www.ijarp.com ISSN 2456-9992 Page: 01-13

International Journal Advanced Research Publications

Review Article

Volume: 02
Issue: 08

A REVIEW ON INTRUSION DETECTION SYSTEMS IN IOT NETWORKS

*[1]D. Malarvizhi, [2]Dr. J. Joselin

[1]Assistant Professor, Department of Software Systems and AIML Sri Krishna Arts and Science College, Coimbatore-08, TamilNadu, India.

[2]Associate Professor, Department of Computer Applications Sri Krishna Arts and Science College, Coimbatore-08, TamilNadu, India.

Article Received: 23 June 2026, Article Revised: 13 July 2026, Published on: 01 August 2026

***Corresponding Author: D. Malarvizhi**

Assistant Professor, Department of Software Systems and AIML Sri Krishna Arts and Science College, Coimbatore-08, TamilNadu, India.

Doi: https://doi-doi.org/101555/ijarp.1173

ABSTRACT

The rapid growth of the Internet of Things (IoT) has transformed various sectors, including healthcare, smart homes, transportation, agriculture, and industrial automation, by enabling seamless communication between connected devices. However, the increasing number of IoT devices has also expanded the attack surface, making IoT networks more vulnerable to cyber threats such as malware, denial-of-service (DoS) attacks, botnets, spoofing, and data breaches[4]. Traditional security mechanisms are often insufficient for IoT environments due to the limited processing power, memory, and energy constraints of IoT devices. Intrusion Detection Systems (IDS) have emerged as a critical security solution for monitoring network activities, identifying malicious behaviour, and protecting IoT infrastructures from evolving cyberattacks. This survey provides a comprehensive review of Intrusion Detection Systems designed for IoT networks, discussing their architecture, classifications, detection techniques, and deployment approaches[11]. It examines signature-based, anomaly-based, specification-based, and hybrid IDS models while highlighting the role of machine learning and deep learning algorithms in improving detection accuracy and reducing false alarms. The survey also explores the challenges associated with IoT intrusion detection, including resource limitations, scalability, privacy concerns, real-time detection requirements, and the emergence of sophisticated attacks[5]. Furthermore, recent research trends and future directions, such as edge computing, fog computing, block chain integration, federated

learning, and artificial intelligence-driven IDS, are presented to enhance IoT security. The findings emphasize that an efficient, lightweight, and intelligent IDS is essential for ensuring the confidentiality, integrity, and availability of IoT networks[12]. This survey aims to provide researchers and practitioners with a clear understanding of existing IDS techniques, their strengths and limitations, and potential research opportunities for developing secure and resilient IoT environments.

KEYWORDS: Internet of Things (IoT), Intrusion Detection System (IDS), IoT Security, Cybersecurity, Network Security, Anomaly Detection, Signature-Based Detection, Machine Learning, Deep Learning.

1. INTRODUCTION

1.1 Background

The Internet of Things (IoT) is a rapidly evolving technology that enables billions of physical devices to communicate and exchange data over the Internet. IoT devices are widely deployed in smart homes, healthcare systems, smart cities, industrial automation, agriculture, transportation, and environmental monitoring. These devices collect real-time data, improve operational efficiency, automate processes, and support intelligent decision-making.

Despite these benefits, IoT networks face significant security challenges due to the resource-constrained nature of IoT devices. Most devices have limited processing power, memory, storage, and battery capacity, making it difficult to implement conventional security mechanisms[6]. In addition, IoT environments consist of heterogeneous devices that communicate using different protocols, increasing the complexity of securing the network. These vulnerabilities expose IoT systems to cyberattacks such as malware, Distributed Denial-of-Service (DDoS), botnets, spoofing, replay attacks, unauthorized access, and data theft.

Intrusion Detection Systems (IDS) have emerged as an effective security solution for monitoring network activities and identifying malicious behaviour. IDS helps detect both known and unknown attacks by analysing network traffic and system events, thereby enhancing the confidentiality, integrity, and availability of IoT systems.

