A Comprehensive Review of Intrusion Detection System for Port Scanning Attacks

Bharti Bandgar[1], Kaivalya Kulkarni[2], Prasad Waghmare[3], Onkar Pomane[4], Shubham Waghmare[5]
[1]*Professor, Department of Computer Engineering, K. J. College of Engineering & Management Research, Pune, India*
[2,3,4,5]*Department of Computer Engineering, K. J. College of Engineering & Management Research, Pune, India*

***Abstract*—In today's world, cyberattacks are hitting computer networks harder than ever, and old-school defences like firewalls or basic rule-checking just aren't cutting it against sneaky, advanced intruders. Hackers often start with stealthy recon moves, like port scanning, that slip right past traditional setups. Our project introduces a smart Machine Learning-powered Intrusion Detection System (IDS) that keeps a real-time eye on network traffic to spot these malicious scans. It grabs live packets using Scapy, pulls out key network features, and sorts good traffic from bad with a Random Forest classifier. To cut down on false alarms, we added flow-based analysis that looks at patterns across multiple packets in a short time window, instead of judging each one alone. The system fires off instant alerts with clear visual cues and keeps thorough logs for digging into incidents later. Overall, this IDS boosts detection rates, slashes false positives, and delivers a lightweight, practical tool ready for real-world use.**

***Index Terms*—Intrusion Detection System, Network Security, Machine Learning, Random Forest, Port Scan Detection, Real-Time Monitoring.**

I. INTRODUCTION

As computer networks continue to expand across industries such as banking, healthcare, education, and e-commerce, the risk of cyber intrusions has grown significantly. Attackers frequently perform reconnaissance attacks such as port scanning to identify vulnerable services before launching more severe exploits. Detecting such early-stage attacks is crucial for preventing major security breaches.

Traditional network security tools like firewalls and access control lists operate based on predefined rules and lack the intelligence to analyze traffic behavior dynamically. These systems often fail to detect internal threats, zero-day attacks, or low-and-slow reconnaissance techniques. As a result, malicious activities may remain unnoticed until substantial damage has already occurred.

An Intrusion Detection System (IDS) plays a vital role by continuously monitoring network traffic and identifying suspicious behavior. Recent advancements in machine learning have enhanced IDS capabilities by enabling systems to learn traffic patterns and distinguish between normal and malicious behavior. This project focuses on developing a machine learning driven IDS that detects port scanning activities in real time with improved accuracy and reduced false positives.

That's where an Intrusion Detection System (IDS) steps in, constantly watching traffic for anything fishy. Machine learning has supercharged these systems lately, teaching them to spot normal patterns versus malicious ones. Our project builds a ML-driven IDS that catches port scanning in real time, with sharper accuracy and way fewer false alarms.

II. FUNDAMENTALS OF INTELLIGENT SURVEILLANCE SYSTEMS

Intrusion Detection Systems (IDS) are security solutions designed to continuously monitor network traffic, system activities, and communication patterns to identify unauthorized access attempts, malicious activities, and potential cyberattacks. The primary objective of an IDS is to detect security violations at an early stage and generate alerts that enable administrators to respond before significant damage

occurs. With the increasing complexity of cyber threats, IDS has become a critical component of modern cybersecurity infrastructures used in organizations, enterprises, cloud environments, and Internet of Things (IoT) networks.

An IDS operates by collecting data from network packets, system logs, application activities, and user interactions. The collected information is analyzed using predefined rules, behavioral models, statistical techniques, or machine learning algorithms to determine whether an activity is normal or suspicious. Modern IDS solutions are capable of detecting a wide variety of attacks including port scanning, denial-of-service attacks, malware propagation, brute-force login attempts, insider threats, and unauthorized network access.

A. Architecture of Intrusion Detection Systems

A typical Intrusion Detection System consists of several interconnected modules that work together to monitor, analyze, and report security incidents.

1. Data Collection Module

The data collection module is responsible for capturing information from various sources such as network traffic, routers, switches, servers, firewalls, and operating systems. Packet capture tools such as Scapy, Wireshark, Tcpdump, and network sensors collect raw traffic data in real time. This module serves as the foundation of the IDS because accurate detection depends on the quality and completeness of the collected data.

2. Feature Extraction Module

Raw network packets contain large amounts of information that cannot be directly processed by detection algorithms. Therefore, the feature extraction module converts raw packet data into meaningful numerical attributes. Common features include source and destination IP addresses, port numbers, packet size, protocol type, TCP flags, connection duration, packet frequency, and flow statistics. These features provide valuable insights into network behavior and serve as input for intrusion detection algorithms.

