www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, Decembaer 2024, pp : 1524-1537

e-ISSN : 2583-1062
Impact Factor : 7.001

ADVANCEMENTS IN INTRUSION DETECTION SYSTEMS: EXPLORING CONCEPTS, INNOVATIONS, METRICS, BENCHMARKS, TRENDS, DIRECTIONS, APPLICATIONS AND CHALLENGES

Lingala Thirupathi[1], Dr. Thejoram Naresh Reddy Boya[2], Vineetha Kaashipaka[3], Ashok Galipelli[4], Nagaraju M[5], Bhukya Raju[6], N. Vinay Kumar[7], Radhika Pulyala[8]

[1]Department of AI & ML, Sreenidhi Institute of Science & Technology, Hyderabad, Telangana, India.
thiru1274@gmail.com

[2]Department of CSE, Aurora's Technological & Research Institute, Hyderabad, Telangana, India.
btrnareshreddy@gmail.com

[3]Department of ECE, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India.
Kashipaka.vineetha@gmail.com

[4]Department of AI & ML, Geethanjali College of Engineering and Technology. Hyderabad, Telangana, India.
gashok.cse@gcet.edu.in

[5]Department of IT, Sreenidhi Institute of Science & Technology, Hyderabad, Telangana, India.
nagarajucse11@gmail.com

[6,7]Department of AI & ML, Sreenidhi Institute of Science & Technology, Hyderabad, Telangana, India.
raju.b@gmail.com, nyatha_vinaykumar@yahoo.com

[8]Department of Cyber Security, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India.
pulyalaradhika@gmail.com

DOI: https://www.doi.org/10.58257/IJPREMS37855

ABSTRACT

This article delves into the dynamic landscape of Intrusion Detection Systems (IDS), focusing on advancements in concepts, innovations, solutions, metrics, benchmarks, trends, directions, and challenges. Beginning with an exploration of fundamental concepts, it navigates through cutting-edge innovations designed to enhance IDS capabilities. The study emphasizes the importance of metrics and benchmarks in evaluating IDS performance, identifying key indicators for effectiveness assessment. Furthermore, it analyzes prevailing trends and forecasts future directions in IDS development, offering valuable insights for cyber-security stakeholders. Despite strides in IDS evolution, challenges such as scalability and evolving threat landscapes persist, highlighting areas for improvement. Overall, this research serves as a comprehensive resource for cyber-security professionals, researchers, and practitioners, fostering dialogue and innovation to advance the effectiveness and resilience of IDS in combating cyber threats.

Key words- Intrusion Detection Systems (IDS), Innovations, Metrics, Challenges, Cyber-security.

1. INTRODUCTION

In today's dynamic cyber security landscape, the importance of Intrusion Detection Systems (IDS) is undeniable. With cyber threats growing in sophistication, the necessity for resilient and adaptive IDS technologies has become critical. This paper delves into advancements in IDS, exploring concepts, innovations, metrics, benchmarks, trends, applications, and challenges. At its core, an IDS acts as a vigilant sentinel, continuously monitoring network or system activities to detect signs of malicious behavior. Integral to cyber-security frameworks, IDS serves as a diligent gatekeeper, protecting digital assets and infrastructure from diverse threats.

Traditional IDS methodologies encompass two primary approaches: signature-based detection and anomaly-based detection. Signature-based detection operates on the premise of recognizing predefined patterns or signatures of known attacks. By comparing network traffic or system events against an extensive database of signatures, this approach can swiftly identify and mitigate known threats. While effective against well-established attack vectors, signature-based detection can be vulnerable to zero-day exploits and polymorphic malware that evade signature recognition.Anomaly-based detection, on the other hand, takes a different approach by scrutinizing deviations from normal behavior. By establishing a baseline of typical network or system activity, anomaly-based IDSs flag any aberrations or outliers that diverge from expected patterns. This technique is particularly adept at identifying novel or previously unseen threats that elude signature-based detection. However, anomaly-based detection may generate false positives if legitimate activities deviate from established norms or if the baseline is inadequately calibrated.

Recognizing the limitations of traditional IDS approaches, recent years have witnessed a paradigm shift towards hybrid IDS solutions. These innovative systems amalgamate the strengths of signature-based and anomaly-based detection while mitigating their respective weaknesses. By leveraging a diverse array of detection techniques, including statistical analysis, machine learning algorithms, and behavioral profiling, hybrid IDSs can achieve heightened accuracy and effectiveness in threat detection. Hybrid IDS solutions offer several advantages over their traditional counterparts. Firstly, by employing a multifaceted approach to threat detection, these systems can cast a wider net and identify a broader spectrum of threats, ranging from known exploits to zero-day vulnerabilities. Secondly, hybrid IDSs exhibit greater resilience against evasion tactics employed by sophisticated attackers, as they do not rely solely on fixed signatures or predetermined baselines. Instead, they adapt and evolve in response to emerging threats and evolving attack vectors. It has the flexibility to tailor their detection strategies to the unique requirements and nuances of diverse environments and threat landscapes. Whether deployed in enterprise networks, cloud environments, or industrial control systems, these adaptive systems can adjust their detection thresholds, algorithms, and models to optimize performance and minimize false positives.

The landscape of IDS is in a perpetual state of evolution, spurred on by constant innovations and technological advancements. One particularly noteworthy trend shaping the trajectory of IDS is the integration of Artificial Intelligence (AI) and Machine Learning (ML) techniques into IDS frameworks. This convergence marks a significant paradigm shift in the field of cyber-security, offering unprecedented capabilities and opportunities to fortify defenses against ever-evolving cyber threats. AI-powered IDS systems represent a new frontier in threat detection and mitigation. Unlike conventional IDS approaches that rely on static rules or signatures to identify known threats, AI-enabled IDS systems possess the ability to autonomously learn and adapt from vast datasets. By leveraging sophisticated ML algorithms, these systems can discern complex patterns and correlations within network traffic or system behavior, enabling them to detect subtle anomalies indicative of potential security breaches.

One of the key advantages of AI-powered IDS lies in its capacity to adapt to dynamic and evolving threat landscapes. Traditional IDS solutions often struggle to keep pace with the rapid evolution of cyber threats, requiring frequent updates and manual intervention to remain effective. In contrast, AI-enabled IDS systems can continuously learn from new data and evolving attack tactics, allowing them to dynamically adjust their detection strategies in real-time. This adaptive capability enhances the resilience of IDS against emerging threats, including zero-day exploits and polymorphic malware. Moreover, AI-powered IDS systems are adept at making real-time decisions based on the insights gleaned from ML models. By analyzing vast volumes of data at lightning speed, these systems can swiftly identify and respond to security incidents, minimizing the time between detection and mitigation. This real-time responsiveness is critical in mitigating the impact of cyber attacks and reducing the window of vulnerability for organizations. It offers the promise of enhanced accuracy and efficacy in threat detection. ML algorithms excel at discerning subtle patterns and anomalies within complex datasets, enabling IDS to differentiate between genuine security threats and benign anomalies. This heightened accuracy helps organizations prioritize and respond to security incidents more effectively, reducing false positives and minimizing the risk of overlooking genuine threats.

