Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/ IJAR01/ 21302
DOI URL: http://dx.doi.org/10.21474/ IJAR01/ 21302
ISSN NO. 2320-5407

RESEARCH ARTICLE

The National Conference on Innovative Trends in Modern Business Environment (ITMBE 2025) , DPG Institute of Technology and Management (DPGITM) Gurugram

SECURING THE INTERNET OF THINGS: A COMPREHENSIVE REVIEW OF INTRUSION DETECTION SYSTEMS

Dr. Anju Rani, Dr. Nidhi Sharma and Ms. Varsha Yadav
1. Asstt. Prof., CAD, DPGITM, Gurugram

Manuscript Info

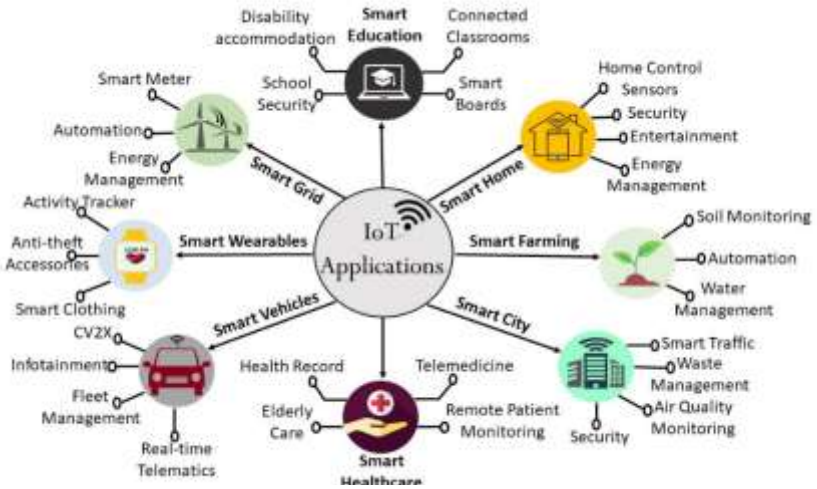
Key words:-
Intrusion, Intrusion detection system, Security, IoT

Abstract

The Internet of Things (IoT) is rapidly advancing, significantly impacting both daily life and large-scale industrial systems. However, this progress has also drawn the attention of cybercriminals, making IoT devices a target for malicious activities and potential attacks on end nodes. To address these threats, numerous IoT Intrusion Detection Systems (IDS) have been developed, which can be categorized based on detection technique, validation strategy, and deployment strategy.
This survey paper offers a comprehensive review of contemporary IoT IDS. Additionally, it examines how current IoT IDS identify intrusive attacks and ensure secure communications within the IoT ecosystem. The paper also classifies different types of IoT attacks and discusses future research challenges aimed at enhancing IoT security.

Introduction:-

The Internet of Things (IoT) represents an emerging field focused on the collection and transmission of data autonomously, without human intervention. It encompasses a network of interconnected objects embedded with sensors, software, and control systems. Advancements like machine learning have propelled the evolution of IoT technology [1].
IoT applications are becoming increasingly prevalent across various domains, as illustrated in Fig. 1. In today's era, virtually every sector is embracing connected devices to keep pace with the world's advancements. Education, for instance, has transitioned beyond traditional methods, with connected classrooms facilitating innovative learning approaches. Technologies such as connected gloves and tablets are aiding differently-abled students, including those with hearing impairments, in their educational journeys. Moreover, IoT holds significant promise for assisting other disabled students as well. In the fast-paced modern lifestyle, smart homes and cities are emerging to address fundamental human needs such as security, waste management, air quality enhancement, and entertainment.



The Internet of Things (IoT) consists of interconnected systems of devices that enable seamless information exchange between physical devices. These devices include medical and healthcare equipment, driverless vehicles, industrial robots, smart TVs, wearable's, and smart city infrastructures, all of which can be remotely monitored and controlled. IoT devices are expected to become more widespread than mobile devices and will handle highly sensitive information, such as personal data. Consequently, this will expand the attack surface and increase the likelihood of cyber attacks. Given the critical importance of security in IoT applications, developing robust IoT intrusion detection systems are essential to ensure secure communications facilitated by IoT technologies.

This paper reviews the state-of-the-art in IDS for IoT, examining their classifications, detection techniques, and the challenges they face.

1. Types of IDS in IoT

IDS in IoT can be broadly categorized into several types based on their deployment and detection methodologies [2] [3] :

2.1 Network-based IDS (NIDS)

NIDS monitor network traffic for suspicious activities. They are deployed at strategic points within the network to analyze incoming and outgoing traffic.