1.2 Motivation

The rapid increase in connected IoT devices has significantly expanded the attack surface for cybercriminals. Traditional security solutions, including firewalls and antivirus software, are often insufficient for protecting IoT environments because they are designed for conventional

computing systems with greater computational resources[2]. As cyber threats become more sophisticated, there is a growing need for intelligent and lightweight security mechanisms capable of detecting attacks in real time.

Recent advances in Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), edge computing, and block chain technologies have improved the performance of Intrusion Detection Systems by increasing detection accuracy and reducing false alarms. However, selecting an appropriate IDS for different IoT applications remains challenging due to variations in network architecture, resource availability, and attack types. This motivates the need for a comprehensive survey that reviews existing IDS techniques, compares their strengths and limitations, and identifies emerging research trends for improving IoT security.

1.3 Problem Statement

Although numerous Intrusion Detection Systems have been proposed for IoT networks, several challenges remain unresolved. Many IDS solutions require high computational resources that are unsuitable for resource-constrained IoT devices[8]. Existing detection techniques often suffer from high false positive rates, poor scalability, and limited adaptability to new attack patterns, and increased communication overhead. Moreover, the heterogeneous nature of IoT environments makes it difficult to develop a universal IDS capable of protecting diverse applications effectively.

The continuous evolution of cyber threats demands IDS solutions that are lightweight, accurate, scalable, and capable of detecting both known and unknown attacks in real time. Therefore, a detailed survey is required to analyse current IDS approaches, evaluate their effectiveness, identify research gaps, and provide recommendations for future developments in IoT network security.

1.4 Research Objectives

The primary objectives of this survey are:

- To provide a comprehensive overview of Intrusion Detection Systems used in IoT networks.
- To examine different types of IDS, including signature-based, anomaly-based, specification-based, and hybrid approaches.
- To analyse the application of Machine Learning, Deep Learning, and Artificial Intelligence techniques in intrusion detection.
- To compare existing IDS techniques based on detection accuracy, computational complexity, scalability, response time, and resource consumption.

- To identify the major security challenges and limitations associated with IoT intrusion detection.
- To review recent advancements such as edge computing, fog computing, block chain, and federated learning in enhancing IDS performance.
- To highlight current research gaps and suggest future research directions for developing intelligent, lightweight, and efficient IDS solutions for IoT networks.

2. MATERIALS AND METHODS

2.1 Internet of Things (IoT)

The Internet of Things (IoT) refers to a network of interconnected physical devices that communicate with each other through the Internet. These devices are equipped with sensors, actuators, processors, and communication modules that enable them to collect, transmit, and process data automatically. IoT technology is widely used in applications such as smart homes, healthcare, agriculture, transportation, industrial automation, and smart cities. The main objective of IoT is to improve efficiency, automate processes, and provide real-time monitoring and decision-making. However, the increasing number of connected devices also introduces significant security risks due to their limited computational resources and diverse communication protocols.

2.2 Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a security mechanism that continuously monitors network traffic and system activities to detect unauthorized access, malicious behavior, and cyberattacks. Unlike preventive security mechanisms such as firewalls, IDS focuses on identifying suspicious activities after they occur and generates alerts for administrators to take appropriate action. In IoT environments, IDS plays a crucial role in protecting devices and networks from threats such as malware, botnets, spoofing attacks, replay attacks, and Distributed Denial-of-Service (DDoS) attacks. A well-designed IDS improves the confidentiality, integrity, and availability of IoT systems.

2.3 Importance of IDS in IoT Networks

IoT devices are often deployed in open and distributed environments, making them attractive targets for cybercriminals. Many devices have limited processing power, memory, storage, and battery capacity, which restrict the implementation of complex security solutions[13]. As a result, Intrusion Detection Systems have become an essential component of IoT security. IDS provides continuous monitoring, early detection of attacks, real-time alert generation,

and support for incident response. It helps prevent unauthorized access, minimizes data loss, protects user privacy, and enhances the overall resilience of IoT networks.

