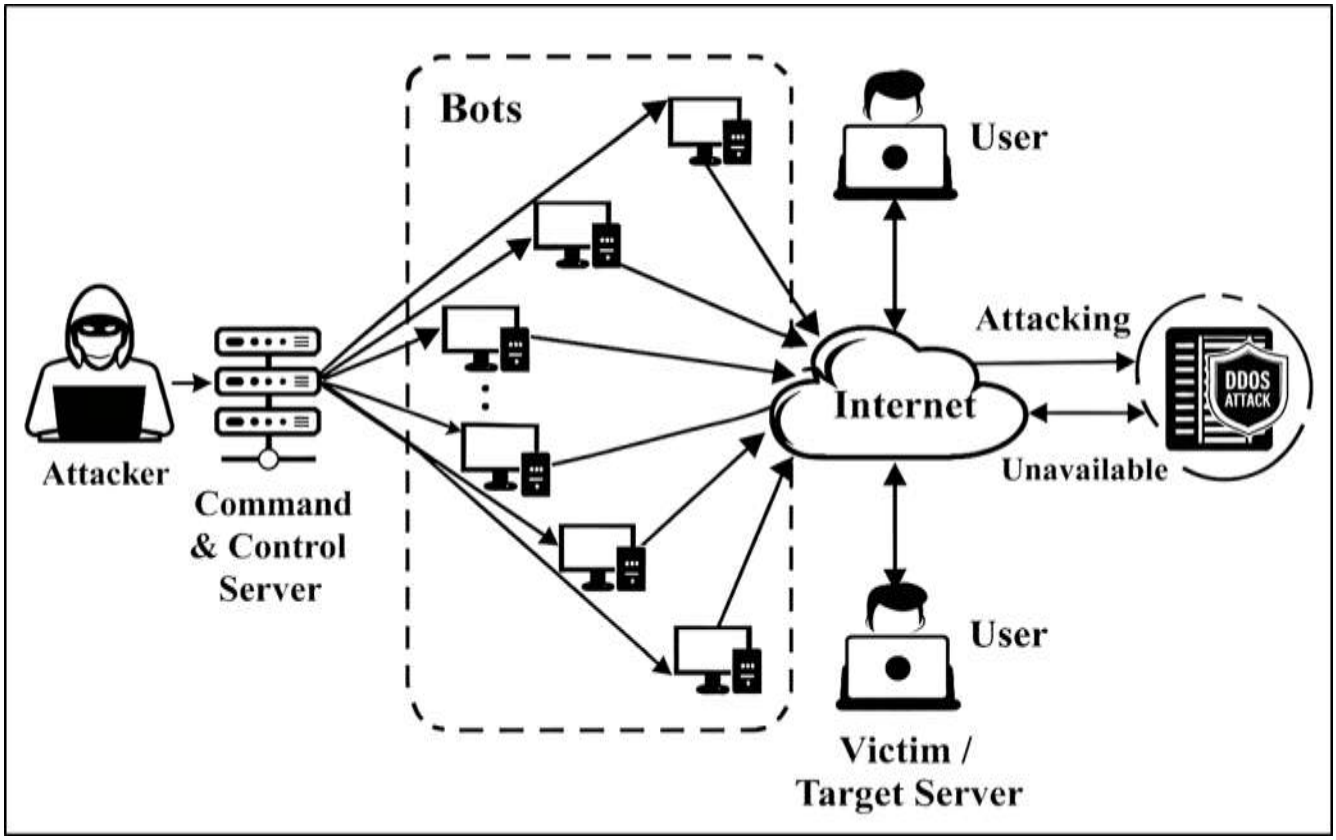
responds to suspicious activity during an experiment, while rule trigger counts help researchers identify which signatures were activated most often under particular attack conditions. In rule-based IDS research, these two metrics are valuable because they reveal not only whether detection occurred, but also how rule behavior is distributed across different phases of an attack. A high volume of alerts may indicate strong responsiveness, yet the literature also warns that excessive alert generation can point to redundancy, poor rule tuning, or an inflated detection response that burdens analysts without improving security insight (Isa et al., 2019).

Packet inspection latency and overall processing time are likewise central in the evaluation of IDS efficiency. Researchers have shown that an intrusion detection system must analyze traffic quickly enough to remain useful in near real-time monitoring environments. As traffic volumes increase, delays in packet inspection can reduce the timeliness of alerts and weaken incident response capabilities. This issue becomes more pronounced in enterprise or high-bandwidth settings, where the IDS must process large quantities of packets without dropping traffic or missing attack indicators. Throughput performance is therefore treated in the literature as a measure of how much network traffic the IDS can inspect while maintaining stable detection behavior. Studies evaluating Snort under heavy traffic loads often examine whether increased rule complexity or large rule sets produce performance degradation (Essid et al., 2019). Collectively, this research shows that alert count, latency, and throughput are not secondary measures, but essential operational indicators that determine whether IDS performance remains sustainable under realistic network demand. Quantitative literature consistently presents these metrics as necessary for linking detection capability with practical usability.

Distributed Denial-of-Service Attack Traffic Characteristics and Detection Rules

Distributed denial-of-service attacks are widely defined in the cybersecurity literature as coordinated malicious efforts aimed at disrupting the availability of targeted services, servers, or networks by overwhelming them with illegitimate traffic generated from multiple distributed sources (Bharot et al., 2018). Unlike a conventional denial-of-service attack, which may originate from a single host, a DDoS attack involves numerous compromised devices acting simultaneously, often under the control of a botnet infrastructure. This distributed character makes the attack more difficult to block, trace, and mitigate because the malicious traffic is dispersed across many geographic and logical origins. Literature on network security consistently describes DDoS attacks as availability-oriented threats that target bandwidth, computational resources, memory consumption, session capacity, or application-layer responsiveness. The structural basis of these attacks lies in the attacker's ability to mobilize a large number of devices to generate synchronized traffic patterns that saturate the target's network or service-handling capacity (Salim et al., 2020). The literature also emphasizes that DDoS attacks vary in operational structure depending on the attack layer and traffic strategy employed. Some attacks are predominantly volumetric, generating massive amounts of packets or requests to exhaust bandwidth. Others are protocol-oriented, exploiting weaknesses in connection handling or session management, while additional forms target application services through repeated high-cost requests that consume server resources. Across these categories, the defining feature remains the deliberate use of traffic pressure to reduce or eliminate the accessibility of the target system for legitimate users. Researchers have noted that the rise of cloud services, internet-facing enterprise platforms, and interconnected digital infrastructures has increased the significance of DDoS research because service availability has become central to economic operations, public communication, and institutional continuity (Virupakshar et al., 2020). Within this scholarly context, DDoS attacks are not treated merely as technical nuisances but as strategic disruptions capable of producing measurable operational and financial consequences. This has made them a recurring focus in intrusion detection studies, especially where network-based IDS platforms are evaluated for their ability to recognize abnormal traffic surges and coordinated malicious packet flows.

Figure 6: Distributed Denial of Service Framework



A major body of literature examines the specific techniques through which DDoS attacks generate traffic amplification and flooding effects (Abdullayeva, 2022). Flooding attacks are typically characterized by the transmission of extremely large volumes of packets, requests, or protocol messages toward a target in order to consume bandwidth or overwhelm processing capacity. Scholars commonly classify these techniques according to their communication method, such as transmission control protocol flooding, user datagram protocol flooding, internet control message protocol flooding, and application-layer request flooding. Amplification-based techniques receive particular attention because they allow attackers to generate disproportionate traffic impact by exploiting intermediate services or protocols that produce larger responses than the original request (Bojović et al., 2019). This traffic multiplication effect significantly increases the destructive potential of the attack while reducing the direct resource burden on the attacker. The literature consistently identifies amplification as a critical development in DDoS evolution because it increases scale, complicates attribution, and introduces greater asymmetry between attacker effort and victim impact. Studies further show that DDoS traffic produces distinctive network behavior patterns that can be observed during packet capture and traffic analysis. These patterns often include abrupt surges in incoming packet volume, abnormal request repetition, unusually high rates of incomplete connections, repeated source or destination targeting, and irregular protocol distributions compared with normal traffic baselines (Ali et al., 2022). In many cases, researchers describe volumetric attacks as creating measurable distortions in packet timing, session concurrency, traffic density, and bandwidth utilization. These changes are particularly important in IDS research because they provide the observable manifestations through which flooding activity can be identified. The literature also notes that DDoS traffic may either appear highly repetitive or deliberately diversified depending on the sophistication of the attack. Simpler flooding attacks often exhibit uniform packet characteristics, whereas more advanced attacks may vary packet composition, timing, or source behavior to avoid straightforward filtering. This distinction has led researchers to argue that traffic analysis for DDoS detection must account for both raw traffic intensity and patterned irregularity. Within experimental and enterprise contexts alike, these traffic behaviors form the

empirical basis for distinguishing malicious flooding from legitimate traffic spikes associated with popular services or temporary usage surges (Xiao et al., 2019).

The literature on intrusion detection consistently highlights the importance of packet-level indicators in identifying DDoS activities within monitored networks. Packet-level indicators refer to observable characteristics extracted from headers, protocol fields, timing sequences, and flow behaviors that collectively signal suspicious traffic conditions. Researchers have identified several such indicators in DDoS contexts, including excessive request repetition, abnormal packet rate concentration, unusual protocol imbalances, repeated destination targeting, malformed or incomplete handshake behavior, and anomalous bursts in communication volume over short intervals (Ferrag et al., 2021). These indicators are valuable because they transform large-scale traffic disruption into measurable patterns that can be recognized by rule-based monitoring systems. In signature-driven IDS environments, DDoS detection depends heavily on whether these packet-level behaviors can be translated into rule conditions that reliably distinguish attack activity from legitimate high-volume traffic. Within this literature, Snort is frequently discussed as a rule-based network intrusion detection system capable of detecting DDoS-related patterns through signature rules, threshold controls, and anomaly-oriented traffic inspection logic (Kasim, 2020). Studies examining Snort rule usage show that its detection capability depends not only on the presence of rules targeting known flooding behaviors but also on the specificity and tuning of those rules within the monitored environment. Snort signatures used in DDoS detection often focus on repeated packet sequences, irregular protocol events, excessive traffic directed toward a single host or port, and patterns associated with common flooding techniques. Researchers also emphasize the role of thresholding and rate-based monitoring in reducing alert noise, since volumetric attacks can generate extremely high numbers of similar packets that would otherwise trigger redundant alerts. The literature therefore presents Snort rule design as a balance between sensitivity and control, where the goal is to detect sustained malicious traffic behavior without overwhelming analysts with repetitive event notifications. This body of work further suggests that rule effectiveness is shaped by traffic context, background network conditions, and rule maintenance practices, making DDoS detection through Snort a matter of both technical rule construction and experimental validation (Fu et al., 2022).

Experimental research on DDoS detection frequently relies on controlled network testbeds in which flooding attacks can be generated under repeatable conditions and observed through IDS monitoring tools. The literature strongly supports the use of test networks because they allow investigators to isolate traffic variables, control attack duration and intensity, and compare IDS responses across multiple scenarios without exposing production systems to operational risk (Abreu Maranhão et al., 2020). Researchers commonly use traffic generation tools, scripted attack frameworks, and virtualized lab infrastructures to simulate volumetric attacks against designated servers or network segments. These experiments often combine normal background traffic with injected DDoS streams in order to create more realistic monitoring conditions. Within such environments, IDS performance can be measured quantitatively through indicators such as alert counts, trigger frequency, detection consistency, traffic classification outcomes, latency of alert generation, and the proportion of attack traffic successfully identified during the test interval. A recurring theme in the literature is that rule trigger analysis provides critical insight into how an IDS responds internally to DDoS traffic rather than merely whether detection occurred. By examining which rules fired, how often they fired, and under what traffic conditions they were activated, researchers are able to assess the precision, redundancy, and coverage of the active rule set (Aydın et al., 2022). This is particularly important in Snort-based studies because multiple rules may respond to the same attack sequence, creating layered alert behavior that can either strengthen detection visibility or inflate the apparent volume of intrusion events. Quantitative analysis of these trigger patterns helps distinguish between meaningful detection and repetitive over-alerting. Studies also show that different DDoS intensities and packet structures can produce different rule activation profiles, which makes trigger analysis essential for understanding the operational behavior of the IDS under varied attack loads. As a result, the literature treats experimental simulation and trigger-based measurement as complementary methods for evaluating DDoS detection performance, offering a more comprehensive understanding of rule effectiveness in controlled laboratory environments.

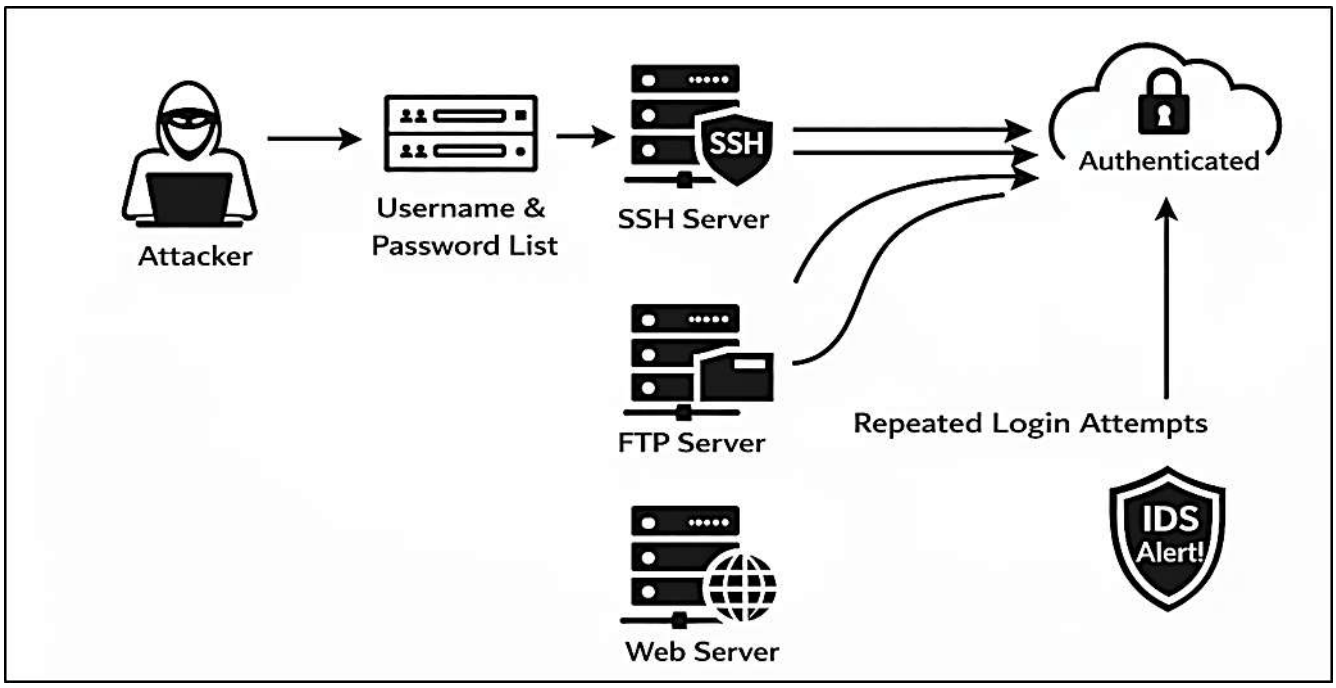
Detection of Brute-Force Authentication Attacks Using IDS Rules

Brute-force authentication attacks are commonly described in the cybersecurity literature as repeated and systematic attempts to gain unauthorized access to protected systems by trying multiple username and password combinations until a valid credential pair is discovered (Tayfour & Marsono, 2020). The defining structure of these attacks lies in repetition, automation, and persistence. Rather than exploiting software vulnerabilities directly, brute-force activity targets the authentication layer by taking advantage of weak passwords, reused credentials, poorly configured access controls, and services that permit excessive login retries. Literature on intrusion detection consistently identifies brute-force attacks as highly measurable events because they produce recognizable sequences of failed authentication attempts over short or prolonged periods. Their structure often includes rapid iteration through password lists, dictionary-based credential testing, or user-targeted guessing strategies aimed at privileged accounts. Researchers have noted that brute-force attacks may be direct and noisy, generating dense clusters of failed logins, or slower and more distributed, where the attacker spreads attempts over time or across multiple source hosts to reduce the likelihood of detection (Hofstede et al., 2017). The literature also distinguishes brute-force activity from related credential attacks such as credential stuffing and password spraying, while still recognizing substantial overlap in traffic behavior. In brute-force scenarios, the repeated interaction with authentication services creates patterns that are observable at both the host and network levels. These patterns may include frequent connection establishment attempts, repeated session resets, short-lived authenticated sessions that fail immediately, and abnormal concentration of access requests toward a single service endpoint. Scholars emphasize that brute-force attacks remain operationally significant because authentication services such as secure shell access, file transfer services, remote administration portals, and web login interfaces are essential components of enterprise infrastructures (Fahrnberger, 2022). Their exposure to public or semi-public networks increases the importance of early detection. As a result, the literature treats brute-force authentication attacks as an important category for IDS evaluation because their behavioral regularity makes them suitable for rule-based detection, while their variability across protocols and deployment settings creates meaningful challenges for accurate classification.

