AI And Intrusion Detection in IOT Application

Abisha J
Department of Computer Science and Engineering
Vellore Institute of Technology
Chennai, India
abisha.j2022@vitstudent.ac.in

Ramya K M
Department of Computer Science and Engineering
Vellore Institute of Technology
Chennai, India
ramya.km2022@vitstudent.ac.in

***Abstract*- The proliferation of Internet of Things (IoT) devices across various domains such as healthcare, industrial automation, and smart homes has introduced unprecedented connectivity and convenience. However, this widespread adoption also creates substantial security vulnerabilities, as IoT devices are often resource-constrained and lack advanced protection mechanisms. To address these threats, Intrusion Detection Systems (IDS) augmented with Artificial Intelligence (AI) have gained significant attention. This paper presents a comprehensive study on the development of an AI-based IDS framework capable of detecting and classifying malicious activities in IoT networks using both Machine Learning (ML) and Deep Learning (DL) techniques. We employ three benchmark datasets—UNSW-NB15, CIC-IDS2017, and NSL-KDD—for training and evaluating various models. Our results indicate that while DL models demonstrate strong capabilities in learning complex patterns, traditional ML models such as Random Forest outperform DL models in terms of accuracy and computational efficiency. This finding underscores the suitability of ML models for real-time intrusion detection in resource-limited IoT environments.**

Keywords*- *IoT Security, Intrusion Detection System, Machine Learning, Deep Learning, Random Forest, Cyber Threats.

I. INTRODUCTION

The Internet of Things (IoT) represents a paradigm shift in technology by enabling seamless connectivity between physical devices and digital networks. These devices, ranging from smart thermostats to industrial sensors, collect and exchange data to enhance automation and decision-making. However, the increased interconnectivity also expands the attack surface, exposing networks to a variety of cyber threats including Distributed Denial-of-Service (DDoS), spoofing, malware, and data exfiltration attacks. Traditional cybersecurity solutions, such as firewalls and signature-based IDS, are often inadequate in IoT environments due to their static nature and inability to adapt to evolving threats.

To counteract these limitations, AI-powered Intrusion Detection Systems have been developed, incorporating techniques from machine learning and deep learning to detect anomalies in network traffic. Unlike static approaches, AI-based IDS can learn from historical attack data, recognize patterns, and adapt to new and emerging threats. In this research, we develop and evaluate an IDS framework that leverages both ML and DL models to classify network traffic and detect potential intrusions in real time.

A. Motivation

As the number of IoT devices grows exponentially, so does the volume and complexity of data generated within these networks. Manual monitoring and traditional IDS frameworks are not only inefficient but also fail to identify novel or zero-day attacks. Moreover, the limited computational and energy resources of IoT devices necessitate the use of lightweight yet accurate models that can operate under constraints. AI-based solutions provide a promising alternative, as they can automatically adapt to changing network conditions and accurately classify traffic patterns without human intervention.

The primary motivation behind this project is to enhance the security of IoT systems by designing an AI-based IDS that is not only accurate but also optimized for performance and energy consumption. By comparing ML and DL models on multiple datasets, this study aims to identify the most efficient algorithms for intrusion detection in resource-constrained environments, ultimately helping to build safer and more resilient IoT systems.

II. BACKGROUND STUDY

The growing complexity and scale of IoT ecosystems have necessitated the development of advanced Intrusion Detection Systems (IDS) capable of real-time threat detection. Traditional IDS frameworks, which often rely on rule-based or signature-based detection mechanisms, are proving to be insufficient in identifying sophisticated or zero-day attacks. As a result, recent research has focused on integrating Artificial Intelligence (AI)—particularly Machine Learning (ML) and Deep Learning (DL)—to enhance intrusion detection capabilities in IoT environments.

Geo and Sheeja et al. [2] explored the integration of AI-driven anomaly detection techniques into IDS frameworks for IoT networks. Their study emphasized the limitations of traditional, rule-based IDS solutions in handling dynamic attack patterns and proposed the use of hybrid AI techniques combining Decision Trees, Random Forest (RF), SVM, and k-Nearest Neighbors (kNN) with deep learning models like CNN, RNN, and MLP. The research, conducted using the CIC-DDoS2019 dataset, demonstrated that hybrid IDS approaches significantly reduce false positives while enhancing overall detection accuracy.