Measuring the efficacy and performance of IDS is paramount in gauging their ability to effectively detect and mitigate cyber threats. In the dynamic landscape of cyber security, where the nature and sophistication of attacks are constantly evolving, accurate assessment metrics play a crucial role in evaluating the effectiveness of IDS solutions. Various metrics and benchmarks have been developed to comprehensively evaluate IDS performance across different dimensions, including detection accuracy, false positive rates, response time, and scalability. Detection accuracy stands as one of the primary metrics used to assess the effectiveness of an IDS. This metric measures the system's ability to accurately identify and classify security incidents, including both true positive detections of actual threats and true negative identifications of benign activities. High detection accuracy indicates that the IDS is adept at discerning genuine security threats from normal network or system behavior, thus minimizing the risk of overlooking critical security incidents.

False positive rates represent another key metric in evaluating IDS performance. False positives occur when the system incorrectly flags benign activities as security threats, leading to unnecessary alerts and potentially overwhelming security personnel with false alarms. A low false positive rate is indicative of an IDS that can effectively differentiate between genuine security threats and benign anomalies, thereby reducing the burden of false alarms on security operations. Response time is another critical metric that measures the speed at which an IDS detects and responds to security incidents. In the context of cyber attacks, swift detection and response are imperative in mitigating the impact of security breaches and minimizing potential damage. IDS solutions with shorter response times can swiftly identify and contain security threats, thereby reducing the window of vulnerability for organizations and limiting the scope of potential damage.

Scalability is also an essential consideration when evaluating IDS performance, especially in large-scale enterprise environments or networks with high volumes of traffic. Scalability metrics assess the ability of IDS to efficiently handle increasing workloads and adapt to growing network demands without sacrificing performance or accuracy. Scalable IDS can effectively accommodate expanding network infrastructures and evolving threat landscapes, ensuring continued effectiveness and relevance in dynamic cyber security environments. Understanding and effectively utilizing these metrics is essential for benchmarking IDS solutions and comparing their performance across different environments. By comprehensively evaluating IDS performance across multiple dimensions, organizations can make informed decisions regarding the selection, deployment, and optimization of IDS solutions that best meet their security requirements and operational needs. Ultimately, robust assessment metrics enable organizations to enhance their cyber-security posture and effectively mitigate the risks posed by cyber threats.

The landscape of IDS is undergoing significant transformation, marked by several notable trends and directions that are shaping the future of cyber-security. One prominent trend in recent years is the increasing adoption of cloud-based IDS solutions. Organizations are leveraging the scalability and flexibility offered by cloud computing infrastructure to deploy IDS systems that can effectively monitor and protect their digital assets across distributed and dynamic cloud environments. Cloud-based IDS solutions offer several advantages over traditional on-premises deployments. By harnessing the resources of cloud platforms, organizations can rapidly scale their IDS infrastructure to accommodate fluctuating workloads and evolving threat landscapes. This scalability enables organizations to effectively monitor large volumes of network traffic and respond to security incidents in real-time, without the need for significant upfront investments in hardware or infrastructure. It provides enhanced visibility and control over cloud-based resources, allowing organizations to centrally manage and monitor security policies across diverse cloud environments. This centralized approach streamlines security operations, facilitates compliance with regulatory requirements, and enables organizations to enforce consistent security measures across their entire cloud infrastructure.

An emerging trend in IDS is the increasing emphasis on specialized solutions designed for the distinct challenges presented by the Internet of Things (IoT) and Industrial Control Systems (ICS). The rise of IoT devices and industrial automation has broadened the attack surface and introduced new security vulnerabilities, which traditional IDS solutions may find challenging to mitigate effectively. To tackle these hurdles, IDS solutions tailored for IoT and ICS environments are under development. These solutions incorporate advanced capabilities for monitoring and securing IoT devices, industrial networks, and critical infrastructure. They leverage techniques such as deep packet inspection, behavior analysis, and anomaly detection to detect and mitigate threats targeting IoT devices and industrial control systems.

Moreover, specialized IDS solutions for IoT and ICS environments often feature built-in support for industry-specific protocols and communication standards, enabling seamless integration with existing IoT and industrial automation systems. This integration ensures compatibility and interoperability with diverse IoT devices and industrial equipment, while also facilitating centralized management and monitoring of security policies across heterogeneous environments. IDS play a pivotal role in safeguarding digital assets and infrastructure across diverse sectors, including finance, healthcare, government, and critical infrastructure. These sectors rely heavily on digital systems and networks to support their operations, making them prime targets for cyber attacks. IDS technologies offer a critical layer of defense by continuously monitoring network and system activities for signs of malicious or suspicious behavior.

In the finance sector, IDS solutions are essential for protecting sensitive financial data, preventing unauthorized access to banking systems, and detecting fraudulent activities such as phishing attacks and identity theft. Similarly, in the healthcare industry, IDS systems help safeguard electronic health records (EHRs), medical devices, and patient information from cyber threats. By monitoring network traffic and detecting anomalous behavior, IDS solutions can mitigate the risk of data breaches and ensure the integrity and confidentiality of patient data. In government agencies, IDS technologies are deployed to protect classified information, national security systems, and critical infrastructure from cyber attacks launched by nation-state actors, cybercriminals, and other malicious entities. By providing real-time threat detection and incident response capabilities, IDS solutions help government organizations detect and thwart cyber threats before they can cause significant damage or disruption.

In critical infrastructure sectors such as energy, transportation, and telecommunications, IDS systems play a vital role in ensuring the reliability and resilience of essential services and networks. These sectors are increasingly reliant on interconnected digital systems and Industrial Control Systems (ICS), making them vulnerable to cyber attacks that could disrupt operations and impact public safety. IDS technologies help identify and mitigate cyber threats targeting critical infrastructure assets, such as power plants, transportation networks, and communication systems, thereby safeguarding against potential cyber-physical attacks. However, deploying effective IDS solutions poses significant

challenges for organizations across all sectors. One such challenge is the need for real-time threat detection, especially in environments where even a slight delay in identifying and responding to security incidents can have serious consequences. IDS solutions must be capable of rapidly analyzing large volumes of network traffic and detecting emerging threats in real-time to minimize the risk of data breaches and system compromises.

Handling large volumes of data is another challenge faced by organizations deploying IDS solutions, particularly in high-traffic environments such as data centers, cloud infrastructure, and IoT networks. IDS systems must be able to efficiently process and analyze massive amounts of network traffic without impacting performance or introducing latency. This requires robust data processing capabilities and scalable architectures that can handle the demands of modern network environments. Ensuring compatibility with existing systems is another challenge in deploying IDS solutions, particularly in heterogeneous IT environments with diverse operating systems, applications, and network infrastructure. IDS technologies must be compatible with a wide range of platforms and protocols to effectively monitor and protect the entire network infrastructure. This requires interoperability with existing security tools, network devices, and management systems to ensure seamless integration and operation.