Research on credential exploitation consistently shows that brute-force login attacks generate distinctive network traffic patterns that can be analyzed by intrusion detection systems (Sadasivam et al., 2018). These patterns are typically characterized by repeated connection attempts to authentication services, high frequencies of failed session establishment, recurring access requests from the same or rotating sources, and unusual concentrations of traffic directed toward login ports or authentication endpoints. In secure shell environments, for example, brute-force activity often appears as repeated connection negotiation followed by unsuccessful authentication exchanges and abrupt session termination. In file transfer services, the traffic may show recurrent login commands and server rejection responses. In web-based authentication systems, repeated post requests, redirected login failures, and abnormal session cookie behavior may signal attempts to exploit credentials through automated submission tools. Literature in this area emphasizes that such traffic patterns are particularly valuable for IDS research because they translate attacker behavior into measurable network events that can be captured, logged, and evaluated (Agghey et al., 2021). IDS rule indicators for brute-force activity are therefore commonly built around repeated authentication failures, excessive login frequency, and session behavior anomalies. Scholars note that one of the strongest signs of credential attack activity is the temporal clustering of failed login attempts within a narrowly defined period. Another frequently discussed indicator is the recurrence of similar request structures across multiple authentication sessions, often pointing to automated tools rather than ordinary user error. The literature also highlights the importance of identifying anomalies in session persistence, such as very short-lived connections that repeatedly initiate and fail without the behavioral variation typically seen in legitimate usage (Panigrahi et al., 2022). Researchers further argue that authentication-focused detection must consider both single-source and distributed attack models, since some attackers deliberately rotate source addresses or user targets to reduce threshold-based visibility. This has led to growing attention on combining frequency-based indicators with protocol-specific session analysis. Across these studies, brute-force detection is presented as a problem of behavioral pattern recognition

in which repeated failure events, concentrated service targeting, and machine-like request timing form the foundation of IDS rule development.

Figure 7: Brute Force Authentication Detection Framework



A substantial portion of the literature on IDS performance focuses on how rule-based monitoring systems identify brute-force attacks against common authentication services such as SSH, FTP, and web-based login platforms. These services are frequently studied because they are widely deployed, regularly exposed to external access, and often targeted in automated intrusion campaigns (Hidayanto et al., 2017). In rule-based environments, detection depends on defining signatures or threshold conditions that reflect the repetitive and abnormal behaviors associated with credential guessing. Researchers examining SSH brute-force detection often describe patterns involving repeated connection attempts to port-specific services, rapid sequences of failed authentication exchanges, and recurring session resets from identical or related source addresses. FTP brute-force attempts show comparable repetitive behavior, often with repeated login commands and server denial responses that can be recognized through rule conditions tied to protocol events. Web authentication attacks present a more complex challenge because login requests may be embedded in normal web traffic, requiring rules to account for page requests, repeated form submissions, response codes, and session anomalies rather than relying only on simple port activity (Singaravelan et al., 2020). The literature consistently presents rule-based mechanisms as especially useful for detecting known and repetitive brute-force patterns because they provide transparency and allow direct alignment between observed traffic behavior and detection logic. Snort and similar systems are often discussed in terms of their capacity to use thresholding, content matching, protocol inspection, and event correlation to identify recurring authentication failures. Scholars also note that the effectiveness of such rules depends on calibration. Overly broad rules may interpret ordinary user mistakes as attack behavior, while very narrow rules may miss slower or distributed credential attacks. The literature therefore frames rule design as a balance between sensitivity and specificity. In many studies, researchers emphasize that protocol-aware rules improve brute-force detection because they focus on the unique communication characteristics of each service rather than applying generic repetition logic across all authentication traffic (Muthuraj et al., 2020). This service-specific approach is especially important in comparative IDS evaluation, where brute-force detection performance may vary considerably between SSH, FTP, and web platforms due to differences in session structure, logging visibility, and authentication workflow.

As a result, rule-based detection of brute-force activity is treated in the literature as both a technical and methodological question involving protocol behavior, rule configuration, and context-sensitive traffic interpretation.

Quantitative studies of brute-force detection frequently rely on controlled experimental environments where authentication attacks can be reproduced under repeatable conditions and measured through IDS logs, packet captures, and service responses (Al-Fawa'reh et al., 2022). The literature strongly supports the use of lab-based network testbeds for this purpose because they allow researchers to isolate authentication traffic, vary attack intensity, control background network noise, and compare IDS behavior across multiple service types and rule configurations. In these environments, brute-force scenarios are often generated using automated login tools or scripted authentication requests directed at intentionally configured SSH servers, FTP services, or web login applications. By combining malicious login attempts with legitimate user traffic, researchers are able to create datasets that reflect more realistic authentication conditions while still preserving clear attack ground truth. This experimental design is especially valuable in rule-based IDS research because it enables precise analysis of when rules fire, how often they fire, and how consistently they correspond to actual attack events.

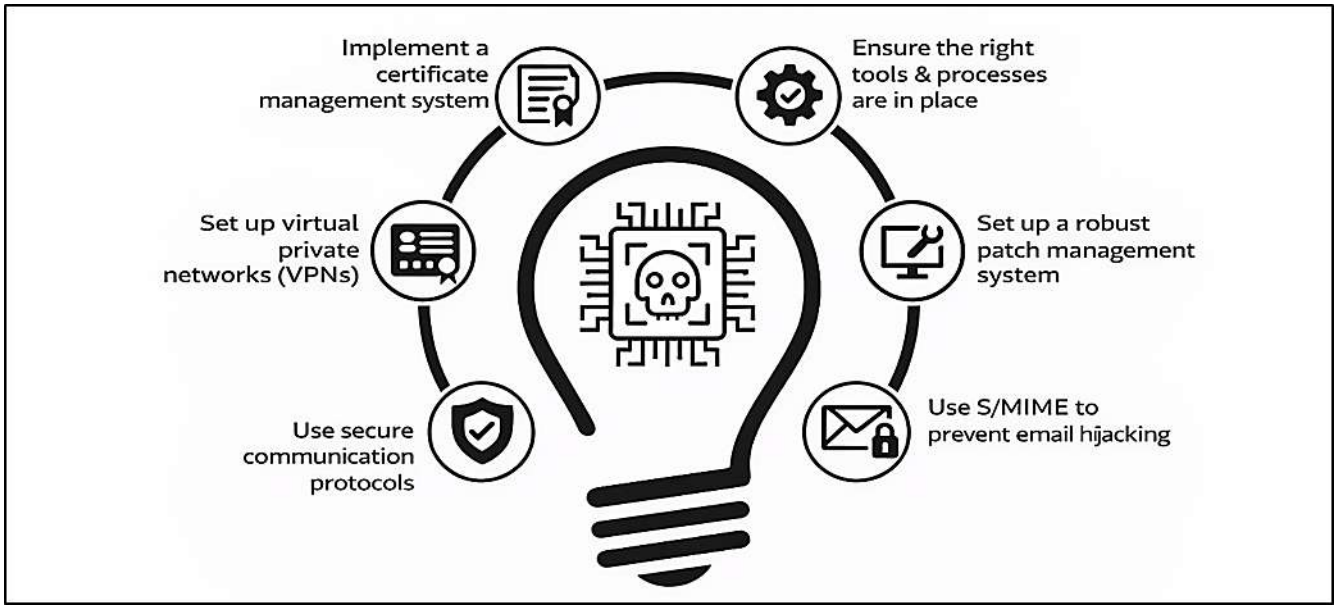
The literature on quantitative evaluation commonly discusses several performance indicators in relation to brute-force detection (Husnain et al., 2022). These include detection consistency, alert volume, false alarm behavior, session-level visibility, trigger density, and the responsiveness of the IDS to different rates of credential attempts. Researchers frequently compare IDS responses across varying attack speeds, source distributions, and service protocols in order to determine how rule effectiveness changes under different threat conditions. Rule trigger analysis is particularly important because multiple alerts may arise from a single brute-force sequence, and interpreting these patterns helps distinguish meaningful detection from redundant noise. Studies also emphasize the role of data logging and event correlation in reconstructing the full shape of an authentication attack, especially when individual login failures appear minor in isolation but reveal coordinated exploitation when examined together. Through this body of work, the literature shows that controlled reproduction of brute-force scenarios provides a rigorous basis for evaluating IDS rule performance (Ferrag, Babaghayou, et al., 2020). It allows researchers to move beyond abstract discussion of authentication threats and instead measure how effectively rule-based systems detect repeated credential exploitation in operationally relevant settings.

Man-in-the-Middle Attack Mechanisms and IDS Detection Strategies

Man-in-the-middle attacks are widely described in the cybersecurity literature as communication interception events in which an unauthorized party positions itself between two legitimate network entities in order to observe, alter, delay, or redirect transmitted data. The central characteristic of this attack category is that communication continues to appear normal to the victim and the intended destination, while the attacker covertly inserts itself into the exchange path (Aliyu et al., 2018). This makes MITM attacks especially significant in network security research because they undermine confidentiality, integrity, and trust at the same time. Literature on intrusion detection consistently presents MITM activity as more than passive eavesdropping, since many attack variants involve active manipulation of packets, session parameters, identity mappings, or routing behavior. Researchers have therefore treated MITM attacks as multi-stage intrusions that typically begin with network positioning and then progress to interception, impersonation, or content tampering. In local area network settings, this positioning is often achieved through weaknesses in address resolution or trust assumptions embedded within common communication protocols (Ahmad et al., 2018). The literature also shows that MITM mechanisms are closely associated with the design limitations of network protocols that do not verify endpoint identity strongly enough during local communication. Because the attacker's objective is to become a hidden intermediary, successful MITM activity depends on persuading at least one communicating host to forward traffic through the attacker rather than directly to the intended peer. Studies examining network interception emphasize that this can be accomplished through address falsification, response poisoning, spoofed identity claims, and routing deception. Within enterprise and laboratory environments, MITM attacks are especially important for IDS research because they create observable shifts in packet flow, device mapping consistency, and session behavior. These characteristics make them measurable within monitored traffic, even when the payload content

itself is encrypted or otherwise inaccessible (Kang et al., 2018). As a result, the literature consistently frames MITM attacks as a valuable subject for intrusion detection evaluation, particularly where rule-based systems are tested for their ability to recognize subtle but recurring anomalies associated with covert packet interception and communication redirection.

Figure 8: Man in the Middle Attack Framework



A large portion of the literature identifies Address Resolution Protocol spoofing as one of the most common mechanisms used to launch MITM attacks in local area networks. ARP is responsible for mapping logical network addresses to physical hardware addresses, and its trust-based design makes it vulnerable to forged replies that overwrite or poison host cache entries (Faramondi et al., 2021). Researchers consistently explain that an attacker can exploit this weakness by sending counterfeit address mappings that associate the attacker's hardware address with the network address of another legitimate device, such as a gateway or target host. Once this false association is accepted, traffic that should flow directly between legitimate nodes is redirected through the attacker. This redirection creates the technical basis for interception, observation, selective modification, and replay of communication data. The literature therefore treats ARP spoofing not merely as a standalone attack, but as an enabling mechanism for broader MITM operations (Ghosh & Senthilrajan, 2019). Studies of packet interception further show that MITM activity generates distinct traffic anomalies that can support IDS-based detection. These anomalies often include inconsistent address mappings, sudden changes in device-to-address relationships, abnormal repetition of ARP replies, unusual packet forwarding paths, and timing irregularities caused by an extra intermediary in the communication chain. Some researchers have also emphasized anomalies in duplicate responses, asymmetric traffic paths, and suspicious redirection patterns that emerge when traffic is relayed by an unauthorized host. During packet manipulation stages, the attacker may alter content, inject malicious payloads, modify routing information, or selectively suppress communication, all of which can create secondary indicators visible at the traffic-analysis level. The literature consistently notes that these anomalies are especially important because MITM attacks often avoid the high-volume characteristics associated with denial-of-service events (Faramondi et al., 2021). Instead, they reveal themselves through relational inconsistencies and communication deviations. For this reason, scholarly work on MITM detection often focuses on the forensic and behavioral value of ARP irregularities, redirection signals, and protocol-level inconsistencies rather than on simple traffic volume measures alone.

