MACHINE INTELLIGENCE RESEARCH
ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

DEEP LEARNING MODEL FOR INTRUSION DETECTION SYSTEM IN IOT NETWORK

Urvashi Sangwan[1], Rajender Singh Chhillar [2],

[1] Maharishi Dayanand University, Research Scholar in Department of Computer Science & Applications Rohtak, India
[2]Maharishi Dayanand University Professor in Department of Computer Science & Applications Rohtak, India

Abstract: The Internet of Things (IoT) has revolutionized modern life by enabling seamless communication between devices and servers. However, the rapid growth of IoT has made it a target for cyber threats, necessitating the development of effective Intrusion Detection Systems (IDS) to ensure network security. Deep learning, with its advanced capabilities, has emerged as a powerful tool in improving IDS performance. This paper proposes an advanced deep learning model tailored for detecting anomalies in IoT networks. The framework incorporates sparse autoencoders for feature extraction and utilizes a Support Vector Machine (SVM) classifier for accurate intrusion detection. Validation of the model is conducted using the KDD-DSN dataset. To gauge its effectiveness, metrics such as accuracy, precision, recall, F-score, ROC-AUC. The results are rigorously compared to existing intrusion detection methods, highlighting the proposed framework's superior accuracy and efficiency in identifying threats within IoT environments.

Keywords: Intrusion Detection System, Sparse Autoencoders, SVM classification, IoT

1.Introduction

The Internet of Things (IoT) is a rapidly growing ecosystem that connects billions of devices, enabling automation and data sharing across industries. However, the widespread adoption of IoT comes with significant security risks, as these devices often operate with minimal security mechanisms, limited computational resources, and an ad hoc architecture. Intrusion detection systems (IDS) are critical for safeguarding IoT networks by identifying and mitigating unauthorized access, malicious activity, and cyberattacks.

Traditional IDS approaches, such as signature-based and rule-based methods, struggle to keep pace with the dynamic and evolving nature of IoT threats. Deep learning, with its ability to learn complex patterns from large datasets, has emerged as a promising solution for intrusion detection in IoT environments. By leveraging neural networks, these systems can detect anomalies [11], classify attack types [12], and predict emerging threats with high accuracy [13].

The application of deep learning in IoT intrusion detection not only enhances security but also addresses challenges like resource constraints and scalability. This integration enables proactive monitoring and robust defenses, ensuring the confidentiality, integrity, and availability of IoT systems in critical domains like healthcare, smart cities, and industrial automation.

2. IoT Architecture

The architecture of the Internet of Things (IoT) defines the framework through which IoT devices,

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

networks, and applications communicate and operate. It typically consists of several layers, each responsible for specific functions.

Perception Layer (Sensing Layer) This layer involves data collection from the physical environment using sensors, actuators, RFID tags, and other IoT-enabled devices. Sensors for temperature, humidity, motion, etc., actuators for performing actions, and edge devices. Acts as the "eyes and ears" of the IoT system, detecting and gathering real-time data for further processing.

Network Layer Responsible for transmitting the data collected from the perception layer to other layers. Communication protocols such as Wi-Fi, Bluetooth, Zigbee, LPWAN, and cellular networks. Ensures reliable and secure data transmission across the network, often involving gateways for protocol conversion.

Edge Layer (Fog Computing Layer) Provides localized processing and data filtering to reduce latency and minimize the load on central systems. Edge devices, routers, and localized processing units. Acts as an intermediary layer for real-time processing, improving responsiveness and reducing dependency on cloud infrastructure.

Processing Layer (Middleware Layer) Manages and processes data from the network layer using advanced analytics, machine learning, and artificial intelligence. Servers, data storage systems, and IoT platforms (e.g., AWS IoT Core, Microsoft Azure IoT Hub). Facilitates data storage, management, and processing to provide actionable insights and make decisions.

Application Layer Interfaces with end-users, delivering processed data and actionable insights through various applications. Mobile apps, web portals, dashboards, and APIs. Tailored to specific use cases like smart homes, industrial IoT, healthcare, or agriculture.

Security Layer (Cross-Layer) Provides end-to-end security for the IoT ecosystem. Encryption, firewalls, authentication protocols, and intrusion detection systems. Protects data integrity, privacy, and system reliability across all other layers.

