International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

A Comparison study of various Wireless Intrusion Detection Systems

E. Ammu[1], Dr. B. Devanathan[2]

[1]Research Scholar, [2]Assistant Professor
[1,2]Department of Computer & Information Science
Annamalai University
[1]ammue2897@gmail.com, [2]devacisau@gmail.com

Abstract:

The growing sophistication of cyberattacks is making it harder to detect breaches accurately. Failure to prevent intrusions can damage the reputation of the security services. A. Data accessibility, confidentiality, integrity. To address computer security risks in wireless sensor networks (WSN), a range of intrusion detection approaches have been presented in the literature, which can be classified into two general categories: anomaly-based intrusion detection systems (AIDS) and signature-based intrusion detection systems (SIDS). This survey study presents an overview of the datasets commonly used for evaluation, the taxonomy of existing IDS, and a detailed review of significant recent research. The evasion strategies used by attackers to avoid detection in WSN are also described, along with the challenges that need to be addressed in future research to oppose these strategies and improve the security of computer systems.

Keywords:WDS- wireless Sensor Network, IDS-Intrusion Detection System, SIDS,- Signature-based IDS,AIDS- Anomaly-based IDS,NBIDS-Network Based IDS,HBIDS-Host Based IDS.

1. INTRODUCTION

The last several decades have seen a radical transformation in wireless networks and systems. In the field of wireless computing, the idea of ubiquitous computing has emerged as a hotspot for research. In this field, users can access all necessary information at any time and from any location . Everywhere and at any time, an ubiquitous device cannot establish wired connectivity with other ubiquitous devices. Centralized infrastructure might not always be accessible in a variety of scenarios. As a result, wireless ad hoc networks have been deemed necessary for connecting these widely used devices. Mobile ad-hoc networks and sensor networks are two significant varieties of wireless ad-hoc networks. Ad hoc networks are perfect for scenarios where infrastructure is either unreliable or not feasible. Numerous military, commercial, and mission-critical applications use these networks. Adhoc networks are susceptible to security risks within certain situations.

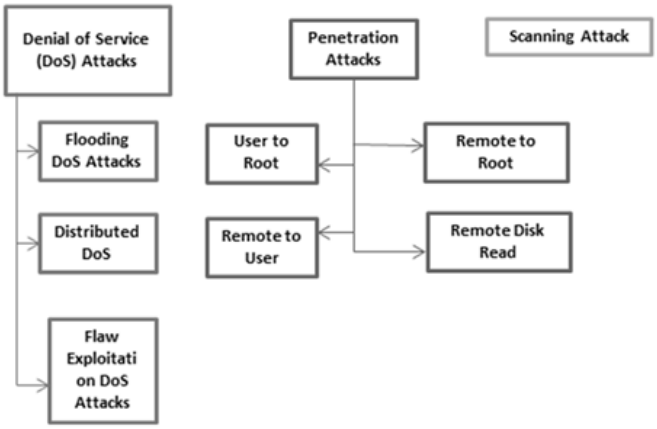

Fig 1: Types of Network Attacks

A Wireless Sensor Network (WSN) is composed of nodes or sensors that are equipped with sensors to monitor the surroundings and send sensed data to the base station or to one or more sinks, which are trusted gateways. WSNs can deploy a large or small number of nodes per unit area, and nodes can be reprogrammed based on the situation [10]. In hostile environments, sensors are set up for environmental monitoring, military surveillance, and other purposes. Home automation and border monitoring are just two of the many uses for WSNs, which are becoming ubiquitous systems[17]. It is frequently necessary for sensors to self-organize in a dispersed fashion. Together with unfavorable operating conditions, the limited computational capacity, memory, and energy supply of sensors make them vulnerable to malfunctions and malevolent attacks, such as message injection, eavesdropping, and impersonation. WSNs are essentially ad hoc networks with stricter limitations. Common methods include public key encryption, secure routing, and tamper-proof hardware.

Security Overview

Due to its higher energy efficiency, multi-hop communication is widely used in wireless Adhoc networks. Additionally, this results in a number of ad-hoc network vulnerabilities. The following discusses the sources that are accountable for these vulnerabilities.

- Channel vulnerabilities: Without a physical channel in the network, an attacker can eavesdrop messages and inject or replay phony messages.
- Node vulnerabilities: Because nodes are not physically protected, they are vulnerable to capture and attacks. Sensitive information can be stolen, network packets can be misrouted, and hardware damage can end a node's network lifetime.
- Network vulnerabilities are increased by decentralized infrastructure, which is characterized by the dispersed nature of node operations without centralized monitoring.
- Frequently changing topology: The network topology is dynamic in wireless communication. As a result, malicious or compromised nodes frequently engage in packet misrouting on networks, resulting in inaccurate routing information. Node mobility, which results from frequent location changes, contributes to network operations malfunctioning.

Security Goals

In wireless ad-hoc networks, the significance and goals of security are as follows.

Availability: Even in cases where the system malfunctions, network operations must always be accessible and serviceable. All nodes are targeted in denial-of-service attacks, which put this security criterion to the test [17]. To disrupt communications in the physical layer and media access control layer, attackers in this instance use jamming techniques. By abusing the key distribution service, attackers also interfere with secure communication and interfere with the network layer's routing protocol [13].

- Data Integrity: Any changes made to messages while they are in transit must be identified quickly to determine whether they were made on purpose or by accident.
- Data confidentiality requires that information be kept private and not is closed to unapproved parties. Although they are common countermeasures, cryptographic techniques re not exclusive to confidential threats..
- Authorization: Network services and other network components are accessible to authorized nodes.
- Authentication: When sending messages over a network, it's critical to confirm the sender's identity. When an attacker gains control of a message, it becomes challenging to discern between authentic and fraudulent messages.
- Non-repudiation: It is necessary to make sure that the person who sent the message is unable to retract their actions.
- Freshness: New information should be shared, and network messages shouldn't be reused. This stops any adversary from deceiving network services.

Security Threats

Depending on behavior and capabilities of attackers, attacks against wireless sensor networks can be classified as follows.

- Attacks by insiders and outsiders: Insiders are malicious nodes that act legitimately, while outsiders are not a part of the network but interfere with its operations.

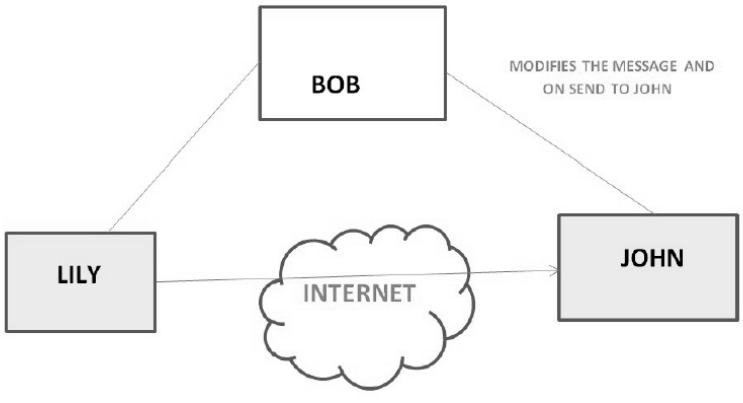

Fig 2: Active attack

- Passive vs. active attack: In Passive attacks occur when an attacker intercepts, steals, collects, or keeps track of packets sent and received within a network. Attackers create fictitious packets, alter or fabricate routing messages, and occasionally pose as authorized users in order to obtain unauthorized privileges.