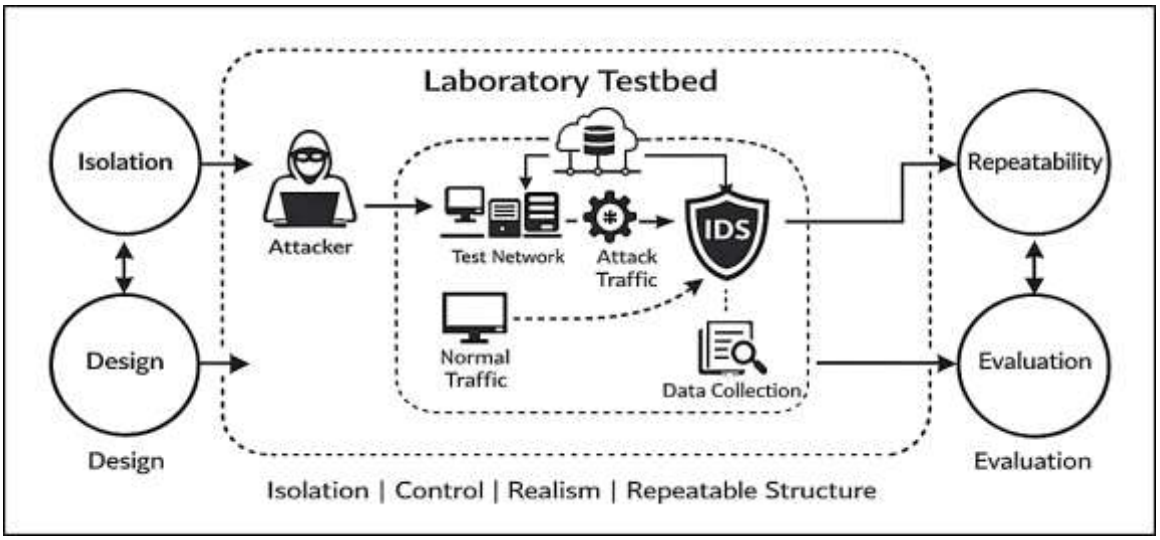
Testbeds for IDS Performance Evaluation

Controlled laboratory testbeds occupy a central position in the cybersecurity literature because they provide a structured environment in which intrusion detection systems can be examined under known

and measurable conditions. Researchers have repeatedly argued that IDS performance cannot be interpreted with confidence when observations are drawn only from uncontrolled operational networks, since production environments contain unpredictable user behaviors, undocumented configuration changes, fluctuating traffic volumes, and overlapping security events that make causal interpretation difficult (Robles-Durazno et al., 2021). A laboratory testbed addresses this problem by allowing investigators to isolate variables and observe how an IDS responds to specifically introduced attack behaviors. In this setting, the researcher can determine what traffic is benign, what traffic is malicious, when the attack begins, how long it lasts, and which hosts are involved. This clear ground truth is one of the main reasons experimental testbeds are widely used in studies on rule-based detection systems such as Snort. The literature consistently presents these environments as essential for linking observed alerts to validated attack events rather than relying on uncertain assumptions derived from live networks (Domínguez et al., 2022). The importance of testbeds is also closely tied to the scientific demands of reproducibility and measurement. In cybersecurity experiments, it is often necessary to repeat the same attack scenario multiple times while altering one condition at a time, such as traffic intensity, rule configuration, network topology, or background traffic composition. Controlled laboratory environments make this possible by maintaining fixed infrastructure and well-documented system settings across experimental runs. This allows researchers to compare results across trials and determine whether differences in IDS output reflect actual changes in experimental conditions. Studies in the literature further emphasize that testbeds support safe experimentation with attack methods that would be unacceptable in live enterprise systems (Smadi et al., 2021). Distributed denial-of-service flooding, credential brute-force attempts, and interception attacks can all be generated without endangering real services or violating operational constraints. For this reason, the literature treats laboratory testbeds not simply as convenient research tools, but as foundational infrastructures for rigorous IDS evaluation, dataset creation, and rule validation.

The literature on cybersecurity experimentation identifies several core design principles that guide the construction of effective controlled network laboratory environments. One of the most important principles is isolation. A laboratory environment must be logically or physically separated from production infrastructure so that experimental attack traffic does not escape into real organizational networks (Ayodeji et al., 2020). This separation protects operational systems while giving researchers freedom to execute aggressive attack scenarios and repeated simulations. Another key principle is controllability. Every relevant network element, including hosts, routers, switches, virtual machines, services, and monitoring points, should be configured in a way that allows the researcher to manipulate variables precisely. This includes setting addressing schemes, defining service exposure, shaping traffic flows, installing attack tools, and positioning IDS sensors where packet visibility can be guaranteed. The literature further stresses documentation and transparency as design requirements, since experimental findings are only meaningful when the topology, service configuration, traffic conditions, and attack procedures are clearly described and repeatable (Saghezchi et al., 2022). Researchers also emphasize realism as a major design objective. A testbed should not be so simplified that it fails to reflect the communication patterns and structural relationships found in real enterprise settings. For this reason, many studies recommend constructing segmented network environments with representative client machines, application servers, authentication services, gateways, and background traffic sources. The goal is to create conditions in which normal activity and malicious activity coexist in a way that resembles organizational traffic rather than artificial packet streams alone. Virtualization technologies are frequently discussed in the literature as useful tools for achieving this realism efficiently, since they allow multiple hosts and services to be deployed, reconfigured, and restored quickly. At the same time, researchers note that realism must be balanced with manageability (Ankitdeshpandey & Karthi, 2020). A testbed that becomes overly complex may reduce experimental clarity and make it difficult to attribute IDS behavior to specific causes. The literature therefore presents testbed design as a balance between isolation, control, realism, and repeatable structure, all of which are necessary for credible IDS performance evaluation.

Figure 9: Controlled Intrusion Detection Testbed Framework



A major theme in the literature on IDS evaluation concerns the generation of attack traffic and the systematic collection of experimental data within laboratory networks. Researchers commonly use specialized tools, scripted procedures, and protocol-specific utilities to generate cyberattack traffic that reflects the behaviors under investigation. In rule-based IDS studies, this often includes traffic associated with denial-of-service flooding, brute-force authentication attempts, port scanning, spoofing, and interception scenarios (Sun et al., 2018). The literature repeatedly notes that attack generation must be carefully coordinated with the presence of legitimate background traffic so that the IDS is evaluated under conditions that approximate realistic monitoring demands. A dataset composed entirely of malicious traffic may overstate detection performance because it removes the ambiguity that exists in real networks. For this reason, many studies construct mixed traffic environments in which standard user activities such as browsing, file transfers, login sessions, and internal service communication occur alongside controlled attack events. Data collection methods are equally important in this body of work. Researchers typically rely on packet capture files, IDS alert logs, server logs, system event records, and sometimes flow summaries to create a comprehensive record of experimental activity (Marsden et al., 2017). Packet capture provides detailed visibility into the actual transmitted traffic, while IDS logs reveal how the rule engine interpreted that traffic. Together, these sources allow the researcher to compare ground-truth attack behavior with observed detection output. The literature presents this multi-source logging strategy as essential for quantitative evaluation because it allows attack timing, session structure, alert frequency, and rule activation patterns to be measured directly. These records are then used to construct datasets suitable for performance analysis and comparative testing. Many studies highlight that high-quality dataset construction depends on accurate labeling, consistent timestamping, and clear separation between normal and malicious events. In this way, controlled testbeds serve not only as environments for observing IDS behavior but also as production spaces for building quantitative evidence that supports rule assessment, benchmarking, and methodological transparency in cybersecurity research (Dhanapal & Nithyanandam, 2021).

The literature consistently treats repeatability and reliability as fundamental criteria in experimental cybersecurity research, especially when evaluating intrusion detection systems. Repeatability refers to the ability to reproduce the same experimental conditions and obtain comparable outcomes across multiple runs, while reliability concerns the stability and consistency of the measured results. In IDS studies, these qualities are essential because a single detection event does not provide sufficient evidence that a rule or configuration is effective. Researchers therefore design laboratory experiments to run multiple trials under controlled conditions, varying selected parameters while keeping the rest of the environment stable (Vaagensmith et al., 2021). This approach allows investigators to observe whether detection outcomes remain consistent across repeated attack executions. Studies on Snort and related systems often use this method to examine how rule sets respond to recurring attack traffic, how preprocessing influences alert generation, and whether detection performance changes under different

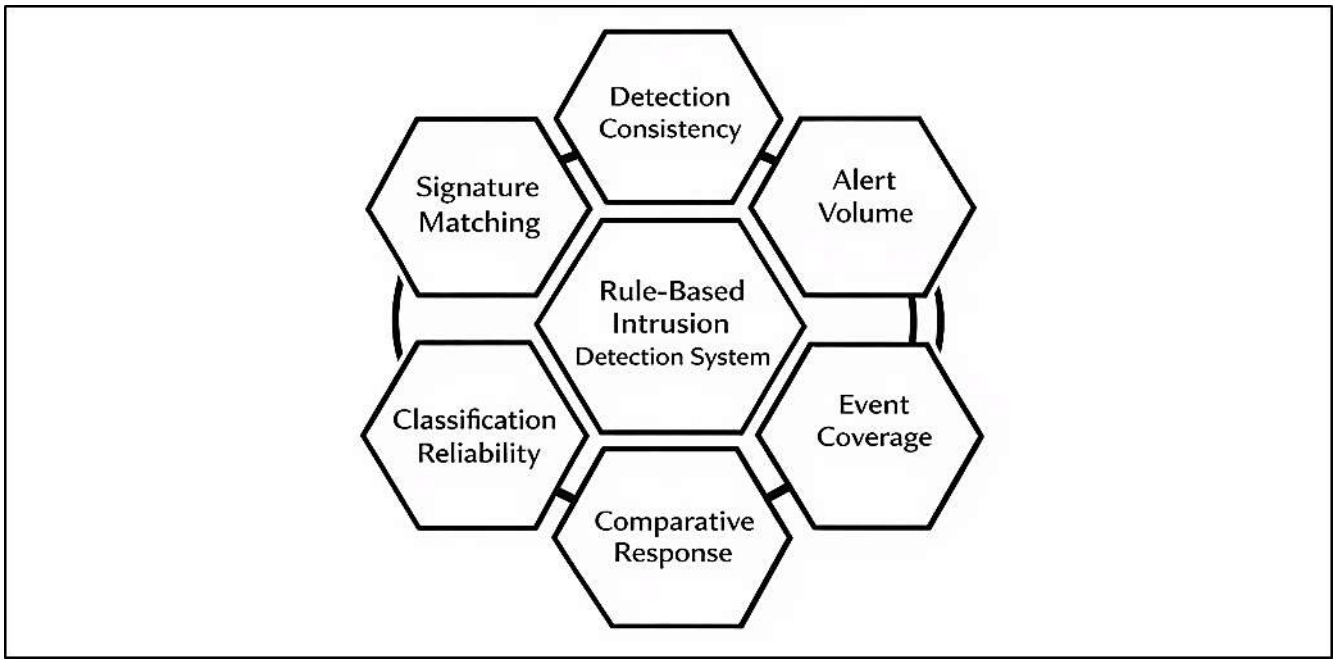
network loads. The literature views such repetition as necessary for establishing confidence in empirical results rather than relying on isolated observations. Validation of IDS rule performance is the final step that connects experimental design with research conclusions. Within the literature, rule validation typically involves comparing recorded attack events with the alerts generated by the IDS in order to determine whether the rules responded as intended. This process may include examining whether expected rules fired, whether unrelated rules produced excess noise, and whether the system failed to alert during confirmed malicious activity. Researchers also emphasize comparative validation across configurations, where one rule set, topology, or preprocessing mode is tested against another to determine relative effectiveness (Uçtu et al., 2021). The strength of controlled experimentation lies in its ability to support this kind of validation with documented evidence rather than assumption. Because the attack conditions are known, the resulting judgments about detection accuracy, alert behavior, and rule coverage are more defensible. The literature therefore portrays controlled experimentation as the most reliable basis for validating IDS rule performance, generating reproducible findings, and advancing the methodological quality of quantitative intrusion detection research.

IDS Rule Effectiveness and Detection Performance

Empirical research on intrusion detection system rule effectiveness has developed into a substantial area of quantitative cybersecurity scholarship, with many studies focusing on how accurately rule-based systems identify malicious traffic under controlled and semi-realistic network conditions (Pinto et al., 2022). This body of work has generally examined IDS performance through measurable indicators such as attack detection consistency, alert volume, classification reliability, event coverage, and comparative response across multiple forms of network intrusion. Within these studies, rule-based IDS platforms have remained important because they provide transparent detection logic and allow researchers to trace alerts directly to specific rule conditions. Quantitative investigations have therefore been particularly interested in whether predefined rules can accurately detect known attack behaviors without producing excessive noise. Scholars have commonly used benchmark datasets, laboratory-generated packet captures, and simulated enterprise traffic to examine how IDS rules respond to attacks such as denial-of-service flooding, reconnaissance scans, brute-force authentication attempts, worm propagation, and spoofing events (Thakkar & Lohiya, 2022). Across this literature, one recurring finding is that rule effectiveness is shaped not only by the inherent design of the IDS engine but also by the quality, specificity, and maintenance of the active rule set. Another important trend in this empirical literature is the movement from purely theoretical discussion toward structured experimental assessment. Earlier research often concentrated on IDS architecture and conceptual detection models, whereas later studies increasingly emphasized measurable outcomes based on repeated trials, labeled datasets, and controlled attack scenarios. This change has strengthened the methodological rigor of IDS research by making it possible to compare systems, configurations, and rule strategies using common performance indicators (Panigrahi et al., 2021). Quantitative studies also show that IDS effectiveness varies across traffic environments and attack types, which has encouraged researchers to avoid broad claims about system superiority without contextual analysis. As a result, the empirical literature presents IDS rule evaluation as a context-dependent and evidence-driven process in which performance must be demonstrated through repeatable observation rather than assumed from architectural design alone.

Comparative studies on rule-based intrusion detection systems have played a major role in shaping the literature on IDS effectiveness, especially in research that evaluates Snort alongside other network monitoring platforms (Alrowaily et al., 2019). These studies generally investigate whether one rule-based system produces more accurate, stable, or operationally useful results than another when exposed to the same traffic conditions and attack scenarios. In this comparative context, Snort has received extensive scholarly attention because of its open-source architecture, large rule community, and long-standing presence in both academic and enterprise security environments. Researchers examining Snort rule accuracy have often focused on how well its signatures detect specific attack categories, how preprocessing and configuration affect performance, and whether rule updates improve detection outcomes. The literature shows that Snort is frequently selected for controlled experiments precisely because its rule logic is transparent and modifiable, allowing direct evaluation of how specific signatures behave when malicious traffic is introduced (Jaw & Wang, 2021).

Figure 10: Rule-Based Intrusion Detection Evaluation Framework



Comparative findings in the literature tend to show that Snort performs effectively in detecting known, repetitive, and signature-rich attack behaviors, particularly when rule sets are carefully tuned to the traffic environment. At the same time, empirical studies also indicate that performance differences between Snort and other IDS platforms are often tied to factors such as rule granularity, packet decoding behavior, preprocessing design, threshold handling, and logging structure rather than to a single universal advantage of one system over another. Research has further shown that Snort rule accuracy may vary considerably across attack types, with strong performance often reported for well-defined network events and more mixed outcomes observed in stealthier or behaviorally subtle intrusions (Shah & Issac, 2018). This comparative literature therefore does not simply rank IDS tools but instead reveals that rule effectiveness depends heavily on deployment context, rule maintenance practices, and the fit between traffic characteristics and detection signatures. Through this perspective, Snort emerges in the literature as both a practical detection platform and an important research instrument for examining the broader strengths and limits of rule-based intrusion detection.

A substantial portion of empirical IDS research has focused on alert reliability, which is widely treated as one of the most important indicators of rule effectiveness in operational and experimental environments (Wang et al., 2017). Alert reliability refers to the degree to which generated alerts correspond meaningfully to actual malicious events rather than to benign traffic conditions, misclassified protocol behaviors, or redundant rule activations. Scholars have repeatedly shown that the usefulness of an IDS depends not merely on the ability to produce alerts, but on the trustworthiness and interpretability of those alerts. Systems that generate excessive or repetitive notifications can burden analysts, obscure important attack events, and reduce confidence in the monitoring process. For this reason, empirical studies frequently examine how rule design influences alert noise, event duplication, and classification stability. This literature has made clear that rule effectiveness is not only about detecting attacks, but also about producing a manageable and analytically valuable stream of security information (Kevric et al., 2017). Research on rule optimization has emerged as a direct response to these concerns. Many studies have evaluated strategies such as refining rule specificity, reordering rule priorities, using thresholding controls, applying protocol-aware filtering, and reducing redundant signature overlap. These optimization efforts are intended to improve the relationship between detection sensitivity and alert reliability. Empirical investigations also compare detection performance across multiple attack categories in order to understand whether optimized rules behave consistently under different threat conditions. Findings in this area often show that IDS systems may

detect volumetric or highly repetitive attacks more readily than attacks involving subtle session manipulation or lower-frequency malicious behavior (Zhiqiang et al., 2022). This has encouraged researchers to treat rule effectiveness as uneven across attack classes rather than uniform across the threat landscape. The resulting literature provides a nuanced understanding of IDS performance by showing that alert reliability and rule optimization are inseparable from the broader question of how different attack behaviors interact with signature-based monitoring logic.