3. Detection Engine

The detection engine is the core component of an IDS. It analyzes extracted features and determines whether observed activities are legitimate or malicious. Depending on the detection methodology, the engine may use signature matching, anomaly detection, statistical analysis, machine learning models, or hybrid techniques. The accuracy and efficiency of the IDS largely depend on the effectiveness of this component.

4. Alert Generation Module

Whenever suspicious activity is detected, the alert generation module creates notifications for security administrators. Alerts typically include information such as attack type, source IP address, destination IP address, timestamp, protocol details, and severity level. Immediate alert generation allows organizations to respond quickly to potential threats.

5. Logging and Reporting Module

All detected events and alerts are recorded in logs for future analysis. Security logs assist administrators in forensic investigations, compliance auditing, incident response, and threat intelligence analysis. Advanced IDS solutions also generate visual reports and dashboards that provide detailed insights into network security status.

III. REVIEW OF EXISTING METHODS

The development of Intrusion Detection Systems (IDS) has evolved significantly over the past few decades, progressing from traditional rule-based systems to advanced Artificial Intelligence (AI) and Machine Learning (ML) driven solutions. Researchers have proposed numerous techniques to improve intrusion detection accuracy, reduce false alarms, enhance scalability, and support real-time network monitoring. Existing IDS approaches can be broadly categorized based on their underlying methodologies and technologies. This section reviews the major intrusion detection methods and analyzes their strengths and limitations.

A. Signature-Based Intrusion Detection Systems

Signature-based IDS represents one of the earliest and most widely deployed intrusion detection approaches. These systems detect attacks by comparing network traffic and system activities against a database of predefined attack signatures. Each signature corresponds to a known malicious pattern, exploit, malware behavior, or attack sequence.

Popular signature-based IDS tools such as Snort and Suricata utilize rule-matching mechanisms to identify threats efficiently. Whenever network traffic matches a stored signature, an alert is generated indicating a potential intrusion.

Signature-based systems offer several advantages, including high detection accuracy for known attacks, low false positive rates, fast processing speed, and ease of implementation. However, their effectiveness depends heavily on regular signature updates. They cannot detect unknown attacks, zero-day exploits, or modified attack variants that do not match existing patterns. As cyber threats continuously evolve, maintaining updated signature databases remains a significant challenge.

Although signature-based IDS solutions continue to be widely used in enterprise environments, their limitations have motivated the development of more intelligent detection techniques capable of identifying novel attack behaviors.

B. Anomaly-Based Intrusion Detection Systems

Anomaly-based IDS was introduced to overcome the limitations of signature-based detection. Instead of relying on predefined attack signatures, anomaly-based systems establish a baseline profile of normal network behavior and identify deviations from that baseline as potential threats.

These systems analyze various network characteristics such as traffic volume, packet frequency, connection duration, protocol usage, user behavior, and communication patterns. Significant deviations from normal behavior are classified as suspicious activities.

Anomaly-based detection offers the major advantage of identifying previously unseen attacks, including zero-day exploits and emerging cyber threats. The approach is highly adaptive and capable of detecting abnormal behaviors even when attack signatures are unavailable.

However, anomaly-based systems often generate a high number of false positives because legitimate but unusual activities may be incorrectly classified as attacks. Establishing accurate baseline profiles is also challenging in dynamic network environments where normal behavior continuously changes. Despite these limitations, anomaly-based detection remains an important foundation for modern machine learning-based IDS solutions.

C. Statistical-Based Intrusion Detection Systems

Statistical IDS methods analyze network traffic using mathematical and probabilistic models. These systems monitor statistical properties of network behavior and identify significant deviations from expected patterns.

Common statistical metrics include:

- Packet arrival rates
- Connection frequencies
- Traffic volume
- Session duration
- Protocol distributions
- Error rates

Techniques such as mean deviation analysis, variance monitoring, Bayesian statistics, Markov models, and time-series analysis have been applied to intrusion detection tasks.

Statistical approaches are computationally efficient and capable of detecting anomalous activities in real time. They provide quantitative insights into network behavior and can identify gradual changes that may indicate malicious activity.

However, statistical models often struggle with highly dynamic environments and complex attack patterns. Their detection accuracy depends heavily on accurate parameter selection and model assumptions. Consequently, statistical IDS methods are frequently combined with machine learning techniques to improve performance.