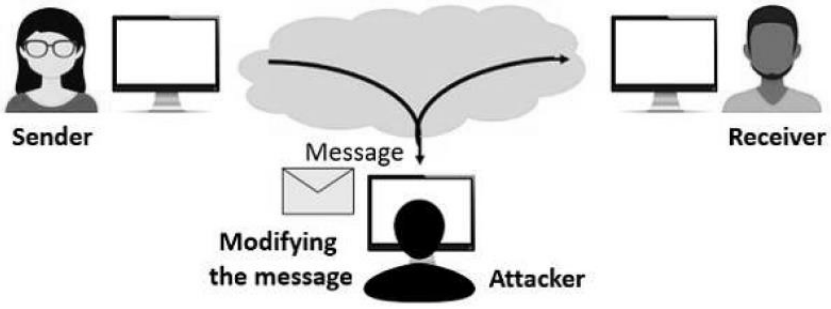

Fig 3: Passive Attack

Taxonomy of Attacks in Wireless Sensor Networks

Our research focuses on network layer attacks that impair network performance and interfere with network availability. There are many different kinds of attacks in WSN. We have focused on the following attacks in this dissertation.

1. **Black hole attack in Mobil Ad-hoc Network**: In a black hole attack on a mobile ad hoc network, compromised nodes discard all incoming packets from nearby nodes. When such black hole nodes appear in a uni-cast or multi-cast route in a MANET, the packet delivery ratio and network throughput drastically decrease. Moreover, average end-to-end latency and routing overhead rise. If these compromised nodes move around, the issue will get worse.
2. **Wormhole attack**: In a wormhole attack, two conspiring attackers are separated by high-speed links and positioned far apart. They record packets at one end, tunnel them through wormhole or high-speed links, and then replay them at the other end. As a result, even though the nodes at the two ends of wormhole links are far apart, they are regarded as neighbors. Every wormhole node has the ability to mimic a shorter path than the one that was originally taken. Wormhole attacks have serious consequences that include packet alteration, network partitioning, and routing disorder. Wormhole attacks can also be combined with eavesdropping or selective forwarding to achieve even more devastating results.
3. **Selective forwarding**: To ensure that packets from a source reach their destination in a multi-hop ad hoc network, nodes rely on one another. Malicious nodes might function as filters, not sending every packet they get to its intended location. An adversary may occasionally intercept packets being transmitted by nearby nodes and cause collisions by selectively forwarding packets.
4. **Sybil attack**: A malicious node assumes several identities in a Sybil attack. Such attacks can readily affect distributed storage algorithms, fault-tolerant schemes, and routing, disrupting multi-path routing protocols and compromising data integrity, among other things.

5. Denial-of-service attacks can occur at the network, MAC, and physical layers. An adversary can initiate denial-of-service attacks at the network layer by flooding packets, creating delays, or sending a large number of route requests. Such attacks often result in performance degradation and network traffic blocking.

2. INTRUSION DETECTION

The purpose of an intrusion detection device is to identify malevolent site visitors. IDS can be imposed in a variety of ways. The most notable of these is anomaly detection. Its foundation is the identification of irregularities in site visitors. Numerous implementations of this approach have been provided, depending on the criteria used to measure traffic profile deviation.

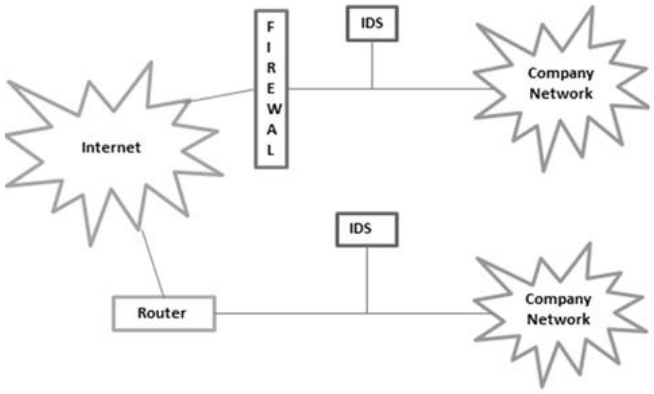

Fig 4: Intrusion Detection Concept

Common wireless network authentication methods and firewall technology can satisfy users' primary safety needs, but they are woefully inadequate in terms of defense against malicious attacks carried out by skilled hackers. Two well-liked intrusion detection techniques, misuse detection and aberrant detection, have issues with low fault detection, false detection rates, and negative feature extraction. Because of their use in IDSys, AI-based detection technique studies make up one of the IDSys hotspots.

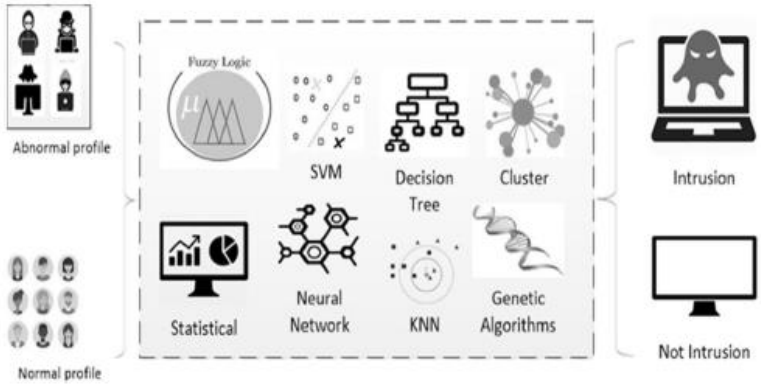

Fig 5: Working of Intrusion Detection System

IDS are divided into two parts according to the techniques employed to detect intrusions. IDS can also be categorized according to the sources of input data used to identify anomalous activity. IDS technology can be broadly classified into two categories based on the data sources: host-based IDS (HIDS) and network-based IDS (NIDS). The operating system, window server logs, firewall logs, application system audits, and database logs are a few of the data sources that HIDS inspects and audits. Network traffic is not a factor in insider assaults that HIDS can detect.

Table 1: Decentralized IDS vs. Centralized IDS

Parameters	Distributed/Decentralized IDS	Centralized IDS
Fault Tolerant	The distributed nature of the intrusion detection system's state makes consistent and recoverable storage more challenging.	The central storage of the intrusion detection system's state facilitates its recovery following a crash.
Scalability	By incorporating additional components as required, a distributed intrusion detection system can expand to accommodate more hosts. Communication amongst the components and the presence of central coordination components may restrict scalability.	The intrusion detection system's fixed number of components limits its size. The analysis components will require additional processing and storage power to handle the load as the number of monitored hosts increases.
Dynamic Reconfiguration	Reconfiguring and restarting individual components won't impact the intrusion detection system as a whole.	All the information is analyzed by a few components. The intrusion detection system probably needs to be restarted in order to reconfigure them.
Overload	Because the components operating on the systems are smaller, there should be minimal overhead. The majority of the systems under observation, however, are subjected to the additional strain.	With the exception of the systems that house the analysis components, which are subjected to a significant load, impose minimal or no overhead on them. It might be necessary to dedicate those hosts to the analysis task.
Execution	More difficult because more parts must be maintained concurrently.	There are comparatively few parts that must be maintained.
Resist Subversion	Monitoring is required for a greater number of components. Nonetheless, components can cross-check one another due to the greater number. Additionally, the parts are typically simpler and smaller.	Fewer components need to be monitored. However, these components are larger, more complex, and difficult to monitor. In this section, we explore some of the more common questions that arise in the field of e-commerce, including how to use e-commerce sustainably.

