International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

# Adaptive Latent Representation Learning with Consensus Decision Intelligence for Trusted IoT Device Identity Verification

Varikol Vinay, K. Srilatha*

Vaagdevi Engineering College, Warangal, 506005, Telangana, India.

*Correspondence: K. Srilatha

**Abstract**

The continuous growth of the Internet of Things (IoT) has led to the deployment of a vast ecosystem of interconnected devices across domains such as healthcare, smart cities, industrial automation, and intelligent infrastructure. While this connectivity offers significant operational benefits, it also introduces serious cybersecurity risks, including unauthorized access, data tampering, malicious attacks, and network service interruptions. Conventional security solutions, such as Access Control Lists (ACLs), signature-based detection techniques, and rule-driven mechanisms, are increasingly inadequate because of their fixed configurations, dependence on continuous manual updates, and inability to effectively recognize newly emerging threats. To overcome these limitations, this research proposes an intelligent IoT security framework based on a Deep Autoencoder (DAE) that performs both device classification and data integrity verification. The DAE learns compact and informative feature representations from IoT network traffic, enabling accurate differentiation between legitimate and malicious device activities. By utilizing labeled datasets during training, the model captures complex communication patterns and detects anomalous behaviour with high precision. In addition, an integrated authentication module validates the authenticity and integrity of device communications before allowing access to the network, thereby strengthening overall system trust and security. Experimental evaluation demonstrates that the proposed framework achieves an accuracy of 97.8%, surpassing conventional machine learning techniques such as K-Nearest Neighbors (KNN) and Logistic Regression Classifier (LRC). Furthermore, a hybrid model referred to as DAE-BFL (BFL), which combines the Deep Autoencoder with Random Forest Classifier (RFC) and Logistic Regression Classifier (LRC), further improves classification reliability and robustness. The overall framework encompasses data preprocessing, model training, validation, and real-time performance assessment, providing a scalable, adaptive, and efficient solution for securing next-generation IoT networks.

**Keywords:** Internet of Things (IoT), Deep Autoencoder (DAE), Device Classification, Data Validation, Intrusion Detection, Network Security, Anomaly Detection, Authentication

## 1. Introduction

The rapid advancement of the IoT has transformed modern digital ecosystems by enabling seamless communication among billions of interconnected devices across healthcare, smart homes, industrial automation, transportation, agriculture, and smart city infrastructures. IoT devices continuously collect, process, and exchange real-time information to improve operational efficiency, automation, and decision-making. The global deployment of IoT technologies has accelerated significantly over the past decade due to the adoption of artificial intelligence, cloud computing, edge computing, and fifth-generation (5G) communication networks. Recent industry reports estimate that more than 21 billion IoT

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

devices were actively connected worldwide in 2025, with projections indicating that this number will reach approximately 39 billion devices by 2030, reflecting sustained double-digit annual growth. Simultaneously, the IoT security market is expected to expand from nearly USD 28.7 billion in 2025 to over USD 80 billion by 2031, highlighting the increasing investment in protecting connected infrastructures from evolving cyber threats.

Despite these technological advancements, the exponential growth of IoT deployments has introduced significant security challenges due to the heterogeneous nature of connected devices, constrained computational resources, and the absence of standardized security mechanisms. Many IoT devices operate with limited processing power and memory, making the implementation of computationally intensive cryptographic techniques difficult. Consequently, attackers increasingly exploit vulnerable devices through malware injection, unauthorized access, distributed denial-of-service (DDoS) attacks, spoofing, replay attacks, and identity impersonation. Recent cybersecurity analyses indicate that more than half of deployed IoT devices contain critical security vulnerabilities, while approximately one-third of modern data breaches involve IoT endpoints, as shown in fig 1. Furthermore, large-scale enterprise studies have revealed that nearly 48% of connections originating from IoT devices are associated with high-risk devices, substantially increasing organizational attack surfaces. These security concerns demonstrate that conventional signature-based intrusion detection techniques and static authentication mechanisms are insufficient for protecting highly dynamic IoT environments.

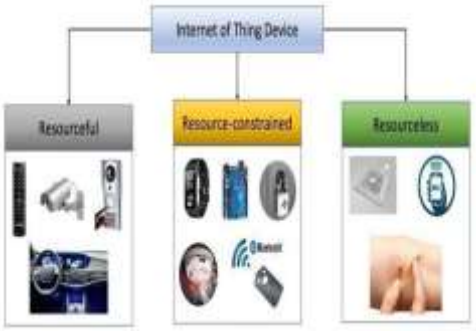



Fig. 1: Classification of IoT devices.