Addressing privacy and compliance requirements is yet another challenge in deploying IDS solutions, particularly in sectors such as healthcare and finance where regulations such as HIPAA and PCI-DSS impose stringent requirements for data protection and privacy. IDS technologies must comply with regulatory standards and industry best practices to ensure the confidentiality, integrity, and availability of sensitive data while also preserving individual privacy rights. The evolution of Intrusion Detection Systems signifies a quest for innovation against cyber threats. Traditional methods provide a foundation, while hybrid solutions enhance cyber security by integrating adaptability. The integration of AI and ML techniques revolutionizes threat detection, offering real-time precision. AI-enabled IDS fortifies defenses, confronting sophisticated threats effectively. Rapidly evolving in response to emerging technologies, IDS trends include cloud-based solutions and specialized IoT and ICS systems. Embracing these trends strengthens cyber security posture, mitigates risks, and protects critical assets against evolving threats.

2. LITERATURE SURVEY

In [1], the authors underscore the necessity of IDS in ad hoc networks despite existing security measures. It surveys IDS components, taxonomies, and architectures, introducing MSDAR, a dynamic IDS combining signature-based and anomaly detection. MSDAR's efficacy against attacks is validated through simulations, showcasing improved performance and sensitivity. In [2], the author outlines the rise of IoT technology and its challenges, such as privacy and security concerns. It suggests block chain integration as a solution but notes vulnerabilities revealed by DDoS attacks. To tackle this, it proposes a distributed IDS using fog computing, assessed with machine learning on real IoT data. Results show Random Forest's efficiency for multi-attack detection and XG Boost's superiority for binary detection on distributed fog nodes.

In [3], explores the integration of Distributed Ledger Technology (DLT) into Collaborative IDS for anomaly detection in IoT networks. Leveraging DLT, CIDS enhances detection accuracy and speed, addressing cyber-security challenges inherent in complex IoT ecosystems. By examining placement strategies, detection methods, security threats, and validation/testing approaches, the review offers insights into optimizing CIDS with DLT. Addressing open issues and lessons learned, it informs future research and aids professionals in crafting effective CIDS solutions tailored for IoT environments. The article [4] advocates quantifying POD and NAR while validating intrusion recognition algorithms in real-world scenarios. It also explores LC-based intrusion detection and CNN architectures to boost security. In [5], explores employing the Random Forest algorithm to build a robust IDS. By amalgamating decision trees, the algorithm creates a precise classifier capable of handling complex network data. This innovative approach promises to fortify critical assets across industries, ensuring uninterrupted network operations. With cyber threats evolving continuously, ongoing exploration into ensemble analytics methodologies are imperative to bolster IDS resilience in a dynamic threat landscape.

This study explores intrusion detection using supervised machine learning, establishing taxonomy for related systems and algorithms. It examines intrusion detection fundamentals, supervised learning techniques, and cyber threats. It highlights strong classification performance, emphasizes feature selection, addresses data imbalance, and underscores the efficacy of deep learning on large datasets [6]. Explores [7] intrusion detection using supervised machine learning methods, aiming to categorize associated systems and algorithms. It discusses intrusion detection concepts, supervised ML techniques, and cyber-security attacks, presenting a taxonomy based on related works. It highlights promising classification performance of supervised learning algorithms on different datasets like KDD’99, NSL-KDD, CICIDS2017, and UNSW-NB15. The study underscores the significance of feature selection for performance

enhancement, addresses data imbalance concerns, and advocates for deep learning techniques on large intrusion detection datasets.

Reviews [8] feature selection and ensemble techniques in anomaly-based IDS research, emphasizing their impact on detection accuracy and computational efficiency. Highlighting the importance of selecting relevant features, it explores various ML techniques, particularly ensemble methods, to enhance IDS performance. The review underscores the significance of ensemble techniques in improving anomaly-based IDS models and suggests future research directions to address ongoing challenges in IDS design. Focuses on host-based IDS, analyzing 21 studies from 2020 to 2023 to address research questions and identify areas for improvement in HIDS technology [9]. Traditional IDS struggle with static security, unable to handle real-time threats or zero-day attacks. Anomaly detection offers hope, but current methods often lag. Their research addresses these challenges, outlining IoT cyber security risks, proposing real-time IDS strategies, and providing a dynamic dataset for community-wide security evaluations [10].

Surveys IDS methodologies from 2008 to 2020, emphasizing feature selection for enhanced performance and discussing IDS datasets, including CIC IDS-2017, as well as challenges and future directions, serving as a valuable resource for network security research [11]. Surveys recent NIDS literature, examining challenges in adapting adversarial learning from Computer Vision, discussing attack methods, defenses, and research trends since 2015 [12]. In [13], in an era of growing dependence on networks, rapid and efficient data transmission is paramount. Intrusion detection systems are essential for identifying unauthorized activities that jeopardize security. Despite security improvements, persistent attacks necessitate robust intrusion detection systems. This article aims to review various approaches and systems, addressing evolving network security challenges.

Propose a method employing various machine learning algorithms to classify normal and attack data, thereby improving anomaly-based intrusion detection accuracy. They validated the approach using the ADFA Linux Dataset, containing system call traces for attacks on modern operating systems. Additionally, they developed and simulated models for host-based intrusion detection systems using ML algorithms in the Arena simulation tool to detect and classify anomalies [14]. Survey [15] reveals significant findings, including unexpectedly high performance scores possibly due to over fitting, unaddressed class imbalance issues, and inadequate data cleaning documentation, raising concerns about experiment reproducibility. Major research gaps are also highlighted. Presents a systematic review of ML and DL methods in intrusion detection, covering benchmark datasets, evaluation metrics, and DL applications. It summarizes recent findings, compares experimental results, and identifies current challenges in DL-based intrusion detection research [16].

Focuses on implementing Software-Defined Network (SDN) in IoT networks, reducing hardware costs significantly. It explores IDS applications in SDN-based IoT networks through various studies, aiming to identify new research directions. Additionally, the paper introduces block chain as a security enhancement for SDN-based IoT networks [17]. It employs systematic literature review to classify and analyze IDS techniques in IoT, categorizing them as signature-based, anomaly-based, specification-based, or hybrid, and assessing their benefits, drawbacks, and potential future directions [18]. It provides a detailed overview of intrusion detection using ML techniques, outlining their steps for intrusion detection and classification. It offers insights into state-of-the-art ML techniques, their advantages, limitations, and summarizes research on ML-based IDS. The paper addresses challenges and suggests future research directions to enhance IDS efficiency. It serves as a valuable resource for novice researchers in ML-based IDS [19]. Outlines taxonomy of contemporary IDS, reviews recent notable works, and discusses commonly used datasets for evaluation. It also addresses evasion techniques employed by attackers to evade detection and highlights future research challenges in countering these techniques to enhance computer system security [20].