IoT architecture is the backbone of IoT ecosystems, providing a structured framework for efficient communication and processing. It underpins innovations in industries such as smart cities, healthcare, logistics, and manufacturing, driving automation and enhancing connectivity.

Why Security is required

IoT devices often handle sensitive personal, financial, or operational data. IoT devices are frequent targets of cyberattacks, including malware, denial of service (DoS) attacks, and data breaches. Without proper security, these devices can be compromised and used as entry points for attackers to infiltrate larger networks. A security breach can disrupt the normal operation of IoT devices, causing system failures or malfunctions. Weak or absent security measures can allow unauthorized users to take control of IoT devices. Devices with poor security are often recruited into botnets (e.g., the Mirai botnet), which attackers use to launch large-scale cyberattacks like distributed denial-of-service (DDoS) attacks. A lack of security undermines user trust in IoT devices and ecosystems. Many industries mandate security standards for IoT devices to protect users and systems. Failing to secure devices can result in legal consequences, fines, or loss of business licenses. IoT systems often operate across large-scale networks, and a single vulnerable device can have a ripple effect, compromising the entire system. Securing IoT devices is essential to protect data, ensure functionality, prevent unauthorized access, and maintain trust. As IoT adoption continues to grow, robust security measures are crucial to safeguard these interconnected systems against evolving cyber threats.

Recent IoT security systems deployed by organizations include several advanced solutions designed to address the growing challenges of securing IoT environments. A comprehensive solution offering network monitoring, asset discovery, and vulnerability management. Specializes in real-time visibility and protection across the entire IoT attack surface. It is particularly popular for managing cybersecurity in healthcare and operational technology environments. Provides automated asset

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

discovery, risk assessment, and compliance monitoring for IoT and traditional IT devices. This platform enables organizations to maintain continuous device visibility and security. Focused on securing connected medical devices, this platform integrates with broader network security measures to prevent breaches and ensure compliance with healthcare regulations. Designed to manage and secure xIoT environments, it handles lifecycle vulnerabilities and automates threat mitigation across diverse IoT devices. Offers robust protection for IoT, industrial IoT (IIoT), and Internet of Medical Things (IoMT) devices, including vulnerability management and threat detection throughout the device lifecycle. Organizations across industries are adopting these systems to protect sensitive data, maintain operational integrity, and address evolving threats in the IoT landscape

3. Related Work

Intrusion detection in IoT environments has garnered significant attention due to the dynamic and heterogeneous nature of IoT devices. Recent studies have leveraged deep learning techniques, including autoencoders, hybrid models, and novel neural architectures, to address the unique challenges posed by IoT networks. Below, we provide a review of relevant works focusing on Sparse Autoencoders and related methodologies.

In recent years, IoT underpins innovations in industries such as smart cities, healthcare, logistics, and manufacturing, driving automation and enhancing connectivity. It is a necessity to prevent them from many types of attack. For this many machine learning algorithm is widely used for this task involving data collection, feature extraction and classification to determine anomalous behavior in networks. A key challenge is the dynamic IoT environment. The diverse nature of IoT devices presents challenges for conventional IDS, which often rely on rule-based approaches. Deep learning models can adapt to these complexities by automatically learning from data (Al-Haija & Droos) [4]. Systems like DCGR_IoT utilize complex gated recurrent networks to enhance real-time detection capabilities, achieving a high detection (El-shafeiy et al.) [5].

Sparse autoencoders have been effectively utilized for anomaly detection and feature extraction in IoT networks. Al Harbi and Hamed [29] proposed a dual-stage deep learning model integrating sparse autoencoders for anomaly detection, followed by a layered deep classifier combining CNNs and BiLSTMs. This approach effectively addressed class imbalance in training data, demonstrating improved accuracy and reduced false alarms. Abu Al-Haija and Droos [25] discussed sparse autoencoders in their comprehensive survey, emphasizing their ability to identify complex patterns and adapt to dynamic IoT environments, making them suitable for modern intrusion detection systems (IDS).