Jayalaxmi and Saha et al. [4] focused on the combined use of supervised and unsupervised learning techniques to detect cyberattacks in IoT environments. Their approach incorporated both ML models such as SVM, RF, kNN, and Naïve Bayes and DL models like CNN, RNN, and Deep Belief Networks (DBN). Evaluated on IoT-23 and CIC-DDoS2019 datasets, their findings confirmed that hybrid frameworks leveraging both ML and DL enhance detection accuracy and robustness, especially against sophisticated botnet and DDoS attacks.

Alghamdi et al. [3] introduced a hybrid intrusion detection model that integrates CNN for deep feature extraction with SVM for classification. This model was tested on realistic network traffic and demonstrated superior classification performance when compared to standalone approaches. The paper highlighted that such a combination improves both the speed and precision of detecting malicious activity, making it suitable for real-world IoT deployments.

Sharma and Sharma et al. [5] investigated the application of Explainable AI (XAI) in intrusion detection systems to enhance transparency and trust. By incorporating models such as SVM, kNN, Decision Trees, and deep learning techniques like CNN, RNN, and Generative Adversarial Networks (GANs), the study showcased how XAI can provide insights into the decision-making process of IDS. This approach was particularly beneficial in critical systems where understanding why a threat was flagged is as important as the detection itself.

Medjek and Tandjaoui et al. [8] addressed the challenge of energy consumption in AI-based IDS models for IoT. Their proposed system, built around Bayesian Networks and ANN, focused on fault tolerance and energy efficiency. Evaluated on the IoT-23 dataset, the model maintained high accuracy while consuming minimal resources, making it ideal for deployment on low-power IoT devices.

Shukla et al. [7] developed a lightweight ML-based IDS tailored for botnet detection in IoT systems. The author implemented classifiers such as Random Forest, SVM, and Decision Trees, achieving high accuracy in identifying botnet activity on the IoT-23 dataset. The study reinforced the viability of traditional ML methods in handling specific threats in IoT environments while maintaining low computational overhead.

Shahin et al. [6] proposed an AI-enhanced IDS optimized for industrial IoT systems. Using Bayesian inference techniques alongside statistical modeling, the study developed a multi-layered detection architecture capable of identifying both known and unknown threats. Their model demonstrated strong performance on the CIC-DDoS2019 dataset, highlighting the potential of AI to improve security in high-stakes environments such as manufacturing and critical infrastructure.

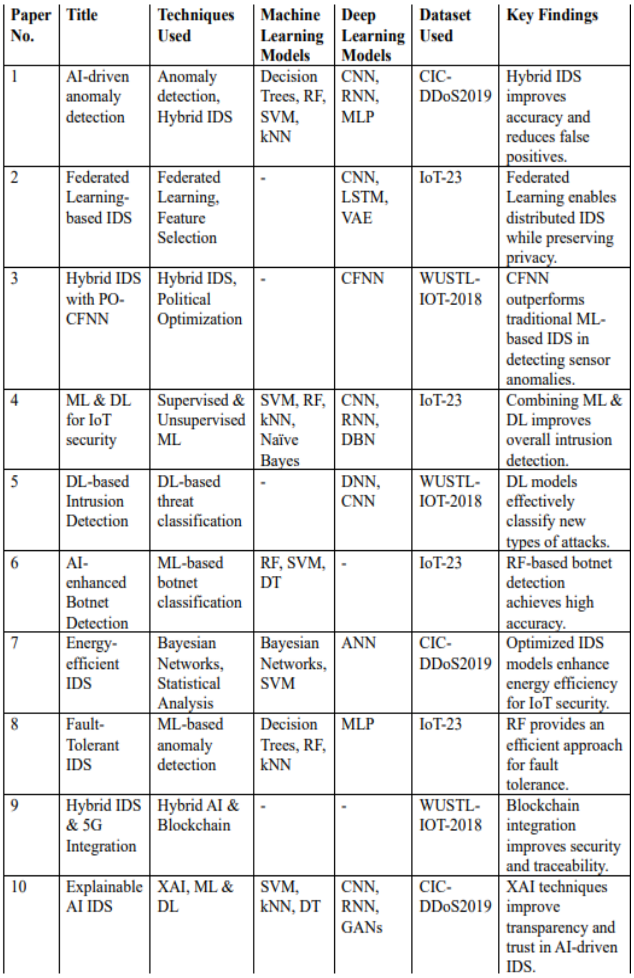
Saied, Guirguis et al. [10] presented a broad review of AI applications in enhancing intrusion detection for IoT. Their study synthesized findings across multiple datasets and models, offering comparative insights into the performance of different ML and DL techniques. They emphasized the importance of context-aware detection mechanisms and proposed the integration of AI with edge computing for scalable deployment.