Host-Based Intrusion Detection

Host-Based Intrusion Detection gathers information from computers, servers, and other host systems and examines it for irregularities or questionable activity. Authentication logs (which document login events) and other security-centric data sources may be among the data that HIDS tools examine. App and operating system logs are among the other types of data that an HIDS usually examines. Unusual patterns

in the latter types of datasets may be connected to security concerns, even though they are not directly related to security.

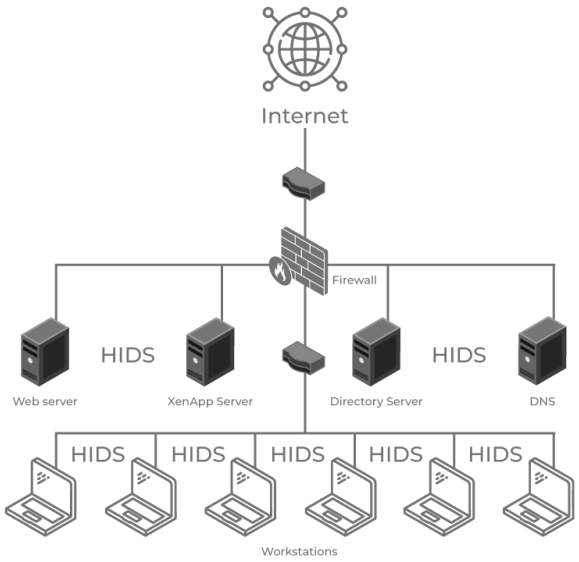

Fig 6: Host based IDS

An application may suddenly start receiving large numbers of requests from unknown external IP addresses, for instance, if an HIDS is monitoring network traffic flows. A brute-force login attempt or an attempt to search the application for security holes that an attacker could exploit could be indicated by this activity. Security teams could use this information to block the offending IP addresses.

Network Based Intrusion Detection System

The most popular type of intrusion detection system (IDS) is a network-based intrusion detection system (NBIDS). This software analyzes network traffic and alerts the system administrator if it detects an attack. The second type of intrusion detection system is called a host-based intrusion detection system (HBIDS). Instead of using the current system, the HIDS examines each host item independently and notifies the host if any odd packets are found. This study examines NIDS, which are separated into two categories: anomaly based and misuse detection.

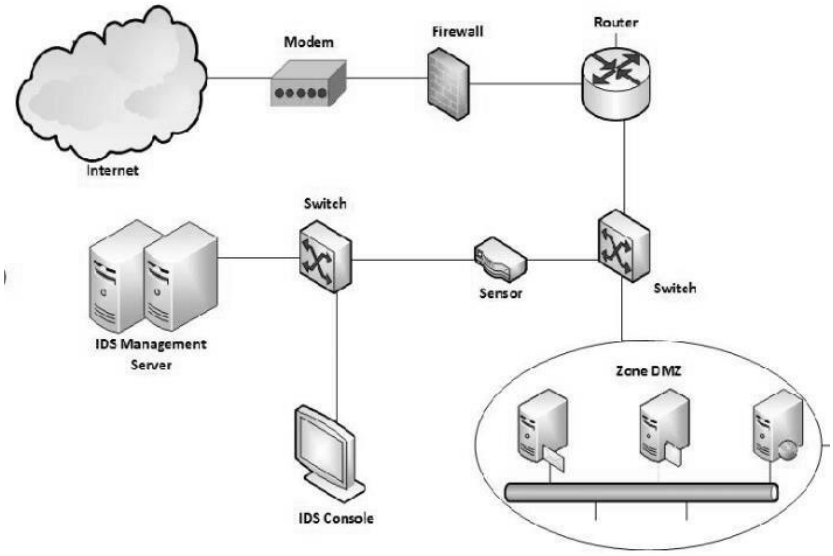

Fig 7: Network Based IDS

A set of attack signatures must be included in the abuse detection system well in advance of their detection. It can't recognize unknown threats as a result. On the other hand, anomaly detection can identify unknown threats because it is predicated on typical usage patterns. The outlier detection system has a high risk of false alarms because it recognizes a variety of common use patterns..

Table 2: HIDS Vs NIDS

IDS Types	Advantages	Disadvantages	Data source
HIDS (Host-based Intrusion Detection System)	• can examine the behavior of encrypted communications from beginning to end. • No additional hardware is needed. checks the host's file system, system calls, or network events to find intrusions. • Each packet is put back together. • Examines the full item rather than just the streams.	• delays in reporting assaults. • uses up host resources. It must be set up on every host. • Only the machine on which it is installed is capable of monitoring attacks.	Audit records, log files, application program interfaces (API), rule patterns, and system calls. In this section, we will explore some of the more common questions that arise in the field of e-commerce, including how to use e-commerce in a sustainable manner.
NIDS (Network-based Intrusion	• NIDS Detects attacks by examining network packets. • You do not need to install on each host.	• Finding attacks in encrypted traffic is a challenge.	• It is difficult to find attacks in encrypted traffic. • It is necessary to have dedicated hardware. It is limited to detecting network attacks.

Detection System)	• Checking different hosts at the same time. • Able to detect the broadest ranges of network protocols. • In this section, we will explore some of the more common questions that arise in the field of e-commerce, including how to use e-commerce in a sustainable manner.	• It is necessary to have dedicated hardware. • It is limited to identifying network attacks. • Analyzing a high-speed network is challenging. Insider attacks pose the greatest threat.	• It is difficult to analyze a high-speed network. • The greatest threat is insider attacks. Simple Network Management Protocol (SNMP) Network packets (TCP/UDP/ICMP) Management Information Base (MIB) Router NetFlow records

Any unauthorized activity that damages a computer system is referred to as intrusion. The goal of an IDS is to detect harmful network intrusion and computer action that a traditional firewall might miss. This is necessary to attain high levels of security against actions that jeopardize the dependability, security, or privacy of computer systems. Two categories of intrusion detection systems (IDS) exist: Anomaly-based IDS (AIDS) and signature-based IDS (SIDS).

Signature based IDS (SIDS)

The premise behind signature or abuse detection techniques is that they store information such as attack or intrusion signatures and trends. via the database. When an intrusion occurs or an attacker attempts to attack, the IDS compares the intrusion signatures with the predetermined signatures that are already saved in the database. When a match was successful, the system sounded an alarm. The IDS analyzes the data it gathers and compares it with large databases of threat signatures as part of misuse detection. In essence, the IDS searches for a specific attack that has been documented in the past. Similar to a virus detection system, detection software is only as good as the database of intrusion signatures it compares with packets.