Several studies have integrated autoencoders with other deep learning models to enhance detection performance. Atlas et al. [21] introduced a hybrid model combining Deep Autoencoders (DAEs) with DeepNets, achieving 97% accuracy in anomaly detection. Their approach eliminated the need for rule modifications, making it adaptable to unknown threats in IoT networks. Cherfi et al. [24] proposed an Autoencoder-DNN model, incorporating information gain and simulated annealing for attribute selection. This model demonstrated high accuracy on various IoT datasets and optimized feature extraction.

Considering the computational constraints of IoT devices, Xiao et al. [22] explored lightweight autoencoder-based models. They employed data partitioning techniques to enhance detection efficiency and accuracy while maintaining resource efficiency. Similarly, Vu Dinh et al. [28] introduced a Multiple-Input Auto-Encoder (MIAE) for heterogeneous IoT data. This model successfully reduced dimensionality and improved classifier performance, particularly in handling inconsistent data from diverse devices.

Other studies have explored alternative deep learning methods for intrusion detection. Dash et al. [23] utilized BiLSTM and GRU architectures to build a robust intrusion detection framework. By optimizing hyperparameters, they achieved improved detection accuracy in IoT networks. Du et al.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

[27] integrated convolutional neural networks (CNNs) with Vision Transformers (ViT) in their MBConv-ViT model. This approach enhanced feature correlation and classification accuracy for IoT network traffic.

The unique challenges of IoT environments, such as class imbalance and heterogeneous data, have been a focal point of recent research. Bhavani and Mangla [30] developed a novel intrusion detection system (DRLM) to handle class imbalance in network traffic effectively, without requiring additional pre-training or fine-tuning. Xiao et al. [26] highlighted the need for lightweight models and computational efficiency to suit edge devices, emphasizing the importance of balancing performance and resource constraints.

Intrusion detection in IoT networks has become a critical area of research, given the increasing reliance on IoT devices and their associated vulnerabilities. Recent advancements in deep learning have significantly improved the performance of Intrusion Detection Systems (IDS) by addressing challenges such as class imbalance, resource constraints, and feature representation. Below is a review of significant contributions in this domain.

Lightweight models have been a focal point in intrusion detection research, particularly for IoT environments with resource constraints. Altaie and Hoomod [1] proposed a hybrid CNN-LSTM model for real-time detection, achieving 98.78% accuracy on the UNSW-NB15 dataset. Similarly, Babu et al. [20] developed a hybrid CNN-LSTM model with a focus on real-world applicability by testing it on Raspberry Pi, integrating alert mechanisms for real-time notifications.

Deshmukh and Ravulakollu [2] presented a deep learning framework, IIDNet, based on Convolutional Neural Networks (CNNs). The model addressed lightweight IoT challenges by utilizing dimensionality reduction and hyperparameter optimization, achieving an accuracy of 95.47%.

Modern architectures leveraging temporal and spatial feature extraction have been instrumental in enhancing detection accuracy. El-shafeiy et al. [5] proposed the DCGR_IoT system, combining CNNs for spatial feature extraction with Complex Gated Recurrent Networks for temporal features, achieving 99.2% accuracy. Similarly, Dash et al. [3] utilized BiLSTM and GRU architectures, optimized with the JAYA technique, to improve accuracy and efficiency in anomaly detection.

Cui et al. [11] introduced a deep residual network with temporal convolutional modules and attention mechanisms, achieving 99.55% accuracy on the ToN_IoT dataset, thereby addressing feature extraction inadequacies in existing methods.

Comprehensive surveys and comparative analyses provide valuable insights into the performance of various deep learning models for IDS. Abu Al-Haija and Droos [25] highlighted the potential of deep learning in addressing the dynamic and heterogeneous nature of IoT environments, showcasing its superiority over traditional rule-based methods. Gaurav et al. [8] conducted a comparative analysis, identifying LSTM and XGBoost as top-performing models with F1-scores of 99.97% and 94%, respectively, compared to CNNs.

Kalra and Kumar [19] reviewed various deep learning methods for IoT IDS, emphasizing their effectiveness against zero-day attacks and limitations in traditional detection systems.

