Intelligent Network Intrusion Detection for IoT Systems Based on Machine Learning: A Review

Goury Vishwakarma[1], Swati Khanve[2]
[1]*M.Tech Scholar, CSE, SIRTE, Bhopal*
[2]*Assistant Professor, CSE, SIRTE, Bhopal*

***Abstract*—The fast proliferation of the Internet of Things (IoT) has generated substantial security issues owing to the enormous number of networked and resource-constrained devices. IoT networks are very susceptible to cyber-attacks that include Distributed Denial of Service (DDoS), botnet infiltration, malware dissemination, and unauthorized access. Traditional security techniques are generally inadequate in IoT systems because of scalability and performance restrictions. As a consequence, intelligent Intrusion Detection Systems (IDS) based on Machine Learning (ML) & Deep Learning (DL) have emerged as viable alternatives. An extensive investigation of ML- & DL-based intrusion detection methods for IoT systems is provided in this article. It examines IDS structures, detection algorithms, widely used datasets, feature engineering methods, and performance assessment measures. Recent developments using Convolutional Neural Network (CNNs), which have shown better performance in identifying intricate and multi-class threats in IoT settings, are highlighted. The report also discusses present obstacles and potential research areas for establishing strong and scalable IoT security solutions. Furthermore, with the emergence of 6G communication networks enabling ultra-high-speed connectivity and massive IoT deployments, intrusion detection systems must become more scalable and computationally efficient. In this review, special emphasis is placed on Convolutional Neural Network (CNN)-based architectures due to their superior capability in detecting intricate, multi-class, and blended IoT attacks.**

***Index Terms*—Internet of Things, Intrusion Detection System, ML, Deep Learning, CNN, IoT Security**

I. INTRODUCTION

In an age when many areas of technology are growing at an incredible rate, like sensors, wireless communication with speeds that will soon be 6G (a technology that promises speeds up to 100 times faster than 5G), high-speed internet, along with embedded systems, it is now possible to integrate smart devices into our daily lives. The name "Internet of Things" (IoT) came up because these smart devices can talk to each other via the Internet. Statista, a website that focuses on statistics, says that by 2025, there might be 30.9 billion linked devices [1]. The IoT industry is also expected to keep growing from 2024 to 2028, reaching a value of $145.4 billion, which represents a 54.75% increase [2]. These devices may be found in many fields, including as agriculture, healthcare, smart homes, smart cities, energy, and more [3]. But this digital revolution has also brought forth new security threats. Attacks against important infrastructure, such as nuclear and military bases, are on the rise [4]. These assaults hurt not just the nation but also the environment.

Also, the fact that there are many different standards and ways to communicate makes it hard for typical security measures to work in the IoT setting. To deal with these problems, there are already a number of security solutions that may make IoT safer, such as cryptographic methods like homomorphic encryption [5] and authentication [6]. Additionally, the methods used to sustain trust across the many components of the IoT paradigm [7]. Even though there were many different security measures, they didn't work against assaults that targeted networks. This makes one wonder whether it's possible to create a new line of defense that can quickly and proactively find and fix security holes. Intrusion detection systems (IDS) are the answer to this problem. Intrusion detection systems (IDS) keep an eye on network traffic and computer activity all the time so they can spot strange behavior. But IDSs need to be changed to work with

IoT devices. Also, it's not hard to get past the current basic IDS models, which sometimes miss new threats. Some researchers have shifted towards anomaly-based IDS categories and machine learning (ML) methodologies owing to their capacity to learn from data and identify novel assaults.