D. Machine Learning-Based Intrusion Detection Systems

Machine Learning has become one of the most influential technologies in modern intrusion detection research. ML-based IDS solutions automatically learn patterns from historical network traffic and classify future activities as normal or malicious without relying solely on predefined rules.

Several supervised learning algorithms have been extensively investigated for intrusion detection applications.

1. Decision Tree-Based IDS

Decision Trees classify network traffic by creating hierarchical decision rules based on selected features. These models are easy to interpret, computationally efficient, and suitable for real-time deployment.

Researchers have reported good detection accuracy using Decision Trees for identifying denial-of-service

attacks, port scans, and unauthorized access attempts. However, single decision trees may suffer from overfitting and reduced generalization capability when applied to large and complex datasets.

2. Random Forest-Based IDS

Random Forest is an ensemble learning technique that combines multiple decision trees to improve classification performance. It has emerged as one of the most successful machine learning algorithms for intrusion detection.

Random Forest offers several advantages including:

- High detection accuracy
- Robustness against overfitting
- Efficient processing
- Strong performance on high-dimensional datasets
- Capability to handle noisy data

Numerous studies have demonstrated that Random Forest achieves superior performance on benchmark datasets such as NSL-KDD, CICIDS2017, and UNSW-NB15. Due to its reliability and efficiency, Random Forest remains one of the most popular choices for real-time IDS implementations.

3. Support Vector Machine (SVM)

Support Vector Machine is a supervised learning algorithm that identifies optimal decision boundaries separating normal and malicious traffic classes.

SVM provides excellent classification performance in high-dimensional feature spaces and demonstrates strong generalization capabilities. It has been successfully applied to intrusion detection tasks involving malware analysis, network anomaly detection, and attack classification.

Despite its advantages, SVM requires careful parameter tuning and becomes computationally expensive when processing very large datasets.

4. K-Nearest Neighbor (KNN)

KNN classifies network traffic based on similarity measurements between new observations and previously labeled examples.

The algorithm is simple to implement and performs effectively on small and medium-sized datasets. However, KNN suffers from high computational complexity during prediction and reduced scalability for large-scale intrusion detection applications.

5. Naïve Bayes Classification

Naïve Bayes is a probabilistic classification method based on Bayes' theorem. It calculates the probability of traffic belonging to different classes and assigns labels accordingly.

The algorithm is computationally efficient and suitable for large datasets. However, its assumption of feature independence often limits detection performance in complex network environments where features exhibit strong correlations.

Overall, machine learning approaches have significantly improved intrusion detection accuracy and adaptability compared to traditional methods.

Table I

Method / Approach	Accuracy	Real-Time	Multi Camera	Privacy Support	Key Limitations
Signature-Based IDS (Snort, Suricata)	Low–Moderate	Yes	No	No	Sensitive to lighting, poor scalability, low robustness
Anomaly-Based IDS	Moderate	Yes	No	No	Limited feature representation, struggles with occlusion
Statistical-Based IDS	Moderate	Yes	Partial	Moderate	Moderate
Decision Tree-Based IDS	High	Yes	Partial	Moderate	High
Random Forest-Based IDS	Very High	Yes	Yes	Low	High
Support Vector Machine (SVM)	High	Partial	Yes	Low–Moderate	Moderate

K-Nearest Neighbor (KNN)	Moderate–High	No	Partial	Moderate	Low
Naïve Bayes IDS	Moderate	Yes	Partial	Moderate	High
CNN-Based IDS	Very High	Partial	Yes	Low	Moderate
RNN/LSTM-Based IDS	Very High	Partial	Yes	Low	Moderate
Autoencoder-Based IDS	High	Partial	Yes	Low	Moderate
Hybrid IDS (ML + Signature)	Very High	Yes	Yes	Very Low	High

A. Analysis of Existing Approaches

The comparative analysis reveals that different Intrusion Detection System approaches focus on specific aspects of network security. Traditional signature-based systems such as Snort and Suricata provide excellent performance in detecting known attacks with minimal false alarms. However, they are ineffective against unknown threats and require continuous signature updates. Anomaly-based systems improve the detection of zero-day attacks by learning normal traffic behavior, but they often suffer from high false positive rates.