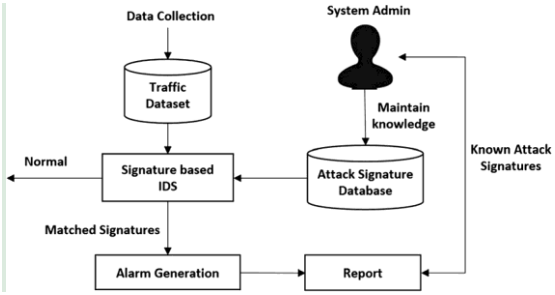

Fig 8: Signature Based IDS

The employment of an expert system to identify intrusions using a pre-existing knowledge base is the basis for misuse detection. This allows misuse systems to identify even the slightest incursions listed in their expert knowledge base with great accuracy; on the other hand, if this expert knowledge base is built correctly, misuse systems can produce relatively few false positives. The less fortunate side effect of this architecture is that a misuse detection system cannot detect intrusions that are not recorded in its

knowledge base. Additionally, subtle variations in well-known attacks may evade detection if a misuse system is poorly built. Therefore, the success of the system mostly rests on the accurate and comprehensive construction of this knowledge base, which usually requires human domain specialists.

Anomaly based IDS (AIDS)

The goal of anomaly detection is to find occurrences that seem out of the ordinary in relation to typical system behavior. The capacity to detect novel and unheard-of attacks is the most alluring aspect of anomaly detection systems.

Various techniques have been explored as alternative solutions to the anomaly detection challenge, including statistical modeling, neural networks, and hidden Markov models. These anomaly-based methods share a common foundation: unusual behavior indicates a potential attack, and the appropriate combination of characteristics can effectively differentiate anomalies from normal system operations.

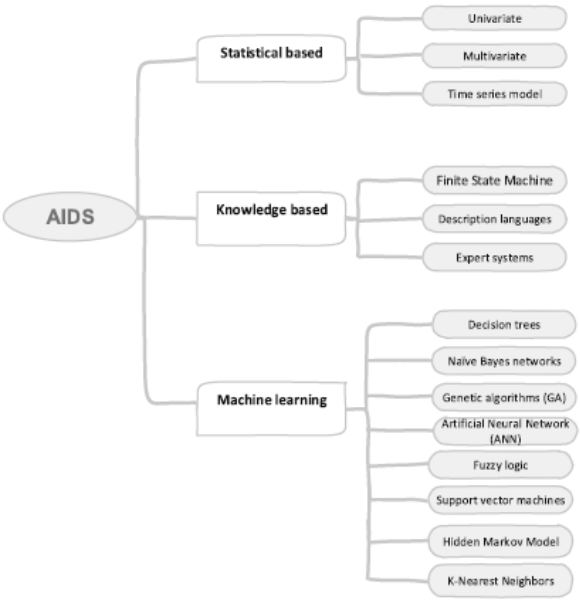

Fig 9: Anomaly based IDS

To execute anomaly detection, the system administrator determines the baseline or typical state of the network traffic load, breakdown, protocol, and average packet size. The anomaly detector monitors network segments and compares their present state with the usual baseline to detect anomalies. The first step in developing such a system is to create a baseline model that represents the normal system behavior and acts as a standard for distinguishing anomalous occurrences. Using this model, the system then assesses an occurrence and uses whether it falls within a particular range of typical behavior to determine whether it is abnormal or normal. Because the process of building a baseline model of typical behavior is usually automated, anomaly systems do not require expert understanding of computer assaults. This approach has certain disadvantages as well, since anomaly detection may overlook known and understood attacks if they do not significantly differ from the regular behavior defined by the system. Anomaly based systems are prone to producing a higher number of false positives because they interpret any unusual

activity as a potential intrusion, even though other factors, such as implementation errors, can also result in behavior that seems out of the ordinary.

Table 3: SIDS Vs AIDS

SIDS	• Very effective in detecting intrusions with low FA. Immediately identify the intrusions. • It is better for detecting known attacks. • It's a simple design. In this section, we will explore some of the more common questions that arise in the field of e-commerce, including how to use e-commerce in a sustainable manner.	• It must be regularly updated with a fresh signature. Slight variations of known attacks may go unnoticed because the system is designed to detect attacks based on known signatures. • Incapable of identifying zero-day attacks. • Multi-step attacks cannot be detected with this method. It offers minimal insight or comprehension of the attacks' nature.
AIDS	• Detection of novel (unknown) attacks is possible. • It is capable of producing intrusion signatures.	• Some attacks can go unnoticed because it is unable to handle encrypted packets. • A high rate of false positive alarms. It is challenging to create a typical profile for dynamic systems. • Unclassified alerts are generated. Initial training is required.

Figure 10 displays the attack models discussed in the preceding sections together with the recommended lines of defense and typical mitigation strategies for each. This figure situates the work covered in the thesis within the context of wireless ad hoc network intrusion detection. The contribution and content of the thesis are based on the point of view that this diagram emphasizes.