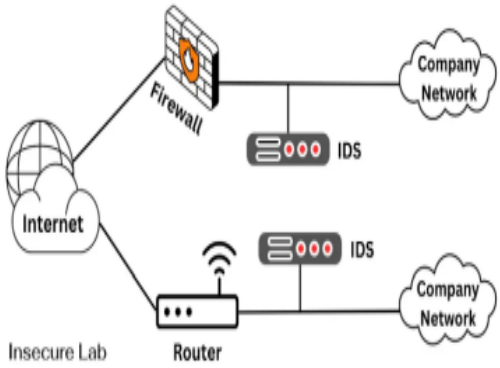

Figure 1 Intrusion Detection System

Intrusion detection systems (IDS) ecosystem: an overview

Intrusion detection is the practice of always observing and analysing network traffic and system activity to uncover behaviour that is odd or hazardous. An IDS is what it's called when it's put into place using hardware or software. An IDS is an important network security tool that looks for probable attacks before they cause service interruptions, unauthorized access, or data loss. In general, there are two main types of IDS: Host-Based Intrusion Detection Systems (HIDS) [8] and Network-Based Intrusion Detection Systems (NIDS) [9]. HIDS works at the host level by monitoring system-level events such file changes, system logs, and memory use. These systems are put on every host in a network and keep an eye on what happens within to find any dangerous or suspicious activity. NIDS, on the other hand, is strategically located in the network design so that it can constantly check the traffic that moves across network segments. The system architecture says that there might be software or hardware options that work with other network protocols, such as Ethernet and FDDI. Most NIDS have two network interfaces: one for system administration, control, and reporting, and another for monitoring all network traffic. HIDS protect individual hosts, whereas NIDS look at traffic across the whole network to find coordinated or spread assaults. HIDS focuses on monitoring internal host-level activities such as file modifications, system logs, and configuration changes, whereas NIDS analyses traffic flowing across network segments to detect coordinated and distributed attacks. This distinction is crucial in IoT environments where both endpoint-level and network-level security are required. IDS may be classified according to their detection methodologies as well as their deployment tactics. Signature-based IDS uses a pre-made database of known attack signatures and looks at traffic all the time to see whether it matches these patterns to find intrusions [10]. Even while this method is effective at finding existing threats with a high level of accuracy, it is limited in its ability to find new or zero-day assaults. Also, keeping a signature database up to date is hard, and if changes take too long, attackers may be able to get around detection mechanisms. On the other hand, anomaly-based IDS create a baseline model of normal network activity and find intrusions by looking for things that don't fit this model [11]. This method lets you find threats that you didn't know about before and changes to the network settings. But it is still challenging to set and maintain an accurate baseline in network systems that are complicated and changeable. When hostile traffic closely mimics legitimate activity or mixes with typical patterns, anomaly-based algorithms may provide false negatives. Hybrid IDS combine signature-based and anomaly-based strategies to get the best of both worlds and get beyond the limitations of each method. Hybrid IDS is a better and more effective way to protect contemporary and diverse network environments, especially in IoT ecosystems. It combines great detection of existing attacks with the ability to predict new threats.

II. LITERATURE REVIEW

Intrusion Detection Systems (IDS) are becoming an important component of current cybersecurity due to of the exponential increase of networked systems, cloud-based systems, & Internet of Things (IoT) environments. Traditional rule-based and signature-based intrusion detection systems struggle to locate new and emerging threats, especially in high-volume and dynamic networks. To solve these limits, present research increasingly relies on machine learning (ML) along with deep learning (DL) algorithms that can automatically understand sophisticated attack patterns

from data. Notable studies that support IDS development in network, IoT, SDN, & cloud computing environments are examined in this section.

Osa et al. [12] introduce an intrusion detection system based on deep neural networks (DNNs) with the goal of improving detection accuracy in existing network environments. Using data sampling techniques like SMOTE and random under sampling, the study addresses the issue of class imbalance using the CICIDS2017 dataset. The recommended DNN architecture effectively learns nonlinear correlations in network traffic data and achieves extraordinarily high detection accuracy, exceeding 99%. The paper reveals that deep learning models outperform traditional machine learning classifiers when dealing with difficult and high-dimensional intrusion data. This article proves the efficacy of deep neural networks for recognizing both known and unexpected cyberattacks.

Bhavsar et al.[13] present an anomaly-based IDS for Internet of Things applications, underlining the necessity of recognizing attacks that have never been identified previously. To improve classification performance, the suggested strategy integrates deep learning and machine learning models with feature extraction techniques. After testing their approach on popular benchmark datasets including NSL-KDD and CICIDS, the authors discover high accuracy and decreased false alarm rates. The research highlights the flexibility of anomaly-based detection in dynamic IoT environments and explores difficulties relating to computing overhead and real-time detection. This study contributes to the development of IDS models for IoT systems that are both lightweight and efficient.