Machine learning techniques such as Decision Trees, Random Forests, Support Vector Machines, and Naïve Bayes significantly improve detection accuracy by automatically learning attack patterns from historical network traffic. Among these methods, Random Forest consistently achieves superior performance due to its robustness, scalability, and ability to handle large feature sets. Deep learning approaches including CNNs and LSTMs further enhance intrusion detection by automatically extracting complex traffic patterns and temporal relationships. Although these methods achieve very high detection accuracy, they require substantial computational resources and large training datasets.

Hybrid Intrusion Detection Systems combine multiple detection techniques to leverage their strengths while minimizing weaknesses. These systems demonstrate the highest detection rates and lowest false positive rates but introduce greater implementation complexity. Recent cloud-based and IoT-specific IDS solutions address emerging cybersecurity challenges in distributed environments; however, privacy concerns, scalability issues, and resource limitations remain active research challenges.

Overall, existing IDS solutions provide significant improvements in network security, yet no single approach completely satisfies the requirements of accuracy, scalability, adaptability, real-time processing, and low computational overhead. This creates opportunities for future research focused on intelligent, hybrid, and privacy-preserving intrusion detection frameworks.

B. Security and Privacy Considerations

As Intrusion Detection Systems (IDS) become increasingly integrated into modern network infrastructures, ensuring security and privacy has become a critical concern. IDS solutions continuously monitor network traffic, system activities, and user behavior, often processing large volumes of sensitive information. While these systems play an essential role in detecting cyber threats and preventing security breaches, they also introduce challenges related to data confidentiality, user privacy, regulatory compliance, and system trustworthiness. Therefore, security and privacy considerations must be carefully addressed during the design, deployment, and operation of IDS frameworks

C. Identified Gaps

The comprehensive analysis of existing Intrusion Detection System (IDS) approaches reveals several significant limitations that continue to hinder their effectiveness in real-world cybersecurity environments. Although substantial progress has been made through machine learning, deep learning, and hybrid detection techniques, many challenges remain unresolved. These gaps highlight the need for next-generation IDS frameworks that are more intelligent, scalable, adaptive, and privacy-aware.

1. Limited Detection of Zero-Day Attacks

Traditional signature-based IDS solutions depend heavily on predefined attack signatures and known threat patterns. While highly effective against previously identified attacks, they struggle to detect zero-day vulnerabilities, novel malware, and emerging cyber threats. As attackers continuously develop new techniques to bypass security mechanisms, the inability to identify unknown attacks remains a major limitation of many existing IDS implementations.

2. High False Positive Rates

Anomaly-based intrusion detection systems often generate excessive false alarms because legitimate network activities may be incorrectly classified as malicious. High false positive rates increase the workload of security administrators, consume organizational resources, and may lead to alert fatigue. As a result, critical threats may be overlooked among numerous false alerts. Reducing false positives while maintaining high detection accuracy remains a significant research challenge.

3. Scalability Challenges in Large Networks

Modern enterprise networks, cloud environments, and Internet of Things (IoT) infrastructures generate enormous volumes of network traffic. Many existing IDS solutions experience performance degradation when processing large-scale data streams in real time. Maintaining detection accuracy while supporting high-speed network environments and large numbers of connected devices remains an important scalability challenge.

4. Computational Complexity of AI-Based IDS

Machine learning and deep learning models have significantly improved intrusion detection accuracy; however, they often require substantial computational resources, memory capacity, and processing power. Deep neural networks such as CNNs and LSTMs demand extensive training datasets and powerful hardware accelerators. These requirements limit their deployment in resource-constrained environments such as IoT devices, embedded systems, and edge computing platforms.

5. Insufficient Encrypted Traffic Analysis

The widespread adoption of encryption protocols such as HTTPS, TLS, and VPN technologies has improved data confidentiality but reduced the visibility of network monitoring systems. Traditional packet inspection methods become less effective when network payloads are encrypted. Existing IDS solutions often struggle to identify malicious activities hidden within encrypted traffic without compromising user privacy or system performance.

6. Vulnerability to Adversarial Attacks

Machine learning-based IDS models themselves can become targets of cyberattacks. Adversarial attacks manipulate input data to deceive detection algorithms and evade security mechanisms. Similarly, data poisoning attacks can corrupt training datasets and reduce model effectiveness. Many existing IDS solutions lack robust defenses against these sophisticated attacks, creating new security vulnerabilities within intelligent detection frameworks.

