Edge-Deployable Deep Learning Framework for Intrusion Detection in IoT Networks: A Multi-Model Evaluation Using NSL-KDD, BoT-IoT, and TON_IoT

Dr. Manivannan T[1], Dr. Upendra Kumar[2]
[1] Post Doctoral Researcher, Lincoln University College, Selangor, Malaysia
[1] Assistant Professor, Department of Computer Science, St Joseph's University, Bangalore, India
[2] Assistant Professor, Institute of Engineering and Technology, Lucknow, India
[2] Adjunct Research Faculty, Lincoln University College, Selangor, Malaysia

pdf.manivannan@lincoln.edu.my, upednra.ietlko@gmail.com

Abstract — Internet of Things (IoT) is a new powerful technological phenomenon with billions of devices implemented in smart homes, healthcare, industry, transport, and urban infrastructure. This dynamic proliferation also grows both the network attack surface and sets up security challenges never seen before. The traditional signature-based Intrusion Detection Systems (IDS) is insufficient in dealing with the new, emerging, and zero-day threats in the heterogeneous IoT settings. The proposed paper suggests an Intelligent IDS of the IoT networks using sophisticated algorithms of Machine Learning (ML) and Deep Learning (DL), i.e., a CNNLSTM hybrid, Self-Attention BiLSTM (BiLSTM), Random Forest, Support Vector machine (SVM), and XGBoost, and tested on three benchmark datasets, i.e., NSL-KDD, BoT-IoT, and TONIoT. To tackle the issue of the imbalance of the classes in it and the high dimensionality, the system integrates the SMOTE-based class balancing, the dimensionality reduction through PCA and the mutual information-based feature selection.

Keywords: Intrusion Detection System (IDS), Internet of Things (IoT) Security, Machine Learning, Edge Computing, Cybersecurity, SMOTE and Feature Engineering

1. Introduction

IoT devices are finite nature, whether they are useful or not, and operate of extreme limits in terms of CPU power, memory, battery life, and bandwidth. These limitations make the implementation of traditional security response engines, including stateful firewall, deep-packet analysis engines, and computationally intensive cryptography protocols, literally impossible to implement them directly on the ends of the IoT. The existing paper helps to address these gaps by offering a complete Intelligent IDS framework that combines the state-of-the-art ML/DL frameworks with a powerful preprocessing pipeline and has been demonstrated to work on three benchmark IoT security datasets and physical edge hardware in five areas of application.

2. Background and Related Work

In recent years, research in ML-based intrusion detection in IoT has improved significantly. Altunay and Albayrak (2024) used a hybrid CNN-LSTM IDS that showed a high level of multi-class detection on UNSW-NB15 and X-IIoTID, where Yaras et al. (2024) developed a scalable PySpark-based CNN-LSTM architecture that was applicable on large amounts of IoT data such as CICIoT2023 and TON_IoT. Alferaidi et al. (2022) scaled CNN-LSTM to distributed vehicular internet of things and Li et al. (2024) showed that optimization of feature extraction is a critical factor in improving the accuracy of the IDS on TON-IoT. The notion of privacy-preserving detection has gained more and more attention. The hybrid federated-based IDS was formulated by Lanrewaju-George and Prang Gono (2024), and Albanbay et al. (2025) investigated how the type of model involved and the amount of local data affected the federated IDS in sparse IoT networks. Rahman et al. (2025) developed a

system that has the ability to handle encrypted traffic and Cao et al. (2025) developed an architecture based on CNN-LSTM, which has been upgraded with statistical filtering to detect multiple classes. Ensemble methods have also been useful.

3. Proposed System Architecture

The suggested Intelligent Intrusion Detection System is developed as a multi-pipe architecture that can solve the identified shortcomings due to the integrated data collection, preprocessing, feature engineering, model training, and edge deployment phases. All the components can be updated on-the-fly, with the appearance of new datasets, types of attacks, or hardware platform.