Ahmad et al.[14] emphasis on boosting IDS performance via data analysis & feature engineering using the UNSW-NB15 dataset. The authors study the dataset in depth and utilize preprocessing procedures to increase data quality. Multiple machine learning classifiers are evaluated to assess detection accuracy, precision, recall, & false positive rates. Even with traditional ML models, the study demonstrates that suitable feature selection or preprocessing substantially boost IDS performance. This research stresses the significance of dataset understanding and optimization in constructing effective intrusion detection systems.

Khan et al.[15] provide an IDS architecture that integrates feature extraction with machine learning classifiers for IoT security. The approach seeks to decrease computational complexity while preserving great detection accuracy. The authors accomplish effective intrusion detection suitable for IoT devices with low resources by selecting key features and using several machine learning techniques. When compared to models that use all attributes without selection, the results show improved performance. This research demonstrates how feature-driven approaches may enhance IDS deployment in IoT environments and highlights the trade-off between accuracy and efficacy.

Diana et al. [16] provide a thorough analysis of intrusion detection technologies used in computer networking security. IDS designs, detection algorithms, popular datasets, and evaluation standards are all examined in this research. It also tackles emerging subjects that include integrating the use of artificial intelligence, distributed IDS frameworks, & blockchain-based security solutions. The authors emphasize open issues include scalability, privacy protection, & real-time threat detection. This overview serves as a wonderful reference for assessing the status of IDS study development as well as discovering potential research pathways.

Yerneni et al. [17] present a full survey on ML & DL-based IDS for cloud security. In cloud environments, where traditional intrusion detection systems suffer due of virtualization, multi-tenancy, & dynamic resource allocation, the study focuses on proactive intrusion detection solutions. The authors highlight issues including data imbalance and deployment complexity, examine several ML and DL algorithms used for cloud IDS, and talk about datasets and performance metrics. The paper indicates that intelligent & cooperative IDS frameworks are required for defending present cloud infrastructures.

Table 1.1 Literature review

Authors (Year)	Focus Area	Methodology	Key Findings	Limitations
Silambarasan et al. [18]	Cloud intrusion detection	ARSO feature optimization + Bi-LSTM classifier tested on NSL-KDD	Integrated ARSO with Bi-LSTM improves detection accuracy and adaptability to dynamic traffic compared to other approaches	Requires extensive labeled data; high computational cost for real-time deployment
Shukla, Dwivedi & Mishra[19]	IoT network intrusion detection	Hybrid deep learning (KPCA + Lévy flight optimization + DNN-LSTM) on CIC-IDS2017, TON-IoT, NSL-KDD	Metaheuristic-tuned DNN-LSTM boosts accuracy and robustness vs standalone DL models	High complexity; may need more testing on real-world streams
Kulshrestha & Vijay Kumar[20]	IoMT intrusion detection	Machine learning models on IoMT traffic using traditional ML classifiers	Shows effectiveness of classical ML in IoMT intrusion detection	Doesn't use deep learning; limited to evaluated ML algorithms
Suthar & Khara [21]	IoT IDS with optimization + DCNN	Swarm intelligence (PSO + ABC) with DCNN on UNSW-NB15	Hybrid PSO–ABC–DCNN significantly improves detection accuracy, achieving 99.41% accuracy and enhanced generalization capability.	High computational cost limits real-time deployment in resource-constrained IoT environments.
Meena & Indian [22]	IoT intrusion detection with RNN	Enhanced LSTM based IDS evaluated across KDD-Cup99, NSL-KDD, UNSW-NB15, CICIoT2023	E-LSTM model shows resilient intrusion detection across multiple datasets	Primarily LSTM-based; may not scale to very high traffic without optimization
Kumari et al. [23]	Privacy-preserving federated IoT IDS	Federated + AE + DNN + CNN evaluated on N-BaIoT	Federated learning enhances privacy and detection across heterogeneous devices	Dataset limitations; complexity of FL training increases overhead
Sathya & Manuel Raj [24]	Adaptive ML IDS for network security	Adaptive ML (Random Forest, Decision Tree, PCA + Q-learning) on NSL-KDD data	ML-driven adaptive IDS improves detection accuracy and response to evolving attack patterns	Limited to traditional ML; not deep learning

III. MACHINE LEARNING AND DEEP LEARNING TECHNIQUES FOR IoT IDS

Intrusion detection has gotten a lot of interest since Machine Learning (ML) along with Deep Learning (DL) can find complex patterns in enormous amounts of network traffic data. ML-based IDS can learn from prior data and find new or zero-day threats, which makes them better for IoT scenarios that change over time than conventional rule-based systems.