7. Lack of Explainability and Transparency

Many advanced machine learning and deep learning models function as “black-box” systems, providing highly accurate predictions without clear explanations of their decision-making processes. Security analysts often find it difficult to understand why a particular event was classified as malicious. This lack of transparency reduces trust, complicates incident investigation, and creates challenges for regulatory compliance and forensic analysis.

8. Limited Adaptability to Evolving Threats

Cyberattack techniques evolve continuously, requiring IDS solutions to adapt rapidly to changing threat landscapes. Many existing systems rely on periodic retraining or manual rule updates, making them less responsive to emerging attack strategies. The development of self-learning and continuously adaptive IDS frameworks remains an active area of research.

9. Privacy and Data Protection Concerns

Intrusion detection systems frequently process sensitive user information, communication records, and network activities. Centralized monitoring architectures may create privacy risks and increase

the likelihood of unauthorized access or data leakage. Existing IDS implementations often lack integrated privacy-preserving mechanisms, making compliance with modern data protection regulations more challenging.

10. Lack of Unified Security Frameworks

Most current IDS solutions focus on individual aspects of cybersecurity such as signature matching, anomaly detection, machine learning classification, or behavioral analysis. Few systems provide comprehensive frameworks that integrate threat detection, response automation, threat intelligence, privacy preservation, and secure data management within a single architecture. The absence of unified solutions limits operational efficiency and overall security effectiveness.

D. Limited Behavior Prediction

Most existing Intrusion Detection Systems are designed primarily to detect attacks after suspicious activities have already occurred. These systems focus on identifying known attack signatures or abnormal network behavior in real time but often lack the capability to predict future threats before they are launched. As cyberattacks become increasingly sophisticated, reactive detection alone is insufficient for ensuring comprehensive network security.

Current IDS solutions generally analyze historical and current network traffic to identify malicious activities. However, they rarely incorporate predictive analytics capable of forecasting potential attack patterns, attacker behavior, or emerging threats. As a result, security administrators receive alerts only after suspicious actions have been detected, reducing the time available for preventive measures and incident response.

Machine learning and deep learning techniques have improved detection accuracy, but many models remain dependent on previously observed attack data. They may struggle to recognize evolving attack strategies, multi-stage intrusions, or advanced persistent threats that gradually develop over time. Furthermore, most IDS frameworks do not effectively analyze long-term behavioral trends, user activity patterns, or threat intelligence information that could support proactive threat prediction.

Developing predictive intrusion detection mechanisms remains an important research challenge. Future IDS solutions should integrate behavioral analytics, artificial intelligence, threat intelligence feeds, and predictive modeling techniques to anticipate potential attacks before they occur. Such capabilities would enable organizations to take preventive actions, strengthen security policies, and improve overall cyber defense effectiveness. By moving from reactive detection toward proactive threat prediction, next-generation IDS frameworks can provide enhanced protection against increasingly complex and evolving cyber threats.

E. Privacy Risks in Centralized Systems

Many modern Intrusion Detection Systems (IDS) utilize centralized architectures in which network traffic, security logs, user activities, and system events from multiple devices are collected and processed at a central server. While centralized systems simplify management, monitoring, and analysis, they also introduce significant privacy and security concerns. The aggregation of large volumes of sensitive information in a single location increases the risk of unauthorized access, data breaches, and misuse of confidential information.

F. Lack of Tamper-Proof Evidence

One of the significant limitations of many existing Intrusion Detection Systems (IDS) is the lack of tamper-proof mechanisms for storing and preserving security logs and forensic evidence. IDS solutions continuously generate large amounts of data, including attack alerts, network activity records, user actions, and system event logs. These records are critical for incident investigation, forensic analysis, compliance audits, and legal proceedings. However, in many traditional IDS architectures, security logs are stored in centralized databases or local storage systems that can be modified, deleted, or manipulated by attackers or unauthorized users

G. Lack of Unified Frameworks

Despite significant advancements in Intrusion Detection Systems (IDS), most existing solutions are designed to address specific aspects of cybersecurity rather than providing a comprehensive and integrated security platform. Traditional IDS architectures often focus on individual functions such as signature matching, anomaly detection, traffic monitoring,

machine learning classification, or threat analysis. As a result, organizations frequently deploy multiple security tools that operate independently, leading to fragmented security management and reduced operational efficiency.

