Lightweight Autoencoder-Based Anomaly Detection for Resource-Constrained IoT Networks

Salihah Alotaibi[1†]

Information Systems Department, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia.

Abstract
The Internet of Things (IoT) is growing quickly and is now used in homes, industries, hospitals, transport systems, and many smart-city services. As more devices get connected, the security risks also increase because most IoT devices have very limited processing power and memory. Many of the current anomaly-detection methods depend on heavy machine-learning models, and these models are difficult to run on small devices that work on low energy. This paper introduces a lightweight anomaly-detection method. The idea is to first reduce the number of features, so the data becomes easier to handle and then use a small autoencoder that learns what normal traffic usually looks like. When the traffic behaves in an unusual way, the reconstruction error becomes higher, which helps in spotting abnormal activity. The method is tested on a synthetic IoT dataset that tries to mimic real network traffic, and it is also compared with some basic existing models. Performance evaluation of the method shows that it can be used for IoT applications with low resources and good accuracy.

Keywords:
IoT Security, Anomaly Detection, Lightweight Autoencoder, Feature Reduction

1. Introduction

Internet of Things (IoT) is part of everyday life and used in many applications. It merges networking with embedded systems and provides a solution to monitor and control objects. IoT provides an update to the previous systems that do not use any real time monitoring. The future applications will use IoT for real-time updates and debugging [1,2]. IoT systems have many challenges, and security is one of the main issues. As Internet is major part of IoT, and data is shared online between devices, objects and servers, secure communications become a challenge. Hence, IoT systems must be aware of security threats and challenges [3-5].

IoT devices face many kinds of attacks, such as denial-of-service, botnet infections, scanning, spoofing, and data-manipulation attacks. These attacks can disturb services, steal sensitive data, or even take control of the device. Some of these threats stay hidden for a long time because IoT traffic keeps changing, and certain attacks create traffic that looks very similar to normal behavior [6, 7].

Although several machine-learning and deep-learning methods have been developed for detecting such attacks, most of them are heavy models and need high computational resources. These models are not practical for small IoT devices that work under strict limits of energy and memory. Also, some existing approaches use many features, which increase complexity and slows down detection. There is a need for a simple and efficient anomaly-detection method that can run on resource-constrained IoT devices while still giving good accuracy [8-10].

To address this, the study presents a lightweight autoencoder model along with a simple feature-reduction step. The feature-reduction process removes repeated or less important attributes from the dataset, which reduces model size and improves speed. After that, the compact autoencoder learns normal traffic behavior and detects abnormal activity using reconstruction error. The method is tested on a synthetic IoT dataset created to reflect realistic IoT traffic and is compared with basic baseline models. In the results, it is observed that less number of resources are used and achieve satisfactory performance for IoT applications.

The rest of the paper is organized as follows. Section 2 reviews related work on IoT anomaly detection. Section 3 explains the proposed method and its steps. Section 4 presents performance evaluation and results. Section 5 gives the conclusion and mentions possible future directions.

2. Related Works

IoT security has been a popular area of research in recent times. The main goals of research in this area are to increase detection accuracy, reduce

Manuscript received December 5, 2025
Manuscript revised December 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.12.4

false alarms, and keep the computational cost within the limits of resource-constrained IoT devices.
The contribution of the work in [11] is based on deep learning model applied to the CICIoT2023 dataset. The goal was to develop intrusion detection system. The main aim of using deep learning was to utilize varying traffic patterns. Performance results highlight that the deep learning based system performs better than normal machine learning techniques.

A deep learning based system was also developed in [12]. The main aim of the system was to use feature selection technique and choose only features that are of most importance. This was done using a genetic algorithm with several intrusion metrics. Convolution layer was applied to capture traffic patterns in the security system. Performance results showed that work improved accuracy with reduced feature set.

A number of traditional machine-learning models were evaluated for anomaly detection in an Internet of Things-based healthcare environment in [13]. Preprocessing techniques such as balancing the classes and eliminating highly correlated features were applied to an intrusion dataset containing various attack types. Models like logistic regression, Random Forest, and boosting techniques were assessed. The best results came from Random Forest, which achieved nearly 99% accuracy. Because of its quick response time, the authors hypothesised that the approach might be useful in real-time healthcare.

In [14], machine-learning methods for IoT anomaly detection were compared more broadly. In this work, XGBoost, SVM, and deep convolutional networks were tested on a number of benchmark datasets as well as on an internal IoT testbed that included actual devices like smart plugs and cameras. The findings demonstrated that XGBoost outperformed SVM and deep CNNs in terms of accuracy and training speed. Because it suggests a model that provides a good balance between speed and performance for large IoT networks, this makes the study valuable.

