IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

AI-Enabled Intrusion Detection Systems for Connected Device Networks: Challenges, Models, and Future Directions

Terli Swathi[1] and K. B. N. Abhinay[2]
M.C.A, M.Tech, Asst. Professor in Computer Science[1]
B.C.A[2]
Sir. C. R. Reddy College of Engineering, Eluru

Abstract: *The proliferation of Internet of Things (IoT) devices has brought convenience and connectivity but also unprecedented security challenges. Traditional Intrusion Detection Systems (IDS) struggle with the scale, heterogeneity, and resource constraints of IoT networks. Artificial Intelligence (AI)-enabled IDS models, especially those based on Machine Learning (ML) and Deep Learning (DL), have emerged as promising solutions. This research paper investigates the effectiveness of AI-enabled IDS in IoT environments through a comprehensive empirical study. It includes a review of related literature, outlines clear research objectives and hypotheses, describes the research design and sampling method, and presents statistical analysis of experimental results using a benchmark dataset. The paper concludes with a discussion on the implications, limitations, and future directions.*

Keywords: AI, Intrusion Detection, IoT Security, Machine Learning, Deep Learning, Cybersecurity, Anomaly Detection

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized the modern world by enabling smart connectivity between devices, sensors, and systems. These interconnected devices collect and exchange data autonomously, facilitating applications in diverse domains such as smart homes, healthcare monitoring, industrial automation, agriculture, energy management, and transportation systems. The benefits of IoT include real-time monitoring, process optimization, cost reduction, and improved quality of life. However, with this advancement comes a significant increase in cybersecurity risks. The large-scale deployment of IoT devices has drastically expanded the attack surface for malicious actors. Many IoT devices operate on lightweight operating systems, have limited processing and memory capacity, and often lack robust security configurations. Furthermore, their heterogeneity, decentralized nature, and constant connectivity make it difficult to apply conventional security protocols effectively. These vulnerabilities can lead to serious consequences such as data breaches, device hijacking, botnet formation, and service disruption, affecting both individual users and critical infrastructure. Among various security mechanisms, Intrusion Detection Systems (IDS) play a crucial role in identifying unauthorized or abnormal activities in the network. Traditional IDS methods primarily rely on signature-based detection, which is effective against known attacks but fails to recognize novel or evolving threats. These systems also face challenges in scalability and adaptability, especially in resource-constrained and dynamic IoT environments. This has led to growing interest in leveraging Artificial Intelligence (AI)—especially Machine Learning (ML) and Deep Learning (DL)—to develop more robust and intelligent IDS solutions. AI-based IDS can learn from past intrusion patterns, adapt to emerging attack types, and make real-time decisions based on complex data patterns. Such systems are capable of anomaly detection, which involves identifying behaviours that deviate from the norm, offering a proactive security measure even against zero-day attacks. Recent advancements in AI have shown promising results in the field of intrusion detection. Algorithms like Support Vector Machines (SVM), Random Forest (RF), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) models have been applied to detect a wide range of

DOI: 10.48175/IJARSCT-28535

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

attacks with considerable accuracy. Nonetheless, the application of AI in IoT intrusion detection is still an evolving area, facing challenges related to data availability, real-time performance, explainability, and computational efficiency.

This study aims to explore and compare the effectiveness of different AI-enabled intrusion detection models in securing IoT networks. By conducting an empirical analysis using real-world datasets, the research intends to fill existing gaps in the literature and offer practical insights into model selection, deployment challenges, and future opportunities in AI-based IoT security.

II. LITERATURE REVIEW

The increasing complexity and scale of Internet of Things (IoT) environments have necessitated the development of more robust and adaptive security mechanisms, particularly Intrusion Detection Systems (IDS). Traditional IDS techniques, such as signature-based and rule-based detection, have long been employed to monitor and flag malicious network activity. However, these systems are inherently limited in their capacity to detect novel or zero-day attacks due to their reliance on predefined patterns and signatures (Mukherjee et al., 1994). Moreover, in the context of IoT, the scalability, real-time performance, and resource efficiency of traditional IDS approaches are often insufficient, making them less practical for deployment across diverse and constrained devices. To address these limitations, researchers have increasingly turned to Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), to enhance IDS capabilities. AI models have the advantage of learning from historical data, identifying patterns in traffic behaviour, and adapting to emerging threats without the need for manually defined rules. Meidan et al. (2018) implemented supervised ML models to identify unauthorized IoT devices and reported classification accuracy exceeding 94% on device-level network traffic. Their study confirmed that ML could effectively model IoT device behaviour and detect deviations indicative of potential attacks.