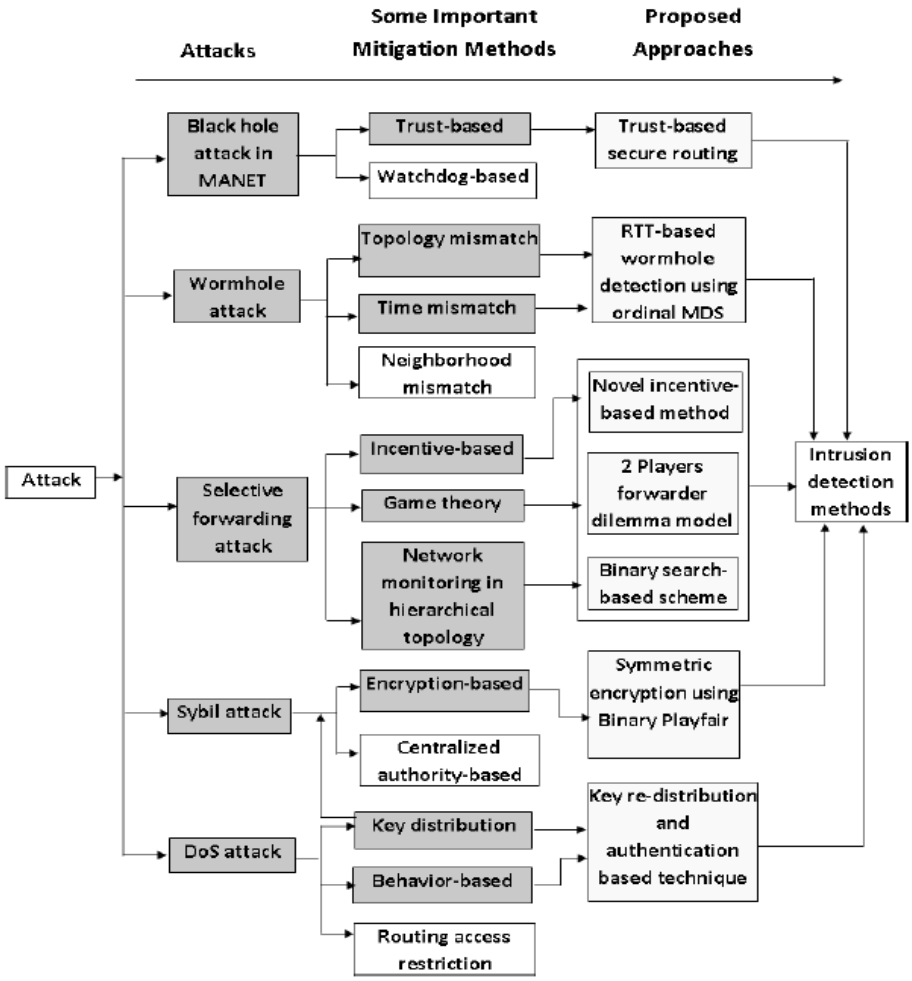

Fig 10: Various attacks and proposed approaches to detect intrusion

3. REVIEW OF LITERATURE

Research conducted between 2020 and 2025 shows that both signature-based and anomaly-based intrusion detection systems have advanced significantly. Although each approach has its own advantages, hybrid models, AI-driven improvements, and domain-specific modifications are progressively addressing their drawbacks. IDS technology is moving toward a more intelligent, independent, and robust future as a result of the confluence of machine learning, interpretability tools, and real-time data analytics. Key techniques, datasets, application areas, and performance indicators for signature-based, anomaly-based, and hybrid intrusion detection systems are highlighted in Table 1, which compiles sample studies from 2020 to 2025.

Year	Detection Method	Domain	Key Insight
2020	Anomaly-Based	Enterprise Networks	Real-time detection accuracy with the help of Dimensionality reduction [3]
2021	Anomaly-Based	Smart Grids	Collaborative learning that protects privacy improves the accuracy of detection. [20]

2023	A network-based intrusion detection system (NIDS)	cloud Environment	Safeguard private information by keeping an eye out for illegal access attempts on the network. [6]
2024	Data Mining classifiers such as K-Neighbors Classifier, Logistic Regression, and Random Forest Classifier.	Big Data/Deep Learning	Effective methodology to find computer network intrusion [14]
2024	A network-based intrusion detection system (NIDS)	Big Data/Deep Learning	Act as a accurate tool to predict high level of intrusion based on network [25]
2024	Identifying attacks in IoT contexts	Internet of Things	The potential for precise intrusion detection using ML-based techniques. [16]
2024	Signature-detection and Anomaly-detection	Internet of Things	Machine learning methods like Support Vector Machines (SVM), Decision Trees, and Random Forests to detect anomalies. [25]
2024	Network intrusion detection system (NIDS)	Artificial Intelligence	a well-rounded strategy that blends modern and traditional techniques to provide a strong defense against a range of online dangers in cloud settings. [65]
2024	Extreme learning machine (ELM) with Genetic Algorithm – GA-ELM	Machine Learning	Enhancement the ELM model's functionality. [2]
2024	K Neighbors Classifier, Logistic Regression, and Random Forest Classifiers are included in NIDS.	Machine Learning	Unique attack patterns are revealed by ICMP, TCP, and UDP protocol analysis, highlighting the necessity of protocol-specific security measures as well as the integration of NIDS with other security systems for a multi-layered defense approach. [4]
2024	block chain with cutting-edge technologies like artificial intelligence (AI) and machine learning (ML).	Endpoint Security	Support a wide range of users and choose future lines of inquiry and development in the crucial field of cyber security. [27]

2024	Network intrusion detection system (NIDS)	edge Computing	Improved defenses against changing cyber threats and resilience. [28]
2024	Machine learning-based approaches such as Gradient Boosting, Decision Trees, and Long Short-Term Memory (LSTM) networks	edge Computing	An ensemble-based detection system to lower computational overhead and increase accuracy. [24]
2024	SVM and Random Forest	fuzzy logic	IDS solutions with LSTM and ANNs that are both dependable and easier to understand. [45]
2025	Signature-Based	Endpoint Security	Automated signatures give the better result to identify network malwares [13]
2025	Anomaly-based and signature-based detection	cloud Environment	Reliable Approach to find and kill cyber threats in cloud environment [52]
2025	AI-based Intrusion Detection Systems	Artificial Intelligence	Identification of different types attacks and Avoiding false alarm [9]
2025	cutting-edge detection and mitigation techniques	Smart Grids	In the context of smart grid security, adversarial machine learning is becoming a growing threat, as are large language models (LLMs). [11]
2025	Signature-based intrusion detection	fuzzy logic	Both SVM and Random Forest are thought to be viable options for practical IDS applications. [54]

Table 4: Survey studies of various Intrustion Detection methods in multiple domains from 2020 to 2025

4. RESULTS AND DISCUSSION

Comparing Signature-Based and anomaly based intrusion detection systems (IDS) provides important insights into their applicability to various cyber security scenarios by exposing subtle trade-offs across several operational parameters. To evaluate the effectiveness of each technique in dynamic threat scenarios, the analysis considered eight key metrics: detection accuracy, false-positive rate, reaction to innovative attacks, computing overhead, maintenance effort, scalability, and real-time performance. Compared to anomaly based IDS, which had an accuracy of 85% and a higher false positive rate of 18%, signature-based IDS fared better in terms of detection accuracy (94%) and showed a noticeably lower false positive rate (3%) than the latter. However, with a score of 8 out of 10 on both criteria, the anomaly based IDS demonstrated a distinct edge in terms of adaptability and reactivity to changing and zero-day threats, underscoring its capacity to uncover new attack routes through behavioral analysis. In contrast, signature-

based IDS only received scores of 5 and 3 in these categories, despite being accurate against known threats owing to their reliance on frequent signature updates. Additionally, because anomaly based IDS rely on resource-intensive methods, they have higher maintenance costs and computational overheads; however, they are more scalable and better suited for distributed or dynamic situations. Both systems performed similarly in real-time, with the Signature-Based IDS outperforming the other by a small margin because of its low processing overhead. This comparison highlights the complementary nature of both strategies; anomaly based IDS are excellent at identifying threats that have not been previously encountered, whereas signature-based IDS provide efficiency and accuracy in threat environments that are well characterized. Therefore, an organization's unique threat exposure, resource availability, and operational priorities should be considered when making a deployment decision.

	Signature Based IDS	Anomaly IDS
Detection Accuracy	94	85
False Positive Rate	3	8

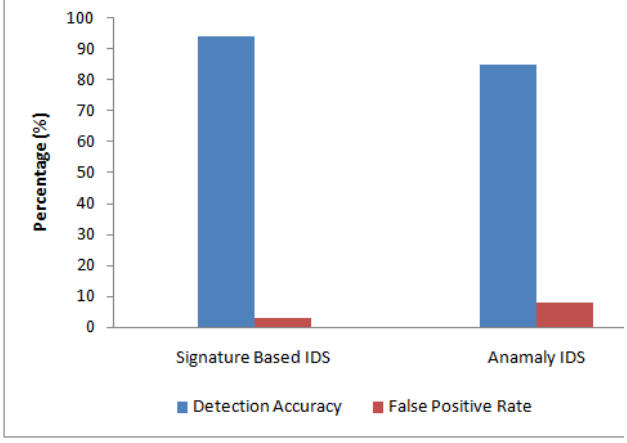

Fig 12: Performance Analysis in terms of Detection Accuracy and False Positive Rate

Comparing different intrusion detection system (IDS) approaches, especially signature-based and anomaly-based IDS, provides valuable insights into the advantages and disadvantages of each approach in terms of different operational metrics. These criteria are essential for assessing IDS's effectiveness, suitability, and overall worth in various cyber security scenarios. Eight comparative metrics—detection accuracy, false positive rate, reaction to emerging threats, computational overhead, maintenance effort, scalability, and real-time performance—are highlighted in the bar chart under consideration. Every metric provides a unique viewpoint on how well these IDS methods function in actual settings, particularly in the face of dynamic and changing threat landscapes.