A. Machine Learning-Based IDS

Decision Trees (DT), Random Forest (RF), Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), Naïve Bayes (NB), & Logistic Regression (LR) are some of the most popular machine learning methods for identifying intrusions. These techniques

rely on specific characteristics acquired from network traffic, such as packet size, protocol type, flow duration, and connection information. ML-based IDS heavily depend on manual feature engineering, which becomes increasingly complex in high-dimensional IoT traffic data. This manual dependency limits scalability and adaptability to evolving attack patterns. Because of their great classification accuracy and durability, Random Forest & SVM are two of the most utilized algorithms. However, ML-based IDS often struggle from feature dependency, scaling issues, and constrained performance when processing high-dimensional or highly imbalanced IoT input. Furthermore, manual feature engineering makes the system more complicated and makes it more difficult to adapt to new attack patterns.

B. Deep Learning-Based IDS

Deep learning approaches overcome several limitations of standard machine learning by automatically acquiring hierarchical feature representations from raw or inadequately processed data. Common DL architectures used in IoT IDS include Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), & Autoencoders (AE). CNN-based IDS models are very effective in extracting geographical information from network traffic representations such as flow-based matrices or packet sequences. Temporal relationships in sequential traffic data may be caught by LSTM and RNN models, which is important for recognizing stealthy and slow attacks. Hybrid models integrating both CNN and LSTM further increase detection accuracy by leveraging both temporal & spatial information. Recent studies show that DL-based IDS achieve more accuracy, better generalization, and increased multi-class attack detection compared to typical ML approaches. Deep learning architectures such as LSTM and RNN are particularly effective in capturing temporal dependencies in sequential network traffic, enabling the detection of stealthy and slow-moving attacks that traditional ML models often fail to identify. However, their main challenges are high computational cost, training time, and deployment complexity on IoT devices with restricted resources.

IV. DATASETS USED IN IoT INTRUSION DETECTION

"Targeting an appropriate dataset that includes the quantity and quality of data as well as the assets we want to predict or find is essential for accurately testing the robustness of an ML algorithms." [25]. We present below some of the most used datasets in the IoT area:

- "CICIDS-2017, the Canadian Institute for Cybersecurity IDS: Developed by the CIC, this dataset is freely available for research, encompassing 15 classes, 80 attributes, and 7 attack modes, including DoS, PortScan, & Brute Force. In response to different study objectives, it includes traffic data from a variety of network services, such as FTP, HTTP, SSH, etc. Several major papers employ this dataset. [26,27]
- UNSW-NB15: The University of New South Wales (UNSW) in Australia created this dataset, which includes nine different attack methods including reconnaissance, DoS, and fuzzers. It is suitable for machine learning applications as it includes 49 features that were developed from network data. Its vast size, with 2.5 million data, permits successful NIDS model training and validation. It has been used in studies [28, 29, 30].
- NSL-KDD: This collection of data is a revised version of the KDD Cup 99 dataset that was produced to remedy its flaws. With 150,000 samples & 41 attributes, it preserves the exact same attack types. The attacks are classified into Denial of Service (DoS), User-to-Root (U2R), Remote-to-Local (R2L), and Probe. It has been employed in various studies [26,27,31].
- IoT-23: The University of Colorado Boulder's NSL (Network Security Lab) invented it. There are twenty traits in all. It features 20 malware captures (including Mirai, Torii, Gagfyt, Kenjiro, ...) run on IoT devices, plus three benign IoT device traffic grabs. It was used in [32]
- Kyoto: It comprises daily records of real network traffic data running from 2006 to 2009. It encompasses 24 distinct characteristics. Specifically, it contains 50,033,015 sessions of ordinary traffic, 43,043,225 sessions of acknowledged attacks, and 425,719 sessions designated as unknown assaults.

- CSE-CIC-IDS-2018: This dataset was created by the CIC and is available to the general public for use in research. It combines 80 features along with assaults that include Brute force, Portscan, Botnet, DoS, & DDoS.
- AFDA: Created by the University of New South Wales, this dataset focuses mostly on Zero-day attacks, Stealth assaults, and Webshell attacks."