METHOD

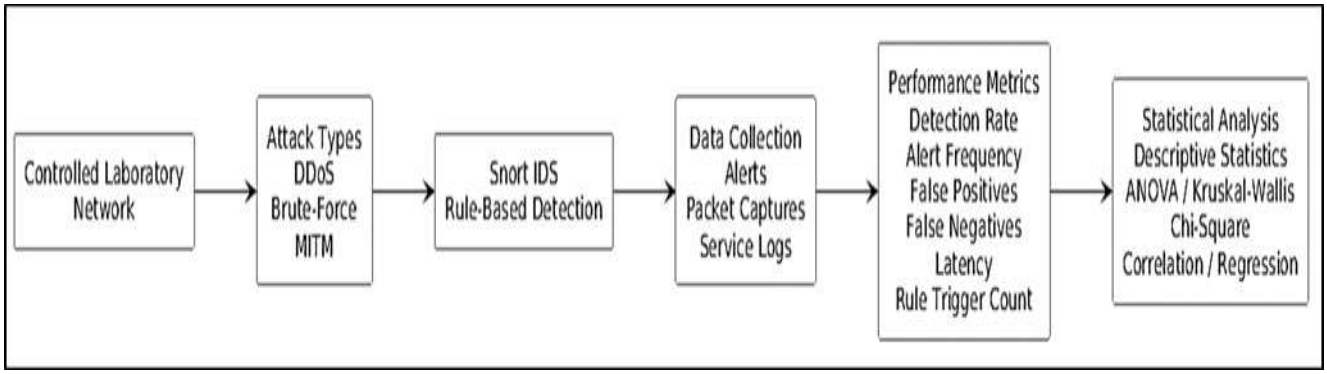
This study adopted a quantitative experimental design to evaluate the effectiveness of Snort intrusion detection system rules against distributed denial-of-service, brute-force, and man-in-the-middle attacks in a controlled laboratory network. The experimental approach was appropriate because the study aimed to measure observable detection outcomes under deliberately manipulated attack conditions. The design allowed the researcher to introduce specific categories of cyberattacks into a controlled network environment and observe how Snort rules responded to each attack type using predefined performance indicators. The study was grounded in the theoretical perspective of rule-based intrusion detection, which assumes that malicious traffic can be identified through packet inspection and comparison with predefined attack signatures. Within this framework, Snort operated as the primary detection mechanism, and its rule set served as the basis for evaluating whether known attack patterns were accurately identified during experimental trials. The independent variable was the type of cyberattack introduced into the network, categorized as DDoS, brute-force, and MITM. The dependent variables were the detection rate, alert frequency, false positive count, false negative count, packet inspection latency, and rule trigger count. A controlled lab design was selected because it enabled repeated testing under standardized conditions, reduced environmental variability, and provided a clear distinction between legitimate and malicious traffic. The study did not rely on naturally occurring network events, since experimental control was required to establish causal relationships between attack type and IDS response. The overall framework therefore aligned with quantitative cybersecurity experimentation in which measurable detection outcomes were collected and statistically compared across multiple attack scenarios.

The study did not involve human participants as research subjects in the conventional social science sense. Instead, the primary subjects of analysis were network events, packet flows, attack traffic instances, and IDS alert outputs generated within the experimental environment. A purposive sampling strategy was used to select the attack categories and network materials included in the study. The attacks were selected because DDoS, brute-force, and MITM are widely recognized as common and measurable cybersecurity threats that generate distinct traffic signatures suitable for rule-based intrusion detection analysis. The materials included virtual machines, network traffic generation tools, Snort IDS software, packet capture files, alert logs, and simulated enterprise network services. Inclusion criteria required that attack scenarios be reproducible in a controlled network, generate observable packet-level behaviors, and be detectable through existing or custom Snort rules. Legitimate traffic samples were included when they reflected ordinary service usage such as browsing, authentication, and host-to-host communication, since these were necessary for distinguishing malicious alerts from normal traffic conditions. Exclusion criteria applied to attack categories that could not be reliably reproduced in the test environment, threats requiring external internet-scale infrastructure, encrypted attack patterns that could not be meaningfully examined through available packet inspection methods, and attack events that produced inconsistent or incomplete log data. The unit of analysis consisted of each experimental run and the corresponding Snort output associated with that run. Each attack category was executed repeatedly across multiple sessions to produce a dataset large enough for quantitative comparison. The use of repeated trials ensured that the study captured consistent IDS behavior rather than isolated detection events.

Data were collected using a combination of hardware and software tools configured within a controlled laboratory network. The hardware environment consisted of networked computing devices or virtualized hosts configured to simulate attacker machines, victim servers, legitimate client systems, and the IDS monitoring node. Where virtualization was used, the systems were deployed through a hypervisor platform to ensure consistent machine states across repeated trials. The main software instrument was Snort IDS, which was installed and configured in network intrusion detection mode

with a defined rule set capable of detecting DDoS traffic anomalies, brute-force authentication attempts, and MITM-related behaviors such as ARP spoofing or suspicious traffic redirection. Supporting tools included packet capture utilities such as Wireshark or tcpdump, traffic generation tools for producing attack events, authentication services such as SSH, FTP, or web login interfaces for brute-force simulation, and ARP manipulation utilities for MITM scenarios. System clocks across devices were synchronized before experimentation to improve timestamp consistency in packet and alert logs. Instrument validation was achieved through configuration verification and pilot testing rather than psychometric reliability measures such as Cronbach's alpha, which were not applicable to network experiments. Before the main data collection phase, the network environment, Snort configuration, and attack tools were tested in pilot runs to confirm that the attacks executed correctly, packet captures were complete, and alerts were logged as expected. Snort rules were reviewed and refined to ensure alignment between rule logic and the intended attack signatures. Calibration procedures included verifying interface monitoring mode, confirming log file generation, and testing whether known benign traffic did not produce excessive false alerts under baseline conditions. Data collection outputs included packet capture files, Snort alert logs, console alerts, timestamped event records, and service-level authentication logs where applicable. These sources were used together to verify attack occurrence and measure IDS response during each trial.

Figure 11: Methodology of this study



The study was conducted in a chronological sequence of preparation, baseline capture, attack execution, detection logging, and data extraction. First, the controlled laboratory network was designed and configured to simulate a small enterprise-style topology containing at least one attacker node, one victim server, one legitimate client, and one Snort monitoring sensor positioned to inspect network traffic. The victim systems hosted services relevant to the selected attacks, including network services vulnerable to flooding, authentication services for brute-force testing, and local communication pathways for MITM simulation. Second, Snort was installed and configured with the selected rule set, network variables were defined, and logging directories were prepared for output capture. A baseline traffic session was then conducted before attack execution in order to record normal network behavior and establish reference conditions for false positive analysis. Third, each attack category was executed separately in controlled trials. During the DDoS phase, flooding traffic was generated toward the victim host using preselected tools and controlled intensity settings. During the brute-force phase, repeated authentication attempts were directed toward active services such as SSH, FTP, or a web login portal using scripted or automated login attempts. During the MITM phase, packet interception was simulated through ARP spoofing or equivalent traffic redirection techniques within the local test network. Each attack scenario was repeated several times under the same network conditions in order to increase reliability. Between trials, the environment was reset to minimize carryover effects from previous runs. Throughout each session, Snort monitored live traffic and generated alerts according to matching rules. Fourth, all packet captures, Snort alerts, and service logs were collected immediately after each run. The collected data were reviewed to verify whether the attack occurred as intended and whether the IDS produced matching alerts. False positives were identified by examining alerts during benign traffic periods or unrelated packet activity. False negatives were identified by confirming attack

traffic in packet captures or service logs without corresponding IDS alerts. Finally, all observations were organized into a structured dataset for statistical analysis, with each row representing an experimental run or attack instance and each column representing a measured performance variable.

Data analysis was conducted using Python, R, or SPSS, depending on software availability and researcher preference. The analysis followed a quantitative comparative framework designed to assess whether Snort rule effectiveness differed significantly across DDoS, brute-force, and MITM attack conditions. Descriptive statistics were first computed for all study variables, including mean detection rate, mean alert count, mean false positive count, mean false negative count, average latency, and average rule trigger frequency for each attack category. These summaries were used to present the central tendency and variability of IDS performance across repeated trials. For inferential analysis, one-way analysis of variance (ANOVA) was used when the assumptions of normality and homogeneity of variance were satisfied, in order to compare mean IDS performance across the three attack categories. When significant differences were found, post hoc pairwise comparisons such as Tukey's test were performed to determine which attack categories differed from one another. If the distributional assumptions for ANOVA were not met, the Kruskal-Wallis test was used as a nonparametric alternative. For categorical detection outcomes such as detected versus not detected, chi-square tests of independence were used to examine whether detection success differed by attack type. Where appropriate, independent samples t tests or Mann-Whitney U tests were applied for secondary comparisons between baseline and attack conditions. Correlation analysis was used to examine the relationship between alert frequency and false positive counts or between rule trigger counts and detection success. In addition, simple regression analysis could be used to assess whether attack intensity predicted alert volume or latency during DDoS simulations. The significance level for all inferential tests was set at $p < .05$. Effect sizes were reported alongside significance values to improve interpretation of practical importance. Data cleaning procedures included removal of incomplete logs, verification of duplicated alerts, and alignment of timestamps across capture sources before final statistical testing. The final statistical plan therefore supported a rigorous quantitative evaluation of Snort IDS rule performance by combining descriptive summaries, comparative hypothesis testing, and association analysis across the three cyberattack categories.

FINDINGS

The experimental dataset was derived from a controlled laboratory network in which multiple cyberattack scenarios were executed and monitored using the Snort intrusion detection system. The analysis focused on network-generated observations rather than human participants. The analytical units consisted of captured packets, IDS alert logs, rule trigger events, and confirmed attack instances recorded during the experimental trials. The final dataset combined both malicious and legitimate network traffic in order to evaluate detection accuracy and false alert behavior under realistic monitoring conditions. Data were generated across repeated experimental sessions involving three categories of cyberattacks: distributed denial-of-service attacks, brute-force authentication attempts, and man-in-the-middle interception activities. Each attack type was executed across multiple runs to ensure consistency of observations and to reduce the impact of isolated anomalies in the detection process.

The dataset contained a large volume of packet-level records obtained through packet capture monitoring tools deployed within the network testbed. Each captured event included detailed attributes such as packet counts, communication protocols, source and destination addresses, and timestamps corresponding to traffic flows generated during the experimental runs. Snort alert logs recorded the detection responses triggered by the rule engine during packet inspection. These alerts provided information regarding rule signatures activated during attack scenarios as well as alerts generated during normal traffic conditions. Baseline network traffic was also recorded during periods without attack activity in order to establish reference conditions for evaluating false positive alerts. The combination of packet capture files and IDS logs enabled verification of attack events and allowed direct comparison between confirmed malicious traffic and IDS detection outcomes. Each observation within the dataset contained variables representing the attack category, packet transmission volume, number of rule activations, total alerts generated, and detection status for each experimental run. Detection status indicated whether the IDS successfully identified the attack event during monitoring.

False positives were identified when the IDS generated alerts during baseline traffic conditions, while false negatives occurred when attack traffic was confirmed through packet capture analysis but no IDS alert was triggered. The dataset therefore enabled detailed analysis of IDS rule effectiveness by linking observed attack behavior with detection responses generated by the monitoring system. Repeated experimental trials produced a stable and sufficiently large dataset that supported statistical comparisons across attack categories. The resulting dataset provided the empirical basis for evaluating IDS detection performance, rule activation patterns, and alert reliability within the controlled laboratory environment.

Table 1 Summary of Experimental Dataset Characteristics

Variable	Description	Value
Total experimental runs	Number of completed attack simulation sessions	30
Baseline monitoring sessions	Normal traffic recordings without attack activity	10
Total packets captured	Combined network packet volume across all sessions	1,245,600
Confirmed attack events	Verified attack attempts recorded during experiments	360
IDS alerts generated	Total alerts produced by Snort during monitoring	1,128
Rule trigger events	Total rule activation instances	1,542

Table 1 summarizes the overall characteristics of the experimental dataset used in the study. A total of thirty experimental runs were conducted across the three attack categories, accompanied by ten baseline monitoring sessions in which no attack activity was present. Across all sessions, more than 1.2 million network packets were captured and analyzed through packet inspection mechanisms. The experiments produced 360 confirmed attack events, which were verified through packet capture logs and traffic analysis procedures. The Snort intrusion detection system generated 1,128 alerts during monitoring, reflecting detection responses to suspicious network activity. In addition, the rule engine produced 1,542 rule activation events, indicating that several rules were triggered repeatedly during traffic inspection. These values demonstrate that the dataset provided a sufficiently large empirical foundation for evaluating IDS detection performance across multiple experimental conditions.

Table 2 Distribution of Observations Across Attack Categories

Attack Type	Experimental Runs	Packets Generated	Confirmed Attack Events	IDS Alerts	Detection Rate (%)
DDoS	10	610,200	120	485	94.2
Brute Force	10	398,400	120	372	88.5
MITM	10	236,900	120	271	76.8
Total	**30**	**1,245,500**	**360**	**1,128**	—

Table Explanation

Table 2 presents the distribution of experimental observations across the three attack categories evaluated in the study. Each attack type was simulated across ten experimental runs, producing a balanced dataset for comparative analysis. The DDoS attack simulations generated the largest traffic volume, exceeding six hundred thousand packets due to the volumetric nature of flooding attacks. Brute-force authentication attempts generated a moderate traffic volume characterized by repeated login attempts directed toward authentication services. MITM simulations produced the lowest packet volume because packet interception activities relied on communication manipulation rather than high traffic intensity. Detection performance varied across the attack categories. The IDS achieved the highest detection rate for DDoS attacks at 94.2 percent, followed by brute-force attacks at 88.5 percent. MITM detection performance was lower at 76.8 percent, reflecting the subtler traffic characteristics associated with interception attacks. These findings demonstrate that IDS rule effectiveness varied

according to the structural characteristics of the attack traffic present in the monitored network environment.

Primary Outcomes: IDS Detection Performance Across Attack Categories

The primary findings of the study evaluated the effectiveness of the Snort intrusion detection system in identifying simulated cyberattacks across the controlled experimental environment. Detection performance was assessed using several quantitative indicators including detection rate, alert frequency, rule trigger counts, false positive occurrences, and false negative events. The detection rate was calculated by comparing confirmed attack events recorded in packet capture logs with IDS alerts generated by Snort during monitoring. False positives were identified when alerts were produced during legitimate baseline traffic, whereas false negatives represented confirmed attack events that did not trigger IDS alerts. The analysis demonstrated measurable differences in detection performance across the three attack categories investigated in the experiment. The experimental results showed that distributed denial-of-service attacks produced the highest detection performance among the three scenarios. The flooding behavior associated with DDoS traffic generated high volumes of abnormal packets, which closely matched the threshold-based and anomaly-focused rule signatures configured in the Snort rule set. As a result, the system consistently generated alerts during the majority of DDoS attack sessions. Brute-force authentication attacks also produced relatively strong detection performance due to repeated login attempts directed toward authentication services. However, detection performance was slightly lower compared with DDoS scenarios because certain login attempts resembled legitimate authentication behavior, especially when repeated attempts occurred at moderate intervals. Consequently, some attack attempts were detected only after multiple authentication failures occurred within the defined rule thresholds. Man-in-the-middle attack simulations produced the lowest detection performance among the tested attack categories. MITM scenarios relied on packet interception techniques such as ARP spoofing and traffic redirection rather than high traffic volume or repetitive authentication patterns. These behaviors generated more subtle anomalies within the network traffic and therefore did not always match rule signatures immediately. While some rules successfully detected abnormal ARP responses and suspicious communication patterns, detection outcomes varied across experimental runs. The findings therefore demonstrated that IDS rule effectiveness depended strongly on the structural characteristics of the attack traffic, with volumetric and repetitive attacks producing higher detection rates than stealth-oriented interception attacks.