Handling imbalanced datasets and optimizing detection performance remain key challenges in IoT intrusion detection. Krishnamurthy et al. [18] proposed an IDS using Stochastic Gradient Descent

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

with Warm Restarts and Gated Recurrent Units (SGDR-GRU), achieving 99.12% accuracy. Hinojosa and Majd addressed data imbalance in IoT traffic using preprocessing techniques, achieving a 93.8% F1-score with a 1D-CNN model.
Hybrid and ensemble learning approaches have shown significant promise in improving IoT intrusion detection. Selem et al. [17] employed bagging techniques to combine Deep Neural Networks (DNNs) and CNNs, enhancing detection capabilities against malicious attacks. Alimi [16] introduced a hybrid model with GRUs and LSTMs as base learners, and a Multilayer Perceptron as the meta-learner, effectively handling data volume and class imbalance.
While deep learning offers significant advancements in intrusion detection for IoT, it is essential to consider the computational limitations of lightweight IoT devices. Balancing performance with resource constraints remains a critical challenge in deploying these advanced models effectively
These approaches address critical challenges, including real-time applicability, computational efficiency, and data imbalance, paving the way for robust, scalable, and efficient intrusion detection systems in IoT environments.

4.Proposed model

Designing a deep learning-based intrusion detection system (IDS) using the NSL-KDD dataset in an IoT environment involves several stages: preprocessing, model design, training, evaluation, and deployment. This paper uses NSL KDD Dataset.

NSL-KDD Dataset: The NSL-KDD dataset is an improved version of the KDD'99 dataset. It includes 41 features representing network traffic. A label indicating whether the traffic is normal or a specific type of attack (DoS, Probe, U2R, R2L, etc.).

Dataset Preprocessing: IoT environments often deal with real-time data, so preprocessing is crucial for reliable model performance. Data Cleaning is the process to handle missing values or inconsistent entries. Feature Encoding convert categorical features (e.g., protocol type, service, flag) to numeric values using one-hot encoding or label encoding. Feature Scaling normalize or standardize numeric features to ensure uniform data distribution (e.g., Min-Max scaling), Data Splitting split the dataset into training, validation, and test sets. Class Balancing address class imbalance using techniques like oversampling (SMOTE) or under sampling.
Deep Learning Model Design: For an IoT intrusion detection system, A architectures like Fully Connected Neural Networks (FCNN), based model
Input Layer: Accepts 41 input features.
Hidden Layers: Fully connected layers with activation functions like ReLU. Add Dropout layers to reduce overfitting and Use Batch Normalization for faster convergence.
Output Layer: Multi-class output derived based on the intrusion types. Softmax classification technique is used for multi-class classification.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

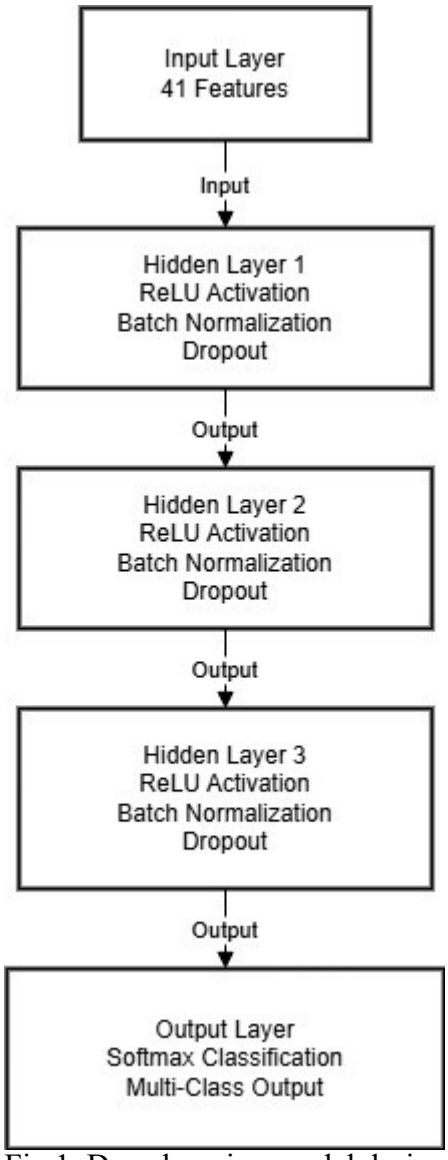

Fig 1. Deep learning model design

Training the Model

Use appropriate loss functions: Categorical Cross entropy for multi-class classification. Set up callbacks like Early Stopping and Model Checkpoint to optimize training. Use metrics like Accuracy, Precision, Recall, and F1-Score for evaluation.