This article [21] clarifies IDS concepts, provides taxonomy of ML and DL techniques in Network-based IDS (NIDS), reviews recent NIDS-based research, discusses strengths and limitations, and highlights research challenges and future directions for enhancing ML and DL-based NID. This study [22] offers an overview of network intrusion detection models within the realm of big data. It surveys a broad range of intrusion detection techniques, including data mining, ML, and deep learning, emphasizing their application in addressing network security challenges amidst increasing data volumes and evolving network landscapes.

3. OBJECTIVES

1. To explore the foundational concepts and fundamental principles underpinning IDS
2. To examine the latest advancements in IDS.
3. To forecast future directions and potential innovations in IDS development.
4. To address challenges and constraints encountered in contemporary IDS implementations.

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 12, Decembaer 2024, pp : 1524-1537
e-ISSN : 2583-1062
Impact Factor : 7.001

4. RELATED WORKS

The architecture of IDS involves representing the sequential steps and interactions between its key components. Here's a simplified flowchart outlining the typical architecture of IDS in Figure 1.

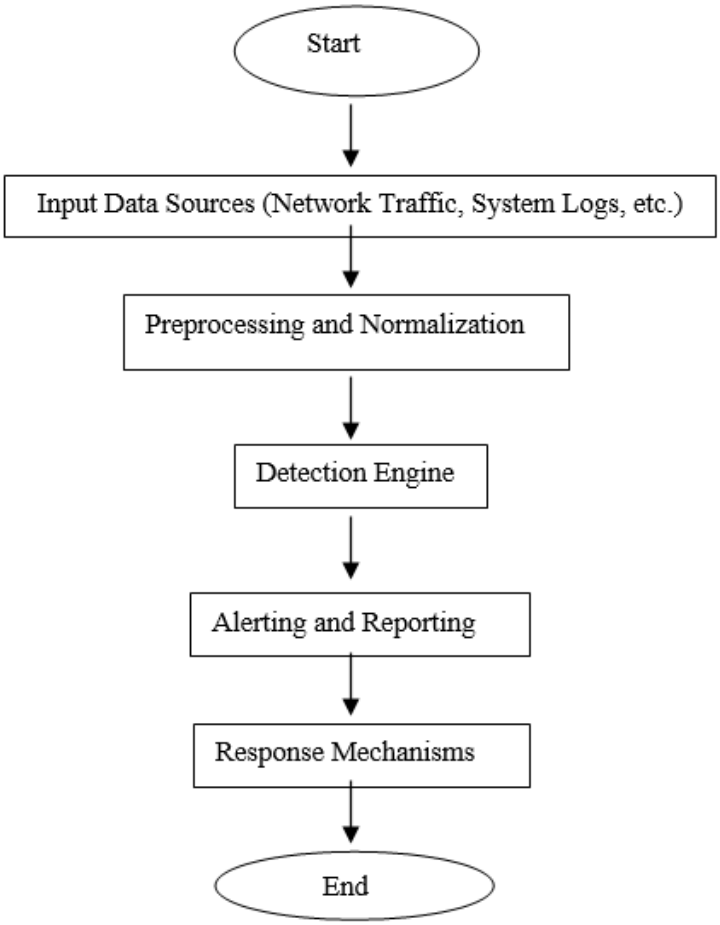

Figure 1: IDS Framework

Input Data Sources: This represents the initial step where data is collected from various sources within the network, such as network traffic, system logs, and application activity. These data sources serve as inputs to the IDS for analysis. Preprocessing and Normalization: The collected data undergoes preprocessing and normalization to convert raw data into a standardized format suitable for analysis. This step involves parsing, cleaning, and enriching data to remove noise, standardize data formats, and extract relevant information. Detection Engine: The preprocessed and normalized data is analyzed by the detection engine, which applies detection algorithms and signatures to identify potential security threats and anomalies. Detection techniques may include signature-based detection, anomaly detection, behavior analysis, and machine learning algorithms.

Alerting and Reporting: When the detection engine identifies suspicious activity or security events, it generates alerts and reports to notify security personnel of potential threats. Alerts include detailed information about the detected event, such as the type of attack, source and destination IP addresses, timestamp, and severity level. Response Mechanisms: IDS may include built-in response mechanisms to automatically respond to detected threats or security incidents. Response actions can range from simple actions like logging the event and blocking IP addresses to more complex actions like quarantining compromised devices or triggering automated incident response workflows.

4.1 Foundational concepts and fundamental principles underpinning IDS

Exploring the foundational concepts and fundamental principles underpinning IDS involves delving into the technical intricacies of network traffic analysis, detection methodologies, and their integration into comprehensive cyber-security frameworks. Network traffic analysis forms the backbone of IDS operation, wherein packets traversing a network are scrutinized for anomalies or suspicious patterns indicative of unauthorized access or malicious activity. This analysis requires a deep understanding of network protocols, packet structures, and traffic behavior to effectively identify security threats.

Two primary categories of IDS—signature-based and anomaly-based—employ distinct detection mechanisms. Signature-based IDS utilize predefined signatures or patterns of known attacks, matching incoming traffic against these signatures to detect threats. Anomaly-based IDS, on the other hand, analyze deviations from normal network behavior, leveraging statistical analysis, machine learning algorithms, or rule-based systems to identify potential threats. IDS detection techniques efficacy relies on factors like detection accuracy, computational demands, and managing false positives versus false negatives. Striking a balance is vital to enhance IDS performance without overwhelming security teams with false alerts or missing genuine threats. IDS functions within cyber-security broader framework, alongside tools like firewalls and antivirus software. Seamless integration into this ecosystem demands precise coordination for effective communication and response to security incidents. Achieving this orchestration is crucial to fortify defenses against evolving cyber threats, safeguarding digital assets and infrastructure.

The evolving threat landscape presents a significant challenge for IDS, necessitating continuous adaptation and updates to detect emerging threats effectively. Staying abreast of the latest threat intelligence, refining detection mechanisms, and regularly updating IDS configurations and signatures are essential for mitigating new attack vectors and safeguarding networks against evolving threats. In essence, exploring the technical intricacies of IDS—from network traffic analysis to detection methodologies and integration into broader security frameworks—provides valuable insights into building robust defense mechanisms against increasingly sophisticated cyber threats. Continuous learning, adaptation, and collaboration across security tools and teams are crucial for maintaining effective cyber-security posture in dynamic and hostile environments.

5. LATEST ADVANCEMENTS IN IDS

5.1. Machine Learning and Artificial Intelligence:

The latest advancements in IDS leveraging ML & AI have significantly transformed the landscape of cyber security. Here's an examination of these advancements shown in Table1.

Table 1. Latest advancements in IDS using ML and AI.