IV. FUTURE DIRECTIONS

The rapid evolution of cyber threats, increasing network complexity, and widespread adoption of emerging technologies such as cloud computing, Internet of Things (IoT), Artificial Intelligence (AI), and edge computing have created new challenges for Intrusion Detection Systems (IDS). Although current IDS solutions have significantly improved threat detection capabilities, several limitations remain unresolved. Future research and development efforts should focus on creating intelligent, adaptive, scalable, privacy-preserving, and autonomous intrusion detection frameworks capable of addressing modern cybersecurity requirements. The following directions represent promising areas for future advancement in IDS technology.

A. Integration of Explainable Artificial Intelligence (XAI)

Modern machine learning and deep learning-based IDS solutions often function as black-box models, making it difficult for security analysts to understand the reasoning behind detection decisions. Explainable Artificial Intelligence (XAI) aims to provide transparency and interpretability by generating understandable explanations for model predictions. Future IDS systems should incorporate XAI techniques to improve trust, support forensic investigations, facilitate regulatory compliance, and assist security administrators in making informed decisions. Explainable models can also enhance the adoption of AI-driven cybersecurity solutions in critical sectors such as healthcare, finance, and government organizations.

B. Federated Learning for Privacy-Preserving Detection

Traditional machine learning models typically require centralized collection of training data, raising concerns regarding privacy and data protection. Federated Learning enables multiple organizations or devices to collaboratively train intrusion detection models without sharing sensitive raw data. Instead, only model updates are exchanged, preserving confidentiality while benefiting from collective learning. Future IDS frameworks should explore federated learning architectures to improve detection accuracy, strengthen privacy protection, and support collaborative threat intelligence across distributed environments.

C. Blockchain-Based Secure Intrusion Detection Systems

Blockchain technology offers decentralized, transparent, and tamper-resistant storage mechanisms that can significantly enhance IDS security. Future IDS architectures may utilize blockchain to securely record attack logs, maintain immutable forensic evidence, verify alert authenticity, and facilitate trusted information sharing among organizations. Smart contracts can automate security policies, access control decisions, and incident response procedures. Research into scalable and energy-efficient blockchain integration remains an important future direction for secure intrusion detection systems.

D. Intelligent Prediction of Cyber Threats

Most existing IDS solutions operate reactively by detecting attacks after suspicious activities have already occurred. Future systems should focus on predictive cybersecurity capabilities that anticipate attacks before they happen. By analyzing historical attack patterns, user behavior, network trends, and threat intelligence feeds, AI-powered predictive models can forecast potential threats and provide early warnings. Such proactive detection mechanisms would allow organizations to implement preventive security measures and significantly reduce attack impact.

E. Advanced Deep Learning Architectures

Deep learning has demonstrated exceptional performance in intrusion detection; however, existing architectures still face challenges related to computational complexity and training requirements. Future research should investigate advanced neural network models such as Graph Neural Networks (GNN), Transformers, Generative Adversarial Networks (GAN), and self-supervised learning techniques. These architectures can improve feature extraction, attack classification, anomaly detection,

and adaptability while reducing dependency on labeled datasets.

F. Intrusion Detection for Internet of Things (IoT) Environments

The rapid growth of IoT devices has expanded the cyberattack surface significantly. Resource-constrained IoT devices often lack sufficient security mechanisms, making them attractive targets for attackers. Future IDS solutions should focus on lightweight and energy-efficient detection models capable of operating effectively within IoT environments. Research efforts should address device heterogeneity, low-power operation, distributed monitoring, and secure communication protocols to protect smart homes, healthcare devices, industrial control systems, and smart city infrastructures.

G. Cloud-Native and Edge-Based Intrusion Detection

The migration of organizational infrastructure to cloud platforms and edge computing environments has transformed network architectures. Traditional IDS solutions may not effectively address the dynamic nature of cloud resources and distributed edge networks. Future IDS frameworks should support cloud-native deployment, containerized applications, virtualization technologies, and edge computing infrastructures. Distributed detection architectures capable of real-time monitoring across geographically dispersed environments will become increasingly important.

H. Automated Incident Response and Self-Healing Systems

Current IDS solutions primarily focus on attack detection and alert generation, leaving response actions to human administrators. Future cybersecurity frameworks should integrate automated incident response mechanisms capable of isolating compromised systems, blocking malicious traffic, updating security policies, and mitigating attacks without human intervention. Self-healing security systems powered by AI can automatically recover from cyber incidents, reduce response time, and improve overall organizational resilience.

