Federated Learning for Detecting Anomalies in IoT-Driven Smart Home Systems

Jeevathuvarakan Thevarajan
Department of Physical Science
University of Vavuniya
Vavuniya, Sri Lanka
tjeevathuvarakan@gmail.com

Vaishali Ravi
Department of Computing
Universiti Teknologi PETRONAS
Seri Iskandar, Malaysia
vaishali_24007113@utp.edu.my

Sivaramalingam Kirushanth
Department of Physical Science
University of Vavuniya
Vavuniya, Sri Lanka
sivaramalingamk@vau.ac.lk

Vijayakanthan Ganesalingam
Department of Physical Science
University of Vavuniya
Vavuniya, Sri Lanka
g.vijayakanthan@vau.ac.lk

Mohd Anuaruddin Ahmadon
Department of Computing
Universiti Teknologi PETRONAS
Seri Iskandar, Malaysia
anuaruddin.ahmadon@utp.edu.my

Nur Syadhila Bt Che Lah
Department of Computing
Universiti Teknologi PETRONAS
Seri Iskandar, Malaysia
nursyadhila.chelah@utp.edu.my

2025 7th International Conference on Advancements in Computing (ICAC) | 979-8-3315-6222-9/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICAC69156.2025.11361509

***Abstract*—The rapid proliferation of Internet of Things (IoT) devices in smart home environments has amplified significant cybersecurity challenges due to their outdated firmware, limited computational resources, and weak protection mechanisms. Traditional centralized anomaly detection approaches are ineffective in these environments owing to single points of failure, privacy risks, and limited scalability. To address these challenges, this study proposes a novel federated learning framework that integrates a lightweight hybrid architecture combining 1D Convolutional Neural Networks (1D-CNN) with shallow autoencoders to support both supervised and unsupervised anomaly detection. The supervised component enables robust binary classification of known attack patterns, while the unsupervised reconstruction mechanism enhances detection of previously unseen anomalies, thus balancing accuracy with adaptability. Distinct from prior approaches, the proposed framework employs dynamic quantization within the federated learning process, enabling substantial reductions in resource consumption without compromising detection performance. Experiments conducted on the TON-IoT dataset, with SMOTE-based class balancing and PCA-driven dimensionality reduction, under a realistic non-IID distribution across three federated clients, demonstrate that the proposed model achieves 97.39% test accuracy. This model is designed for deployment on resource-constrained devices, employing post-training dynamic range quantization that reduces the model size by 81.5% (42.60 KB to 7.87 KB) without compromising accuracy. The experiment performed using Raspberry Pi 4 confirmed sub-millisecond inference and real-time responsiveness, validating the practical viability of the framework for efficient anomaly detection in smart IoT systems.**

***Index Terms*—1D-CNN, Anomaly Detection, Autoencoder, Federated Learning, IoT Security**

I. Introduction

Internet of Things (IoT) devices have been seamlessly integrated into almost every aspect of human life, ranging from wearable and smart home systems to industrial sensors and healthcare monitors, allowing real-time data collection, decision-making, and automation [1]. These devices have revolutionized industries by improving efficiency, reducing costs, and enhancing user experiences. Despite their shrinking physical size that enables widespread deployment, IoT devices generate and process vast amounts of sensitive data, including personal, financial, and operational information. It is estimated that by the end of 2025, the number of IoT devices will have reached approximately 64 billion [2], driving innovations in smart cities, healthcare, and transportation. However, this critical role in modern ecosystems indicates the urgent need to address associated security and privacy challenges [3], [4]. These vulnerabilities are not limited to the potential for hacking and data breaches but extend to more intrusive risks, such as unauthorized surveillance and access to personal information [5]. Traditionally, centralized machine learning models have been employed to detect anomalies in IoT networks, where it is analyzed to identify unusual patterns or behaviors indicative of security threats or system failures. While these strategies are effective to a certain degree, centralized methods come with significant drawbacks and limitations [6], [7]. Specifically, they introduce single-point failure, high communication overhead, and scalability bottlenecks. In addition to that, they raise privacy concerns due to raw data aggregation at central servers. These inherent limitations make evident the need for decentralized approaches. Federated learning (FL) aligns naturally with the distributed architecture of IoT, facilitating local processing and global anomaly detection. Building on this foundation, our work advances secure, efficient, and privacy-preserving FL for smart home IoT environments [8].

This study tackles IoT security amid rising cyber threats and privacy issues. While centralized detection faces scalability and privacy limits, the supervised models rely on labels and struggle with zero-day attacks in constrained environments [9]. To overcome these limitations, we propose a federated learning approach that integrates a hybrid architecture that combines a one-dimensional Convolutional Neural Network (1D-CNN) and a shallow autoencoder(AE) to preserve privacy and detect novel attacks without central data aggregation, providing a