To address these challenges, intelligent security frameworks integrating deep learning with robust authentication mechanisms have emerged as promising solutions for securing next-generation IoT networks. Deep Autoencoders have demonstrated exceptional capability in learning compact latent representations of high-dimensional network traffic, effectively distinguishing legitimate device behavior from anomalous or malicious activities without extensive manual feature engineering. When combined with secure data authentication mechanisms, these models not only improve device classification accuracy but also verify the authenticity and integrity of transmitted information, thereby preventing unauthorized device access and data manipulation. Such an integrated framework enhances network trustworthiness by simultaneously performing feature extraction, anomaly detection, secure device identification, and authenticated communication. Therefore, the proposed Deep Autoencoder-based Secure IoT Device Classification with Data Authentication framework aims to provide an intelligent, scalable, and resilient security solution capable of supporting the rapidly expanding IoT ecosystem while improving classification performance, reducing false detections, and strengthening end-to-end data security against sophisticated cyber threats.

## 2. Literature Survey

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

Alaghbari, et al. [1] proposed an integrated Intrusion Detection System (IDS) for Internet of Things (IoT) networks that combines a deep Autoencoder (AE) for anomaly detection and feature extraction within a unified framework. The proposed AE model was trained exclusively on normal network traffic to learn its underlying patterns and identify anomalous activities without requiring labeled attack data. Unlike conventional dimensionality reduction methods such as Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA), the autoencoder simultaneously reduced feature dimensionality while preserving important network characteristics. The extracted features were further classified using several Machine Learning (ML) and Deep Learning (DL) algorithms, including Decision Tree, Random Forest, Deep Neural Network (DNN), Convolutional Neural Network (CNN), and CNN-LSTM. Experimental evaluation on the N-BaIoT and MQTTset datasets demonstrated superior accuracy, precision, recall, F1-score, and detection speed compared with traditional anomaly detection techniques such as One-Class Support Vector Machine (OC-SVM) and Isolation Forest (iForest). The rapid expansion of IoT devices has also attracted significant attention from cybercriminals due to the widespread vulnerabilities present in resource-constrained devices. Compromised IoT devices are frequently recruited into botnets that launch large-scale Distributed Denial-of-Service (DDoS) attacks by exhausting computing resources, memory, and network bandwidth **[2]**. Modern botnets such as Bashlite (Gafgyt) and Mirai exploit vulnerable IoT devices through Command-and-Control (C&C) servers to perform malicious activities including vulnerability scanning, malware propagation, spam distribution, and coordinated cyberattacks, posing serious threats to smart environments and critical infrastructures [3,4].

Zavrak, et al. [5] investigated the use of Autoencoder (AE) and Variational Autoencoder (VAE) models for detecting unknown cyberattacks in network traffic using the CICIDS2017 dataset. The study compared both deep learning models with the traditional One-Class Support Vector Machine (OC-SVM) by evaluating Receiver Operating Characteristic (ROC) curves and Area Under the Curve (AUC) metrics. Experimental results demonstrated that the VAE model consistently outperformed both AE and OC-SVM in identifying previously unseen attacks, highlighting the effectiveness of generative deep learning models for anomaly detection. Min, et al. [6] proposed a Memory-Augmented Autoencoder (MemAE) to overcome the over-generalization problem commonly observed in conventional autoencoder-based intrusion detection systems. The architecture incorporated a memory module that enabled the model to reconstruct anomalous samples more accurately while preserving the distinction between normal and malicious traffic. Extensive experiments conducted on the NSL-KDD, UNSW-NB15, and CICIDS2017 datasets showed that MemAE significantly outperformed existing OC-SVM-based approaches. However, the authors noted that the absence of feature selection or dimensionality reduction increased computational complexity due to the large number of network features. Kolhar, et al. [7] developed a deep learning-based stacking ensemble framework to strengthen IoT security in smart city environments. The proposed ensemble combined multiple learning models to identify complex attack patterns across large-scale network traffic datasets. Performance evaluation using the ToN-IoT and InSDN datasets achieved detection accuracies of 99.8% and 99.6%, respectively, demonstrating the robustness and scalability of ensemble learning techniques for securing modern IoT infrastructures. Guo [8] proposed a two-stage anomaly detection

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

framework consisting of dimensionality reduction followed by network traffic classification. The study employed PCA and LDA for feature reduction before applying Naïve Bayes and K-Nearest Neighbors (KNN) classifiers to detect anomalous traffic. Experimental analysis achieved an overall detection accuracy of 84.82%, confirming that dimensionality reduction improves computational efficiency while maintaining satisfactory detection performance.