No.	Key Advancement	Description
1	Enhanced Threat Detection Accuracy	ML and AI algorithms have transformed IDS, enhancing threat detection accuracy and adaptability. Unlike traditional systems reliant on static signatures, ML-based IDS analyze extensive data, learning historical patterns to identify subtle anomalies, thereby improving accuracy and reducing false alarms, bolstering security.
2	Detection of Complex Threats	ML and AI excel in spotting intricate, novel threats evading traditional methods. Deep learning models like Convolution Neural Networks and Recurrent Neural Networks adeptly analyze diverse, high-dimensional data like network traffic and system event logs, pinpointing patterns signaling advanced attacks like zero-day exploits, polymorphic malware, and insider threats.
3	Behavioral Analysis and Anomaly Detection	ML-based IDS utilize behavioral analysis and anomaly detection to spot deviations from typical network behavior. Establishing baselines of user and system behavior, these systems detect anomalies signaling intrusions or insider threats. ML algorithms analyze diverse behavioral attributes like login patterns, file access, and network traffic to flag suspicious activities indicating security breaches.
4	Dynamic Adaptation to Evolving Threats	ML-based IDS systems dynamically adjust to evolving threats. Unlike traditional methods needing manual updates for new threats, ML algorithms continually learn from data, adapting detection strategies. This adaptability allows IDS to spot emerging threats like new malware or sophisticated attacks without human intervention or predefined signatures.
5	Reduced False Positives and Improved Response Times	ML-based IDS systems enhance efficiency by minimizing false positives and expediting responses. They prioritize alerts accurately and automate actions, analyzing context and correlating events across data sources to distinguish real threats from benign anomalies. This eases the burden on security teams, enabling timely focus on investigating and mitigating genuine threats.

No.	Key Advancement	Description
6	Scalability and Efficiency	ML-based IDS systems provide scalability and efficiency, analyzing vast network data volumes in real-time. Leveraging distributed computing and cloud resources, they process data effectively. ML algorithms, trained on diverse datasets, enable IDS to adapt to unique network characteristics, addressing each organization's infrastructure challenges effectively.

5.2. Behavioral Analysis: Traditional signature-based IDS rely on predefined patterns or signatures of known attacks, which may not detect novel or previously unseen threats. Behavioral analysis techniques analyze the behavior of users and systems to detect anomalies indicative of potential intrusions. By establishing baselines of normal behavior, IDS can identify deviations and flag suspicious activities for further investigation.

The latest advancements in IDS utilizing behavioral analysis have significantly enhanced the ability to detect and respond to cyber threats. Here's an examination of these advancements:

5.2.1. Granular Insight into User and System Behavior: Behavioral analysis techniques provide granular insight into user and system behavior within the network environment. By monitoring activities such as user logins, file access patterns, application usage, and network traffic behavior, IDS can establish baselines of normal behavior for individual users, devices, and applications. This allows the system to detect deviations or anomalies that may indicate potential security breaches or insider threats.

5.2.2 Anomaly Detection and Threat Identification: Behavioral analysis enables IDS to identify anomalous behavior that deviates from established baselines. By leveraging statistical analysis, machine learning algorithms, and heuristic rules, IDS can detect unusual patterns or deviations in user behavior, system interactions, and network traffic. These anomalies may include unauthorized access attempts, unusual file modifications, abnormal resource usage, or suspicious network communication, which could indicate the presence of malware, unauthorized access attempts.

5.2.3. Dynamic Profiling and Adaptive Learning: Advanced IDS systems employ dynamic profiling and adaptive learning techniques to continuously update and refine behavioral baselines. Instead of relying on static profiles, these systems dynamically adjust baseline models based on evolving user and system behavior. By continuously learning from new data and adapting to changes in the network environment, IDS can better differentiate between normal and suspicious behavior, reducing false positives and improving detection accuracy.

5.2.4. Contextual Analysis and Correlation: Behavioral analysis techniques enable IDS to perform contextual analysis and correlation of security events across multiple data sources. By correlating behavioral patterns with contextual information such as user roles, device attributes, network topology, and threat intelligence feeds, IDS can gain deeper insights into the nature and severity of security incidents. This contextual analysis helps prioritize alerts, identify patterns of coordinated attacks, and distinguish between benign anomalies and genuine security threats.

5.2.5. Operational Efficiency and Incident Response: Behavioral analysis enhances IDS efficiency and incident response by automating security incident detection and investigation. Leveraging behavioral indicators and anomaly detection, IDS produces actionable alerts, triggers automated responses, and offers analysts contextual insights for swift incident triage. This reduces manual analysis efforts, enabling focused mitigation of genuine threats.

5.3. Cloud-Based IDS: With the increasing adoption of cloud computing and infrastructure-as-a-service (IaaS) platforms, there's a growing need for IDS solutions designed specifically for cloud environments. Cloud-based IDS offer scalability, flexibility, and visibility into network traffic across distributed and dynamic cloud infrastructures. These solutions leverage cloud-native technologies and integrations with platform-as-a-service (PaaS) offerings to provide comprehensive threat detection and response capabilities.

The latest advancements in IDS leveraging Cloud-Based IDS have introduced innovative approaches to protect cloud environments and address the evolving threat landscape. Here's an examination of these advancements:

5.3.1. Scalability and Flexibility: Cloud-Based IDS offer scalability and flexibility, allowing organizations to deploy IDS solutions that can dynamically scale with their cloud infrastructure. Unlike traditional on-premises IDS deployments, which may be limited by hardware resources and capacity constraints, Cloud-Based IDS leverage cloud computing resources to scale horizontally or vertically based on demand. This enables organizations to handle fluctuating workloads, accommodate rapid growth, and adapt to changing network environments without compromising detection capabilities.

5.3.2. Visibility Across Distributed Environments: Cloud-Based IDS provide enhanced visibility into network traffic across distributed and dynamic cloud environments. By integrating with cloud-native monitoring and logging services, such as Amazon VPC Flow Logs, Azure Network Watcher, or Google Cloud Audit Logs, IDS can analyze network traffic flows, API calls, and infrastructure events in real-time. This visibility extends to multi-cloud and hybrid cloud environments, enabling organizations to monitor and protect their assets regardless of their deployment model.

5.3.3. Native Integration with Cloud Platforms: Cloud-Based IDS integrate seamlessly with cloud platforms and services, leveraging native APIs and integrations to enhance threat detection capabilities. These integrations allow IDS to leverage cloud-native security controls, such as AWS Security Groups, Azure Security Center, or Google Cloud IAM, to enforce network segmentation, control access, and enforce security policies. By leveraging platform-as-a-service (PaaS) offerings and infrastructure-as-code (IaC) tools, organizations can automate the deployment and configuration of IDS solutions, reducing operational overhead and ensuring consistency across cloud environments.

5.3.4. Real-Time Threat Detection and Response: Cloud-Based IDS enable real-time threat detection and response in cloud environments, leveraging cloud-native technologies and automation capabilities to accelerate incident detection and response. By analyzing network traffic, API calls, and infrastructure logs in real-time, IDS can detect suspicious activities, unauthorized access attempts, and potential security breaches as they occur. Automated response actions, such as blocking malicious IP addresses, isolating compromised instances, or triggering alerts to security teams, help mitigate threats before they escalate.