Another notable contribution is a study titled *"Intrusion Detection and Prevention in Industrial IoT: A Technological Survey"*[9] which reviewed various IDS architectures and emerging AI techniques. This survey emphasized the role of hybrid systems and the integration of blockchain and federated learning for securing distributed IoT networks, especially in industrial contexts where latency and trust are critical factors.

Lastly, an innovative study on federated learning-based IDS models proposed the use of decentralized CNN, LSTM, and Variational Autoencoders (VAE) across distributed edge nodes. Using the IoT-23 dataset, this approach maintained user privacy while enabling collaborative learning. The research found that federated learning can significantly improve detection performance without centralizing sensitive data [Federated IDS Study, 2022].

Together, these studies form the foundation for the current research, showcasing the potential of AI to revolutionize IoT security. They collectively emphasize the need for adaptive, interpretable, and efficient IDS architectures that can cater to the unique challenges posed by IoT networks. Our project builds upon these insights by comparing multiple ML and DL models across real-world datasets to identify the most effective approach for practical IoT intrusion detection.

Table 1. Comparison Table of existing papers



Paper No.	Title	Techniques Used	Machine Learning Models	Deep Learning Models	Dataset Used	Key Findings
1	AI-driven anomaly detection	Anomaly detection, Hybrid IDS	Decision Trees, RF, SVM, kNN	CNN, RNN, MLP	CIC-DDoS2019	Hybrid IDS improves accuracy and reduces false positives.
2	Federated Learning-based IDS	Federated Learning, Feature Selection	-	CNN, LSTM, VAE	IoT-23	Federated Learning enables distributed IDS while preserving privacy.
3	Hybrid IDS with PO-CFNN	Hybrid IDS, Political Optimization	-	CFNN	WUSTL-IOT-2018	CFNN outperforms traditional ML-based IDS in detecting sensor anomalies.
4	ML & DL for IoT security	Supervised & Unsupervised ML	SVM, RF, kNN, Naïve Bayes	CNN, RNN, DBN	IoT-23	Combining ML & DL improves overall intrusion detection.
5	DL-based Intrusion Detection	DL-based threat classification	-	DNN, CNN	WUSTL-IOT-2018	DL models effectively classify new types of attacks.
6	AI-enhanced Botnet Detection	ML-based botnet classification	RF, SVM, DT	-	IoT-23	RF-based botnet detection achieves high accuracy.
7	Energy-efficient IDS	Bayesian Networks, Statistical Analysis	Bayesian Networks, SVM	ANN	CIC-DDoS2019	Optimized IDS models enhance energy efficiency for IoT security.
8	Fault-Tolerant IDS	ML-based anomaly detection	Decision Trees, RF, kNN	MLP	IoT-23	RF provides an efficient approach for fault tolerance.
9	Hybrid IDS & 5G Integration	Hybrid AI & Blockchain	-	-	WUSTL-IOT-2018	Blockchain integration improves security and traceability.
10	Explainable AI IDS	XAI, ML & DL	SVM, kNN, DT	CNN, RNN, GANs	CIC-DDoS2019	XAI techniques improve transparency and trust in AI-driven IDS.

III. PROPOSED METHODOLOGY

The intrusion detection system for IoT networks employs a multi-stage approach combining Machine Learning (ML) and Deep Learning (DL) techniques. The methodology includes dataset selection, preprocessing, feature selection, model training, and performance evaluation.

1.Dataset Collection: Three benchmark datasets—UNSW-NB15, CIC-IDS2017, and NSL-KDD—were used to ensure diverse and realistic attack representation. They cover various attack types such as DoS, brute force, botnet, and probing, supporting robust and comprehensive model evaluation.