Interpretability and privacy have also been examined by some researchers. An explainable anomaly-detection framework that integrated various individual models and ensemble approaches with multiple explanation techniques was presented in [15]. Botnet traffic and IoT sensor data were used with the system. It not only achieved high accuracy but also gave clear information about which features contributed most to the final decision, helping operators understand why a certain event was marked as an attack.

The privacy of IoT devices in smart city is addressed by the work in [16]. It uses federated learning and combines it with split learning. The data sent to the server is reduced and also data is kept private and local to own clusters. Results of the work highlight improvement in accuracy at lower communication overhead.

Overall, these studies show good progress in IoT anomaly detection, but many of the existing methods still depend on complex deep models or large feature sets that are hard to run on low-power devices. This creates the need for simpler and more lightweight approaches, such as compact autoencoders with fewer input features, that can still give reliable detection in practical IoT environments.

3. Methodology

In this section, the explanation about methodology of the lightweight auto encoder technique is discussed in detail. The work is explained step by step in several subsections.

3.1 Details of the used dataset

The dataset used for the work is synthetically created to simulate both normal and malicious types of traffic. The feature set is based on IoT data that is normally shared with other devices. A big advantage of using this dataset is that frequency of traffic types can be controlled for better evaluation of the algorithms. The features used include packet related parameters such as packet length, interarrival time, flow duration etc.

3.2 Data cleaning and feature reduction

At the start of the simulation, the dataset is first cleaned and processed to remove duplicates. Similarly, some of the features have extra large or extra small values and scaling is applied to keep them in a fixed range. As a result, the autoencoder can allocate the weights fairly to all features. The dataset is labeled into normal and malicious traffic. The data is further split into training and testing.

3.4 Proposed Technique: Lightweight autoencoder

The key idea of the work is to use a light weight autoencoder and get it aligned with IoT traffic. By using the related IoT parameters, the encoder compresses the feature vectors whereas the decoder performs the opposite function. The autoencoder model is first trained on the normal data. In the next step, the evaluation is performed on the testing data. Anomalies are marked by calculating the difference between encoded and decoded outputs.

3.5 Anomaly Detection Using Reconstruction Error

As discussed in the last subsection, the anomaly is detected based on error between encoded and decoded output. A threshold is selected to evaluate the reconstruction error. The values below the threshold are treated as normal whereas the values above that threshold are deemed as attack data. This approach of autoencoding is fast and light weight and does not result in a lot of processing overhead. Hence, it is ideal for low processing devices such as IoT.

4. Performance Evaluation

Results of the proposed autoencoder method is compared with three other baseline algorithms. The other methods include Isolation Forest, One-Class SVM, and K-Means. The dataset used for the performance evaluation is explained in section 3.1. The performance evaluation is based on important metrics such as accuracy, precision, recall, and F1-score. In addition, confusion matrix and computational cost is also evaluated.

4.1 Training Loss

The training loss of the proposed autoencoder is shown in Figure 1. It can be seen that the loss of the model is reduced after the first few epochs. The stability is achieved after around 35 epochs. After this the training loss is flat and hence equilibrium condition is achieved.

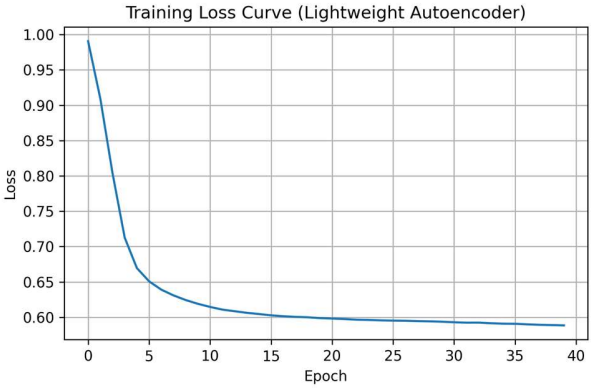

Figure 1: Training loss curve of the lightweight autoencoder

4.2 Reconstruction Error

Results in figure 2 highlight the reconstruction-error values for normal data and attack data samples. It can be seen that normal samples fall in the lower threshold of the graph. The attack data however remain in the higher threshold region. As the threshold line is fixed and easily detectable, the anomaly can be reliably detected.