5.3.5. Compliance and Governance: Cloud-Based IDS assist organizations in meeting compliance requirements and enforcing governance policies in cloud environments. By monitoring network traffic and auditing infrastructure configurations, IDS can help organizations identify security miss configurations, policy violations, and compliance gaps. Additionally, Cloud-Based IDS provide audit trails, forensic capabilities, and reporting tools to support incident investigation, regulatory compliance, and security audit requirements.

5.3.6. Cost-Effective Security: Cloud-Based IDS offer cost-effective security solutions by leveraging pay-as-you-go pricing models and avoiding upfront hardware investments. Organizations can benefit from the elasticity and cost efficiency of cloud computing, scaling IDS resources up or down based on workload demands and optimizing resource utilization to meet budgetary constraints. Additionally, Cloud-Based IDS reduce the need for maintenance, upgrades, and patching, as cloud service providers manage underlying infrastructure and software updates, freeing up resources for strategic security initiatives.

5.4. Threat Intelligence Integration: IDS are increasingly integrating with threat intelligence feeds to enhance detection capabilities and prioritize alerts based on the relevance and severity of threats. By leveraging up-to-date threat intelligence from external sources such as security vendors, government agencies, and industry groups, IDS can better identify emerging threats and proactively guard against virtual attacks.

The latest advancements in IDS utilizing Threat Intelligence Integration have significantly enhanced the ability to detect and respond to cyber threats in real-time. Here's an examination of these advancements:

5.4.1. Up-to-Date Threat Intelligence Feeds: IDS systems are now integrating with a wide range of threat intelligence feeds, providing access to up-to-date information on known threats, vulnerabilities, and indicators of compromise (IOCs). These feeds are sourced from reputable sources such as security vendors, government agencies, industry groups, and open-source threat intelligence platforms. By ingesting and correlating threat intelligence data with network traffic, IDS can identify and prioritize alerts based on the relevance and severity of threats.

5.4.2. Enhanced Detection Capabilities: Integrating threat intelligence bolsters IDS detection, enriching network analysis with external insights. Correlating activity with threat indicators, IDS spots suspicious patterns and compromise signs like malware or malicious IPs. This proactive stance enhances threat detection, slashing response times, and mitigating security incidents' impact efficiently.

5.4.3. Automated Threat Response: Integrated with threat intelligence feeds, IDS systems automate response actions according to preset rules. These may involve blocking malicious IPs, quarantining compromised devices, or adjusting firewall rules to thwart attacks. Automating responses slashes reaction times, curbs threat escalation, and lightens security teams' workload for strategic initiatives.

5.4.4. Threat Hunting and Investigation: Integrating threat intelligence empowers IDS for threat hunting and investigations, offering analysts actionable insights. Detailed alerts with enriched data, including indicators of compromise and attack patterns, enable efficient root cause analysis. This equips analysts to correlate events, identify security incidents' origins, and conduct thorough investigations with ease.

5.4.5. Collaborative Threat Intelligence Sharing: IDS systems facilitate collaborative threat intelligence sharing among organizations, industry partners, and cyber-security communities. By participating in threat intelligence sharing

platforms and information-sharing and analysis centers (ISACs), organizations can contribute and receive timely threat intelligence updates, share insights on emerging threats, and collaborate on joint threat mitigation efforts. This collaborative approach strengthens collective defenses, enhances situational awareness, and enables organizations to better protect against common adversaries and attack techniques.

5.5. Automation and Orchestration: Automating threat detection and response processes is a significant advancement in IDS. Actions like blocking malicious IPs or quarantining devices mitigate threats in real-time, lessening the load on security teams. Orchestration platforms seamlessly integrate IDS with other security tools, streamlining incident response and threat mitigation.

The recent strides in IDS, employing Automation and Orchestration, have transformed how organizations identify, address, and alleviate cyber threats. Let's delve into these innovations:

5.5.1. Dynamic Incident Response: Automation enables IDS systems to orchestrate dynamic incident response workflows based on predefined rules and policies. When a security event is detected, IDS can automatically trigger response actions such as isolating compromised devices, blocking malicious IP addresses, or quarantining suspicious files. By orchestrating incident response actions in real-time, IDS helps organizations contain threats and mitigate their impact on the network environment.

5.5.2. Integration with Security Orchestration Platforms: IDS systems merge with Security Orchestration, Automation, and Response (SOAR) platforms to simplify incident response workflows and automate actions across various security tools. SOAR centralizes orchestration, enabling IDS to sync response actions with tools like firewalls, ensuring a unified and efficient response to security incidents.

5.5.3. Policy-Driven Automation: IDS systems leverage policy-driven automation to enforce security policies, compliance requirements, and regulatory mandates. Organizations can define granular policies that specify how IDS should respond to different types of security events based on their severity, impact, and relevance. Policy-driven automation ensures consistent enforcement of security controls and response actions across the network environment, reducing the risk of human error and ensuring compliance with industry standards and regulations.

5.5.4. Threat Intelligence Integration: Automation and orchestration empower IDS to sync with threat intelligence feeds, enriching event data with external insights. By correlating events with intelligence, IDS prioritizes alerts, spots malicious patterns, and initiates responses. This integration boosts IDS effectiveness, equipping analysts with actionable insights for informed incident responses and investigations.

5.5.5. Continuous Improvement through Machine Learning: IDS employs machine learning to analyze security data, enhancing detection accuracy. Learning from history and adapting to threats, IDS evolves, reducing false positives. This automation ensures protection against evolving cyber threats and tactics.

5.6. Network Traffic Analysis:

The latest advancements in IDS utilizing Network Traffic Analysis have brought about significant improvements in threat detection, analysis, and response capabilities. Here's an examination of these advancements:

5.6.1. Deep Packet Inspection (DPI): Sophisticated IDS systems utilize deep packet inspection to scrutinize network traffic intricately. DPI enables examination of packet headers, payloads, and protocol headers, uncovering hidden threats in encrypted or obfuscated traffic. By real-time analysis, IDS detects malicious payloads, command-and-control communications, and other indicators evading traditional methods.

5.6.2. Behavioral Analysis and Anomaly Detection: Network Traffic Analysis empowers IDS with behavioral analysis and anomaly detection, spotting deviations from normalcy. Establishing baseline activity and user behavior, IDS detects anomalies like irregular access patterns, unusual resource usage, and suspicious communications. Leveraging statistical models, ML, and heuristic rules, behavioral analysis highlights potential security breaches or insider threats.

5.6.3. Protocol Analysis and Heuristic Detection: IDS systems leverage protocol analysis and heuristic detection techniques to identify protocol violations, misuse, and abnormal behaviors that may indicate a security incident. By analyzing network protocols such as TCP/IP, UDP, HTTP, and DNS, IDS can detect anomalies such as malformed packets, excessive traffic, or unexpected protocol behavior. Heuristic detection algorithms identify patterns of suspicious behavior that may indicate the presence of malware, exploitation attempts, or other security threats.