I. Adversarially Robust Machine Learning Models

Machine learning-based IDS solutions are vulnerable to adversarial attacks designed to manipulate detection outcomes. Attackers may craft malicious inputs that evade detection or corrupt training datasets through poisoning attacks. Future IDS research should prioritize the development of adversarially robust learning algorithms capable of maintaining detection accuracy under hostile conditions. Techniques such as adversarial training, robust optimization, and secure model validation can improve system resilience against intelligent attackers.

J. Multi-Layer Hybrid Detection Frameworks

No single detection technique can effectively address all cybersecurity threats. Future IDS architectures should combine signature-based detection, anomaly detection, behavioral analysis, machine learning, deep learning, threat intelligence, and rule-based systems within unified frameworks. Multi-layer hybrid architectures can leverage the strengths of different detection methodologies while minimizing individual weaknesses. Such systems are expected to achieve higher detection accuracy, lower false positive rates, and improved adaptability to emerging threats.

K. Privacy-Preserving Intrusion Detection

As data privacy regulations become increasingly stringent, future IDS solutions must balance effective threat detection with user privacy protection. Techniques such as differential privacy, homomorphic encryption, secure multi-party computation, and federated analytics can intrusion detection without exposing sensitive information. Privacy-preserving IDS architectures will play a crucial role in maintaining regulatory compliance and building user trust in cybersecurity systems.

L. Integration with Threat Intelligence Platforms

Threat intelligence provides valuable information about emerging attack techniques, malicious indicators, vulnerabilities, and cybercriminal activities. Future IDS frameworks should integrate real-time threat intelligence feeds to enhance detection capabilities and improve situational awareness. Combining local monitoring data with global threat intelligence can enable faster identification of sophisticated attacks and support proactive defense strategies.

M. Development of Unified Security Frameworks

The future of intrusion detection lies in the development of comprehensive security ecosystems that integrate IDS, Intrusion Prevention Systems (IPS), firewalls, SIEM platforms, endpoint security solutions, blockchain-based logging, and AI-driven analytics. Unified frameworks can provide centralized visibility, automated threat correlation, coordinated incident response, and simplified security management. Such integrated architectures will enable organizations to address increasingly complex cybersecurity challenges more effectively.

V. CONCLUSION

Intrusion Detection Systems (IDS) have become an essential component of modern cybersecurity infrastructures, providing continuous monitoring and protection against a wide range of cyber threats. As organizations increasingly rely on interconnected networks, cloud platforms, Internet of Things (IoT) devices, and digital services, the need for effective intrusion detection mechanisms has grown significantly. Traditional security solutions such as firewalls and antivirus software alone are no longer sufficient to defend against sophisticated and evolving attack techniques. Consequently, IDS technologies play a crucial role in identifying malicious activities, detecting unauthorized access attempts, and supporting timely incident response.

This review examined the evolution of Intrusion Detection Systems from traditional signature-based approaches to advanced machine learning and deep learning-based solutions. Signature-based IDS techniques remain effective for detecting known attacks; however, their inability to identify unknown threats and zero-day vulnerabilities limits their effectiveness in modern environments. Anomaly-based systems address some of these limitations by detecting deviations from normal behavior, although they often suffer from high false positive rates. Recent advances in machine learning algorithms such as Random Forest, Support Vector Machine, Decision Tree, and Naïve Bayes have significantly improved intrusion detection accuracy and adaptability. Furthermore, deep learning models including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Autoencoders have demonstrated exceptional capabilities in identifying complex attack patterns and advanced persistent threats.

The review also highlighted several critical challenges that continue to affect IDS performance, including limited detection of zero-day attacks, high false positive rates, computational complexity, scalability issues, encrypted traffic analysis, adversarial machine learning attacks, privacy concerns, lack of tamper-proof evidence, and the absence of unified security frameworks. These limitations indicate that further research is required to develop more intelligent, explainable, scalable, and privacy-preserving intrusion detection solutions capable of addressing emerging cybersecurity threats.

Future advancements in Artificial Intelligence, Federated Learning, Blockchain Technology, Explainable AI, Predictive Threat Analytics, Cloud Security, and IoT Protection offer promising opportunities for enhancing IDS capabilities. The integration of these technologies can improve detection accuracy, transparency, automation, resilience, and real-time responsiveness while ensuring compliance with privacy and security requirements. Hybrid detection architectures combining multiple analytical approaches are expected to play a vital role in next-generation intrusion detection frameworks.