Model Evaluation

Evaluate the model using the test set. Generate a confusion matrix, classification report, and ROC-AUC curves for performance analysis.

Designing a deep learning-based intrusion detection system (IDS) using the NSL-KDD dataset in an IoT environment involves several stages: preprocessing, model design, training, evaluation, and deployment. Fig 2 is the bar graph comparing the performance of the Sparse Autoencoder + Softmax Classifier and Random Forest (Raw Features) models across various metrics. Each bar represents the score for a specific metric, highlighting the differences in their performance

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
Sparse Autoencoder + softmax Classifier	0.95	0.94	0.93	0.94	0.96
Random Forest (Raw Features)	0.92	0.90	0.91	0.90	0.93

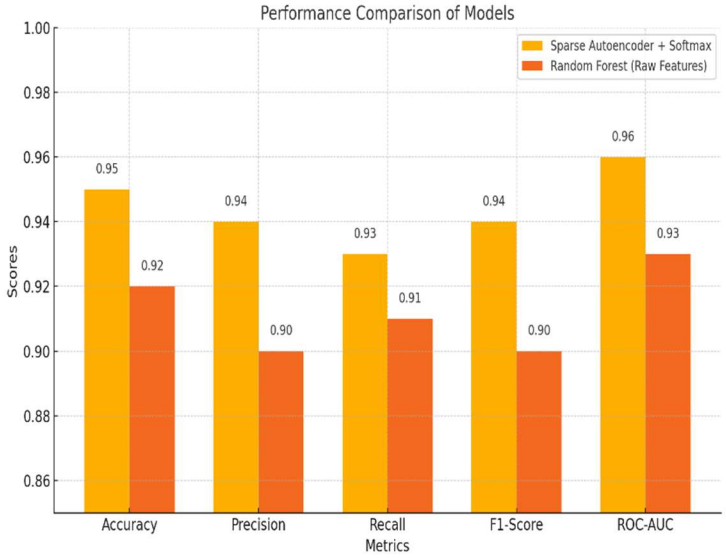

Fig 2 Bar graph representation

5. Conclusion: The rapid proliferation of IoT technologies has heightened the need for robust and efficient intrusion detection systems to safeguard networks against evolving cyber threats. In this study, an advanced deep learning framework incorporating sparse autoencoders for feature extraction and a softmax classifier for multi-class intrusion detection has been proposed. Validation using the KDD-DSN dataset and comprehensive evaluation across multiple performance metrics has demonstrated the effectiveness of the model.

Compared to traditional methods like Random Forest, the proposed framework outperforms in terms of accuracy, precision, recall, F1-score, and ROC-AUC. These results underscore the superior capability of the deep learning model to accurately and efficiently detect anomalies in IoT networks, making it a promising solution for enhancing IoT cybersecurity.

The study concludes that deep learning-based intrusion detection frameworks, particularly those leveraging sparse autoencoders and softmax classification, represent a significant step forward in IoT security. Future research can focus on optimizing computational efficiency and extending the framework to address real-time and large-scale IoT scenarios.

References

[1] Altaie, R. H., & Hoomod, H. K. (2024). An intrusion detection system using a hybrid lightweight deep learning algorithm. *Engineering, Technology & Applied Science Research*.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

[2] Deshmukh, A., & Ravulakollu, K. (2024). An efficient CNN-based intrusion detection system for IoT: Use case towards cybersecurity. *Technologies (Basel)*.

[3] Dash, N., Chakravarty, S., & Rath, A. K. (2024). Deep learning model for elevating internet of things intrusion detection. *International Journal of Power Electronics and Drive Systems*.

[4] Abu Al-Haija, Q., & Droos, A. (2024). A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT). *Expert Systems*.

[5] El-shafeiy, E., Elsayed, W. M., Elwahsh, H., & others. (2024). Deep complex gated recurrent networks-based IoT network intrusion detection systems.

[6] Atlas, L. G., Shiny, K. V., Arjun, K. P., & others. (2024). Detection of intrusions in Internet of Things based deep auto encoder using DeepNets. *International Journal of Sensors, Wireless Communications and Control*.