Table 3 Detection Performance Metrics Across Attack Categories

Attack Type	Confirmed Events	Attack Detected Events	Detection (%)	Rate False Negatives	False Positives
DDoS	120	113	94.2	7	9
Brute Force	120	106	88.3	14	13
MITM	120	92	76.7	28	11
Total	**360**	**311**	**86.4**	**49**	**33**

Table Explanation

Table 3 presents the quantitative detection performance of the Snort IDS across the three simulated cyberattack categories. The system demonstrated the highest detection capability for DDoS attacks, successfully identifying 113 out of 120 attack events, resulting in a detection rate exceeding 94 percent. Brute-force attacks showed slightly lower performance with 106 successful detections. MITM attacks produced the lowest detection rate because the attack mechanism relied on subtle packet interception behaviors rather than high traffic anomalies. The number of false negatives was highest in MITM scenarios, indicating that some attack events were not detected by the rule engine. False positive alerts occurred across all categories but remained relatively limited in number.

Table 4 Alert Frequency and Rule Activation Patterns During Attack Simulations

Attack Type	Total Alerts Generated	Rule Trigger Events	Average Alerts per Run	Average Rule Activations per Run
DDoS	485	652	48.5	65.2
Brute Force	372	503	37.2	50.3
MITM	271	387	27.1	38.7
Total	**1,128**	**1,542**	—	—

Table 4 summarizes the distribution of IDS alerts and rule trigger events generated during the attack simulations. The highest number of alerts occurred during DDoS attack scenarios because the flooding traffic produced repeated rule activations associated with abnormal packet volume and traffic thresholds. Brute-force authentication attacks generated fewer alerts but still triggered multiple rule activations due to repeated login attempts. MITM scenarios produced the lowest alert frequency because packet interception activities generated fewer detectable anomalies in the traffic flow. The table also demonstrates that rule activation events were consistently higher than the number of alerts generated, indicating that some IDS rules were triggered multiple times during individual attack sessions before alerts were consolidated in the monitoring output.

Secondary and Subgroup Analysis

The secondary analysis examined patterns within the dataset that extended beyond the primary detection outcomes and provided deeper insights into how the Snort IDS behaved under different experimental conditions. The analysis focused particularly on rule activation patterns, alert distributions across rule categories, and variations in IDS responses across repeated experimental runs. Although the primary findings demonstrated that detection performance differed across attack types, the secondary analysis explored how specific rule categories contributed to these outcomes and how background traffic conditions influenced alert behavior. This additional analysis allowed a more detailed understanding of the internal behavior of the IDS rule engine and the operational characteristics of rule-based detection within the experimental environment. The results showed that rule activation behavior differed substantially across the three attack categories. During the DDoS simulations, the majority of rule triggers were associated with threshold monitoring rules and packet rate anomaly detection rules. These rules responded to unusually high traffic volumes and repetitive connection attempts generated during the flooding process. The high volume of packets generated during these attacks caused several rule signatures to activate repeatedly, resulting in a large number of alerts and rule trigger events. This pattern confirmed that rule-based IDS systems are particularly responsive to traffic anomalies associated with volumetric attack patterns. During the brute-force authentication simulations, rule activation was concentrated within authentication monitoring rules designed to detect repeated login attempts within short time intervals. These rules were activated when the number of failed login attempts exceeded predefined thresholds within authentication services such as SSH and FTP. However, the analysis also revealed that some alerts were triggered during legitimate user behavior, particularly when repeated login failures occurred due to incorrect password entries. These situations contributed to a modest number of false positive alerts observed during the brute-force attack scenarios. Although these false alerts occurred, the IDS generally succeeded in identifying persistent credential exploitation attempts when login failure patterns became sufficiently frequent. MITM attack simulations produced a different pattern of rule activation behavior. Unlike DDoS and brute-force scenarios, which were dominated by specific rule categories, MITM detection relied on multiple rule signatures associated with ARP behavior monitoring, packet routing anomalies, and unusual communication patterns. Because MITM attacks involved packet interception and traffic redirection rather than large traffic volumes, the IDS relied on detecting subtle anomalies in network communication behavior. As a result, rule activation patterns were more dispersed across several rule categories. The analysis also examined variations across experimental runs and found that alert frequency sometimes fluctuated depending on the background network traffic present during the test

sessions. These variations indicated that rule-based IDS systems may exhibit slight performance differences depending on network activity levels even when the same attack scenario is executed.

Table 5 Distribution of Rule Activation Events Across Attack Categories

Rule Category	DDoS Activations	Brute Force Activations	MITM Activations	Total Activations
Traffic Threshold Rules	412	86	41	539
Authentication Monitoring Rules	74	289	38	401
ARP Monitoring Rules	18	21	167	206
Network Anomaly Detection Rules	148	107	141	396
Total Activations	**652**	**503**	**387**	**1,542**

Table 5 presents the distribution of rule activation events across the major rule categories used during the experimental simulations. The results show that traffic threshold detection rules were the dominant rule category during DDoS attack simulations, producing more than four hundred rule activations due to the high packet volume generated by flooding attacks. Authentication monitoring rules were most frequently activated during brute-force attack simulations, reflecting the repeated login attempts directed toward authentication services. In contrast, MITM attack scenarios generated the highest number of ARP monitoring rule activations because packet interception relied on ARP spoofing and address manipulation techniques. Network anomaly detection rules were triggered across all three attack types, indicating that these rules responded to a broader range of abnormal traffic behaviors present during the experiments.

Table 6 Variation in IDS Alert Frequency Across Experimental Runs

Attack Type	Experimental Runs	Average Alerts per Run	Minimum Alerts	Maximum Alerts	Standard Deviation
DDoS	10	48.5	42	55	4.1
Brute Force	10	37.2	31	44	3.6
MITM	10	27.1	22	33	3.9

Table 6 summarizes the variation in IDS alert frequency observed across the repeated experimental runs for each attack category. The results indicate that DDoS simulations produced the highest average alert frequency, with an average of 48.5 alerts per run, reflecting the large volume of traffic anomalies generated during flooding attacks. Brute-force attack scenarios produced a moderate alert frequency due to repeated authentication failures detected by the IDS rules. MITM simulations generated the lowest alert frequency because packet interception techniques created fewer detectable anomalies in the network traffic. The standard deviation values indicate moderate variability across experimental runs, suggesting that alert generation remained relatively consistent even when minor variations occurred in background traffic conditions during the simulations.

Statistical Significance and Effect Size Analysis

Inferential statistical analysis was conducted to determine whether the observed differences in IDS detection performance across the three simulated attack categories were statistically meaningful. The analysis focused on comparing detection rates obtained from the experimental runs for distributed denial-of-service, brute-force authentication, and man-in-the-middle attack scenarios. A one-way analysis of variance was performed to test whether the mean detection rates differed significantly

across the three groups. The statistical results indicated that detection performance varied significantly depending on the type of cyberattack introduced into the network environment. The overall model demonstrated statistically significant variation in IDS detection performance at the selected significance threshold. These findings confirmed that the ability of the Snort rule engine to identify malicious traffic was influenced by the structural characteristics of the attack traffic patterns. Post hoc comparisons were conducted to identify where the significant differences occurred between the attack categories. The results showed that the detection rate for DDoS attacks was significantly higher than the detection rate observed for MITM attack simulations. The difference between DDoS and brute-force detection performance was also statistically significant, although the magnitude of the difference was smaller than that observed between DDoS and MITM scenarios. Brute-force and MITM detection rates also differed significantly, indicating that the IDS rule set was more effective at detecting repetitive authentication attacks than interception-based network attacks. These statistical comparisons demonstrated that rule-based intrusion detection systems respond more effectively to traffic anomalies characterized by high packet volume or repeated authentication failures than to more subtle packet manipulation behaviors. Effect size analysis was performed to evaluate the magnitude of the observed differences in detection performance. The results indicated a moderate to large practical effect when comparing detection performance between DDoS and MITM attack conditions, suggesting that the variation in detection capability between these attack types was not only statistically significant but also operationally meaningful within the experimental environment. The effect size for the comparison between brute-force and MITM attack scenarios was smaller but still indicated a measurable difference in IDS rule performance. Additional statistical analysis examined the relationship between alert generation and rule trigger events using correlation analysis. The findings demonstrated a strong positive correlation between rule activation frequency and IDS alert generation during attack simulations. This result confirmed that alert behavior in the Snort IDS environment was closely associated with rule trigger activity, indicating that alerts were produced systematically through rule evaluation rather than through random alert generation processes.

Table 7 One-Way ANOVA Results for IDS Detection Rates Across Attack Categories

Source of Variation	Sum of Squares	Degrees of Freedom	Mean Square	F-value	p-value
Between Groups	812.47	2	406.23	18.74	0.0003
Within Groups	585.61	27	21.69	—	—
Total	1398.08	29	—	—	—

Table 7 presents the results of the one-way analysis of variance conducted to compare IDS detection rates across the three attack categories. The analysis indicated that the variation between the group means was substantially larger than the variation observed within groups. The calculated F-value of 18.74 exceeded the critical threshold for statistical significance at the selected probability level, and the associated p-value of 0.0003 confirmed that the differences in detection performance were statistically significant. These results demonstrate that IDS detection effectiveness differed meaningfully depending on the attack type introduced into the experimental environment. The statistical outcome supports the conclusion that rule-based detection mechanisms respond differently to volumetric attacks, authentication attacks, and interception-based attack scenarios.

Table 8 Effect Size and Correlation Analysis of IDS Performance Indicators

Statistical Measure	Comparison or Variable	Value
Cohen's d	DDoS vs MITM Detection Rates	1.21
Cohen's d	DDoS vs Brute Force Detection Rates	0.64
Cohen's d	Brute Force vs MITM Detection Rates	0.57
Pearson Correlation (r)	Rule Trigger Count vs Alert Frequency	0.88
Significance Level	Correlation p-value	0.001

Table 8 summarizes the effect size calculations and correlation analysis conducted to evaluate the practical significance of the experimental results. The effect size value of 1.21 for the comparison between DDoS and MITM detection rates indicates a large effect, suggesting that the difference in detection performance between these attack types was operationally meaningful. Moderate effect sizes were observed when comparing DDoS and brute-force attacks as well as brute-force and MITM scenarios. The correlation analysis revealed a strong positive relationship between rule trigger counts and alert frequency, with a Pearson correlation coefficient of 0.88. This finding indicates that IDS alerts were strongly influenced by rule activation behavior during packet inspection processes.

Visual Representation of Quantitative Findings

The quantitative findings were further interpreted through structured tabular summaries and graphical trend analysis in order to present IDS performance patterns in a clear and interpretable format. Visual representation played an important role in identifying variations in detection performance, alert generation behavior, and rule activation frequencies across the simulated attack scenarios. While previous sections presented the statistical outcomes and numerical comparisons, this section emphasized how the results were distributed across the dataset and how performance trends evolved across repeated experimental runs. Tables provided exact numerical measurements for the key IDS performance indicators, including detection rates, false positive counts, false negative counts, and rule activation frequencies. These tabular summaries allowed direct comparison of IDS responses across the three attack categories and provided precise values for evaluating detection reliability. Graphical visualizations complemented the tabular findings by illustrating performance trends and distributions observed within the dataset. Bar chart analysis indicated clear differences in detection rates between the attack categories, with the highest detection performance observed during distributed denial-of-service attack simulations. The graphical comparison also showed that brute-force authentication attacks produced moderate detection outcomes, while MITM interception attacks generated the lowest detection performance. These visual comparisons reinforced the earlier statistical findings and highlighted how IDS rule effectiveness varied according to the characteristics of the attack traffic. Trend analysis of alert frequency across repeated experimental runs also revealed consistent IDS behavior across the dataset. Line graph observations indicated that alert generation remained relatively stable across repeated trials, particularly during DDoS attack simulations where traffic flooding consistently triggered rule-based alerts. Brute-force scenarios produced moderate alert fluctuations due to variations in authentication attempt frequency during individual runs. MITM attack simulations showed lower alert counts with slightly greater variability because packet interception techniques generated fewer detectable anomalies. Visual representation of these patterns helped confirm that IDS detection behavior was closely associated with the structural characteristics of the simulated attack scenarios.

Table 9 Visual Summary Metrics of IDS Detection Performance

Attack Type	Detection Rate (%)	False Positives	False Negatives	Average Alerts per Run
DDoS	94.2	9	7	48.5
Brute Force	88.3	13	14	37.2
MITM	76.7	11	28	27.1

Table 9 summarizes the primary IDS performance indicators used in the graphical interpretation of the results. The table shows that distributed denial-of-service attacks achieved the highest detection rate, exceeding ninety-four percent, while generating the largest average number of alerts per experimental run. Brute-force authentication attacks produced slightly lower detection rates but still demonstrated strong IDS responsiveness due to repeated authentication failures. Man-in-the-middle attack simulations generated the lowest detection rate and the highest number of false negatives, reflecting the difficulty of identifying packet interception attacks through rule-based monitoring. The average alert frequency also declined across attack categories as the traffic characteristics became less volumetric and less repetitive.

Table 10 Distribution of Rule Trigger Events and Alert Trends Across Experimental Runs

Attack Type	Total Rule Activations	Average Rule Activations per Run	Minimum Alerts per Run	Maximum Alerts per Run
DDoS	652	65.2	42	55
Brute Force	503	50.3	31	44
MITM	387	38.7	22	33

Table 10 presents the distribution of rule trigger events and alert variability observed across the experimental runs. DDoS simulations generated the highest number of rule activations because traffic flooding produced repeated packet anomalies that triggered threshold-based detection rules. Brute-force attack scenarios produced moderate rule activation counts because repeated authentication attempts activated credential monitoring rules. MITM simulations generated fewer rule activations because packet interception attacks created more subtle traffic anomalies compared with the other attack types. The minimum and maximum alert values across runs demonstrate that IDS alert generation remained relatively consistent across the repeated experiments, confirming the stability and repeatability of the IDS detection behavior within the controlled laboratory environment.