	Signature Based IDS	Anomaly IDS
Adaptability to new threats	15	8
Possibility of New Threats	3	8
Computational Overhead	8	8
Maintenance Effort	7	5
Scalability	7	8
Performance	9	7

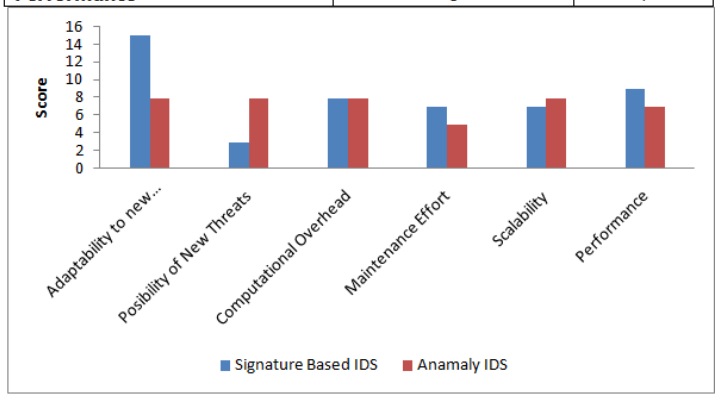

Fig 12: Performance Analysis in terms of reaction to emerging threats, computational overhead, maintenance effort, scalability, and real-time performance

5. CONCLUSION

Cybercriminals target computer users using both sophisticated technology and social engineering strategies. Some cybercriminals are becoming more sophisticated and driven. Cybercriminals have proven that they can use infrastructure that is hard to hack, conceal their communications, obscure their identities, and keep their identities apart from illegal gains. As a result, using advanced intrusion detection systems that can recognize modern malware to protect computer systems is becoming increasingly important. To sum up, the comparison of signature-based versus anomaly-based intrusion detection systems emphasizes how crucial it is to match IDS capabilities to particular organizational needs and threat environments. Although Signature-Based IDS is very good at accurately identifying existing threats, with low false positive rates and effective real-time performance, it is not very flexible or sensitive to new threats. On the other hand, although it has higher false positive rates and computational expenses, anomaly-based intrusion detection systems (IDS) are excellent at seeing new threats and adjusting to different contexts. These opposing advantages and disadvantages imply that there is no one IDS type that is always best; rather, the most complete security posture is provided by a calculated fusion of the two methods. Integrating these systems into layered defense architecture offers the flexibility, precision, and effectiveness required for proactive and resilient cyber security as cyber threats become more complex and varied. In order to keep security measures effective against both present and potential threats, this analysis emphasizes the necessity of ongoing innovation and optimization in IDS systems. Finally, this paper discusses different kinds of network attacks, the working and benefits of the Intrusion Detection System (IDS).

REFERENCES

1. R. Tahri, Y. Balouki, A. Jarrar, and A. Lasbahani, “Intrusion Detection System Using machine learning Algorithms,” ITM Web Conf., vol. 46, p. 02003, 2022, doi: 10.1051/itmconf/20224602003.
2. H. Sadia et al., “Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach,” IEEE Access, vol. 12, no. March, pp. 52565–52582, 2024, doi: 10.1109/ACCESS.2024.3380014.
3. R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim, “Machine-learning-enabled intrusion detection system for cellular connected uav networks,” Electron., vol. 10, no. 13, pp. 1–28, 2020, doi: 10.3390/electronics10131549.
4. G. H S and M. Seetha, “A Novel Intrusion Detection System for Wireless Enterprise Networks using Ensembled Machine Learning Models,” Ijarcce, vol. 12, no. 8, pp. 176–186, 2023, doi: 10.17148/ijarcce.2023.12825.
5. M. A. Talukder, S. Sharmin, M. A. Uddin, M. M. Islam, and S. Aryal, “MLSTL-WSN: Machine Learning-based Intrusion Detection using SMOTETomek in WSNs,” Int. J. Inf. Secur., 2024, doi: 10.1007/s10207-024-00833-z.
6. A. Fatani et al., “Enhancing Intrusion Detection Systems for IoT and Cloud Environments Using a Growth Optimizer Algorithm and Conventional Neural Networks,” Sensors, vol. 23, no. 9, pp. 1–14, 2023, doi: 10.3390/s23094430.
7. B. N. Chiriac, F. D. Anton, A. D. Ioniță, and B. V. Vasilică, “A Modular AI-Driven Intrusion Detection System for Network Traffic Monitoring in Industry 4.0, Using Nvidia Morpheus and Generative Adversarial Networks,” Sensors, vol. 25, no. 1, 2025, doi: 10.3390/s25010130.
8. A. Riaz, H. F. Ahmad, A. K. Kiani, J. Qadir, R. U. R. Rasool, and U. Younis, “Intrusion detection systems in cloud computing: A contemporary review of techniques and solutions,” J. Inf. Sci. Eng., vol. 33, no. 3, pp. 611–634, 2017, doi: 10.6688/JISE.2017.33.3.2.
9. A. Nizam, “A Comparative Study on AI-IDS Artificial Intelligence-Based Intrusion Detection System,” vol. 14, no. 02, pp. 0–4, 2025.
10. V. Ponnusamy, A. Yichiet, N. Z. Jhanjhi, M. Humayun, and M. F. Almufareh, “IoT Wireless Intrusion Detection and Network Traffic Analysis,” Comput. Syst. Sci. Eng., vol. 40, no. 3, pp. 865–879, 2021, doi: 10.32604/CSSE.2022.018801.
11. A. R. Singh et al., “AI-enhanced smart grid framework for intrusion detection and mitigation in EV charging stations,” Alexandria Eng. J., vol. 115, no. December 2024, pp. 603–621, 2025, doi: 10.1016/j.aej.2024.12.061.
12. B. S. Sukhadeo, R. N. Patil, R. Atole, Y. D. Sinkar, U. C. Patkar, and R. Chopade, “MLIDS: A Machine Learning-Based Intrusion Detection System Using the NSLKDD Data,” Int. J. Intell. Syst. Appl. Eng., vol. 12, no. 4s, pp. 167–179, 2024.
13. A. Biju and S. W. Franklin, “Dual Feature-Based Intrusion Detection System for IoT Network Security,” Int. J. Comput. Intell. Syst., vol. 18, no. 1, 2025, doi: 10.1007/s44196-025-00790-y.
14. M. A. Talukder et al., “Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction,” J. Big Data, vol. 11, no. 1, 2024, doi: 10.1186/s40537-024-00886-w.
15. G. Kumar, K. Kumar, and M. Sachdeva, “The use of artificial intelligence based techniques for intrusion detection: A review,” Artif. Intell. Rev., vol. 34, no. 4, pp. 369–387, 2010, doi: 10.1007/s10462-010-9179-5.