2.4 Architecture of an Intrusion Detection System

A typical IDS for IoT networks consists of several functional components that work together to detect malicious activities.

- **Data Collection Module:** Collects network traffic, system logs, sensor data, and device activities from IoT nodes.
- **Data Pre-processing Module:** Cleans, filters, and transforms the collected data into a suitable format for analysis.
- **Detection Engine:** Analyses the processed data using predefined rules, statistical methods, or machine learning algorithms to identify suspicious behaviour.
- **Alert Generation Module:** Generates notifications when an intrusion or abnormal activity is detected.
- **Response Module:** Initiates appropriate actions such as blocking malicious traffic, isolating compromised devices, or informing the network administrator.

2.5 Types of Intrusion Detection Systems

2.5.1 Network-Based Intrusion Detection System (NIDS)

A Network-Based IDS monitor's network traffic flowing between IoT devices and communication gateways. It detects attacks by analysing packets passing through the network without affecting individual devices. NIDS is suitable for identifying network-wide attacks such as DDoS, port scanning, and malware propagation.

2.5.2 Host-Based Intrusion Detection System (HIDS)

A Host-Based IDS operates directly on individual IoT devices or gateways. It monitors system logs, file integrity, application behaviour, and operating system activities to detect suspicious actions occurring within a specific device. HIDS is effective in identifying insider attacks and unauthorized modifications.

2.5.3 Distributed Intrusion Detection System (DIDS)

A Distributed IDS consists of multiple IDS sensors deployed across different IoT devices and network segments. These sensors share security information with a central management system to provide comprehensive monitoring of the entire IoT network. DIDS improves detection accuracy and supports large-scale IoT deployments.

2.6 Intrusion Detection Techniques

Signature-Based Detection

Signature-based IDS identifies attacks by comparing network activities with a database of known attack signatures. It provides high accuracy for previously identified threats but cannot detect newly emerging or unknown attacks.

Anomaly-Based Detection

Anomaly-based IDS establishes a model of normal network behaviour and identifies deviations from this baseline as potential intrusions. It can detect zero-day attacks and previously unknown threats but may produce a higher number of false alarms.

Specification-Based Detection

Specification-based IDS uses predefined rules that describe the expected behaviour of IoT devices and applications. Any activity violating these specifications is treated as suspicious. This approach combines the advantages of signature-based and anomaly-based detection while reducing false positives.

Hybrid Detection

Hybrid IDS integrates two or more detection techniques, such as signature-based and anomaly-based methods, to improve detection accuracy. Hybrid systems can identify both known and unknown attacks while maintaining lower false alarm rates.

2.7 Common Cyberattacks in IoT Networks

IoT networks are exposed to various cyber threats due to their large-scale deployment and limited security capabilities. Some of the most common attacks include:

- **Distributed Denial-of-Service (DDoS):** Overwhelms network resources by sending excessive traffic, making services unavailable.
- **Malware Attacks:** Infect IoT devices to steal information, damage systems, or create botnets.
- **Botnet Attacks:** Compromised IoT devices are remotely controlled to launch coordinated cyberattacks.
- **Spoofing Attacks:** Attackers impersonate legitimate devices or users to gain unauthorized access.
- **Replay Attacks:** Previously transmitted data packets are captured and retransmitted to deceive the system.

- **Man-in-the-Middle (MitM) Attacks:** Attackers intercept and modify communication between two IoT devices without their knowledge.

2.8 Challenges of IDS in IoT Networks

Designing an effective IDS for IoT environments is challenging because of several factors:

- Limited processing power, memory, and battery life of IoT devices.
- Large-scale deployment involving thousands of interconnected devices.
- Diverse communication protocols and heterogeneous network architectures.
- Requirement for real-time intrusion detection with minimal latency.
- High false positive and false negative rates in some detection methods.
- Privacy concerns related to monitoring user and device data.
- Continuous evolution of sophisticated cyber threats.