V. EVALUATION METRICS

"Several measures are required to evaluate an intrusion detection method's resilience in the Internet of Things. The following is a summary of the potential outcomes of attack prediction:
True positive (TP): It identifies attack classes that were anticipated accurately.
False positive (FP): Identifies typical classes incorrectly labeled as assaults.
False negative (FN): Indicates attack types that were incorrectly classified as typical.
True Negative (TN) : The correctly predicted normal classes are referred to as true negatives (TN).
Using all the factors mentioned above, we can calculate the Accuracy (A). It represents the overall proportion of accurately recognized instances relative to the entire number of instances in the test dataset, which is defined as

$$A = \frac{TP + TN}{TP + FN + FP + TN'}$$

These numbers are used to evaluate the model. First, the Recall (R) measure the model's power to properly predict TPs by calculating the percentage of TPs recognized among all real positives. It is defined as

$$R = \frac{TP}{TP + FN}$$

Second, Precision (P) may be calculated by dividing the total positives (false and TPs) by the number of TPs. It displays the prediction quality of the model, which is described as

$$P = \frac{TP}{TP + FP}$$

Furthermore, we may evaluate accuracy and recall at the same time using the F1-score, which is defined as

$$F1 - score = 2 * \frac{P * R}{P + R}$$

The F1-score runs from 0 to 1, where 1 implies flawless accuracy and recall, and 0 denotes the worst."

VI. CONCLUSION

With a focus on machine learning and deep learning-based methods, this study examined intelligent network intrusion detection solutions for Internet of Things scenarios. The study shows that current security protocols are inadequate for protecting vast, varied, and resource-constrained IoT networks, especially since they are unable to detect emerging and undetected attacks. When combined with appropriate feature engineering and data preprocessing, machine learning techniques like Random Forest, Support Vector Machines, and Decision Trees provide great baseline solutions. However, deep learning models, notably CNN-, LSTM-, and hybrid CNN–LSTM-based architectures, are more effective at learning complicated spatial and temporal traffic patterns. This makes it feasible to identify multi-class attacks more precisely across a broad variety of IoT datasets, including CICIDS-2017, UNSW-NB15, NSL-KDD, and IoT-23. Even with these improvements, there are still unresolved research questions like data imbalance, high computational cost, scalability, real-time deployment, and privacy protection. Future research should focus on Federated Learning-based IDS to enable privacy-preserving distributed training across IoT devices without centralized data sharing. Additionally, Edge Computing-based IDS deployment can significantly reduce latency and computational burden by processing intrusion detection tasks closer to the data source. Lightweight CNN models optimized for edge devices will be essential for secure 6G-enabled IoT ecosystems. Future intrusion detection solutions should emphasize lightweight and flexible learning models, architectures based on edge and federated learning, and the application of realistic IoT traffic datasets to bridge experimental evaluation with practical deployment, thereby augmenting the

overall security along with resilience of IoT ecosystems [33].

REFERENCE

[1] "Global IoT and non-IoT connections 2010-2025: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

[2] "Europe: internet of things market revenue 2018-2028: https://www.statista.com/forecasts/1283723/revenue-from-internet-of-things-in-europe

[3] Y. Perwej, al., "The Internet of Things (IoT) and its Application Domains," IJCA, Apr. 2019,

[4] E. Ronen, al., "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," IEEE Symposium on Security and Privacy (SP), May 2017

[5] B. Chah, al., "H3PC: Enhanced Security and Privacy-Preserving Platoon Construction Based on Fully Homomorphic Encryption,"IEEE 26th International Conference on Intelli-gent Transportation Systems (ITSC), Sep. 2023,

[6] T. Shah, al., "Authentication of IoT Device and IoT Server Using Secure Vaults," in 2018 IEEE International Conference. 2018,

[7] K. M. Sadique, al., "Towards Security on Internet of Things: Applications and Challenges in Technology," Procedia Computer Science, 2018,

[8] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," Journal of Network and Computer Applications, Jan. 2013,

[9] O. Chaieb, al., "Machine Learning-Based Intrusion Detection System: Review and Taxono-my," in Proceedings International Conference on Big Data and Internet of Things, 2023

[10] M. Masdari, al.,"A survey and taxonomy of the fuzzy signature-based Intrusion Detection Systems," Applied Soft Computing, Jul. 2020

[11] A. Patcha, al., "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Computer Networks. 2007

[12] Osa, E., Orukpe, P. E., & Iruansi, U. (2024). Design and implementation of a deep neural network approach for intrusion detection systems. Pr ime Journal of Engineering and Applied Sciences, Article 100434.