16. A. Kaushik and H. Al-Raweshidy, “A novel intrusion detection system for internet of things devices and data,” Wirel. Networks, vol. 30, no. 1, pp. 285–294, 2024, doi: 10.1007/s11276-023-03435-0.
17. Mohammad Taghi Sadeghi, “Strengthening Wireless Network Security: Supervised Machine Learning-Based Intrusion Detection for Enhanced Threat Mitigation,” J. Electr. Syst., vol. 20, no. 4s, pp. 1904–1912, 2024, doi: 10.52783/jes.2280.
18. M. A. Talukder, M. Khalid, and N. Sultana, “A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction,” Sci. Rep., vol. 15, no. 1, pp. 1–23, 2025, doi: 10.1038/s41598-025-87028-1.
19. S. K. R. Mallidi and R. R. Ramisetty, Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: a systematic literature review, vol. 5, no. 1. Springer International Publishing, 2025. doi: 10.1007/s43926-025-00099-4.
20. S. Khan, K. Kifayat, A. Kashif Bashir, A. Gurtov, and M. Hassan, “Intelligent intrusion detection system in smart grid using computational intelligence and machine learning,” Trans. Emerg. Telecommun. Technol., vol. 32, no. 6, 2021, doi: 10.1002/ett.4062.
21. S. Banik, T. Banik, and S. Banik, “Intrusion Detection System in Smart Grid-A Review,” pp. 1–24, 2023, doi: 10.20944/preprints202309.0611.v1.
22. P. Ganesan and S. Arockia Edwin Xavier, “An Intelligent Intrusion Detection System in Smart Grid Using PRNN Classifier,” Intell. Autom. Soft Comput., vol. 35, no. 3, pp. 2979–2996, 2023, doi: 10.32604/iasc.2023.029264.
23. V. Kumar Gandam and E. Aravind, “Enhancing Cloud Security: A Novel Intrusion Detection System Using Deep Learning Algorithms,” 7th Int. Semin. Res. Inf. Technol. Intell. Syst. Adv. Intell. Syst. Contemp. Soc. ISRITI 2024 - Proc., vol. 186, no. 44, pp. 457–462, 2024, doi: 10.1109/ISRITI64779.2024.10963477.
24. A. Kumar, D. S. Ahuja, and D. G. Gupta, “Edge Computing-Based Intrusion Detection System for Wireless Sensor Networks Utilizing Deep Learning Algorithms,” SSRN Electron. J., 2024, doi: 10.2139/ssrn.5038712.
25. F. Ullah, A. Turab, S. Ullah, D. Cacciagrano, and Y. Zhao, “Enhanced Network Intrusion Detection System for Internet of Things Security Using Multimodal Big Data Representation with Transfer Learning and Game Theory,” Sensors, vol. 24, no. 13, 2024, doi: 10.3390/s24134152.
26. A. Nisar, “Intrusion Detection Systems: Categories, Attack Detection and Response,” SSRN Electron. J., 2023, doi: 10.2139/ssrn.4478816.
27. E. I. Elsedimy, H. Elhadidy, and S. M. M. Abohashish, “A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer,” Cluster Comput., vol. 27, no. 7, pp. 9917–9935, 2024, doi: 10.1007/s10586-024-04458-8.
28. A. Singh, “Real Time Intrusion Detection In Edge Computing Using Machine Learning Techniques,” Turkish J. Eng., no. January, 2024, doi: 10.31127/tuje.1516046.
29. D. R. Wilson, “Towards Effective Wireless Intrusion Detection using AWID Dataset,” Theses, no. January, 2021, [Online]. Available: https://scholarworks.rit.edu/theses/10700
30. W. Zhong, N. Yu, and C. Ai, “Applying big data based deep learning system to intrusion detection,” Big Data Min. Anal., vol. 3, no. 3, pp. 181–195, 2020, doi: 10.26599/BDMA.2020.9020003.
31. N. E. Park et al., “Performance evaluation of a fast and efficient intrusion detection framework for advanced persistent threat-based cyberattacks,” Comput. Electr. Eng., vol. 105, no. December 2022, p. 108548, 2023, doi: 10.1016/j.compeleceng.2022.108548.

32. V. Shakhov, O. Sokolova, and I. Koo, “On the suitability of intrusion detection system for wireless edge networks,” Energies, vol. 14, no. 18, pp. 1–13, 2021, doi: 10.3390/en14185954.
33. M. Natkaniec and M. Bednarz, “Wireless Local Area Networks Threat Detection Using 1D-CNN,” Sensors, vol. 23, no. 12, pp. 1–25, 2023, doi: 10.3390/s23125507.
34. N. Sherman and A. Shabtai, “Function-based malware detection technique for android,” Intrusion Detect. Prev. Mob. Ecosyst., pp. 135–164, 2017, doi: 10.1201/b21885.
35. B. Singh and S. Bansal, “A Review : Intrusion Detection System in Wireless Sensor Networks,” Int. J. Comput. Math. Sci., vol. 6, no. 6, pp. 13–19, 2017.
36. A. Pinto, L. Herrera, and Y. Donoso, “Survey on Intrusion Detection Systems Based on Machine,” pp. 1–18, 2023.
37. T. Senthamizhchudar, “Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks by using Fuzzy Technic,” vol. 6, no. 07, pp. 1–4, 2018.
38. S. Murugan and M. Sundara Rajan, “Fuzzy based anomaly intrusion detection system for clustered WSN,” Res. J. Appl. Sci. Eng. Technol., vol. 9, no. 9, pp. 760–769, 2015, doi: 10.19026/rjaset.9.2622.
39. D. Chou and M. Jiang, “A Survey on Data-driven Network Intrusion Detection,” ACM Comput. Surv., vol. 54, no. 9, pp. 1–10, 2022, doi: 10.1145/3472753.
40. R. Mitchell and I. R. Chen, “A survey of intrusion detection in wireless network applications,” Comput. Commun., vol. 42, pp. 1–23, 2014, doi: 10.1016/j.comcom.2014.01.012.
41. Vasudev Karthik Ravindran, Sharad Shyam Ojha, and Arvind Kamboj, “A Comparative Analysis of Signature-Based and Anomaly-Based Intrusion Detection Systems,” Int. J. Latest Technol. Eng. Manag. Appl. Sci., vol. 14, no. 5, pp. 209–214, 2025, doi: 10.51583/ijltemas.2025.140500026.
42. I. Laassar and M. Y. Hadi, “Intrusion detection systems for internet of thing based big data: a review,” Int. J. Reconfigurable Embed. Syst., vol. 12, no. 1, pp. 87–96, 2023, doi: 10.11591/ijres.v12.i1.pp87-96.
43. R. Shanmugavadivu and D. N. Nagarajan, “Network intrusion detection system using fuzzy logic,” Indian J. Comput. Sci. Eng., vol. 2, no. 1, pp. 101–111, 2011, [Online]. Available: http://www.ijcse.com/docs/IJCSE11-02-01-034.pdf
44. J. Dumoulin et al., “UNICITY: A depth maps database for people detection in security airlocks,” Proc. AVSS 2018 - 2018 15th IEEE Int. Conf. Adv. Video Signal-Based Surveill., 2018, doi: 10.1109/AVSS.2018.8639152.
45. N. Kamuni, I. G. A. Cruz, Y. Jaipalreddy, R. Kumar, and V. K. Pandey, “Fuzzy Intrusion Detection Method and Zero-Knowledge Authentication for Internet of Things Networks,” Int. J. Intell. Syst. Appl. Eng., vol. 12, no. 16s, pp. 289–296, 2024.
46. V. G. Saranyavaishalini, A. Ramathilagam, R. Palanikumar, P. Raghavan, P. Gopikannan, and K. Manikandan, “International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING Comprehensive Survey of Deep Learning-Based Intrusion Detection and Prevention Systems for Secure Communication in the Internet of Things,” Orig. Res. Pap. Int. J. Intell. Syst. Appl. Eng. IJISAE, vol. 2024, no. 3, pp. 1822–1828, 2024, [Online]. Available: www.ijisae.org
47. A. H. Farooqi and F. A. Khan, “A survey of intrusion detection systems for wireless sensor networks,” Int. J. Ad Hoc Ubiquitous Comput., vol. 9, no. 2, pp. 69–83, 2012, doi: 10.1504/IJAHUC.2012.045549.