3. IOT SECURITY CHALLENGES

The rapid growth of the Internet of Things (IoT) has revolutionized various sectors by connecting billions of smart devices. However, the unique characteristics of IoT networks, such as limited resources, heterogeneous devices, and large-scale connectivity, introduce several security challenges[15]. These challenges make IoT environments more vulnerable to cyberattacks and increase the need for efficient Intrusion Detection Systems (IDS). The major IoT security challenges are discussed below.

3.1 Resource Constraints

Most IoT devices have limited processing power, memory, storage capacity, and battery life. These limitations make it difficult to implement traditional security mechanisms such as complex encryption algorithms and advanced intrusion detection techniques. Therefore, lightweight and energy-efficient security solutions are required for IoT environments.

3.2 Device Heterogeneity

IoT networks consist of a wide variety of devices manufactured by different vendors. These devices use different hardware configurations, operating systems, communication protocols, and security standards. Such diversity makes it difficult to establish a unified security framework and increases the complexity of intrusion detection.

3.3 Scalability

The number of IoT devices continues to grow rapidly, creating large and highly dynamic networks. As the network expands, monitoring all connected devices and detecting attacks in

real time becomes increasingly challenging. Intrusion Detection Systems must be scalable enough to handle millions of connected devices without reducing detection performance.

3.4 Authentication and Access Control

Weak authentication mechanisms are one of the major security concerns in IoT networks. Many IoT devices use default passwords or simple authentication methods, making them vulnerable to unauthorized access. Strong authentication and proper access control policies are essential to prevent attackers from compromising IoT devices.

3.5 Data Privacy and Confidentiality

IoT devices collect and transmit sensitive information such as personal, financial, industrial, and healthcare data. If this information is intercepted or accessed by unauthorized users, it can lead to serious privacy violations. Protecting data confidentiality through secure communication and encryption is a significant challenge.

3.6 Data Integrity

Maintaining the integrity of data is essential for reliable IoT operations. Attackers may modify, delete, or manipulate transmitted data, leading to incorrect decisions or system failures. Security mechanisms must ensure that data remains accurate and unaltered during transmission and storage.

3.7 Availability and Denial-of-Service (DoS) Attacks

IoT services must remain continuously available for users and applications[11]. However, attackers often launch Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks to overload network resources and disrupt normal operations. Ensuring high availability while defending against such attacks remains a major challenge.

3.8 Secure Communication

IoT devices communicate using various wireless technologies such as Wi-Fi, Bluetooth, Zigbee, LoRaWAN, and 5G. Securing these communication channels is difficult because each protocol has different security requirements and vulnerabilities. Encryption and secure communication protocols are necessary to protect data transmission.