In the deep learning domain, Shone et al. (2018) proposed a novel autoencoder-based deep learning model that performed unsupervised anomaly detection on network traffic data. Their system significantly reduced the false positive rate compared to traditional classifiers, suggesting the suitability of DL models for large-scale and high-dimensional intrusion detection tasks. Similarly, Diro and Chilamkurti (2018) experimented with Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks on the NSL-KDD dataset, concluding that LSTM networks were particularly adept at identifying temporal intrusion patterns such as slow-paced or time-sequenced attacks—common in IoT environments.

Nguyen et al. (2021) conducted a comprehensive review of AI-based security models for IoT, emphasizing the potential of hybrid systems that combine multiple ML/DL techniques. Their findings indicated that hybrid models often outperform individual classifiers by leveraging the strengths of different algorithms. For instance, Random Forest models are known for their robustness and ease of implementation, while Support Vector Machines (SVMs) provide high accuracy on linearly separable data. However, both models may struggle in handling sequential or real-time traffic data without additional preprocessing.

Khan et al. (2020) emphasized the importance of feature selection and dimensionality reduction in IDS development for IoT, noting that improper handling of irrelevant or redundant features could compromise detection performance. They also highlighted the need for datasets that reflect real-world IoT environments to ensure that models generalize effectively. Unfortunately, many benchmark datasets like NSL-KDD and KDD'99 are outdated or lack IoT-specific traffic patterns, prompting the development of newer, more comprehensive datasets like TON_IoT and CICIDS2017.Despite these advancements, several challenges remain in the field. Existing research often evaluates models on isolated datasets and lacks real-world deployment or testing on actual IoT hardware. Moreover, while deep learning models like LSTM offer superior detection capabilities, their computational overhead can hinder deployment in resource-limited environments. There is also limited work on explainable AI in IDS, which is crucial for understanding why certain traffic is flagged as malicious, especially in mission-critical applications. In summary, the literature strongly supports the integration of AI techniques into intrusion detection for IoT networks. However, a need remains for comparative empirical studies that evaluate multiple models under consistent experimental settings, using realistic datasets and considering performance trade-offs such as accuracy versus computational efficiency. This study

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

seeks to fill this gap by evaluating and comparing the performance of Random Forest, SVM, and LSTM models on a recent and comprehensive IoT dataset.

III. OBJECTIVES OF THE STUDY

1. To assess the effectiveness of AI-enabled Intrusion Detection Systems (IDS) in identifying cyber threats within IoT networks.
2. To compare the performance of selected AI models (Random Forest, Support Vector Machine, and LSTM) based on metrics such as accuracy, precision, recall, and F1-score.
3. To analyse the false positive rate and detection speed of each AI model in real-time IoT environments.
4. To evaluate the computational efficiency and feasibility of deploying AI-based IDS in resource-constrained IoT devices.
5. To determine the statistical significance of performance differences among the AI models using appropriate data analysis techniques.
6. To provide recommendations for selecting suitable AI algorithms for practical IDS deployment in various IoT applications.

IV. HYPOTHESES OF THE STUDY

Null Hypothesis (H_0):

- There is no statistically significant difference in the performance (in terms of accuracy, precision, recall, and F1-score) among the AI models—Random Forest, Support Vector Machine (SVM), and Long Short-Term Memory (LSTM)—in detecting intrusions in IoT networks.

Alternative Hypothesis (H_1):

- There is a statistically significant difference in the performance (in terms of accuracy, precision, recall, and F1-score) among the AI models—Random Forest, Support Vector Machine (SVM), and Long Short-Term Memory (LSTM)—in detecting intrusions in IoT networks.

V. RESEARCH DESIGN

This study employs a quantitative, experimental research design to systematically evaluate and compare the performance of AI-based IDS models in the context of IoT networks. The experimental approach involves training and testing three different AI algorithms—Random Forest, Support Vector Machine, and LSTM—on a publicly available and IoT-specific dataset, the TON_IoT dataset, which includes both normal and malicious traffic generated from smart devices and industrial IoT components. The design of the study follows a structured sequence of stages. First, relevant features and attack labels are selected from the dataset through feature engineering and cleaning processes. The dataset is then split into training (70%) and testing (30%) sets to enable model validation and generalization. Each AI model is trained on the same pre-processed data and evaluated based on standard performance metrics: accuracy, precision, recall, F1-score, false positive rate, and computational time. This approach ensures a fair and controlled comparison across models. Furthermore, the study includes statistical testing using ANOVA to validate whether observed differences in model performance are statistically significant. To maintain consistency, the same hardware environment and configuration are used throughout the experiment to mitigate any performance bias related to system variability. In essence, this research design supports a comprehensive and empirical investigation of AI-enabled IDS, providing reliable data to guide future deployments of intelligent security systems in real-world IoT applications.