2.Data Preprocessing: Preprocessing involved handling missing values, encoding categorical features, and normalizing numerical values. Datasets were split into 80% training and 20% testing to evaluate model generalization on unseen data.

3.Feature Selection: To reduce complexity, correlation-based filtering removed redundant features. Random Forest was then used to rank feature importance, ensuring the use of the most relevant attributes for efficient model training.

***4.ML Model Training**:* Random Forest, SVM, and Decision Tree algorithms were implemented using Scikit-learn. Hyperparameter tuning via grid search and cross-validation optimized each model for high classification accuracy.

5.DL Model Training: A Feedforward ANN built with TensorFlow/Keras was trained using dense layers with ReLU activation and dropout for regularization. The model used softmax for output, Adam optimizer, and categorical cross-entropy loss.

6. Model Evaluation: Models were evaluated using accuracy, precision, recall, and F1-score. Confusion matrices visualized performance across attack categories, enabling a clear comparison between ML and DL approaches in terms of detection capability.

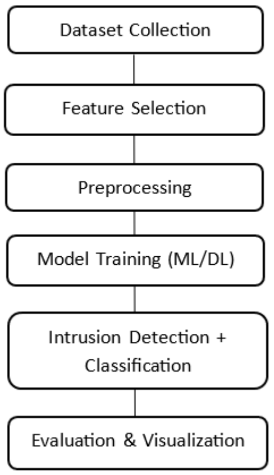


Fig 1. Flowchart of system

IV. METHODOLOGY

A. Evaluation Methods

To assess the performance of the implemented models, several standard evaluation metrics were applied:

- ***Accuracy**:* Measures the overall proportion of correctly classified instances in the dataset.
- ***Precision**:* Represents the proportion of true positives among all instances classified as positive, indicating the exactness of the model.
- ***Recall**:* Indicates the model's ability to identify all relevant positive cases, i.e., its sensitivity.
- ***F1-Score**:* A harmonic mean of precision and recall, providing a balance between the two.
- ***Confusion Matrix**:* A visualization tool used to describe the performance of a classification model by showing the actual versus predicted classifications for each class.
- ***Training Time and Computational Efficiency***: For ML vs. DL comparison, the time taken to train and infer predictions was recorded and compared, especially considering the resource-constrained nature of IoT devices.

These metrics were computed for both ML and DL models across all three datasets to conduct a fair and comprehensive comparison of performance.

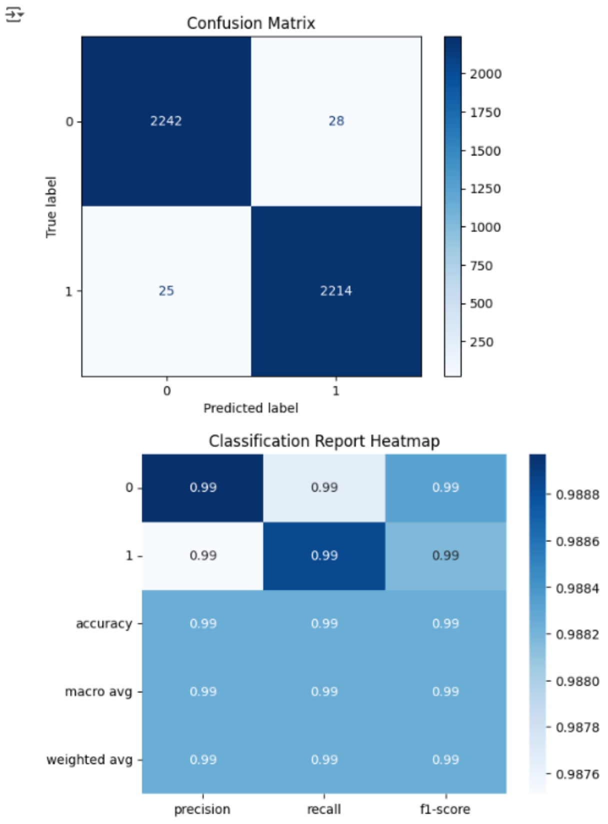


Fig 2. Evaluation metrics of KDD dataset training model

V. Results

From the performance analysis, it is evident that machine learning models like Random Forest are not only easier to interpret and deploy but also offer comparable or even better accuracy than deep learning models in certain datasets. For instance, in the NSL-KDD dataset, ML models surpassed DL by over 1% in accuracy. Although DL models can model more complex patterns, their training time and resource requirements are significantly higher, making them less suitable for real-time IoT environments.