4. RESULT AND DISCUSSION

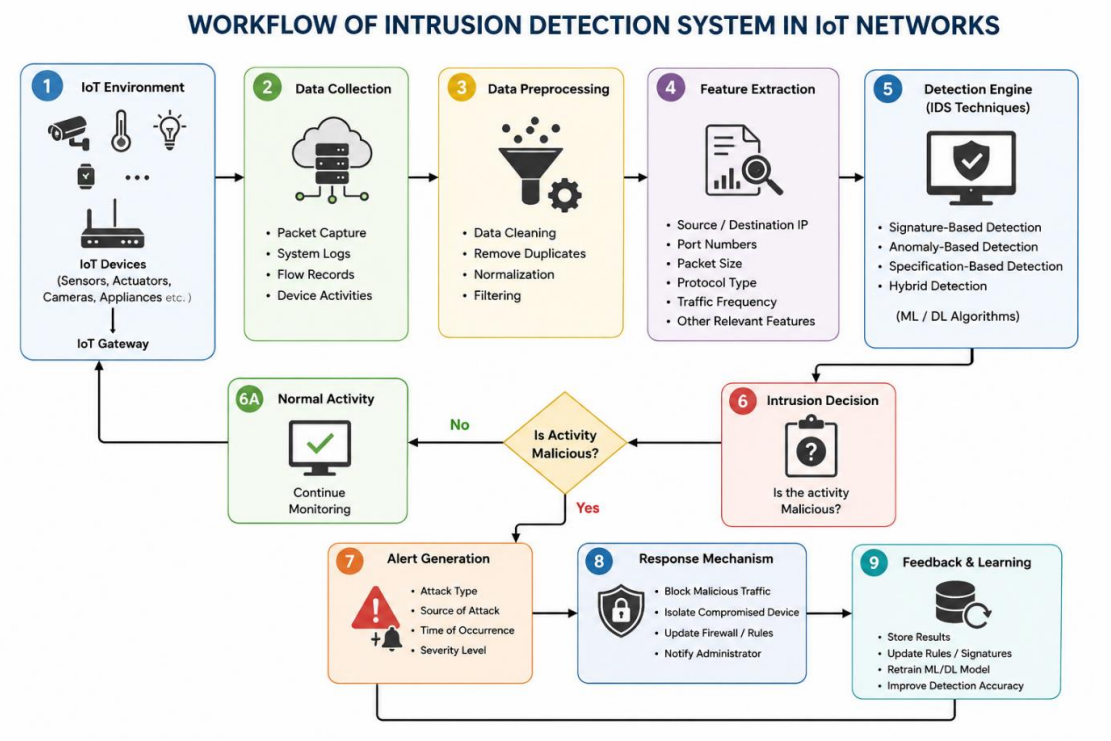

Figure 1: workflow of an Intrusion Detection System (IDS) in IoT networks.

4.1. Explanation of the Workflow

The workflow of an Intrusion Detection System (IDS) in IoT networks begins with IoT devices generating and transmitting data. This data is collected and pre-processed by removing unnecessary information and extracting important features such as IP addresses, protocols, and packet details. The Intrusion Detection Engine then analyses the data using signature-based, anomaly-based, specification-based, or hybrid detection techniques. If suspicious activity is detected, the IDS generates an alert and initiates appropriate response actions, such as blocking malicious traffic, isolating the affected device, or notifying the administrator. Finally, the system updates its detection rules or machine learning model through feedback and learning, enabling continuous improvement in detecting future cyberattacks.

The Response Mechanism takes appropriate actions such as blocking malicious traffic, isolating compromised devices, notifying the network administrator, and updating security policies or firewall rules. Finally, the Feedback and Learning Module stores detection results and updates attack signatures or retrains machine learning models.