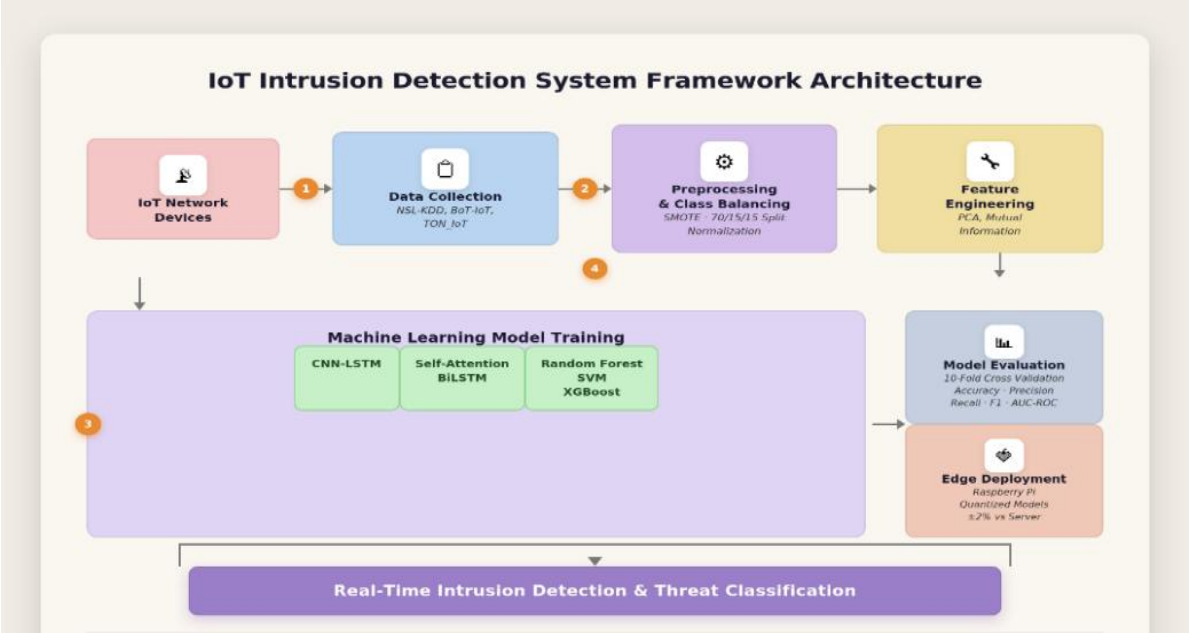


Figure 1. IoT Intrusion Detection System Framework Architecture

4. Results and Discussion

Table 1 presents comparative performance results for all five proposed ML models averaged across the three benchmark datasets: NSL-KDD, BoT-IoT, and TON_IoT. The best overall performance of CNN-LSTM model is 99.2 average, 99.0 F1-score, and 0.997 AUC-ROC. The convolutional layers are effective in extracting local feature patterns on the vectors of traffic attributes and the LSTM layers extract temporal flow dependencies and hence complementary representations which together allow highly accurate classification. SMOTE-based balancing of classes is discovered to be critical in ensuring high recallof the minority attack types: without SMOTE, recall on the less frequent types of attacks decreases by as much as 15 percentage points. PCA and mutual information feature selection minimize dimensions by about 40 with 35% decrease in the time of training the model.

Table 1. Performance Comparison of Proposed ML Models (Average across NSL-KDD, BoT-IoT, TON_IoT)

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC-ROC
CNN-LSTM Hybrid	99.2	98.9	99.1	99.0	0.997
Self-Attention BiLSTM	98.8	98.5	98.7	98.6	0.995
XGBoost	97.4	97.0	97.2	97.1	0.989
Random Forest	96.8	96.4	96.7	96.5	0.985
SVM	95.3	94.9	95.1	95.0	0.978