Kozik, et al. [9] introduced a cloud-based intrusion detection framework that combined Apache Spark distributed computing with the Extreme Learning Machine (ELM) algorithm to efficiently analyse large volumes of NetFlow network traffic. The proposed architecture enabled high-speed processing of network packets while maintaining effective attack detection performance, making it suitable for large-scale cloud and IoT environments. L. Rondon, et al. [10] emphasized that cybersecurity considerations are often overlooked during the design and development of IoT devices, leaving numerous vulnerabilities that attackers can exploit. The study highlighted the importance of incorporating security mechanisms during the early stages of IoT system development to improve resilience against cyber threats. F. Safara, et al. [11] proposed an Artificial Neural Network (ANN)-based intrusion detection system specifically designed for communication networks within IoT environments. The proposed framework effectively distinguished malicious activities from legitimate network traffic, demonstrating the capability of neural networks to improve intrusion detection performance in resource-constrained IoT systems. M. Abdel-Basset, et al. [12] reviewed the application of deep learning techniques for IoT security and privacy protection, highlighting their effectiveness in detecting sophisticated cyberattacks while preserving sensitive information. The study also discussed rule-based intrusion detection systems that utilize predefined security rules to identify known attack patterns with high reliability when deployed in appropriate network environments. Rhachi, et al. [13] proposed an anomaly detection framework that combined Deep Autoencoders (DAE) with Analysis of Variance (ANOVA) F-Test feature selection for IoT network security. The feature selection mechanism reduced redundant network attributes while improving classification efficiency, and the proposed model achieved accuracies of 85% for binary classification and 92% for multi-class classification on the NSL-KDD dataset. The study demonstrated that integrating deep learning with effective feature selection significantly enhances anomaly detection performance while reducing computational overhead in IoT security applications.

## 3. Proposed System

The proposed system architecture provides an intelligent framework for secure IoT device classification by integrating machine learning and deep learning techniques into a unified workflow. Initially, raw IoT network data undergoes preprocessing to eliminate inconsistencies, encode categorical attributes, and normalize numerical features for effective model training. The processed dataset is then divided into training and testing subsets, after which baseline models are trained and evaluated to establish performance benchmarks. Subsequently, the hybrid framework combines RFC, Deep Autoencoder, and LRC to extract discriminative feature representations and perform accurate device classification. The Random Forest generates encoded leaf features that are compressed by the Deep Autoencoder into informative bottleneck representations before being classified using Logistic Regression. Finally, the trained models are utilized in the prediction pipeline

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

to classify unseen IoT devices with high accuracy while supporting secure and scalable deployment, as illustrated in Fig 2.

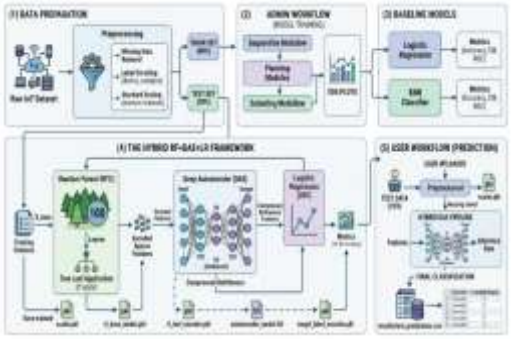


Fig. 2: Proposed system architecture

The processed feature vectors are further analysed using multiple classification techniques to accurately identify device categories. Additionally, an intelligent feature refinement mechanism is incorporated through an autoencoder to learn compact and discriminative representations of high-dimensional data. A graphical user interface facilitates seamless interaction for data handling, model training, performance visualization, and prediction tasks, A lightweight storage mechanism manages trained models and preprocessing components, while the system ensures efficient prediction workflows for new input data. Continuous evaluation and retraining capabilities enhance analytical accuracy and enable adaptability to evolving IoT environments.

**Data Preparation**

The system begins by collecting the raw IoT dataset containing device communication and network traffic information. During preprocessing, missing values are removed, categorical attributes such as device categories are label encoded, and numerical features are standardized using feature scaling techniques. The processed dataset is then divided into training (80%) and testing (20%) subsets to support reliable model development and evaluation.

**Model Training and Exploratory Analysis**

The training data is used to perform exploratory data analysis (EDA) for understanding feature distributions and identifying meaningful relationships among variables. Statistical visualizations assist in examining data characteristics before training. This stage prepares the dataset for both baseline machine learning models and the proposed hybrid classification framework.