5.6.4. Flow-Based Analysis and Statistical Profiling: Flow-based analysis empowers IDS to scrutinize traffic flows, sessions, and communication patterns for threats and anomalies. By aggregating data from various sources, IDS detects suspicious behavior patterns, prioritizing alerts based on incident severity. Statistical profiling builds behavioral models, uncovering deviations indicative of breaches or unauthorized activities.

5.6.5. Integration with Threat Intelligence Feeds: Network Traffic Analysis merges with threat intelligence feeds, enriching event data with external insights. Correlating network activity with threat intelligence, such as malware signatures and IP reputation scores, IDS pinpoints malicious patterns and prioritizes alerts based on threat severity. This integration enhances IDS effectiveness, equipping analysts with actionable insights for informed incident responses and investigations.

5.6.6. Real-Time Monitoring and Alerting: IDS systems offer real-time monitoring and alerting, allowing swift response to security threats. Continuously analyzing network traffic, IDS generates alerts for suspicious activities and unauthorized access, aiding in prompt response and threat mitigation, safeguarding the network environment.

In conclusion, the integration of advanced technologies like Machine Learning, Artificial Intelligence, and Behavioral Analysis into IDS marks a significant advancement in cyber-security. These integrations enhance threat detection accuracy, enable the identification of complex threats, and facilitate dynamic adaptation to evolving threat landscapes. Cloud-Based IDS offer scalable and cost-effective security solutions tailored to modern cloud environments, enhancing visibility and compliance capabilities. Similarly, Threat Intelligence Integration empowers IDS to detect, analyze, and respond to threats more effectively by leveraging external context and insights. Automation and Orchestration advancements streamline incident response workflows and improve detection capabilities through machine learning. Network Traffic Analysis techniques provide comprehensive threat detection and response capabilities, strengthening cyber-security defenses against diverse cyber threats. Continuous evaluation and adaptation of IDS solutions are crucial to ensure robust protection against emerging attack vectors in today's complex digital environment.

6. FORECAST FUTURE DIRECTIONS & POTENTIAL INNOVATIONS IN IDS DEVELOPMENT

The future of IDS development holds several key directions and potential innovations aimed at addressing the evolving threat landscape and enhancing cyber-security measures. Advancements in AI & ML integration are expected to take part in a decisive part in improving IDS capabilities. Deep learning techniques, reinforcement learning, and natural language processing will be leveraged to enhance detection accuracy and reduce false positives, enabling IDS to better analyze and detect complex and evolving threats.

Another significant trend is the development of cloud-native IDS solutions tailored for cloud environments. These solutions will offer scalability, flexibility, and visibility into network traffic across distributed cloud infrastructures. By leveraging server less computing, containers, and micro services architectures, cloud-native IDS will provide comprehensive threat detection and response capabilities suitable for modern cloud deployments.

Additionally, IDS will increasingly focus on securing Internet of Things (IoT) and Operational Technology (OT) environments. Integration with specialized IoT and OT security solutions will enable IDS to monitor and protect IoT devices, industrial control systems (ICS), and critical infrastructure from cyber threats.

Automation and orchestration capabilities will continue to evolve to streamline incident response workflows and integrate with SOAR platforms. This will empower organizations to respond faster to security incidents and mitigate cyber threats more effectively. Additionally, IDS will be pivotal in fostering threat intelligence sharing among organizations and cyber-security communities. Integration with threat intelligence platforms will facilitate timely updates, insights on emerging threats, and collaborative mitigation efforts.

Deception technologies integration is also on the horizon, enhancing threat detection capabilities by deploying decoy assets and lures to identify and mitigate threats before they cause harm to the network environment. In summary, the future of IDS development will prioritize advancements in machine learning, cloud-native solutions, IoT and OT security, automation and orchestration, threat intelligence sharing, deception technologies, and continuous monitoring and threat hunting capabilities to bolster cyber security defenses and safeguard organizations against evolving cyber threats.

7. CHALLENGES & CONSTRAINTS ENCOUNTERED IN CONTEMPORARY IDS MPLEMENTATIONS

Contemporary IDS implementations face several challenges and constraints that impact their effectiveness and operational efficiency. These challenges include:

False Positives and Negatives: IDS systems commonly produce false positives, mistakenly flagging benign activities as threats, while false negatives occur when genuine security incidents evade detection. Striking a balance between detection accuracy and false alerts poses a major challenge for IDS implementations. Scalability and Performance: As network traffic volumes continue to grow exponentially, IDS must scale to handle the increasing data throughput

while maintaining real-time analysis capabilities. Ensuring that IDS solutions can scale horizontally to accommodate growing network infrastructures without sacrificing performance is a challenge, particularly for large enterprises and high-traffic networks.

Complexity and Resource Requirements: IDS implementations can be complex to deploy, configure, and maintain, requiring skilled personnel and significant resources. Managing and tuning IDS policies, and signatures to reduce false positives and optimize detection accuracy can be time-consuming and resource-intensive, particularly for organizations with limited cyber-security expertise. Encryption and Evasion Techniques: The widespread adoption of encryption protocols such as TLS/SSL presents challenges for IDS, as encrypted traffic obscures malicious payloads and communication channels. Attackers also employ evasion techniques to bypass IDS detection, such as fragmentation, obfuscation, and tunneling, making it challenging for IDS to accurately identify and mitigate threats.

Insider Threats and Advanced Persistent Threats (APTs): IDS must effectively detect and respond to insider threats, including unauthorized access and insider attacks. APTs pose additional challenges, as they employ sophisticated techniques to evade detection, persist within the network. High Volume of Alerts and Noise: IDS often generates a high volume of alerts, overwhelming security teams with false positives and noise. Prioritizing and triaging alerts to focus on genuine security incidents while filtering out false alarms requires robust incident response processes and automation capabilities.

Privacy and Compliance Concerns: IDS implementations must comply with privacy regulations and data protection laws, particularly concerning the collection, storage, and analysis of sensitive information. Balancing security requirements with privacy concerns, legal constraints, and regulatory obligations poses challenges for IDS deployments, particularly in regulated industries such as healthcare and finance. Meeting these challenges demands a comprehensive strategy integrating technological advancements, process enhancements, and stakeholder collaboration. Organizations must invest in advanced IDS solutions with capabilities such as machine learning, behavioral analytics, and threat intelligence integration to enhance detection accuracy and reduce false positives. Automation and orchestration technologies can streamline incident response workflows and improve operational efficiency, while ongoing training and education programs can empower cyber-security professionals to effectively manage and maintain IDS deployments.

The applications of IDS are diverse and crucial across various domains and are shown below Table 2.