[13] Bhavsar, M., Roy, K., Kelly, J., & Odeyomi, O. (2023). Anomaly-based intrusion detection system for IoT application. Discover Internet of Things, 3, 5.

[14] Ahmad, T. S., Hasan, I., & Shoaib, M. (2024). Enhanced intrusion detection systems performance with UNSW-NB15 data analysis. Algorithms, 17(2),

[15] Khan, A. S., Khan, M. A., & Ahmad, T. (2023). Intrusion detection system using feature extraction with machine learning algorithms in IoT. Internet of Things, 12(2),

[16] Diana, L., Dini, P., & Paolini, D. (2025). Overview on intrusion detection systems for computers networking security. Computers, 14(3),

[17] Yerneni, K. S., Avireneni, R. T., Harsha, S., & Reddy, N. K. (2025). Towards proactive cloud security: A survey on ML and deep learning-based intrusion detection systems [PDF]. Journal of Contemporary Education Theory & Artificial Intelligence

[18] Silambarasan, E., Suryawanshi, R., & Reshma, S. (2024). Enhanced cloud security: A novel intrusion detection system using ARSO algorithm and Bi-LSTM classifier. International Journal of Information Technology, 16, 3837–3845.

[19] Shukla, A. K., Dwivedi, S., & Mishra, A. (2025). An effective hybrid deep learning metaheuristic model for robust IoT intrusion detection. Discover Computing, 28(1), Article 200

[20] Kulshrestha, P., & Vijay Kumar, T. V. (2024). Machine learning based intrusion detection system for IoMT. International Journal of System Assurance Engineering and Management, 15, 1802–1814.

[21] Suthar, M. B., & Khara, S. (2025). Enhancing IoT security through machine learning-based intrusion detection systems. Indian Journal of Science and Technology, 18(35), 2884–2896

[22] Meena, G., & Indian, A. (2025). IDS-IoT: Intrusion detection system for the Internet of Things using enhanced Long-Short Term Memory. Artificial Intelligence and Applications.

[23] Kumari, S., Singh, S., Rajput, A., & Karsoliya, S. (2025). A privacy-preserving hybrid intrusion detection system for IoT networks using federated and deep learning models. SMART Moves Journal IJOSCIENCE, 11(10)

[24] Sathya, S., & Manuel Raj, P. A. (2025). Enhancing network security through machine learning-driven adaptive intrusion detection. International Journal of Scientific Research in Science and Technology.
[25] C. Alex, al., "A Comprehensive Survey for IoT Security Datasets Taxonomy, Classification and Machine Learning Mechanisms," Computers & Security, Sep. 2023,
[26] P. K. Keserwani, al., "A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model," J Reliable Intell Environ, Mar. 2021
[27] S. Shitharth, al., "An Innovative Perceptual Pigeon Galvanized Optimization (PPGO) Based Likelihood Naïve Bayes (LNB) Classification Approach for Network Intrusion Detection System," IEEE Access, 2022
[28] J. Liu, al., "Research on Intrusion Detection Based on Particle Swarm Optimization in IoT," IEEE Access, 2021
[29] N. Sayed, Augmenting IoT Intrusion Detection System Performance Using Deep Neural Network. Computers, Materials and Continua, 2022
[30] D. Chen, al., "Heterogeneous IoT Intrusion Detection Based on Fusion Word Embedding Deep Transfer Learning," IEEE Transactions on Industrial Informatics, Aug. 2023
[31] A. Raghuvanshi, al., "Intrusion Detection Using Machine Learning for Risk Mitigation in IoT-Enabled Smart Irrigation in Smart Farming," Journal of Food Quality, Feb. 2022 [19] A. K. Sahu, al., "Internet of Things attack detection using hybrid Deep Learning Model," Computer Communications, Aug. 2021
[32] I. Ullah, al., "Network Traffic Flow Based Machine Learning Technique for IoT Device Identification," IEEE International Systems Conference (SysCon), Apr. 2021
[33] Mitchell, R., & Chen, I.-R. (2014). A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys, 46(4), 55.