4.2.Flow chart

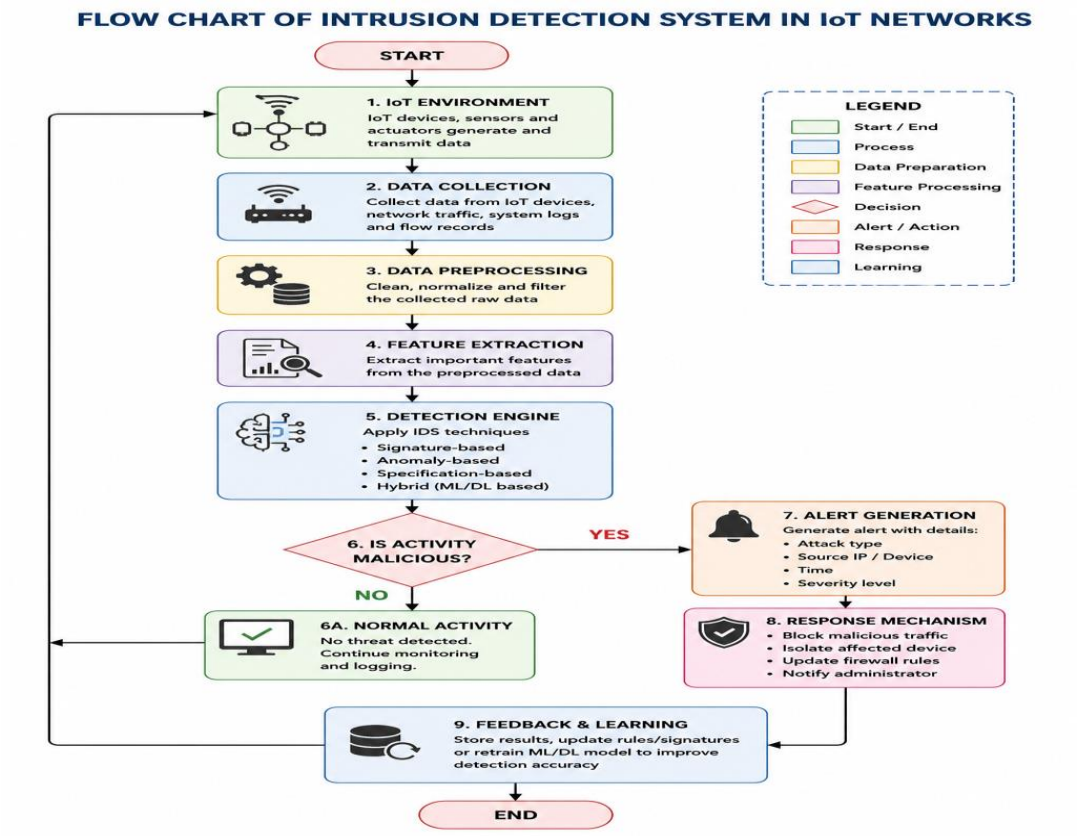

Figure 2: Flow chart of an Intrusion Detection System (IDS) in IoT networks.

4.3.Performance Comparison

The performance comparison of Intrusion Detection Systems (IDS) in IoT networks shows that each detection approach has its own strengths and limitations. **Signature-based IDS** provides high accuracy for detecting known attacks and has a low false positive rate, but it cannot detect new or zero-day attacks. **Anomaly-based IDS** is effective in identifying unknown attacks by detecting abnormal behaviour; however, it often generates a higher number of false alarms