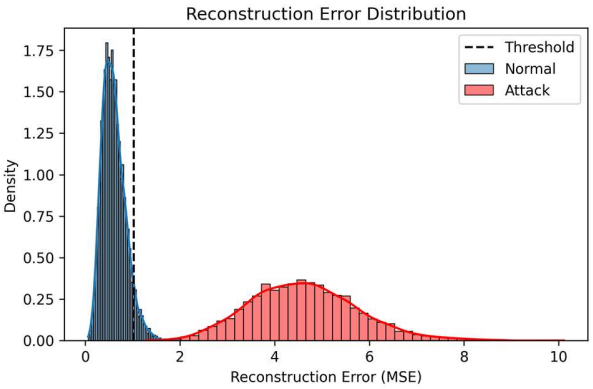

Figure 2: Reconstruction error distribution

4.3 Detection Performance

The results in table 1 highlight the four key metrics namely accuracy, precision, recall, and F1-score for all four models. These models are the lightweight autoencoder, Isolation Forest, One-Class SVM, and K-Means. The overall best results are achieved by the autoencoder model as it shows highest values of recall and reasonable values of all other metrics. In comparison, Isolation forest and SVM do not show good performance across all three metrics.

K-means algorithm shows best performance however it will be seen that it results in use of more memory for computations. Moreover, K-means algorithm also results in lower recall values.

Table 1: Performance Comparison of Anomaly Detection Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Lightweight Autoencoder (Proposed)	93.2	92.0	100.0	96.5
Isolation Forest	75.8	70.1	88.0	33.9
One-Class SVM	64.7	60.0	79.5	23.3
K-Means	95.0	95.1	99.8	99.0

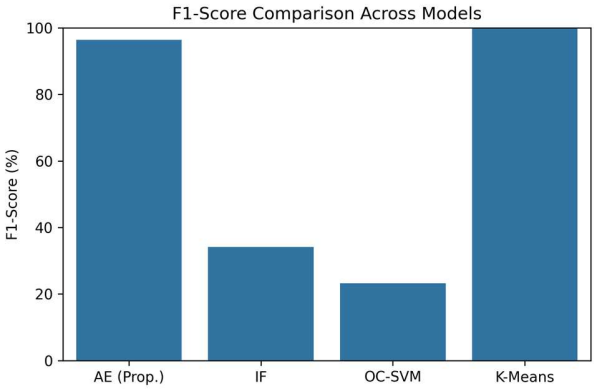

Figure 3: F1 score of models

4.4 Confusion Matrix Evaluation

In Table 2 and Figure 4, confusion matrix of the proposed autoencoder model is shown. It can be seen that the model detects normal and abnormal attacks in an accurate manner. The number of attack samples detected accurately is 4,050 attack samples and there is no false negative. Hence, no attack goes undetected. In addition, the normal samples are also detected accurately. For example, 4,650 are labeled accurately as normal traffic and only 300 are marked as false positives. The performance results show excellent performance for IoT networks that are vulnerable to security attacks. Not only anomaly accuracy is good but the reduction of false positives and false negatives save lot of time and processing power for low constrained IoT nodes.

Table 2: Confusion matrix of the lightweight autoencoder

	Predicted Normal	Predicted Attack
Actual Normal	4650	300
Actual Attack	0	4050

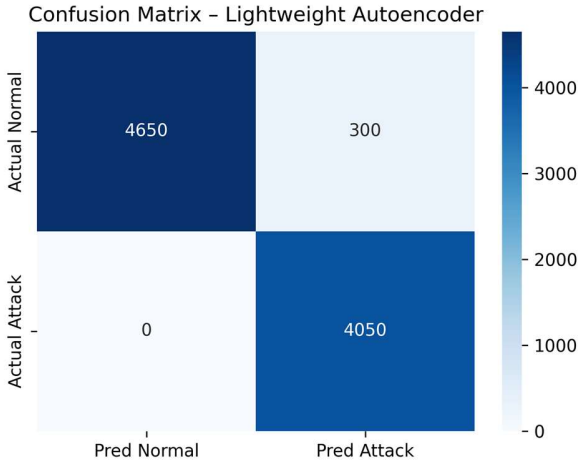

Figure 4: Confusion matrix

4.5 Computational Efficiency

In Table 3, the results of training time, the test time per sample, and the memory use are given for all the models. The lightweight autoencoder has a fast-running time and also gives good results for anomaly detection. Similarly, the memory taken for the autoencoder algorithm is low and ideal for IoT devices with limited resources.

Table 3: Computational Efficiency of Anomaly Detection Models

Model	**Training Time (s)**	**Test Time per Sample (ms)**	**Approx. Memory Usage (MB)**
Lightweight Autoencoder (Proposed)	30.896	0.054	0.0036
Isolation Forest	0.403	0.0076	0.0153
One-Class SVM	4.928	0.2515	12
K-Means	0.114	0.00036	8

5. Conclusion

The main theme of this work is focused on anomaly detection for low constrained IoT devices. A number of attacks exist that target IoT devices. In this work, a light weight autoencoder scheme is proposed that can reduce the processing time and memory while giving good anomaly detection performance. The performance evaluation of the results show that the proposed autoencoder achieves good performance in terms of accuracy and reduces false positives while also meeting low computational and memory requirements for IoT devices.