Table 2: Applications of IDS

Application	Description
Network Security	Monitors network traffic for anomalies and suspicious activities, such as unauthorized access attempts or malware infections.
Host-based Security	Scrutinizes system logs and activities on individual devices or servers, detecting unauthorized access or malware infections.
Cloud Security	Safeguards cloud environments by detecting unauthorized access attempts, data breaches, between cloud services.
Critical Infrastructure	Protects essential infrastructure, like power grids and transportation systems, by identifying and mitigating cyber threats.
Compliance & Regulation	Ensures adherence to regulatory requirements by continuously monitoring for security incidents and maintaining audit trails.
Incident Response	Provides real-time alerts and forensic data to aid in investigating and mitigating security breaches promptly.
Threat Intelligence	Integrates with threat intelligence feeds to identify known threats, analyze attack patterns, and enhance threat detection capabilities.
Insider Threat Detection	Monitors user activities and detects unusual behavior or unauthorized access attempts within the network, aiding in identifying insider threats.
Cyber Threat Hunting	Proactively searches for hidden threats or indicators of compromise within the network environment, using advanced detection techniques and methodologies.

Application	Description
Integration with SIEM	Correlates alerts with other security events within Security Information and Event Management (SIEM) systems, providing a comprehensive security posture overview.

8. CONCLUSIONS

This comprehensive examination of advancements in IDS has shed light on the dynamic landscape of cyber-security. By covering a wide array of topics, including concepts, innovations, metrics, benchmarks, trends, directions, applications, and challenges, this study has provided a thorough understanding of the complexities surrounding IDS. Despite the progress made, challenges such as scalability and evolving threat landscapes persist, indicating the need for continuous innovation and collaboration. Ultimately, this study serves as an extensive guide for cyber-security professionals, researchers, and practitioners, promoting dialogue and innovation to enhance the effectiveness and resilience of IDS in countering cyber threats.

9. REFERENCES

[1] A. M. El Shafee and M. A. Azer, "MSDAR: Multi-Stage Dynamic Architecture Intrusion Detection System", *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 7, pp. 517-526, 2022.

[2] R. Kumar et al., "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network", *Journal of Parallel and Distributed Computing*, vol. 164, pp. 55-68, 2022.

[3] A. A. Wardana et al., "Collaborative Intrusion Detection System for Internet of Things Using Distributed Ledger Technology: A Survey on Challenges and Opportunities", *14th Asian Conference on Intelligent Information and Database Systems (ACIIDS)*, 2022.

[4] S. S. Mahmoud, "Practical Aspects of Perimeter Intrusion Detection and Nuisance Suppression for Distributed Fiber-Optic Sensors," in IEEE Transactions on Instrumentation and Measurement, vol. 72, pp. 1-11, 2023, Art no. 2517311, doi: 10.1109/TIM.2023.3284133.

[5] N. Bhattacharya, A. Subudhi, S. Mishra, V. Sharma, A. P. Aderemi and C. Iwendi, "A Novel Ensemble based Model for Intrusion Detection System," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 620-624, doi: 10.1109/IC2PCT60090.2024.10486584

[6] Abdallah Emad, EleisahWafa and Otoom Ahmed, "Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey", *Procedia Computer Science*, vol. 201, pp. 205-212, 2022.

[7] A. Tomar, S. Umrao and D. Kumar, "To Decrease the Rate of Cyber Anomalies Using Intrusion Detection System with Feature Selection Approach," 2024 2nd International Conference on Disruptive Technologies (ICDT), Greater Noida, India, 2024, pp. 1439-1442, doi: 10.1109/ICDT61202.2024.10489366.

[8] Torabi, Majid &Udzir, Nur & Abdullah, MohdTaufik&Yaakob, Razali. (2021). A Review on Feature Selection and Ensemble Techniques for Intrusion Detection System. International Journal of Advanced Computer Science and Applications. 12. 10.14569/IJACSA.2021.0120566.

[9] H. Satilmiş, S. Akleylek and Z. Y. Tok, "A Systematic Literature Review on Host-Based Intrusion Detection Systems," in IEEE Access, vol. 12, pp. 27237-27266, 2024, doi: 10.1109/ACCESS.2024.3367004.

[10] I. Martins, J. S. Resende, P. R. Sousa, S. Silva, L. Antunes and J. Gama, "Host-based IDS: A review and open issues of an anomaly detection system in IoT", *Future Gener. Comput. Syst.*, vol. 133, pp. 95-113, Aug. 2022.

[11] A. Thakkar and R. Lohiya, "A survey on intrusion detection system: Feature selection model performance measures application perspective challenges and future research directions", *Artif. Intell. Rev.*, vol. 55, no. 1, pp. 453-563, Jan. 2022.

[12] K. He, D. D. Kim and M. R. Asghar, "Adversarial machine learning for network intrusion detection systems: A comprehensive survey", *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 538-566, 1st Quart. 2023.

[13] M. R. Ayyagari, N. Kesswani, M. Kumar and K. Kumar, "Intrusion detection techniques in network environment: A systematic review", *Wireless Netw.*, vol. 27, no. 2, pp. 1269-1285, Feb. 2021.

[14] Y. Shin and K. Kim, "Comparison of anomaly detection accuracy of host-based intrusion detection systems based on different machine learning algorithms", *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2, pp. 252-259, 2020.

[15] J. L. Leevy and T. M. Khoshgoftaar, "A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 big data", *J. Big Data*, vol. 7, no. 1, pp. 1-19, Dec. 2020.

[16] G. Kocher and G. Kumar, "Machine learning and deep learning methods for intrusion detection systems: Recent developments and challenges", *Soft Comput.*, vol. 25, no. 15, pp. 9731-9763, Aug. 2021.

[17] D. Schubert, H. Eikerling and J. Holtmann, "Application-aware intrusion detection: A systematic literature review implications for automotive systems and applicability of AutoML", *Frontiers Comput. Sci.*, vol. 3, Aug. 2021.

[18] H. A. Hassan, E. E. Hemdan, W. El-Shafai, M. Shokair and F. E. A. El-Samie, "Intrusion detection systems for the Internet of Thing: A survey study", *Wireless Pers. Commun.*, vol. 128, no. 4, pp. 2753-2778, Feb. 2023.

[19] A. Heidari and M. A. Jabraeil Jamali, "Internet of Things intrusion detection systems: A comprehensive review and future directions", *Cluster Comput.*, vol. 26, no. 6, pp. 3753-3780, Dec. 2023.

[20] A. Thakkar and R. Lohiya, "A review on challenges and future research directions for machine learning-based intrusion detection system", *Arch. Comput. Methods Eng.*, vol. 30, no. 7, pp. 4245-4269, Sep. 2023.

[21] A. Khraisat, I. Gondal, P. Vamplew and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques datasets and challenges", *Cybersecurity*, vol. 2, no. 1, pp. 1-22, Dec. 2019.

[22] Majid Torabi , Nur IzuraUdzir , MohdTaufik Abdullah , Razali Yaakob “A Review on Feature Selection and Ensemble Techniques for Intrusion Detection System “ (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 5, 2021.