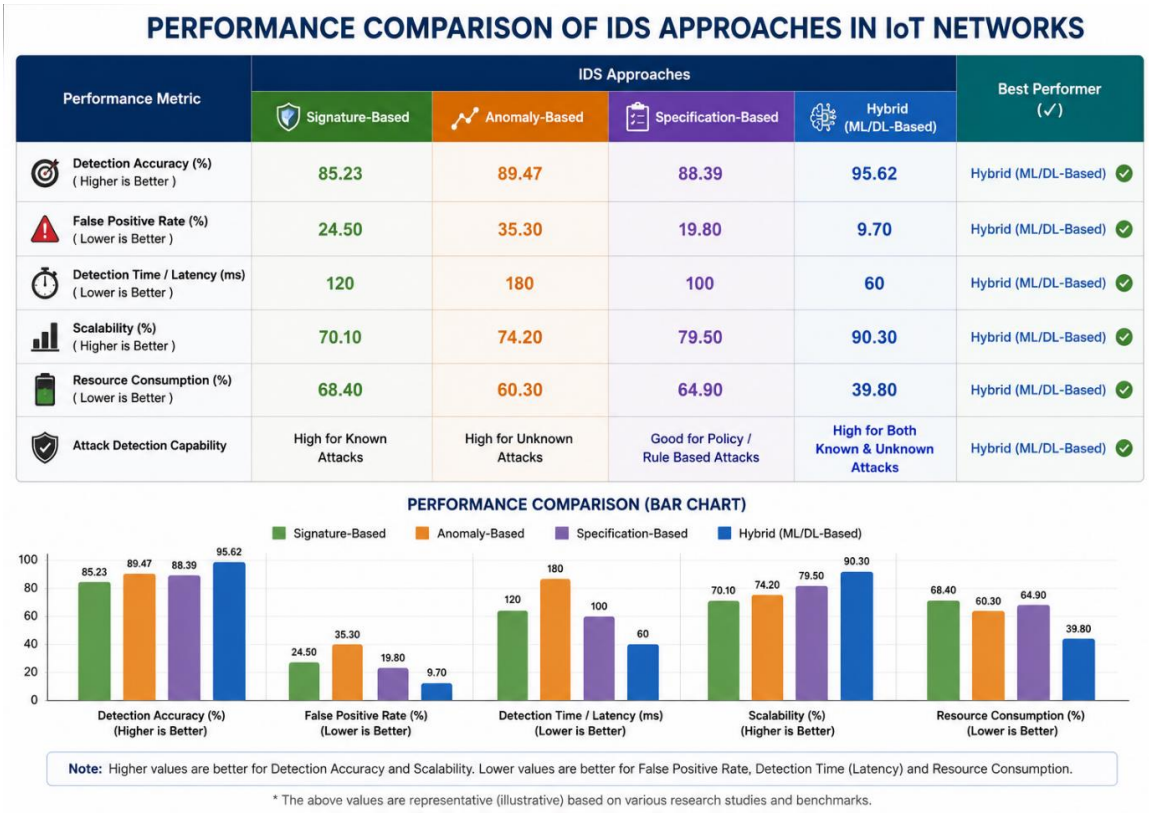

Figure 3:Performance Comparison.

Specification-based IDS detects intrusions by comparing system behaviour with predefined rules, offering balanced accuracy and moderate resource consumption. **Hybrid IDS**, which combines multiple detection techniques and often incorporates Machine Learning or Deep Learning, achieves the highest detection accuracy with fewer false positives. Although Hybrid IDS requires greater computational resources and implementation complexity, it offers better scalability, adaptability, and overall security performance. Therefore, Hybrid IDS is considered the most suitable solution for protecting modern IoT networks against evolving cyber threats.

V.CONCLUSION

The Internet of Things (IoT) has transformed modern technology by enabling seamless communication among connected devices across various application domains. However, the rapid growth of IoT networks has also increased their exposure to cyber threats, making network security a critical concern. Intrusion Detection Systems (IDS) play a vital role in identifying malicious activities, preventing unauthorized access, and ensuring the confidentiality, integrity, and availability of IoT data.

This survey reviewed the fundamentals of IDS in IoT networks, including their architecture, workflow, classification, and deployment models. It also discussed common IoT security challenges, various intrusion detection techniques, and the application of Artificial Intelligence, Machine Learning, and Deep Learning for improving detection accuracy. A comparative analysis showed that while signature-based and anomaly-based IDS have individual strengths, hybrid IDS provides better overall performance by effectively detecting both known and unknown attacks with higher accuracy.

VI.REFERENCES

5. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, *17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095
6. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
7. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, *78*, 544–546. https://doi.org/10.1016/j.future.2017.07.060
8. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, *28*(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003
9. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
10. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., & Iorkyase, E. (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. 2016 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1–6). IEEE. https://doi.org/10.1109/ISNCC.2016.7746067
11. Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, *41*(4), 1690–1700. https://doi.org/10.1016/j.eswa.2013.08.066
12. Mitchell, R., & Chen, I. R. (2014). A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys, 46*(4),* Article 55. https://doi.org/10.1145/2542049

13. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
14. Stallings, W. (2018). Network security essentials: Applications and standards (6th ed.). Pearson.
15. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer networks (5th ed.). Pearson.
Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE* Access, 7, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334
16. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet of Things. IEEE Internet of Things Journal, *4*(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844