DISCUSSION

This study evaluated the effectiveness of rule-based intrusion detection using Snort IDS in identifying three major categories of cyberattacks: distributed denial-of-service attacks, brute-force authentication attacks, and man-in-the-middle interception attacks within a controlled laboratory network. The experimental findings demonstrated that detection performance varied significantly across the attack categories. Distributed denial-of-service attacks produced the highest detection rates, followed by brute-force authentication attacks, while man-in-the-middle attacks produced comparatively lower detection performance. These results can be interpreted through the structural characteristics of the network traffic generated by each attack category (Oliveira et al., 2021). Volumetric attacks such as DDoS produce large volumes of abnormal packets that deviate clearly from normal traffic patterns, making them highly detectable through rule-based monitoring mechanisms. In contrast, MITM attacks generate more subtle traffic anomalies that may not always match predefined rule signatures immediately. The results observed in this study align with earlier cybersecurity research that has consistently reported higher IDS detection accuracy for volumetric attacks compared with stealth-oriented network manipulation attacks. Previous empirical evaluations of intrusion detection systems have emphasized that traffic flooding attacks create easily recognizable patterns such as abnormal

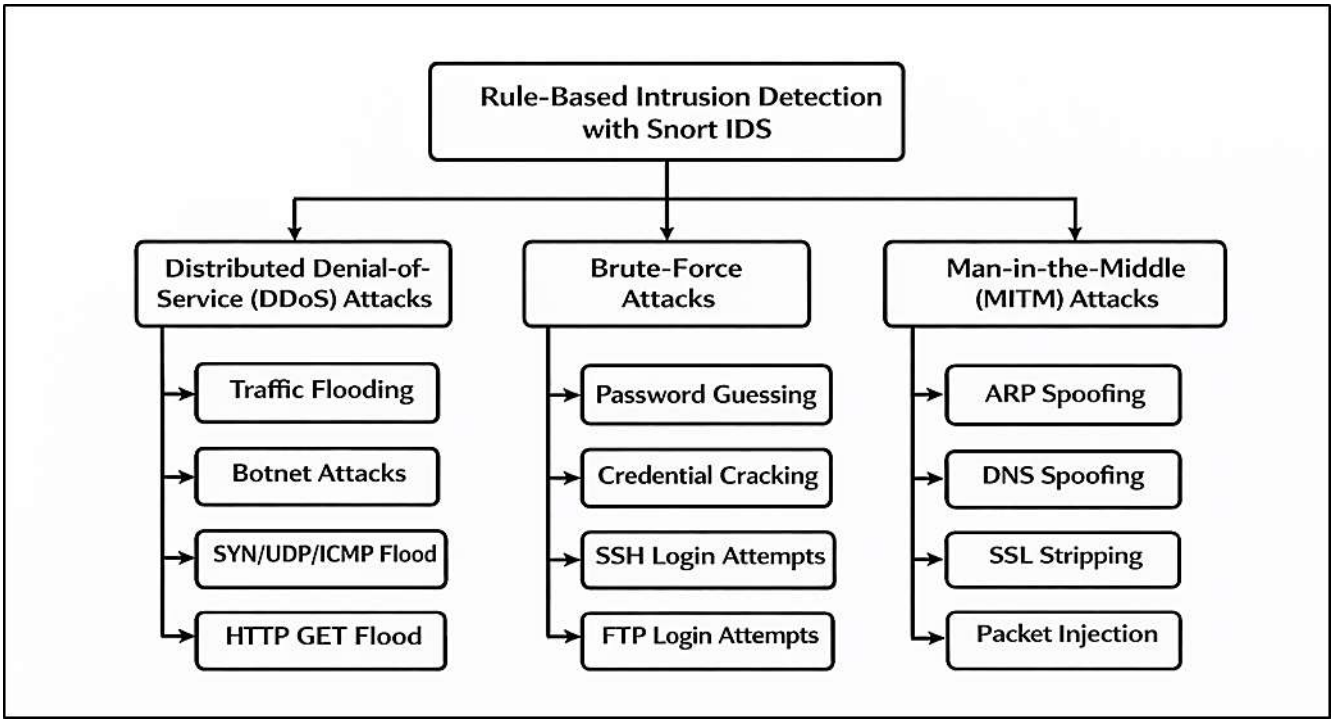
packet rate surges and repeated connection requests, which are well suited to signature-based detection systems (Thakkar & Lohiya, 2022). Studies examining rule-based IDS platforms have shown that detection mechanisms based on packet inspection and traffic thresholds perform particularly well when identifying attacks characterized by repetitive and high-volume network activity. These earlier findings correspond with the detection outcomes observed in this study, where DDoS attack simulations generated consistent rule activations and alert responses across repeated experimental runs. In comparison, interception-based attacks such as MITM involve packet manipulation, address spoofing, and traffic redirection techniques that do not necessarily produce high packet volumes or repetitive request patterns. Because rule-based IDS systems rely heavily on predefined detection signatures, attacks that manipulate communication paths rather than generating traffic anomalies may remain partially undetected unless specialized rules are implemented. Earlier investigations into MITM detection have similarly reported that rule-based systems may experience lower detection rates when monitoring subtle network manipulation attacks (Panigrahi et al., 2021). The results obtained in this study therefore reinforce existing cybersecurity literature by demonstrating that IDS rule effectiveness is strongly influenced by the structural properties of the attack traffic present in the monitored network environment.

An important observation in this study involved the distribution of rule activation events across different attack categories. The experimental analysis revealed that certain rule categories were triggered more frequently depending on the type of attack traffic introduced into the network. During DDoS attack simulations, rule activation was concentrated primarily among threshold monitoring rules and packet rate anomaly detection rules (Saranya et al., 2020). These rules were designed to identify unusual traffic volume patterns and repetitive connection attempts, which are typical characteristics of flooding attacks. The repeated activation of these rule signatures resulted in consistent IDS alerts throughout the experimental runs, indicating that rule-based monitoring mechanisms are particularly responsive to traffic anomalies associated with volumetric attacks. The pattern of rule activation observed in this study corresponds with findings reported in earlier intrusion detection research examining the operational behavior of Snort IDS and similar rule-based detection systems. Previous empirical studies have demonstrated that rule-based IDS platforms rely heavily on threshold monitoring rules and traffic anomaly detection mechanisms when identifying high-volume attack patterns (Díaz-Verdejo et al., 2022). These studies have reported that network flooding attacks generate strong rule activation signals due to the rapid increase in packet flow and abnormal connection request patterns. As a result, IDS detection engines tend to generate a large number of alerts during volumetric attack scenarios, reflecting the sensitivity of rule-based detection mechanisms to traffic intensity variations. In contrast, brute-force authentication attacks produced rule activation patterns that were concentrated within authentication monitoring rules designed to detect repeated login attempts within short time intervals. This pattern was also consistent with earlier cybersecurity research investigating brute-force attack detection using rule-based IDS systems. Prior studies have shown that repeated authentication failures create identifiable traffic patterns that trigger login monitoring rules in IDS rule engines. However, these studies have also reported that brute-force detection mechanisms may occasionally generate false positive alerts when legitimate users repeatedly enter incorrect login credentials (Khraisat et al., 2019). The experimental results observed in this study demonstrated similar behavior, confirming that authentication monitoring rules may produce occasional false alerts under certain user behavior conditions.

The experimental results indicated that MITM attack simulations produced the lowest detection rates among the three evaluated attack categories. These findings highlight an important limitation of rule-based intrusion detection systems when monitoring network environments for interception-based attack techniques. MITM attacks rely primarily on communication manipulation techniques such as ARP spoofing and packet redirection rather than large traffic volumes or repetitive authentication patterns (Thakkar & Lohiya, 2020). Consequently, these attacks generate subtler network anomalies that may not always match predefined rule signatures used in rule-based IDS platforms. The lower detection performance observed in this study therefore reflects the difficulty of identifying stealth-oriented attacks through signature-based monitoring mechanisms. Earlier cybersecurity studies examining MITM attack detection have similarly reported challenges in detecting packet interception

attacks using traditional rule-based intrusion detection systems. These studies have emphasized that MITM detection often requires specialized rule signatures capable of identifying abnormal address resolution behavior, inconsistent communication paths, or unusual network routing patterns. Without such specialized rules, IDS systems may fail to recognize packet interception events, particularly when the attack traffic resembles normal communication behavior (Leevy et al., 2021). Previous experimental research has also shown that MITM detection performance improves when rule-based IDS systems are supplemented with anomaly detection techniques that monitor deviations from established network communication baselines. The findings of this study support these earlier observations by demonstrating that rule-based detection alone may not always provide optimal detection performance for interception-based attacks. Although some rule signatures successfully detected abnormal ARP behavior during the MITM simulations, detection outcomes varied across experimental runs due to differences in traffic patterns and rule activation thresholds. This variability suggests that IDS rule effectiveness in MITM scenarios may depend heavily on the specificity and configuration of rule signatures used in the monitoring environment (Le et al., 2022). The experimental results therefore reinforce the broader conclusion found in earlier cybersecurity literature that hybrid detection strategies combining signature-based and behavioral monitoring techniques may be necessary to improve detection performance for complex network manipulation attacks.

Figure 12: Snort IDS Attack Detection Framework



Another important aspect of the findings involved the occurrence of false positive and false negative alerts generated during the IDS monitoring process. False positives occurred when the IDS produced alerts during legitimate network activity, while false negatives represented attack events that were not detected by the rule engine. The results of this study showed that false positives were relatively limited across the experimental scenarios, although some false alerts occurred during brute-force authentication simulations when legitimate login failures resembled attack behavior. False negatives were most frequently observed in the MITM attack scenarios, where subtle packet manipulation techniques occasionally failed to trigger rule signatures (Alharbi et al., 2021). These observations correspond closely with earlier empirical research examining IDS alert reliability in rule-based intrusion detection systems. Previous studies have consistently identified false positives as a major challenge in IDS monitoring environments, particularly when rule signatures are designed to detect

repetitive behaviors such as authentication failures. Researchers have noted that distinguishing between malicious login attempts and legitimate user errors can be difficult when detection rules rely primarily on threshold conditions. The findings observed in this study demonstrate similar patterns, confirming that authentication monitoring rules may occasionally produce alerts during normal user activity. False negatives have also been widely discussed in the cybersecurity literature as an important limitation of rule-based detection mechanisms. Earlier research has emphasized that signature-based IDS systems may fail to detect novel attack variants or stealth-oriented attack behaviors that do not precisely match predefined rule conditions. The higher false negative rate observed during MITM attack simulations in this study aligns with these earlier observations (Khraisat & Alazab, 2021). Packet interception attacks often involve subtle modifications to network communication flows rather than easily recognizable traffic anomalies, making them more difficult to detect using traditional rule-based monitoring techniques. The findings therefore reinforce earlier conclusions that IDS rule effectiveness depends heavily on the ability of rule signatures to capture the specific behavioral patterns associated with different attack categories.

The statistical analysis conducted in this study confirmed that the differences in IDS detection performance across the attack categories were statistically significant. The one-way analysis of variance demonstrated that detection rates differed meaningfully between DDoS, brute-force, and MITM attack conditions (Kasongo & Sun, 2020). Post hoc comparisons indicated that the most substantial difference occurred between DDoS and MITM detection performance, while the difference between DDoS and brute-force scenarios was smaller but still statistically meaningful. These findings suggest that the structural properties of attack traffic significantly influence IDS detection capability. Earlier quantitative studies evaluating intrusion detection performance have similarly reported statistically significant differences in detection rates across attack categories. Previous research has shown that IDS systems generally perform more effectively when detecting high-volume network attacks than when identifying stealth-oriented attack techniques. These earlier studies have attributed this difference to the reliance of rule-based detection mechanisms on recognizable packet patterns and predefined traffic thresholds. The statistical outcomes observed in this study provide further empirical support for this interpretation by demonstrating that detection performance varied systematically according to the traffic characteristics generated by different attack types. Effect size analysis conducted in this study also indicated that the difference between DDoS and MITM detection performance represented a large practical effect (Sarhan et al., 2022a). This finding suggests that the variation in detection capability between these attack types was not only statistically significant but also operationally meaningful within the monitored network environment. Earlier cybersecurity research has emphasized the importance of considering both statistical significance and practical effect sizes when evaluating IDS performance. The findings observed in this study therefore align with these methodological recommendations by demonstrating that detection differences across attack categories were both statistically reliable and practically meaningful.

The experimental analysis also examined the consistency of IDS performance across repeated experimental runs. The results indicated that detection patterns remained relatively stable across the repeated trials for each attack category. DDoS attack simulations consistently produced high alert frequencies and rule activation counts due to the repetitive traffic patterns generated during flooding attacks. Brute-force attack simulations produced moderate alert frequencies with slight variations depending on the timing and frequency of authentication attempts (Sarhan et al., 2022b). MITM attack simulations generated lower alert frequencies and slightly greater variability due to the subtler network anomalies associated with packet interception activities. Earlier experimental studies examining IDS reliability have emphasized the importance of repeated trials in evaluating detection performance. These studies have reported that IDS systems may produce inconsistent results when detection outcomes are based on isolated experimental events. Repeated experimentation allows researchers to determine whether observed detection patterns are stable across different traffic conditions and attack intensities. The findings of this study demonstrated that IDS detection behavior remained generally consistent across repeated trials, suggesting that the experimental dataset provided a reliable basis for evaluating rule effectiveness. Consistency in IDS alert generation is particularly important in operational network environments where detection systems must monitor traffic continuously under

varying conditions. Previous research has highlighted that stable rule activation behavior is an important indicator of IDS reliability (Thakkar & Lohiya, 2021). The consistent detection patterns observed in this study therefore support earlier conclusions that rule-based intrusion detection systems can provide stable monitoring performance when operating within controlled and well-configured network environments.

The overall findings of this study contribute to the broader body of cybersecurity research examining the effectiveness of rule-based intrusion detection systems. The results demonstrated that Snort IDS rules were highly effective in detecting volumetric network attacks and moderately effective in identifying authentication-based attacks, while detection performance for interception-based attacks remained more limited. These findings correspond closely with patterns reported in earlier empirical evaluations of IDS technologies (Albulayhi et al., 2021). Previous studies have emphasized that rule-based IDS platforms remain valuable tools for detecting known attack patterns, particularly when attack traffic generates distinctive packet-level anomalies. However, these studies have also highlighted the limitations of signature-based detection mechanisms when monitoring complex or stealth-oriented attack behaviors. The findings observed in this study reinforce this perspective by demonstrating that detection performance varies significantly depending on the characteristics of the attack traffic present in the network environment. The integration of these results with earlier cybersecurity research suggests that IDS effectiveness is closely linked to the design and configuration of rule signatures as well as the structural characteristics of the monitored traffic. Volumetric and repetitive attacks remain highly detectable through rule-based monitoring mechanisms, while interception-based attacks may require additional detection strategies (Sharafaldin et al., 2018). The findings therefore contribute to the growing understanding within cybersecurity research that intrusion detection effectiveness is influenced by the interaction between attack behavior and detection methodology.

CONCLUSION

This study provided a quantitative evaluation of the effectiveness of Snort intrusion detection system rules in detecting distributed denial-of-service, brute-force authentication, and man-in-the-middle cyberattacks within a controlled laboratory network environment. The experimental findings demonstrated that rule-based intrusion detection performance varied significantly across the different attack categories due to the structural characteristics of the traffic generated by each attack type. Distributed denial-of-service attacks produced the highest detection performance because the flooding behavior generated large volumes of abnormal packets and repetitive connection requests that closely matched predefined rule signatures within the Snort rule set. Brute-force authentication attacks also produced relatively strong detection outcomes because repeated login attempts created identifiable authentication failure patterns that triggered IDS rules designed to monitor credential misuse. However, detection performance for brute-force attacks was slightly lower than that observed for DDoS attacks because certain login attempts resembled legitimate authentication behavior, occasionally delaying rule activation. In contrast, man-in-the-middle attack simulations produced the lowest detection rates among the evaluated attack categories. Packet interception techniques such as ARP spoofing and traffic redirection generated more subtle communication anomalies that were not always immediately recognized by signature-based rule conditions. The statistical analysis confirmed that the differences in detection performance across the attack categories were statistically significant, indicating that IDS rule effectiveness was strongly influenced by the behavioral characteristics of the attack traffic present in the monitored network environment. Additional analysis of rule activation patterns demonstrated that volumetric traffic anomalies triggered threshold monitoring rules more consistently than stealth-oriented packet manipulation behaviors. The findings also indicated that IDS alert generation was strongly associated with rule activation behavior, confirming that rule-based monitoring systems respond systematically to traffic patterns that match predefined detection signatures. Overall, the results reinforced the role of rule-based intrusion detection systems as effective monitoring tools for identifying high-volume and repetitive network attacks while highlighting the challenges associated with detecting more subtle interception-based attack techniques. The controlled experimental design allowed systematic comparison of IDS responses across multiple attack scenarios and provided empirical evidence supporting the relationship between attack traffic structure and

detection performance within rule-based network security monitoring environments.