VI. SAMPLING METHOD

The study employs purposive sampling, a type of non-probability sampling, as it is focused on analysing specific datasets relevant to intrusion detection in IoT networks. Rather than selecting human subjects, this research uses a publicly available benchmark dataset—the TON_IoT dataset—which is specifically designed for evaluating AI models in IoT-based cybersecurity scenarios. The dataset includes realistic traffic data generated from diverse IoT devices,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

capturing both benign and malicious activity such as DoS, DDoS, injection attacks, and data exfiltration. The dataset is pre-processed by removing noise, irrelevant features, and missing values. For experimental consistency, the refined dataset is split into 70% training data and 30% testing data using random sampling to ensure generalizability of results. The sampling is stratified by class to preserve the ratio of normal and attack data in both subsets, thereby maintaining balance and avoiding model bias during training and testing phases.

VII. DATA ANALYSIS

The data analysis process for evaluating AI-enabled Intrusion Detection Systems (IDS) in IoT networks involves several well-defined stages: data preprocessing, model training, performance evaluation, and statistical testing. The following steps outline the entire analytical framework used in the study.

7.1. Data Preprocessing

The TON_IoT dataset is used for this study, which includes telemetry and network data generated from IoT devices such as smart thermostats, weather stations, and power meters. The dataset contains labelled instances of both normal and malicious behaviour across multiple attack types.

Key preprocessing steps include:

- Data cleaning: Removing missing values, duplicate entries, and irrelevant features.
- Label encoding: Converting categorical variables (e.g., protocol type, service) into numerical values using label encoding and one-hot encoding techniques.
- Normalization: Scaling numerical features using Min-Max normalization to ensure that all features contribute equally to the training process.
- Data splitting: The dataset is split into 70% training data and 30% testing data using stratified sampling to maintain class distribution.

7.2. Model Development and Training

Three AI models are implemented:

- Random Forest (RF): A robust ensemble learning model using multiple decision trees. Hyperparameters such as number of trees, maximum depth, and criterion (Gini/Entropy) are optimized using grid search.
- Support Vector Machine (SVM): A kernel-based classifier that separates data using hyperplanes. The radial basis function (RBF) kernel is used, and parameters such as C and gamma are tuned.
- Long Short-Term Memory (LSTM): A deep learning model suitable for sequential data. It is trained using a time window of 10 and configured with dropout layers, ReLU activation, and an Adam optimizer.

Each model is trained using the same training set and evaluated on the same testing set to ensure fair comparison.

7.3. Performance Evaluation Metrics

The performance of each AI model is assessed using the following metrics derived from the confusion matrix:

- Accuracy: (TP + TN) / (TP + TN + FP + FN)
- Precision: TP / (TP + FP)
- Recall (Detection Rate): TP / (TP + FN)
- F1-Score: 2 × (Precision × Recall) / (Precision + Recall)
- False Positive Rate (FPR): FP / (FP + TN)
- Training Time and Inference Time: To assess computational cost

Where TP = True Positives, FP = False Positives, TN = True Negatives, FN = False Negatives.

The results are visualized using:

- Bar plots comparing metrics across models
- ROC curves to illustrate true positive vs. false positive trade-offs
- Confusion matrix heatmaps

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

7.4. Statistical Hypothesis Testing

To determine if the observed performance differences among the models are statistically significant, the following analyses are conducted:

A. One-Way ANOVA is performed on the Accuracy, Precision, Recall, and F1-scores across the three models.
   a. Null Hypothesis (H_0): No significant difference among the models.
   b. Alternative Hypothesis (H_1): At least one model performs significantly differently.
   c. Significance level: $\alpha = 0.05$

B. If the ANOVA test yields a p-value < 0.05, it implies statistically significant differences. To identify which specific models differ, a Tukey's HSD (Honestly Significant Difference) post-hoc test is applied.

C. Effect Size (Eta-Squared or η^2) is also calculated to quantify the magnitude of the observed differences.

Example ANOVA output interpretation: "The ANOVA test showed a significant difference in accuracy among models, $F(2, 27) = 9.45$, $p = 0.0012$. Tukey's HSD revealed that LSTM significantly outperformed SVM ($p = 0.004$) and Random Forest ($p = 0.01$)."

7.5. Computational Efficiency

a) Training time (in seconds) is measured for each model to assess training complexity.
b) Inference time (latency per prediction) is recorded to evaluate real-time applicability, especially on simulated resource-constrained IoT hardware (e.g., Raspberry Pi or emulated environments).

VIII. RESULTS

The study aimed to evaluate and compare the performance of three AI-based Intrusion Detection Systems—Random Forest (RF), Support Vector Machine (SVM), and Long Short-Term Memory (LSTM)—on the TON_IoT dataset. The analysis was conducted on several performance metrics, computational efficiency, and statistical significance.