A. Evaluation Results

The models were evaluated on their ability to detect intrusions in each of the three datasets. The evaluation focused on metrics such as accuracy, which measures overall correctness, and F1-score, which balances precision and recall. Below is the summary of the results obtained

Table 2. Accuracy results of ML and DL

Dataset	**ML Accuracy (%)**	**DL Accuracy (%)**
UNSW-NB15	92.12	92.30
CIC-IDS2017	100	100
NSL-KDD	98.85	97.19

B. Comparative Analysis of ML vs DL

A detailed comparative analysis was conducted to evaluate the practical implications of choosing ML over DL. While deep learning models offer advantages in learning complex, nonlinear relationships in data, they demand more memory, processing power, and training time. This makes them less viable in embedded IoT devices. On the other hand, ML models such as Random Forest strike a balance between accuracy and efficiency, which is critical in constrained environments.

Table 3. Comparative Table

Metric	**Machine Learning (RF)**	**Deep Learning (ANN)**
Accuracy	High	Moderate to High
Training Time	Low	High
Interpretability	High	Low
Resource Usage	Low	High

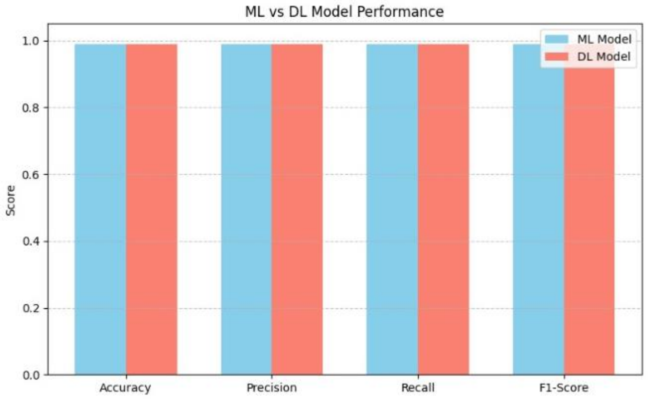


Fig 3. Performance bar chart of ML vs DL

VI. Conclusion

This paper presented a detailed study on the application of AI techniques, specifically ML and DL, for intrusion detection in IoT environments. Through the implementation and evaluation of various models on three benchmark datasets, we conclude that ML models such as Random Forest provide superior performance in terms of both accuracy by a few points and resource efficiency than DL model since the datasets taken were labeled. These models are especially well-suited for deployment in IoT networks where processing power and energy consumption are limited. Future work could explore the integration of federated learning and explainable AI to further enhance the security and trustworthiness of intrusion detection systems in the IoT landscape.

References

[1] Schmitt M. (2023). *Securing The Digital World: AI-enabled Malware and Intrusion Detection. Elsevier.*

[2] Geo, F. E., & Sheeja, S. (2023). *Intrusion detection system and mitigation of threats in IoT networks using AI techniques: A review.*

[3] Alghamdi, H. (2022). *A Hybrid Model for Intrusion Detection in IoT Applications.*

[4] Jayalaxmi, P. L. S., & Saha, R. (2022). *Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey. IEEE.*

[5] Sharma, B., & Sharma, L. (2024). *Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning-based approach.*

[6] Shahin M., Maghanaki, M., Hosseinzadeh, A., & Chen, F. F. (2024). *Advancing Network Security in Industrial IoT: AI-Enabled Intrusion Detection Systems.*

[7] Shukla, K. A. (2021). *Artificial Intelligence Assisted IoT Data Intrusion Detection.*

[8] Medjek, F., & Tandjaoui, D. (2021). *Fault-tolerant AI-driven Intrusion Detection System for the Internet of Things*.

[9] *Intrusion Detection and Prevention in Industrial IoT: A Technological Survey (2021).*

[10] Saied, M., Guirguis, S., & Madbouly, M. (2024). *Review of artificial intelligence for enhancing intrusion detection in the Internet of Things***.**