2.2 Host-based IDS (HIDS)

HIDS are installed on individual devices to monitor and analyze the internal state of the device for signs of compromise.

2.3 Hybrid IDS

Hybrid IDS combine the features of NIDS and HIDS, providing a more comprehensive security solution by monitoring both network traffic and host activities.

2. Detection Techniques

The effectiveness of an IDS depends on its detection technique. The primary techniques include [4][5]:

3.1 Signature-based Detection

This technique uses predefined patterns of known attacks to identify intrusions. It is effective against known threats but fails to detect new or unknown attacks.

3.2 Anomaly-based Detection

Anomaly-based IDS establish a baseline of normal behavior and detect deviations from this baseline. This method can identify novel attacks but may suffer from high false positive rates.

3.3 Specification-based Detection

This approach involves defining a set of rules or policies that describe the correct behavior of the system. Any deviation from these specifications is flagged as a potential intrusion.

3. Review of Literature

Khraisat (2021) summarizes recent research and explores contemporary models aimed at improving IoT IDS performance to address security issues [1]. Additionally, the paper discusses the limitations of traditional IoT IDS, current IDS challenges, and future research directions. To develop reliable IoT IDS for heterogeneous device categories, the paper identifies four crucial elements: Low false alarm rates due to large data volumes, High adaptability to IoT communication systems' extreme conditions, Capability to detect zero-day attacks and Autonomous operation using machine learning and deep learning techniques. Future IoT IDS should also feature self-configuration, self-optimization, self-protection, and self-healing.

Philokypros et al. (2018)presented a high-level IDS architecture and its main components, focusing on both centralized and distributed modules for detecting intrusions from external networks and internal compromised nodes [6]. The proposed IDS was developed and tested on the Cooja simulator, which supports application development for the Contiki OS. An attack scenario was demonstrated in Cooja, where a compromised node performed DoS attacks using "Hello" flooding and version number modification, leading to some nodes becoming unreachable and negatively impacting their power consumption. Future work includes implementing and testing the proposed design in Cooja, improving IDS performance by reducing false positives during attack detection, and importing the IDS modules to Contiki OS for testing in a real-world IoT environment.

Sheikh et al. (2019) proposed a signature-based IDS using a fast pattern matching algorithm that excels in detecting known attacks [7]. The simulation results indicate promising potential for future research. Graphs illustrating the occurrence of false alarms were presented. Our ongoing efforts aim to transition this offline IDS into a real-time efficient intrusion detection and prevention system (IDPS) that will not only detect abnormal network traffic but also protect networks from suspicious activities.

Snehi (2020) discussed various signature-based Intrusion Detection Systems (IDS) and their advantages [8]. By using a set of signatures and basic patterns that estimate the relative importance of each IDS feature, system administrators can identify cyber-attacks and network threats. Signature-based detection methods can easily and promptly detect 80% of incidents if used as a precautionary measure for vulnerability detection. The remaining 20% of incidents can be detected by anomaly-based IDS, which compares definitions of normal activity with observed events to identify significant deviations and flag suspicious traffic. Applying the Pareto principle ("80/20 rule"), 80% of events can be effectively detected by signature-based methods, making them fundamentally important. The remaining 20% of problems cause 80% of the issues, which can be addressed through focused behavioral research and anomaly-based detection.

Liu et al. (2020) explore efforts to enhance IoT security through anomaly detection on the IoT Network Intrusion Dataset using multiple machine learning approaches [9]. Notably, high accuracies are achieved alongside efficiency, such as 99% accuracy with KNN in 2 minutes and 97% accuracy with XGBoost in 10.8 seconds. Consistency between F1 scores and accuracies is observed. Future research directions include expanding from binary to multiclass classification, normalizing data to improve accuracy in LR approaches, and ultimately developing a secure IoT framework equipped with efficient IDS for Smart environments.

Shurman et al. (2019) presented a hybrid-based IDS for IoT networks, proposing a framework scheme to detect suspicious network traffic from any node [10]. This approach involves conducting experiments with datasets of IPs to assess the framework's ability to identify unusual packets and preemptively block unwelcome IPs before they escalate into potential DoS threats. In future work, involves to develop and implement an IP sniffer compatible with their framework and conduct comprehensive testing in a mobile setting. Additionally, enhance the IDS performance by reducing false positives during the initial detection phase of suspected IoT DoS attacks.