48. M. Hosseini Shirvani and A. Akbarifar, “A Survey Study on Intrusion Detection System in Wireless Sensor Network: Challenges and Considerations,” J. Electr. Comput. Eng. Innov., vol. 12, no. 2, pp. 449–474, 2024, doi: 10.22061/jecei.2024.10148.683.
49. A. Aldaej, I. Ullah, T. A. Ahanger, and M. Atiquzzaman, “Ensemble technique of intrusion detection for IoT-edge platform,” Sci. Rep., vol. 14, no. 1, pp. 1–16, 2024, doi: 10.1038/s41598-024-62435-y.
50. S. N. Dhage, B. B. Meshram, R. Rawat, S. Padawe, M. Paingaokar, and A. Misra, “Intrusion detection system in cloud computing environment,” in Proceedings of the International Conference & Workshop on Emerging Trends in Technology, in ICWET ’11. New York, NY, USA: Association for Computing Machinery, 2011, pp. 235–239. doi: 10.1145/1980022.1980076.
51. Y. Sun and Z. Wang, “Intrusion detection in IoT and wireless networks using image-based neural network classification,” Appl. Soft Comput., vol. 177, p. 113236, 2025, doi: https://doi.org/10.1016/j.asoc.2025.113236.
52. G. Aarthi, S. S. Priya, and W. A. Banu, “RID-Cloud: Spectral Recurrent Neural Network-Based Intrusion Detection in Cloud Environment,” IETE J. Res., vol. 71, no. 2, pp. 499–510, 2025, doi: 10.1080/03772063.2024.2428740.
53. T. Sowmya and E. A. Mary Anita, “A comprehensive review of AI based intrusion detection system,” Meas. Sensors, vol. 28, p. 100827, 2023, doi: https://doi.org/10.1016/j.measen.2023.100827.
54. U. Ahmed et al., “Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering,” Sci. Rep., vol. 15, no. 1, pp. 1–33, 2025, doi: 10.1038/s41598-025-85866-7.
55. M. M. Morshedur Hassan, “Current Studies On Intrusion Detection System, Genetic Algorithm And Fuzzy Logic,” Int. J. Distrib. Parallel Syst., vol. 4, no. 2, pp. 35–47, 2013, doi: 10.5121/ijdps.2013.4204.
56. A. Zibaeirad, F. Koleini, S. Bi, T. Hou, and T. Wang, “A Comprehensive Survey on the Security of Smart Grid: Challenges, Mitigations, and Future Research Opportunities,” pp. 1–30, 2024, [Online]. Available: http://arxiv.org/abs/2407.07966
57. M. A. Talukder, S. Sharmin, M. A. Uddin, M. M. Islam, and S. Aryal, “MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs,” Int. J. Inf. Secur., vol. 23, no. 3, pp. 2139–2158, 2024, doi: 10.1007/s10207-024-00833-z.
58. S. Ahmadi, “Network Intrusion Detection in Cloud Environments: A Comparative Analysis of Approaches,” Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 3, pp. 1–8, 2024, doi: 10.14569/IJACSA.2024.0150301.
59. M. Ramaiah, C. Vanmathi, M. Z. Khan, M. Vanitha, and M. Deepa, “An Efficient Intrusion Detection System to Combat Cyber Threats using a Deep Neural Network Model,” J. ICT Res. Appl., vol. 17, no. 3, pp. 292–315, 2023, doi: 10.5614/itbj.ict.res.appl.2023.17.3.2.
60. F. Siyi et al., “International Journal of Research Publication and Reviews Investigating the Role of Intrusion Detection Systems in Edge Computing : A Comprehensive Review,” no. 6, pp. 6999–7008, 2025.
61. A. Popalzai, “Internetworking security,” Edpacs, vol. 24, no. 1, pp. 1–14, 1996, doi: 10.1080/07366989609451722.
62. K. Zhang, Z. Hu, Y. Zhan, X. Wang, and K. Guo, “A smart grid AMI intrusion detection strategy based on extreme learning machine,” Energies, vol. 13, no. 18, pp. 1–19, 2020, doi:

10.3390/en13184907.
63. Y. Chen, “Big data technology for computer intrusion detection,” Open Comput. Sci., vol. 13, no. 1, 2023, doi: 10.1515/comp-2022-0267.
64. G. Kumar and J. Thakur, “Machine Learning Approaches for Network Intrusion Detection: An Evaluation of their Efficacy in Bolstering Security,” Int. J. Res. Appl. Sci. Eng. Technol., vol. 12, no. 7, pp. 297–307, 2024, doi: 10.22214/ijraset.2024.63565.
65. V. Reddy, R. Sunitha, M. Anusha, S. Chaitra, and A. P. Kumar, “Artificial Intelligence Based Intrusion Detection Systems,” 4th IEEE Int. Conf. Mob. Networks Wirel. Commun. ICMNWC 2024, vol. 04002, 2024, doi: 10.1109/ICMNWC63764.2024.10872055.
66. A. Meliboev, “Iot Network Intrusion Detection System Using Machine Learning Techniques,” Qo‘Qon Univ. Xabarnomasi, vol. 11, pp. 112–115, 2024, doi: 10.54613/ku.v11i11.972.
67. F. Thabit, O. Can, S. Abdaljlil, and H. A. Alkhzaimi, “Enhanced an Intrusion Detection System for IoT networks through machine learning techniques: an examination utilizing the AWID dataset,” Cogent Eng., vol. 11, no. 1, p., 2024, doi: 10.1080/23311916.2024.2378603.
68. H. Gajjar and Z. Malek, “INTELLIGENT SYSTEMS AND APPLICATIONS IN A Secure Model for Detecting Intruder on Cloud Environment,” vol. 12, no. 4, pp. 3436–3438, 2024.
69. K. Alsubhi, “A Secured Intrusion Detection System for Mobile Edge Computing,” Appl. Sci., vol. 14, no. 4, p. 1432, 2024, doi: 10.3390/app14041432.