**Baseline Model Development**

Conventional machine learning algorithms, including LRC and KNN, are trained using the processed training data. Their performance is evaluated using metrics such as accuracy, confusion matrix, and ROC analysis. These baseline results serve as a reference for comparing the effectiveness of the proposed hybrid model.

**Hybrid RFC–DAE–LRC Framework**

The proposed framework first applies the RFC to generate tree leaf representations, which are transformed into encoded sparse features. These encoded features are passed through the Deep Autoencoder to obtain compact bottleneck representations that preserve important information while reducing redundancy. Finally, Logistic Regression classifies the compressed features, resulting in improved classification accuracy and robust IoT device identification.

**User Prediction Workflow**

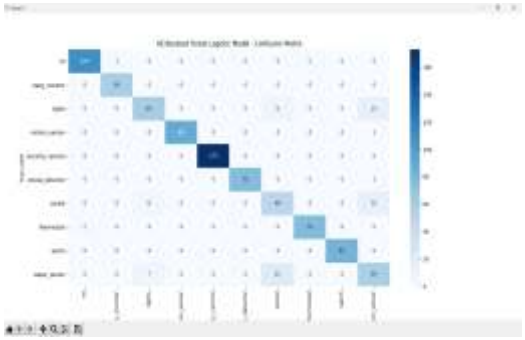
For real-time prediction, users upload new IoT test data that undergoes the same preprocessing and feature transformation procedures used during training. The saved scaler, encoder, Random Forest model, Deep Autoencoder, and Logistic Regression classifier are loaded to process the incoming data. The system then produces the final device classification results and stores the predictions for further analysis and secure IoT network management.

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

## 4. Result Description

The result analysis demonstrates the effectiveness of the proposed analytical framework in accurately classifying IoT device categories using both traditional and hybrid learning techniques. Experimental outcomes indicate that preprocessing and feature engineering significantly enhance data quality, leading to improved model performance. Among the evaluated models, the hybrid approach integrating ensemble learning with deep autoencoder-based feature extraction achieves superior accuracy and generalization capability. Comparative analysis using metrics such as accuracy, precision, recall, and F1-score highlights the robustness of the developed framework. Visualization tools, including confusion matrices and ROC curves, provide deeper insights into classification behavior and error distribution. The results also confirm that the system effectively handles high-dimensional data and diverse device patterns.

Fig 3 presents the Confusion matrix and ROC curve of the DAE-BFL model, which outperformed the baseline models. This hybrid approach integrating Random Forests, an autoencoder for feature compression, and LRC for classification achieved 91.70% accuracy, 90.63% precision, 90.58% recall, and 90.55% F1-score. Its superior performance confirms the effectiveness of combining ensemble learning and deep representation for robust device classification.



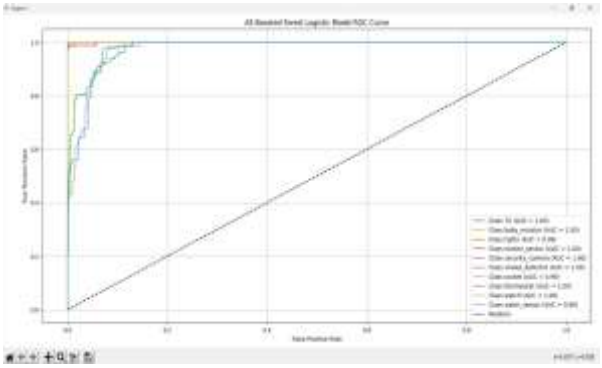


Fig. 3: Confusion matrix and ROC curve obtained using DAE-BFL Model

Fig 4 presents the model prediction output on unseen test data. Once the user uploads new data, the preprocessing pipeline is applied, and predictions are generated using the trained models. The predicted device categories are displayed alongside sample records, ensuring the user receives an immediate and interpretable outcome. This step validates the usability of the system for real-world datasets.


Fig. 4: Model Prediction on Test Data using proposed model

Received: 30-05-2026 | Accepted: 01-07-2026 | Published: 08-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

Table 1: Performance comparison for the all-ml models.

| Algorithms Name | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|
| **LR** | 87.06 | 87.43 | 84.97 | 84.24 |
| **KNN** | 88.16 | 86.96 | 86.53 | 86.66 |
| **DAE-BFL** | 91.70 | 90.63 | 90.58 | 90.55 |

Table 1 presents the performance comparison of three classification algorithms: LRC, KNN, and AE-BFL. LRC achieved an accuracy of 87.06% with balanced precision and recall, establishing a reliable baseline model. The KNN model slightly improved the performance with an accuracy of 88.16% and an F1-score of 86.66%, showing better handling of neighborhood-based feature similarities. The AE-BFL model demonstrated superior performance with 91.70% accuracy, 90.63% precision, 90.58% recall, and 90.55% F1-score. This hybrid approach effectively combined ensemble learning, autoencoder-based feature representation, and LRC, outperforming the traditional models. The table highlights that while LRC and KNN provided competitive results, the AE-BFL model delivered the most accurate and consistent outcomes. This makes it the most robust choice for reliable device category prediction in the system.