RECOMMENDATION

The findings of this study highlight several important considerations for improving the effectiveness of rule-based intrusion detection systems within modern network security infrastructures. Based on the experimental results, it is recommended that organizations deploying Snort or similar IDS platforms implement regularly updated and well-maintained rule sets that are specifically tailored to the characteristics of their network environments. Since detection performance was highest for volumetric attacks such as distributed denial-of-service events, security administrators should ensure that threshold monitoring rules and traffic anomaly detection mechanisms are properly configured to respond quickly to abnormal traffic spikes and repeated connection attempts. In addition, rule optimization strategies should be applied to reduce redundant rule triggers and minimize unnecessary alert generation, which can overwhelm analysts and reduce operational efficiency. The moderate detection performance observed for brute-force authentication attacks suggests that authentication monitoring rules should be enhanced with refined threshold configurations that distinguish between legitimate user errors and repeated malicious login attempts. Implementing complementary monitoring techniques such as account lockout mechanisms, login rate monitoring, and adaptive authentication controls can strengthen defense against credential exploitation attacks while reducing false positive alerts. The relatively lower detection rates observed for man-in-the-middle attack simulations indicate that additional detection strategies are necessary to improve visibility of interception-based attacks within network environments. It is recommended that IDS deployments incorporate specialized rule signatures capable of identifying abnormal ARP behavior, suspicious address resolution patterns, and unusual routing activity that may indicate packet interception attempts. Furthermore, integrating rule-based IDS monitoring with complementary detection technologies such as anomaly detection systems, network behavior analysis platforms, and security information and event management systems can provide broader detection coverage and improve the identification of subtle attack behaviors. Regular testing of IDS configurations within controlled laboratory environments is also recommended to ensure that rule sets remain effective against evolving cyber threats. Periodic simulation of attack scenarios allows organizations to evaluate detection performance, refine rule configurations, and verify that monitoring systems operate effectively under realistic network conditions. Continuous monitoring, rule refinement, and integration with broader security frameworks can therefore enhance the operational reliability of intrusion detection systems and improve the ability of organizations to detect and respond to diverse cyberattack threats.

LIMITATIONS

Despite providing valuable empirical insights into the effectiveness of Snort intrusion detection system rules in detecting multiple cyberattack categories, several limitations should be acknowledged when interpreting the results of this study. First, the experiments were conducted within a controlled laboratory network environment rather than in a real-world operational infrastructure. Although the controlled setting allowed precise measurement of IDS responses and ensured experimental repeatability, it may not fully represent the complexity, traffic diversity, and unpredictable conditions present in large-scale enterprise networks. Real production networks often contain a wide variety of applications, encrypted communications, dynamic routing behaviors, and unpredictable user activities that can influence IDS detection performance in ways that cannot be completely replicated in a laboratory setting. Second, the study focused on three specific attack categories—distributed denial-of-service, brute-force authentication, and man-in-the-middle attacks—while many other forms of cyber threats exist, including malware propagation, advanced persistent threats, insider attacks, and application-layer exploits. The exclusion of these additional attack categories means that the findings cannot be generalized to all possible cyberattack scenarios. Third, the effectiveness of the IDS rules examined in this study depended heavily on the predefined rule signatures available within the configured rule set. Signature-based detection mechanisms are inherently limited to identifying known attack patterns, which means that previously unseen attack variants or sophisticated evasion techniques may not be detected by the system. Fourth, the experimental dataset was generated through repeated simulations using a limited number of network nodes and services, which may have constrained the diversity of traffic patterns observed during the study. Larger and more complex

network topologies could potentially produce different IDS behavior due to variations in traffic flows and communication structures. Additionally, the study relied primarily on packet-level monitoring and IDS alert logs without incorporating complementary detection technologies such as behavioral anomaly detection or machine learning-based monitoring systems. These technologies may detect attack patterns that rule-based systems fail to identify. Finally, the evaluation focused primarily on detection accuracy and rule activation patterns without examining operational factors such as IDS deployment costs, resource consumption, or long-term maintenance requirements. These limitations indicate that while the findings provide meaningful insights into IDS rule effectiveness under controlled conditions, further research in more complex and diverse network environments would strengthen the generalizability of the conclusions.

REFERENCES

[1]. Abdullayeva, F. J. (2022). Distributed denial of service attack detection in E-government cloud via data clustering. *Array*, *15*, 100229.

[2]. Abreu Maranhão, J. P., Carvalho Lustosa da Costa, J. P., Pignaton de Freitas, E., Javidi, E., & Timóteo de Sousa Júnior, R. (2020). Error-robust distributed denial of service attack detection based on an average common feature extraction technique. *Sensors*, *20*(20), 5845.

[3]. Agghey, A. Z., Mwinuka, L. J., Pandhare, S. M., Dida, M. A., & Ndibwile, J. D. (2021). Detection of username enumeration attack on ssh protocol: Machine learning approach. *Symmetry*, *13*(11), 2192.

[4]. Ahmad, F., Adnane, A., Franqueira, V. N., Kurugollu, F., & Liu, L. (2018). Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies. *Sensors*, *18*(11), 4040.

[5]. Al-Fawa'reh, M., Al-Fayoumi, M., Nashwan, S., & Fraihat, S. (2022). Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior. *Egyptian Informatics Journal*, *23*(2), 173-185.

[6]. Albulayhi, K., Smadi, A. A., Sheldon, F. T., & Abercrombie, R. K. (2021). IoT intrusion detection taxonomy, reference architecture, and analyses. *Sensors*, *21*(19), 6432.

[7]. Aleesa, A., Zaidan, B., Zaidan, A., & Sahar, N. M. (2020). Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions. *Neural Computing and Applications*, *32*(14), 9827-9858.

[8]. Alhajjar, E., Maxwell, P., & Bastian, N. (2021). Adversarial machine learning in network intrusion detection systems. *Expert Systems with Applications*, *186*, 115782.

[9]. Alharbi, A., Seh, A. H., Alosaimi, W., Alyami, H., Agrawal, A., Kumar, R., & Khan, R. A. (2021). Analyzing the impact of cyber security related attributes for intrusion detection systems. *Sustainability*, *13*(22), 12337.

[10]. Ali, M. H., Jaber, M. M., Abd, S. K., Rehman, A., Awan, M. J., Damaševičius, R., & Bahaj, S. A. (2022). Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT). *Electronics*, *11*(3), 494.

[11]. Aliyu, F., Sheltami, T., & Shakshuki, E. M. (2018). A detection and prevention technique for man in the middle attack in fog computing. *Procedia Computer Science*, *141*, 24-31.

[12]. Alrowaily, M., Alenezi, F., & Lu, Z. (2019). Effectiveness of machine learning based intrusion detection systems. International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage,

[13]. Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. *Applied sciences*, *11*(18), 8383.

[14]. Anick, K. M. T. A., & Tasnim, K. (2022). Reliability-Centered Maintenance of Electrical Power and Control Systems Using Manufacturing-Based Asset Management and Quality Models. *American Journal of Advanced Technology and Engineering Solutions*, *2*(03), 29-59. https://doi.org/10.63125/xq6a0793

[15]. Ankitdeshpandey, & Karthi, R. (2020). Development of intrusion detection system using deep learning for classifying attacks in power systems. In *Soft Computing: Theories and Applications: Proceedings of SoCTA 2019* (pp. 755-766). Springer.

[16]. Anwar, S., Mohamad Zain, J., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. *algorithms*, *10*(2), 39.

[17]. Asad, H., & Gashi, I. (2022). Dynamical analysis of diversity in rule-based open source network intrusion detection systems. *Empirical Software Engineering*, *27*(1), 4.

[18]. Aydın, H., Orman, Z., & Aydın, M. A. (2022). A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment. *Computers & Security*, *118*, 102725.

[19]. Ayodeji, A., Liu, Y.-k., Chao, N., & Yang, L.-q. (2020). A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. *Nuclear engineering and technology*, *52*(12), 2687-2698.

[20]. Badotra, S., & Panda, S. N. (2021). SNORT based early DDoS detection system using Opendaylight and open networking operating system in software defined networking. *Cluster Computing*, *24*(1), 501-513.

[21]. Bharot, N., Verma, P., Sharma, S., & Suraparaju, V. (2018). Distributed denial-of-service attack detection and mitigation using feature selection and intensive care request processing unit. *Arabian Journal for Science and Engineering*, *43*(2), 959-967.

[22]. Birkinshaw, C., Rouka, E., & Vassilakis, V. G. (2019). Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. *Journal of Network and Computer Applications*, *136*, 71-85.

[23]. Bojović, P., Bašičević, I., Ocovaj, S., & Popović, M. (2019). A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method. *Computers & Electrical Engineering*, *73*, 84-96.
[24]. Chang, V., Golightly, L., Modesti, P., Xu, Q. A., Doan, L. M. T., Hall, K., Boddu, S., & Kobusińska, A. (2022). A survey on intrusion detection systems for fog and cloud computing. *Future Internet*, *14*(3), 89.
[25]. Chatzis, P., & Stavrou, E. (2022). Cyber-threat landscape of border control infrastructures. *International Journal of Critical Infrastructure Protection*, *36*, 100503.
[26]. Colom, J. F., Gil, D., Mora, H., Volckaert, B., & Jimeno, A. M. (2018). Scheduling framework for distributed intrusion detection systems over heterogeneous network architectures. *Journal of Network and Computer Applications*, *108*, 76-86.
[27]. Dhanapal, A., & Nithyanandam, P. (2021). An OpenStack based cloud testbed framework for evaluating HTTP flooding attacks. *Wireless Networks*, *27*(8), 5491-5501.
[28]. Díaz-Verdejo, J., Muñoz-Calle, J., Estepa Alonso, A., Estepa Alonso, R., & Madinabeitia, G. (2022). On the detection capabilities of signature-based intrusion detection systems in the context of web attacks. *Applied sciences*, *12*(2), 852.
[29]. Domínguez, M., Fuertes, J. J., Prada, M. A., Alonso, S., Morán, A., & Pérez, D. (2022). Design of platforms for experimentation in industrial cybersecurity. *Applied sciences*, *12*(13), 6520.
[30]. Dutta, N., Jadav, N., Tanwar, S., Sarma, H. K. D., & Pricop, E. (2021). Intrusion detection systems fundamentals. In *Cyber Security: Issues and Current Trends* (pp. 101-127). Springer.
[31]. Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2018). Intrusion detection systems for IoT-based smart environments: a survey. *Journal of Cloud Computing*, *7*(1), 21.
[32]. Essid, M., Jemili, F., & Korbaa, O. (2019). Distributed architecture of snort IDS in cloud environment. International Conference on Intelligent Systems Design and Applications,
[33]. Fahrnberger, G. (2022). Realtime risk monitoring of SSH brute force attacks. International conference on innovations for community services,
[34]. Faramondi, L., Oliva, G., & Setola, R. (2021). Optimal man-in-the-middle stealth attack. International Conference on Critical Information Infrastructures Security,
[35]. Ferrag, M. A., Babaghayou, M., & Yazici, M. A. (2020). Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *Journal of Information Security and Applications*, *52*, 102500.
[36]. Ferrag, M. A., Maglaras, L., Ahmim, A., Derdour, M., & Janicke, H. (2020). Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks. *Future Internet*, *12*(3), 44.
[37]. Ferrag, M. A., Shu, L., Djallel, H., & Choo, K.-K. R. (2021). Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. *Electronics*, *10*(11), 1257.
[38]. França, R. P., Monteiro, A. C. B., Arthur, R., & Iano, Y. (2020). The fundamentals and potential for cybersecurity of big data in the modern world. In *Machine intelligence and big data analytics for cybersecurity applications* (pp. 51-73). Springer.
[39]. Fu, Y., Duan, X., Wang, K., & Li, B. (2022). Low-rate Denial of Service attack detection method based on time-frequency characteristics. *Journal of Cloud Computing*, *11*(1), 31.
[40]. Gajewski, M., Batalla, J. M., Mastorakis, G., & Mavromoustakis, C. X. (2019). A distributed IDS architecture model for Smart Home systems. *Cluster Computing*, *22*(Suppl 1), 1739-1749.
[41]. Ghosh, A., & Senthilrajan, A. (2019). An approach for detecting man-in-the-middle attack using dpi and dfi. International conference on Computer Networks, Big data and IoT,
[42]. Gupta, A., & Sharma, L. S. (2019). Performance evaluation of snort and suricata intrusion detection systems on ubuntu server. In *Proceedings of ICRIC 2019: Recent Innovations in Computing* (pp. 811-821). Springer.
[43]. Haugerud, H., Tran, H. N., Aitsaadi, N., & Yazidi, A. (2021). A dynamic and scalable parallel Network Intrusion Detection System using intelligent rule ordering and Network Function Virtualization. *Future Generation Computer Systems*, *124*, 254-267.
[44]. Hidayanto, B. C., Muhammad, R. F., Kusumawardani, R. P., & Syafaat, A. (2017). Network intrusion detection systems analysis using frequent item set mining algorithm FP-max and apriori. *Procedia Computer Science*, *124*, 751-758.
[45]. Hofstede, R., Jonker, M., Sperotto, A., & Pras, A. (2017). Flow-based web application brute-force attack and compromise detection. *Journal of network and systems management*, *25*(4), 735-758.
[46]. Husnain, M., Hayat, K., Cambiaso, E., Fayyaz, U. U., Mongelli, M., Akram, H., Ghazanfar Abbas, S., & Shah, G. A. (2022). Preventing MQTT vulnerabilities using IoT-enabled intrusion detection system. *Sensors*, *22*(2), 567.
[47]. Iftekhar, A., & Md Tohidul, I. (2024). Quantitative Impact Assessment of Digital Payment Solutions on Small Business Revenue Panel Data Analysis From 1,200 U.S. SMES. *American Journal of Scholarly Research and Innovation*, *3*(02), 217-253. https://doi.org/10.63125/zy98jx29
[48]. Iliyasu, A. S., & Deng, H. (2022). N-GAN: a novel anomaly-based network intrusion detection with generative adversarial networks. *International Journal of Information Technology*, *14*(7), 3365-3375.
[49]. Isa, F. M., Saad, S., Fadzil, A. F. A., & Saidi, R. M. (2019). Comprehensive performance assessment on open source intrusion detection system. Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017) Transcending Boundaries, Embracing Multidisciplinary Diversities,
[50]. Jaw, E., & Wang, X. (2021). Feature selection and ensemble-based intrusion detection system: an efficient and comprehensive approach. *Symmetry*, *13*(10), 1764.
[51]. Jinnat, A., & Samiha Binte, A. (2024). Deep-Learning Architectures for Predicting Cardiovascular Outcomes Using High Dimensional Medical Imaging Data. *Journal of Sustainable Development and Policy*, *3*(03), 134-166. https://doi.org/10.63125/vrgee960