Otoum (2021) proposed a model that combines signature-based and anomaly-based IDS, structured into three phases: traffic filtering, preprocessing, and hybrid IDS [11]. In the traffic filtering phase, features of incoming packet streams are extracted and validated by the IoT gateway. During preprocessing, these features are converted into numeric values, normalized, and redundancy is reduced. In the hybrid IDS phase, signature-based IDS is applied using signature

matching and the Light Net algorithm, while unknown packets are processed by an anomaly-based IDS using a deep Q-learning algorithm for attack classification. The AS-IDS model shows significant improvement over other IDS methods. Future work includes incorporating additional critical attacks from various datasets, integrating an Intrusion Prevention System (IPS) for autonomous attack response, and enhancing security with biometric and other authentication methods.

Gulhare et al. (2022) introduced a Mean-Shift and Local Outlier Factor (LOF) based ensemble machine learning (ML) approach for anomaly detection in IoT devices [12]. The UNSW-NB15 IoT-based network dataset is utilized for model evaluation. LOF is employed in conjunction with Mean-Shift clustering for clustering, while an ensemble of ML techniques is utilized for classifying usual or unusual activities. The proposed model undergoes testing and evaluation using various performance metrics including Precision (P), Recall (R), Accuracy (ACC), and F1-score. Through comprehensive evaluation and comparison with different ML methods, the proposed model demonstrates superior performance in anomaly detection.

Alghamdi (2023) presents a deep ensemble-based Intrusion Detection System (IDS) using the Lambda architecture, implementing a multi-pronged classification approach [13]. For binary classification, Long Short-Term Memory (LSTM) is used to differentiate between malicious and benign traffic. For multi-class classification, an ensemble of LSTM, Convolutional Neural Network (CNN), and Artificial Neural Network (ANN) classifiers is utilized to identify the types of attacks. Model training occurs in the batch layer, while real-time evaluation is performed through model inferences in the speed layer of the Lambda architecture. This approach achieves a high accuracy of over 99.93% and optimizes processing time due to the efficient classification strategy and the Lambda architecture.

Table 1 summarizes the main contributions, methodologies, results, and future directions of various research efforts aimed at enhancing IoT Intrusion Detection Systems (IDS).

Table 1: Summary of contributions

Author(s)	Key Focus	Methodology	Results	Future Work
Khraisat [1]	Summarizes IoT IDS research and contemporary models	Review of existing models and identification of key elements for reliable IDS	Identifies elements: low false alarm rates, high adaptability, zero-day attack detection, autonomous operation	Focus on self-configuration, self-optimization, self-protection, self-healing
Philokypros et al. [6]	High-level IDS architecture	Centralized and distributed modules; Tested on Cooja simulator	Demonstrated DoS attack scenario; Identified impacts on node reach ability and power consumption	Implement and test in real-world environments; Reduce false positives; Improve IDS performance
Sheikh et al. [7]	Signature-based IDS	Fast pattern matching algorithm	Promising potential for future research; Presented false alarm occurrence graphs	Transition to real-time IDPS; Enhance detection and prevention capabilities
Snehi [8]	Signature-based IDS and advantages	Set of signatures and basic patterns for detection	Effective in detecting 80% of incidents using signature-based methods	Focus on anomaly-based detection for the remaining 20%; Apply Pareto principle
Liu et al. [9]	Enhancing IoT security through anomaly detection	Multiple machine learning approaches	High accuracies achieved: 99% with KNN in 2 minutes, 97% with XGBoost	Expand to multiclass classification; Normalize data for improved accuracy;

			in 10.8 seconds	Develop a secure IoT framework
Shurman et al. [10]	Hybrid-based IDS for IoT networks	Framework for detecting suspicious traffic; Experiments with datasets	Effective in identifying unusual packets and preemptively blocking unwelcome IPs	Develop and implement IP sniffer; Comprehensive testing in mobile settings; Reduce false positives
Otoum [11]	Combining signature-based and anomaly-based IDS	Three-phase model: traffic filtering, preprocessing, hybrid IDS	Significant improvement over other IDS methods	Incorporate additional critical attacks; Integrate IPS for autonomous response; Enhance security with biometric methods
Gulhare et al. [12]	Ensemble ML approach for anomaly detection in IoT devices	Mean-Shift and Local Outlier Factor (LOF) with ensemble ML techniques	Superior performance in anomaly detection; Evaluated with various metrics (Precision, Recall, Accuracy, F1-score)	Continued comprehensive evaluation and comparison with different ML methods
Alghamdi [13]	Deep ensemble-based IDS using Lambda architecture	Multi-pronged classification approach (LSTM, CNN, ANN); Lambda architecture	High accuracy of over 99.93%; Optimized processing time	Continued refinement of the ensemble model; Real-time evaluation and processing improvements

Challenges in Implementing IDS in IoT

Implementing IDS in IoT environments presents unique challenges, including:

4.1 Resource Constraints

IoT devices often have limited processing power, memory, and battery life, making it difficult to implement complex IDS algorithms.