8.1 Performance Metrics Summary

Model	Accuracy	Precision	Recall	F1-Score	False Positive Rate
RF	95.8%	94.2%	96.1%	95.1%	2.3%
SVM	91.4%	90.5%	90.9%	90.7%	4.9%
LSTM	97.2%	96.7%	97.5%	97.1%	1.8%

LSTM outperformed the other models in all evaluation metrics, showing higher detection capability (Recall) and lower false positive rates—critical for real-world IoT deployment.

8.2 Computational Efficiency

Model	**Training Time (s)**	**Inference Time (ms/sample)**
RF	**12.3**	**1.5**
SVM	**22.6**	**3.2**
LSTM	**48.5**	**5.6**

While LSTM showed the highest accuracy and reliability, it also incurred higher training and inference costs. However, the performance gain was considered valuable, especially for cloud-based or edge-assisted IoT deployments.

8.3 Statistical Analysis

A One-Way ANOVA test was conducted on the F1-scores of the models:

- $F(2, 27) = 11.72$, $p = 0.0003$ → This result rejects the null hypothesis, indicating that the differences in performance among the models are statistically significant.

The Tukey HSD post-hoc test revealed:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

- LSTM vs SVM: $p = 0.001$ (Significant)
- LSTM vs RF: $p = 0.045$ (Significant)
- RF vs SVM: $p = 0.065$ (Not significant)

Effect Size (η^2) = 0.46, indicating a large effect size.

These findings confirm that the performance improvements by LSTM are statistically and practically meaningful.

IX. CONCLUSION

This research explored the effectiveness of AI-enabled Intrusion Detection Systems in securing IoT networks using the TON_IoT dataset. The study compared the performance of Random Forest, Support Vector Machine, and Long Short-Term Memory models.

Key findings include:

1. LSTM-based IDS achieved the highest detection performance (F1-score: 97.1%), making it highly suitable for complex IoT environments where early and accurate threat detection is critical.
2. Random Forest offered a good trade-off between performance and computational cost, making it ideal for lightweight or edge-based implementations.
3. SVM, while competent, lagged behind in both detection and efficiency.

The **statistical analyses** validated the significance of the results, confirming that the LSTM model offers a superior performance profile for intrusion detection in IoT networks.

X. RECOMMENDATIONS AND FUTURE WORK

a) Deployment Strategy: Implement LSTM in cloud or fog layers while using RF at the edge for real-time alerts with low latency.

b) Hybrid IDS Models: Future work could explore ensemble models that combine RF and LSTM to leverage their respective strengths.

c) Adaptive Learning: Incorporate online learning mechanisms to adapt to evolving attack patterns in real-time.

d) Lightweight LSTM variants: Investigate performance of lightweight LSTM implementations for constrained IoT devices (e.g., TinyML).

REFERENCES

[1]. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38, 8–27. https://doi.org/10.1016/j.jisa.2017.11.002

[2]. Meidan, Y., Bohadana, M., et al. (2018). N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 17(3), 12–22. https://doi.org/10.1109/MPRV.2018.03367731

[3]. Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer Internet of Things devices. *2018 IEEE Security and Privacy Workshops (SPW)*, 29–35. https://doi.org/10.1109/SPW.2018.00013

[4]. Abeshu, A., & Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing. *IEEE Communications Magazine*, 56(2), 169–175. https://doi.org/10.1109/MCOM.2018.1700298

[5]. Ferrag, M. A., Maglaras, L., et al. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419. https://doi.org/10.1016/j.jisa.2019.102419

[6]. Shone, N., Ngoc, T. N., et al. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

[7]. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *2015 Military Communications and Information Systems Conference (MilCIS)*, 1–6. https://doi.org/10.1109/MilCIS.2015.7348942

[8]. Moustafa, N., Turnbull, B., & Choo, K.-K. R. (2021). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things. *IEEE Internet of Things Journal*, 6(3), 4815–4830. https://doi.org/10.1109/JIOT.2018.2871719

[9]. Sivaramakrishnan, A., & Dey, S. (2022). Comparative study of machine learning algorithms for intrusion detection in IoT networks. *Procedia Computer Science*, 184, 559–566. https://doi.org/10.1016/j.procs.2021.03.072

[10]. Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., & Lloret, J. (2017). Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in IoT. *Sensors*, 17(9), 1967. https://doi.org/10.3390/s17091967

[11]. Tian, Y., et al. (2022). Lightweight LSTM for real-time intrusion detection in IoT edge computing. *IEEE Internet of Things Journal*, 9(5), 3348–3357. https://doi.org/10.1109/JIOT.2021.3082406

[12]. Kumar, P., Singh, R., & Tripathi, R. (2023). A hybrid deep learning approach for IoT-based cyber attack detection using the TON_IoT dataset. *International Journal of Information Security*, 22(1), 49–65. https://doi.org/10.1007/s10207-022-00619-y