## 5. Conclusion

The research successfully demonstrated an intelligent IoT device classification and authentication system using machine learning and deep learning techniques. By integrating LRC, KNN, and the AE-BFL hybrid model, the system achieved high accuracy, precision, recall, and F1-scores, with the hybrid model outperforming others at 91.70% accuracy. The research automated device identification, feature extraction, and classification while ensuring secure authentication, overcoming the challenges of manual monitoring in large-scale IoT environments. Data preprocessing, exploratory data analysis, and train-test splitting improved model reliability, and visualizations provided clear insights into performance. The system demonstrated scalable, robust, and automated device management, significantly enhancing IoT network security and operational efficiency.

## References

[1] Alaghbari, K.A.; Lim, H.-S.; Saad, M.H.M.; Yong, Y.S. Deep Autoencoder-Based Integrated Model for Anomaly Detection and Efficient Feature Extraction in IoT Networks. *IoT* **2023**, *4*, 345-365. https://doi.org/10.3390/iot4030016

[2] Cruz, A.R.S.A.; Gomes, R.L.; Fernandez, M.P. An Intelligent Mechanism to Detect Cyberattacks of Mirai Botnet in IoT Networks. In Proceedings of the 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS), Pafos, Cyprus, 14–16 July 2021; pp. 236–243.

[3] Marzano, A.; Alexander, D.; Fonseca, O.; Fazzion, E.; Hoepers, C.; Jessen, K.S.; Chaves, M.H.; Cunha, I.; Guedes, D.; Meira, W. The evolution of Bashlite and Mirai IoT botnets. In Proceedings of the 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 25–28 June 2018; pp. 00813–00818.

[4] Alaghbari, K.A.; Saad, M.H.; Hussain, A.; Alam, M.R. Complex event

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

processing for physical and cyber security in datacenters—Recent progress, challenges and recommendations. J. Cloud Comp. 2022, 11, 65.

[5] Zavrak, S.; İskefiyeli, M. Anomaly-Based Intrusion Detection from Network Flow Features Using Variational Autoencoder. IEEE Access 2020, 8, 108346–108358.

[6] Min, B.; Yoo, J.; Kim, S.; Shin, D.; Shin, D. Network Anomaly Detection Using Memory-Augmented Deep Autoencoder. IEEE Access 2021, 9, 104695–104706.

[7] Kolhar, M.; Aldossary, S.M. A Deep Learning Approach for Securing IoT Infrastructure with Emphasis on Smart Vertical Networks. *Designs* **2023**, *7*, 139. https://doi.org/10.3390/designs7060139

[8] Guo, Y.; Wang, Y.; Khan, F.; Al-Atawi, A.A.; Abdulwahid, A.A.; Lee, Y.; Marapelli, B. Traffic Management in IoT Backbone Networks Using GNN and MAB with SDN Orchestration. Sensors 2023, 23, 7091. [Google Scholar] [CrossRef]

[9] Sivaramakrishnan, R.; SenthilKumar, G. Workload Characterization in Embedded Systems Utilizing Hybrid Intelligent Gated Recurrent Unit and Extreme Learning Machines. Int. J. Intell. Syst. Appl. Eng. 2024, 12, 233–243.

[10] Rondon, L.P.; Babun, L.; Aris, A.; Akkaya, K.; Uluagac, A.S. Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective. *Ad Hoc Netw.* **2022**, *125*, 102728.

[11] Safara, F.; Souri, A.; Serrizadeh, M. Improved intrusion detection method for communication networks using association rule mining and artificial neural networks. IET Commun. 2020, 14, 1192–1197.

[12] Abdel-Basset, M.; Moustafa, N.; Hawash, H.; Ding, W. Deep Learning Techniques for IoT Security and Privacy; Springer: New York, NY, USA, 2022; Volume 997.

[13] Rhachi, H.; Balboul, Y.; Bouayad, A. Enhanced Anomaly Detection in IoT Networks Using Deep Autoencoders with Feature Sele