4.2 Scalability

The vast number of IoT devices requires scalable IDS solutions that can handle large volumes of data and numerous connections simultaneously.

4.3 Heterogeneity

IoT ecosystems are highly heterogeneous, comprising devices with varying capabilities and protocols, complicating the deployment of a uniform IDS solution.

4.4 Real-time Detection

The need for real-time intrusion detection is critical in IoT, necessitating IDS solutions that can provide immediate responses to threats without significant delays.

Conclusion:-

The Internet of Things (IoT) has profoundly transformed various domains by enabling seamless connectivity and data exchange among devices. However, this advancement has also introduced significant security challenges, particularly the increased risk of cyber attacks on IoT systems. Intrusion Detection Systems (IDS) play a crucial role in safeguarding IoT environments by identifying and mitigating unauthorized access and malicious activities.

This survey has provided a comprehensive review of contemporary IDS for IoT, examining their classification, detection techniques, and deployment strategies. Despite the progress in IDS development, several challenges persist, including resource constraints, scalability issues, heterogeneity of IoT devices, and the need for real-time detection. Addressing these challenges requires innovative approaches, such as leveraging machine learning and artificial intelligence,

developing lightweight IDS algorithms, and employing collaborative and distributed IDS frameworks. Future research should focus on enhancing the adaptability and efficiency of IDS in IoT environments.

References:-

[1] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," Cybersecurity, vol. 4, no. 1, Mar. 2021, doi: 10.1186/s42400-021-00077-7.
[2] J. C. S. Sicato, S. K. Singh, S. Rathore, and J. H. Park, "A Comprehensive Analyses of Intrusion Detection System for IoT environment," J Inf Process Syst, vol. 16, no. 4, pp. 975–990, Aug. 2020, doi: 10.3745/jips.03.0144.
[3] R. Alghamdi and M. Bellaiche, "An ensemble deep learning based IDS for IoT using Lambda architecture," Cybersecurity, vol. 6, no. 1, Mar. 2023, doi: 10.1186/s42400-022-00133-w.
[4] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," Cybersecurity, vol. 4, no. 1, Mar. 2021, doi: 10.1186/s42400-021-00077-7.
[5] J. Snehi, A. Bhandari, V. Baggan, and M. S. Ritu, "Diverse Methods for Signature based Intrusion Detection Schemes Adopted," International Journal of Recent Technology and Engineering, vol. 9, no. 2, pp. 44–49, Jul. 2020, doi: 10.35940/ijrte.a2791.079220.
[6] P. P. Ioulianouet al., "A signature-based intrusion detection system for the internet of things," conference-proceeding, Jul. 2018. [Online]. Available: https://www.researchgate.net/publication/326376629
[7] T. U. Sheikh, H. Rahman, H. S. Al-Qahtani, T. K. Hazra, and N. U. Sheikh, "Countermeasure of Attack Vectors using Signature-Based IDS in IoT Environments," 0th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2019, pp. 1130–1136, Oct. 2019, doi: 10.1109/iemcon.2019.8936231.
[8] J. Snehi, A. Bhandari, V. Baggan, and M. S. Ritu, "Diverse Methods for Signature based Intrusion Detection Schemes Adopted," International Journal of Recent Technology and Engineering, vol. 9, no. 2, pp. 44–49, Jul. 2020, doi: 10.35940/ijrte.a2791.079220.
[9] Z. Liu, K. Roy, Niraj Thapa, X. Yuan, A. Shaver, and S. Khorsandroo, "Anomaly Detection on loT Network Intrusion Using Machine Learning," International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD),.
[10] M. M. Shurman, R. M. Khrais, A. A. Yateem, and Jordan Univ. of Science and Technology, "IoT Denial-of-Service Attack Detection and Prevention using Hybrid IDS," IEEE, conference-proceeding, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8862019
[11] Y. Otoum and A. Nayak, "AS-IDS: anomaly and signature based IDS for the internet of things," Journal of Network and Systems Management, vol. 29, no. 3, Mar. 2021, doi: 10.1007/s10922-021-09589-6.
[12] A. K. Gulhare, A. Badholia, and A. Sharma, "Mean-Shift and local Outlier Factor-Based ensemble machine learning approach for anomaly detection in IoT devices," 2022 International Conference on Inventive Computation Technologies (ICICT), Jul. 2022, doi: 10.1109/icict54344.2022.9850880.
[13] R. Alghamdi and M. Bellaiche, "An ensemble deep learning based IDS for IoT using Lambda architecture," Cybersecurity, vol. 6, no. 1, Mar. 2023, doi: 10.1186/s42400-022-00133-w.