In conclusion, Intrusion Detection Systems remain a fundamental defense mechanism for protecting modern digital infrastructures. While considerable progress has been achieved through machine learning and artificial intelligence-based approaches, continuous innovation is necessary to keep pace with the rapidly evolving threat landscape. Future IDS solutions should focus on proactive threat prediction, adaptive learning, secure information sharing, privacy preservation, and automated incident response to provide comprehensive and intelligent cybersecurity protection. Through ongoing research and technological advancements, IDS technologies will continue to strengthen organizational security and contribute significantly to the development of safer and more resilient cyber ecosystems.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Prof. Bharti Bandgar for her valuable

guidance, continuous support, and insightful suggestions throughout the development of this review paper on Intrusion Detection Systems (IDS). Her expertise, encouragement, and constructive feedback greatly contributed to the successful completion of this work.

The authors also extend their heartfelt thanks to the Department of Computer Engineering, K. J. College of Engineering and Management Research, Pune, for providing the necessary resources, technical facilities, and academic environment required for conducting this study. The support and motivation provided by the faculty members and staff members of the department played a significant role in the successful preparation of this review paper.

Special appreciation is extended to all researchers, academicians, and authors whose published work, research articles, journals, conference papers, and technical reports served as valuable references and contributed significantly to understanding the concepts, methodologies, challenges, and future directions of Intrusion Detection Systems.

Finally, the authors would like to thank their family members, friends, and colleagues for their constant encouragement, motivation, and moral support throughout the research and documentation process. Their support was instrumental in the successful completion of this work.

REFERENCES

[1] National Institute of Standards and Technology, Guide to Intrusion Detection and Prevention Systems (IDPS), Special Publication 800-94, 2007.

[2] Martin Roesch, "Snort – Lightweight Intrusion Detection for Networks," Proceedings of the 13th USENIX Conference on System Administration (LISA), pp. 229–238, 1999.

[3] Robin Sommer and Vern Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," IEEE Symposium on Security and Privacy, pp. 305–316, 2010.

[4] Mahbod Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009.

[5] Nour Moustafa and Jill Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," Military Communications and Information Systems Conference (MilCIS), 2015.

[6] Leo Breiman, "Random Forests," Machine Learning Journal, vol. 45, no. 1, pp. 5–32, 2001.

[7] Scapy Documentation, Accessed 2026.

[8] Suricata Documentation, Accessed 2026.

[9] Canadian Institute for Cybersecurity, "CICIDS2017 Dataset: Intrusion Detection Evaluation Dataset," 2017.

[10] Ahmed A. Ghorbani, W. Lu, and M. Tavallaee, "Network Intrusion Detection Using Machine Learning: A Survey," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16–24, 2013.

[11] Yisroel Mirsky et al., "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," Network and Distributed Systems Security Symposium (NDSS), 2018.

[12] Vinayakumar R, K. P. Soman, and P. Poornachandran, "Applying Deep Learning Approaches for Network Intrusion Detection," International Journal of Engineering Research and Technology, vol. 5, no. 6, pp. 195–200, 2016.

[13] Wei Wang, M. Zhu, J. Wang, and X. Zeng, "HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks for Intrusion Detection," IEEE Access, vol. 6, pp. 1792–1806, 2018.

[14] Muhammad Aamir and S. M. A. Zaidi, "Clustering Based Semi-Supervised Machine Learning for DDoS Attack Classification," Journal of King Saud University – Computer and Information Sciences, vol. 33, no. 4, pp. 436–446, 2021.

[15] Muneeb Ahmed, A. Naser Mahmood, and J. Hu, "A Survey of Network Anomaly Detection Techniques," Journal of Network and Computer Applications, vol. 60, pp. 19–31, 2016.

[16] Shone Nathan et al., "A Deep Learning Approach to Network Intrusion Detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.

[17] Ashfaq Rana et al., "Fuzziness Based Semi-Supervised Learning Approach for Intrusion

Detection System," Information Sciences, vol. 378, pp. 484–497, 2017.

[18] Khaled Salah, M. H. U. Rehman, and N. Nizamuddin, "Blockchain for AI: Review and Open Research Challenges," IEEE Access, vol. 7, pp. 10127–10149, 2019.

[19] Ian Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press, Cambridge, MA, 2016.

[20] Nicolas Papernot et al., "Practical Black-Box Attacks Against Machine Learning," ACM Asia Conference on Computer and Communications Security, pp. 506–519, 2017.