References

[1] F. Nie et al., "Empowering Anomaly Detection in IoT Traffic Through Multiview Subspace Learning," IEEE Internet of Things Journal, vol. 12, no. 11, pp. 15911–15925, 1 June 2025, doi: 10.1109/JIOT.2025.3530771.

[2] H. Mancy and Q. H. Naith, "SwinIoT: A Hierarchical Transformer-Based Framework for Behavioral Anomaly Detection in IoT-Driven Smart Cities," IEEE Access, vol. 13, pp. 48758–48774, 2025, doi: 10.1109/ACCESS.2025.3551207.

[3] N. Watanabe et al., "Self-Adaptive Traffic Anomaly Detection System for IoT Smart Home Environments," IEICE Transactions on Communications, vol. E108-B, no. 3, pp. 230–242, March 2025, doi: 10.23919/transcom.2024EBT0002.

[4] V. M. U et al., "AI-Powered IoT: A Survey on Integrating Artificial Intelligence With IoT for Enhanced Security, Efficiency, and Smart Applications," IEEE Access, vol. 13, pp. 50296–50339, 2025, doi: 10.1109/ACCESS.2025.3551750.

[5] K. Istiaque Ahmed, M. Tahir, S. Lun Lau, M. Hadi Habaebi, A. Ahad and A. Mughees, "Trust-Aware Authentication and Authorization for IoT: A Federated Machine Learning Approach," IEEE Internet of Things Journal, vol. 12, no. 8, pp. 9889–9904, 15 April 2025, doi: 10.1109/JIOT.2024.3512657.

[6] Enahoro, S. C. Ekpo, M. Uko, F. Elias and S. Alabi, "Integrating IoT With Adaptive Beamforming for Enhanced Urban Sensing in Smart Cities," IEEE Access, vol. 13, pp. 96120–96134, 2025, doi: 10.1109/ACCESS.2025.3571468.

[7] M. Rabbani et al., "Device Identification and Anomaly Detection in IoT Environments," IEEE Internet of Things Journal, vol. 12, no. 10, pp. 13625–13643, 15 May 2025, doi: 10.1109/JIOT.2024.3522863.

[8] X. Jiang, C. Lu, H. Luo and Y. Sun, "Unsupervised Distributed Anomaly Detection Framework for IoT in Edge AI Network," IEEE Internet of Things Journal, vol. 12, no. 12, pp. 22058–22072, 15 June 2025, doi: 10.1109/JIOT.2025.3549765.

[9] Q. Lin et al., "Anomaly Detection in Smart IoT Systems Based on Contextual Semantics of Behavior Graphs," IEEE Internet of Things Journal, vol. 12, no. 10, pp. 13683–13696, 15 May 2025, doi: 10.1109/JIOT.2024.3523998.

[10] B. Guha Roy, D. Guha Roy, P. Datta, S. Bhatia Khan, F. Asiri and M. Ayadi, "Quality of Service-Aware 6G-Enabled NB-IoT for Health Monitoring in Long Distance High-Speed Trains," IEEE Transactions on Consumer Electronics, vol. 71, no. 1, pp. 1136–1147, Feb. 2025, doi: 10.1109/TCE.2025.3540197.

[11] S. K. Erskine, "Real-time large-scale intrusion detection and prevention system (IDPS) CICIoT dataset traffic assessment based on deep learning," Applied System Innovation, vol. 8, no. 2, p. 52, 2025.

[12] A. Behera, K. S. Sahoo, T. K. Mishra, and M. Bhuyan, "A combination learning framework to uncover cyber attacks in IoT networks," Internet of Things, vol. 28, p. 101395, 2024.

[13] M. M. Khan and M. Alkhathami, "Anomaly detection in IoT-based healthcare: machine learning for enhanced security," Scientific Reports, vol. 14, no. 1, p. 5872, 2024.

[14] M. Balega, W. Farag, X. W. Wu, S. Ezekiel, and Z. Good, "Enhancing IoT security: optimizing anomaly detection through machine learning," Electronics, vol. 13, no. 11, p. 2148, 2024.

[15] A. Namrita Gummadi, J. C. Napier and M. Abdallah, "XAI-IoT: An Explainable AI Framework for Enhancing Anomaly Detection in IoT Systems," in IEEE Access, vol. 12, pp. 71024-71054, 2024, doi: 10.1109/ACCESS.2024.3402446.

[16] I. Priyadarshini, "Anomaly detection of IoT cyberattacks in smart cities using federated learning and split learning," Big Data and Cognitive Computing, vol. 8, no. 3, p. 21, 2024.

Salihah Alotaibi is working as Assistant Professor at Information Systems Department, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU) Riyadh, Saudi Arabia.