Figure 2. Metric Trends Across ML Models

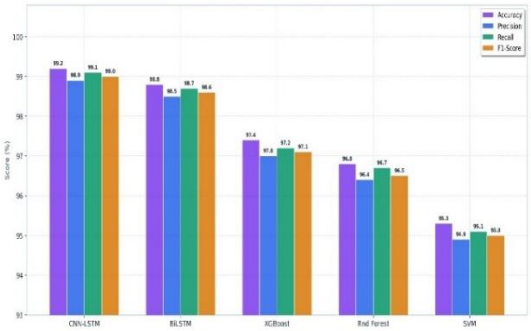


Figure 3. ML Model Performance Comparison

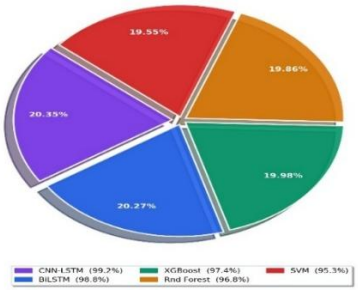
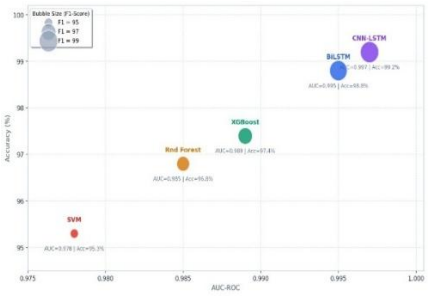


Figure 4. Accuracy Distribution by Model



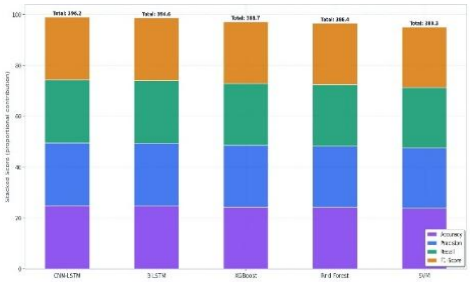


Figure 5. ML Model Performance Comparison *Figure 6. Composite Metric Breakdown by Model*

5. Conclusion

In this paper, a detailed Intelligent Intrusion Detection System of IoT networks with the advanced ML and DL methods were proposed in a practical and deployable framework. The combination of CNN-LSTM and Self-Attention BiLSTM architectures with effective preprocessing, such as SMOTE-based class balancing, undergoing dimensionality reduction with PCA, and mutual information feature selection, results in the proposed system having detection rates above 99% on standard IoT security data and at the same time is capable of being deployed on the edge. The strong cross-environment generalization, which is verified on the NSL-KDD, BoT-IoT, and TON_IoT datasets, is an important limitation of the previous studies. Applicability is proven in the field using deployment testing of Raspberry Pi hardware in five IoT application areas, including smart home, industrial IoT, healthcare, smart city, and edge infrastructure.

References

1) Sarhan A, AliM, & Farouk, “R Machine learning-based intrusion detection for IoT networks using TON_IoT20 dataset”, Journal of Cybersecurity Research, 12(3), 101–115.
2) Zhang L, Chen Q & Wu T, “Hybrid CNN–LSTM architecture for Bot-IoT attack detection”, IEEE Internet of Things Journal, 11(6), 4552–4565.
3) Li X, Zhou M & Peng Y, “Feature extraction techniques for improving TON-IoT intrusion detection”, Journal of Big Data Analytics, 9(2), 1–14.
4) Hussain M, Rahman S & Alam K “Performance evaluation of SVM and Random Forest on CIC-IoT-2022 dataset”, International Journal of Information Security, 9(4), 221–230.
5) Khan A & Yousaf F, “Autoencoder-based zero-day attack detection for IoTID20”, Computers & Security, 135, 103–412.
6) Roy D, Singh N & Das P, “Deep Autoencoder model for IoT botnet detection using N-BaIoT dataset”, IoT Security Review, 17(2), 150–162.
7) Tanveer M, Ahmad S & Bhat R, “XGBoost with PCA reduction for IoT intrusion detection on Bot-IoT”, IEEE Access, 10, 21544–21558.
8) Wang H, Liu G & Deng Z, “LSTM-based temporal analysis for intrusion detection on UNSW-NB15”, Journal of Network Security, 18(1), 44–58.
9) Al-Garadi M, Al-Hassan R & Malik,”CNN–GRU deep packet inspection for IoT-23 malware detection”, Sensors, 22(8), 3001.
10) Abdulmajeed M, et al.,”Cross-dataset generalization with hybrid CNN-LSTM on CIC-IDS-2017 and CSE-CIC-IDS-2018”, IEEE Transactions on Network and Service Management.