[7] K. V., Arjun & others. (2024). Leveraging deep learning for intrusion detection in industrial IoT landscapes. *Computer Science, Engineering and Technology*.

[8] Sushant, C. G., Ajay, V. L., & Sahay, R. (2024). A comparative analysis of deep learning algorithms for intrusion detection in IoT.

[9] Varaprasad, R., Chakkaravarthy, P. A., & Veeresha, M. (2024). A comprehensive analysis of intrusion detection system using machine learning and deep learning algorithms.

[10] Hinojosa, A., & Majd, N. E. (2024). Edge computing network intrusion detection system in IoT using deep learning.

[11] Cui, B., Chai, Y., Yang, Z., & others. (2024). Intrusion detection in IoT using deep residual networks with attention mechanisms. *Future Internet*.

[12] Ashish, K., & Manoi, K. (2024). Classification of deep learning methods in intrusion detection for IoT devices.

[13] Du, C., Guo, Y., & Zhang, Y. (2024). A deep learning-based intrusion detection model integrating convolutional neural network and vision transformer for network traffic attack in the Internet of Things. *Electronics*.

[14] Nagarajan, S. (2024). Secure IoT: Deep learning-based intrusion detection for attack detection and prevent. *International Journal of Scientific Research in Engineering & Technology*.

[15] Surisetti, S., Bhavanam, S. N., Oruganti, V., & others. (2024). Intrusion detection system in Internet of Things-empowered cybersecurity by using various algorithms.

[16] Alimi, O. A. (2024). Hybrid data-driven learning-based Internet of Things network intrusion detection model.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 02 (2024)

[17] Selem, M., Farah, J., & Korbaa, O. (2024). Deep learning for intrusion detection in IoT networks.

[18] Krishnamurthy, R., Alabdeli, H., Rajani, N. F., & others. (2024). Intrusion detection in IoT environment using stochastic gradient descent with warm restarts and gated recurrent unit.

[19] Awad, O. F., Hazim, L. R., Jasim, A. A., & others. (2024). Enhancing IIoT security with machine learning and deep learning for intrusion detection. *Malaysian Journal of Computer Science*.

[20] Babu, C. S., Hruday, B. S. S., Krishna, S., & others. (2024). IoT threat mitigation: Leveraging deep learning for intrusion detection. *Journal of Advanced Zoology*.

[21] Atlas, L. G., Shiny, K. V., Arjun, K. P., & others. (2024). Detection of intrusions in Internet of Things based deep autoencoder using DeepNets. *International Journal of Sensors, Wireless Communications and Control*.

[22] Xiao, Y., Feng, Y., & Sakurai, K. (2024). An efficient detection mechanism of network intrusions in IoT environments using autoencoder and data partitioning. *Computers*.

[23] Dash, N., Chakravarty, S., & Rath, A. K. (2024). Deep learning model for elevating Internet of Things intrusion detection. *International Journal of Power Electronics and Drive Systems*.

[24] Cherfi, S., Boulaiche, A., & Lemouari, A. (2024). Enhancing IoT security: A deep learning approach with autoencoder-DNN intrusion detection model.

[25] Abu Al-Haija, Q., & Droos, A. (2024). A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT). *Expert Systems*.

[26] Xiao, Y., Feng, Y., & Sakurai, K. (2024). An efficient detection mechanism of network intrusions in IoT environments using autoencoder and data partitioning.

[27] Du, C., Guo, Y., & Zhang, Y. (2024). A deep learning-based intrusion detection model integrating convolutional neural network and vision transformer for network traffic attack in the Internet of Things. *Electronics*.

[28] Dinh, P. V., Hoang, D. T., Uy, N. Q., & others. (2024). Multiple-input autoencoder for IoT intrusion detection systems with heterogeneous data. *Proceedings Article*.

[29] Al Harbi, O., & Hamed, A. A. (2023). A dual-stage deep learning model based on a sparse autoencoder and layered deep classifier for intrusion detection with imbalanced data. *International Journal of Sensor Networks*.

[30] Bhavani, A. D., & Mangla, N. (2023). A novel approach of intrusion detection system for IoT against modern attacks using deep learning.