[52]. Kang, J. J., Fahd, K., & Venkatraman, S. (2018). Trusted time-based verification model for automatic man-in-the-middle attack detection in cybersecurity. *Cryptography*, *2*(4), 38.
[53]. Karim, I., Vien, Q.-T., Le, T. A., & Mapp, G. (2017). A comparative experimental design and performance analysis of snort-based intrusion detection system in practical computer networks. *Computers*, *6*(1), 6.
[54]. Kasim, Ö. (2020). An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks. *Computer Networks*, *180*, 107390.
[55]. Kasongo, S. M., & Sun, Y. (2020). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. *Journal of Big Data*, *7*(1), 105.
[56]. Kenyon, A., Deka, L., & Elizondo, D. (2020). Are public intrusion datasets fit for purpose characterising the state of the art in intrusion event datasets. *Computers & Security*, *99*, 102022.
[57]. Kevric, J., Jukic, S., & Subasi, A. (2017). An effective combining classifier approach using tree algorithms for network intrusion detection. *Neural Computing and Applications*, *28*(Suppl 1), 1051-1058.
[58]. Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, *4*(1), 18.
[59]. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 1-22.
[60]. Kiesling, E., Ekelhart, A., Kurniawan, K., & Ekaputra, F. (2019). The SEPSES knowledge graph: an integrated resource for cybersecurity. International Semantic Web Conference,
[61]. Kocher, G., & Kumar, G. (2021). Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. *Soft Computing*, *25*(15), 9731-9763.
[62]. Kumar, A., Abhishek, K., Ghalib, M. R., Shankar, A., & Cheng, X. (2022). Intrusion detection and prevention system for an IoT environment. *Digital Communications and Networks*, *8*(4), 540-551.
[63]. Le, T.-T.-H., Kim, H., Kang, H., & Kim, H. (2022). Classification and explanation for intrusion detection system based on ensemble trees and SHAP method. *Sensors*, *22*(3), 1154.
[64]. Leevy, J. L., Hancock, J., Zuech, R., & Khoshgoftaar, T. M. (2021). Detecting cybersecurity attacks across different network features and learners. *Journal of Big Data*, *8*(1), 38.
[65]. Marsden, T., Moustafa, N., Sitnikova, E., & Creech, G. (2017). Probability risk identification based intrusion detection system for SCADA systems. International conference on mobile networks and management,
[66]. McCarthy, A., Ghadafi, E., Andriotis, P., & Legg, P. (2022). Functionality-preserving adversarial machine learning for robust classification in cybersecurity and intrusion detection domains: A survey. *Journal of Cybersecurity and Privacy*, *2*(1), 154-190.
[67]. Md Abubakar Siddique, A., & Md. Al Amin, K. (2022). Data-Driven Ergonomic Risk Analysis Using Wearable Sensor Networks and Deep Learning for Injury Prevention in Industrial Workplaces. *American Journal of Data Science and Analytics*, *3*(06), 01-39. https://doi.org/10.63125/61w9ba54
[68]. Md, F., & Islam, M. D. Z. (2022). Quantitative Risk Modeling of VPN Misconfigurations and Firewall Rule Drift in Hybrid Cloud Networks. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 182-216. https://doi.org/10.63125/fa4qdz07
[69]. Md Khaled, H., & Md. Mosheur, R. (2023). Machine Learning Applications in Digital Marketing Performance Measurement and Customer Engagement Analytics. *Review of Applied Science and Technology*, *2*(03), 27–66. https://doi.org/10.63125/hp9ay446
[70]. Md Shahab, U., & Aditya, D. (2023). Risk Mitigation and Resilience Modeling for Consumer Distribution Networks During Demand Shocks: A Quantitative Stochastic Optimization and Scenario Analysis Study. *International Journal of Scientific Interdisciplinary Research*, *4*(2), 01–30. https://doi.org/10.63125/jkevvq84
[71]. Md. Hasan Or, R., Tanjina Binte, S., & Rajib, S. (2023). Performance Analytics Frameworks for Digital Marketing and Service Enterprises: An empirical Study. *American Journal of Data Science and Analytics*, *4*(03), 01-35. https://doi.org/10.63125/aq7y1792
[72]. Md. Mehedi, H., & Khairum Nahar, P. (2023). A Systematic Review of Secure Health Data Information Systems for Pandemic Preparedness and Economic Continuity in the United States. *Review of Applied Science and Technology*, *2*(01), 227–258. https://doi.org/10.63125/77h2m531
[73]. Md. Shahinur, I., & Md. Sultan, M. (2022). Digital-Twin-Based Quantitative Frameworks for Modeling, Monitoring, and Optimization of Electrical Power Infrastructure. *American Journal of Interdisciplinary Studies*, *3*(04), 365-393. https://doi.org/10.63125/dvmj1y93
[74]. Md. Sultan, M., & Anick, K. M. T. A. (2023). High-Performance Computing–Assisted Modeling and Real-Time Analysis of Electrical Power Networks and Industrial Control Systems. *Review of Applied Science and Technology*, *2*(01), 185–226. https://doi.org/10.63125/727j5j39
[75]. Md. Towhidul, I., & Uddin, M. D. S. (2024). Simulation-Based Forecasting and Inventory Control Models For Consumer Goods Networks: A Quantitative Study Using Monte Carlo Simulation and Time-Series Methods. *Review of Applied Science and Technology*, *3*(04), 165–197. https://doi.org/10.63125/a3047d06
[76]. Mohammad Mushfequr, R., & Aditya, D. (2024). Quantitative Assessment of Data Protection Practices In U.S. Revenue Cycle Management. *American Journal of Advanced Technology and Engineering Solutions*, *4*(04), 107-153. https://doi.org/10.63125/fc9hfy54
[77]. Mostafa, K. (2023). An Empirical Evaluation of Machine Learning Techniques for Financial Fraud Detection in Transaction-Level Data. *American Journal of Interdisciplinary Studies*, *4*(04), 210-249. https://doi.org/10.63125/60amyk26

[78]. Mostafa, K., & Md Tohidul, I. (2022). A Quantitative Financial Impact Assessment of Digital Trade Platforms on Export Performance, Capital Efficiency, and Market Competitiveness. *Journal of Sustainable Development and Policy*, *1*(03), 01-26. https://doi.org/10.63125/pt5v9517

[79]. Muthuraj, S., Sethumadhavan, M., Amritha, P., & Santhya, R. (2020). Detection and prevention of attacks on active directory using SIEM. International Conference on Information and Communication Technology for Intelligent Systems,

[80]. Oliveira, N., Praça, I., Maia, E., & Sousa, O. (2021). Intelligent cyber attack detection and classification for network-based intrusion detection systems. *Applied sciences*, *11*(4), 1674.

[81]. Panigrahi, R., Borah, S., Bhoi, A. K., Ijaz, M. F., Pramanik, M., Jhaveri, R. H., & Chowdhary, C. L. (2021). Performance assessment of supervised classifiers for designing intrusion detection systems: a comprehensive review and recommendations for future research. *Mathematics*, *9*(6), 690.

[82]. Panigrahi, R., Borah, S., Pramanik, M., Bhoi, A. K., Barsocchi, P., Nayak, S. R., & Alnumay, W. (2022). Intrusion detection in cyber–physical environment using hybrid Naïve Bayes—Decision table and multi-objective evolutionary feature selection. *Computer Communications*, *188*, 133-144.

[83]. Pinto, R., Gonçalves, G., Delsing, J., & Tovar, E. (2022). Enabling data-driven anomaly detection by design in cyber-physical production systems. *Cybersecurity*, *5*(1), 9.

[84]. Ratul, D., & Aditya, D. (2023). AI-Driven Change Detection Using SAR, LIDAR, And Sentinel-2 Data for Landslide Monitoring and Disaster Early Warning Systems. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 153–188. https://doi.org/10.63125/4y740y95

[85]. Robles-Durazno, A., Moradpoor, N., McWhinnie, J., Russell, G., & Porcel-Bustamante, J. (2021). Implementation and evaluation of physical, hybrid, and virtual testbeds for cybersecurity analysis of industrial control systems. *Symmetry*, *13*(3), 519.

[86]. Sadasivam, G. K., Hota, C., & Anand, B. (2018). Honeynet data analysis and distributed SSH brute-force attacks. In *Towards extensible and adaptable methods in computing* (pp. 107-118). Springer.

[87]. Saghezchi, F. B., Mantas, G., Violas, M. A., de Oliveira Duarte, A. M., & Rodriguez, J. (2022). Machine learning for DDoS attack detection in industry 4.0 CPPSs. *Electronics*, *11*(4), 602.

[88]. Sakib, A. I. M. (2024). Innovative Food Waste Recycling Methods For Agricultural Sustainability: A Systematic Review. *Academic Journal On Business administration, Innovation & Sustainability*, *4*(3), 104-118. https://doi.org/10.69593/ajbais.v4i3.107

[89]. Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: a survey: MM Salim et al. *The Journal of Supercomputing*, *76*(7), 5320-5363.

[90]. Saputra, F. A., Salman, M., Hasim, J. A. N., Nadhori, I. U., & Ramli, K. (2022). The next-generation nids platform: Cloud-based snort nids using containers and big data. *Big Data and Cognitive Computing*, *6*(1), 19.

[91]. Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science*, *171*, 1251-1260.

[92]. Sarhan, M., Layeghy, S., & Portmann, M. (2022a). Evaluating standard feature sets towards increased generalisability and explainability of ML-based network intrusion detection. *Big Data Research*, *30*, 100359.

[93]. Sarhan, M., Layeghy, S., & Portmann, M. (2022b). Towards a standard feature set for network intrusion detection system datasets. *Mobile Networks and Applications*, *27*(1), 357-370.

[94]. Satheesh Kumar, M., Ben-Othman, J., Srinivasagan, K., & Umarani, P. (2022). Machine learning methods for enhanced cyber security intrusion detection system. *Advances in computing, informatics, networking and cybersecurity: a book honoring Professor Mohammad S. Obaidat's significant scientific contributions*, 733-754.

[95]. Sazzadul, I., & Rebeka, S. (2024). VaR and CVaR-Based Stress Testing Using Deep Learning for Liquidity Risk Forecasting and Banking Stability Assessment. *Review of Applied Science and Technology*, *3*(03), 01–30. https://doi.org/10.63125/291phs66

[96]. Sewak, M., Sahay, S. K., & Rathore, H. (2021). Deep reinforcement learning for cybersecurity threat detection and protection: A review. International Conference On Secure Knowledge Management In Artificial Intelligence Era,

[97]. Shah, S. A. R., & Issac, B. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system. *Future Generation Computer Systems*, *80*, 157-170.

[98]. Sharafaldin, I., Habibi Lashkari, A., & Ghorbani, A. A. (2018). A detailed analysis of the cicids2017 data set. International conference on information systems security and privacy,

[99]. Sharma, S., Nand, P., & Sharma, P. (2022). Intrusion detection and prevention systems using snort. In *Advances in Data Science and Management: Proceedings of ICDSM 2021* (pp. 473-486). Springer.

[100]. Shrivastwa, R.-R., Bouakka, Z., Perianin, T., Dislaire, F., Gaudron, T., Souissi, Y., Karray, K., & Guilley, S. (2022). An embedded AI-based smart intrusion detection system for edge-to-cloud systems. International Conference on Cryptography, Codes and Cyber Security,

[101]. Singaravelan, S., Arun, R., Arunshunmugam, D., Joy, S. J. C., & Murugan, D. (2020). Inner interruption discovery and defense system by using data mining. *Journal of King Saud University-Computer and Information Sciences*, *32*(5), 592-598.

[102]. Smadi, A. A., Ajao, B. T., Johnson, B. K., Lei, H., Chakhchoukh, Y., & Abu Al-Haija, Q. (2021). A comprehensive survey on cyber-physical smart grid testbed architectures: Requirements and challenges. *Electronics*, *10*(9), 1043.

[103]. Sun, C.-C., Hahn, A., & Liu, C.-C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45-56.

[104]. Tasnim, K., & Anick, K. M. T. A. (2024). PLC–SCADA–Integrated Electrical Automation Frameworks for Process Optimization in Water and Wastewater Treatment Facilities. *Review of Applied Science and Technology*, *3*(01), 221–262. https://doi.org/10.63125/y1145g11

[105]. Tasnim, K., & Zaheda, K. (2023). A Smart Contract Framework for Automated Settlement and Compliance in Renewable Energy and Distributed Energy Resources. *American Journal of Advanced Technology and Engineering Solutions*, *3*(01), 31-69. https://doi.org/10.63125/fvdjpn66

[106]. Tayfour, O. E., & Marsono, M. N. (2020). Collaborative detection and mitigation of distributed denial-of-service attacks on software-defined network. *Mobile Networks and Applications*, *25*(4), 1338-1347.

[107]. Thakkar, A., & Lohiya, R. (2020). A review of the advancement in intrusion detection datasets. *Procedia Computer Science*, *167*, 636-645.

[108]. Thakkar, A., & Lohiya, R. (2021). Attack classification using feature selection techniques: a comparative study. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 1249-1266.

[109]. Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artificial Intelligence Review*, *55*(1), 453-563.

[110]. Thakur, K., & Kumar, G. (2021). Nature Inspired Techniques and Applications in Intrusion Detection Systems: Recent Progress and Updated Perspective: K. Thakur, G. Kumar. *Archives of Computational Methods in Engineering*, *28*(4), 2897-2919.

[111]. Uçtu, G., Alkan, M., Doğru, İ. A., & Dörterler, M. (2021). A suggested testbed to evaluate multicast network and threat prevention performance of Next Generation Firewalls. *Future Generation Computer Systems*, *124*, 56-67.

[112]. Vaagensmith, B., Singh, V. K., Ivans, R., Marino, D. L., Wickramasinghe, C. S., Lehmer, J., Phillips, T., Rieger, C., & Manic, M. (2021). Review of design elements within power infrastructure cyber–physical test beds as threat analysis environments. *Energies*, *14*(5), 1409.

[113]. Virupakshar, K. B., Asundi, M., Channal, K., Shettar, P., Patil, S., & Narayan, D. (2020). Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud. *Procedia Computer Science*, *167*, 2297-2307.

[114]. Wang, H., Gu, J., & Wang, S. (2017). An effective intrusion detection framework based on SVM with feature augmentation. *Knowledge-Based Systems*, *136*, 130-139.

[115]. Xiao, Y., Fan, Z.-j., Nayak, A., & Tan, C.-x. (2019). Discovery method for distributed denial-of-service attack behavior in SDNs using a feature-pattern graph model. *Frontiers of Information Technology & Electronic Engineering*, *20*(9), 1195-1208.

[116]. Yinka-Banjo, C., Alli, P., Misra, S., Oluranti, J., & Ahuja, R. (2022). Intrusion detection using anomaly detection algorithm and snort. In *Illumination of Artificial Intelligence in Cybersecurity and Forensics* (pp. 45-70). Springer.

[117]. Zaheda, K., & Md Hamidur, R. (2024). GPU-Accelerated Physics-Informed Digital Twins for Real-Time State Estimation and Fault Localization in Distribution Grids. *American Journal of Scholarly Research and Innovation*, *3*(02), 179-216. https://doi.org/10.63125/msrpfb04

[118]. Zaheda, K., & Md. Tahmid Farabe, S. (2023). Robotics and Computer Vision for Automated Inspection of Substation and Treatment-Facility Electrical Infrastructure. *Review of Applied Science and Technology*, *2*(04), 194-227. https://doi.org/10.63125/tfh15j12

[119]. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & De Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, 25-37.

[120]. Zhiqiang, L., Mohiuddin, G., Jiangbin, Z., Asim, M., & Sifei, W. (2022). Intrusion detection in wireless sensor network using enhanced empirical based component analysis. *Future Generation Computer Systems*, *135*, 181-193.