Chapter 3
A Distributed Model for IoT Anomaly Detection Using Federated Learning

Sidra Tahir
UIIT, Pakistan

Anam Zaheer
UIIT, Pakistan

ABSTRACT

Anomaly detection in IoT-based sleep patterns is crucial for early identification of health issues. This chapter presents a distributed model using federated learning for privacy and data security. The proposed approach involves data collection, preprocessing, model initialization, federated learning server, model distribution, and anomaly detection. Sleep pattern data is preprocessed to extract features, initializing the global anomaly detection model. A federated learning server enables collaborative learning with devices, distributing the updated global model iteratively for synchronized anomaly detection. Precision and accuracy metrics yielded 0.67% precision and 0.84% accuracy, showcasing the effectiveness of the distributed model. Leveraging federated learning ensures privacy, data security, and synchronized anomaly detection across devices, supporting early detection of sleep-related anomalies and health interventions.

INTRODUCTION

The technique of discovering and recognizing unusual behavior or occurrences inside an IoT system or network is known as IoT (Internet of Things) anomaly detection. IoT anomaly detection is essential for guaranteeing the safety, dependability, and effective functioning of IoT systems in light of the proliferation of connected devices and sensors. In the IoT, anomaly detection approaches look for departures from anticipated patterns, behaviors, or thresholds. Both malicious and non-malicious incidents, such as equipment breakdowns or sensor failures, can be classified as anomalies. Malicious actions include cyberattacks and unauthorized access attempts. Organizations can proactively address possible risks,

DOI: 10.4018/978-1-6684-7625-3.ch003

save downtime, enhance system efficiency, and guarantee the accuracy of data generated by IoT devices by spotting abnormalities (Al-Amri et al., 2021).

In the context of the Internet of Things, centralized anomaly detection refers to a method in which anomaly detection duties are carried out at a central location or server, generally in the cloud, utilizing information gathered from several IoT devices or sensors. While this strategy has several benefits, there are also a number of drawbacks: Data privacy and security, Network Bandwidth and Latency, Scalability, Dependence on Network Connectivity and regulatory compliances. Distributed anomaly detection distributes the detection process across multiple edge devices or gateways, allowing for localized analysis and faster response times while minimizing data transmission to the central server (Alrashdi et al., 2019).

The detection of anomalies in sleep patterns is of significant importance for early identification of sleep disorders and potential health issues. In this study, we propose a solution for anomaly detection in sleep patterns using federated learning in IoT environments. A distributed method to machine learning known as federated learning allows for the training of models across a number of decentralized devices or edge nodes without the need for centralized data collection. It enables businesses to take use of machine learning's capabilities while safeguarding data privacy, cutting communication costs, and overcoming issues with data centralization. Data is often gathered from numerous sources and centralized on a central server or cloud platform for model training in traditional machine learning techniques. Privacy issues are raised by this centralized data collecting, though, as it's possible for sensitive or private information to be revealed during data transit or storage. This problem is solved by federated learning, which allows model training on data spread across several devices without transferring the raw data.

For the following reasons, federated learning is extremely important for IoT anomaly detection: data privacy, decentralized data, reduced communication costs, Real time anomaly detection, edge intelligence Scalability and adaptability and Collaborative Learning (Al-mashhadi, Anbar, Hasbullah, & Alamiedy, 2021; Hussain, Irfan, Jhanjhi, Hussain, & Humayun, 2021; Tahir, Hafeez, Abbas, Nawaz, & Hamid, 2022).

The proposed solution involves collecting sleep pattern data from IoT devices, wearables, and smart mattresses, and preprocessing the data by normalizing network flow and extracting relevant features. The global anomaly detection model is initialized using the preprocessed data to establish a starting point for learning and adaptation. The federated learning server facilitates collaborative learning by communicating with participating devices, allowing them to perform local updates and fine-tuning based on their unique sleep pattern data. Model updates are aggregated using gradient descent optimization and cluster model aggregation methods to derive a comprehensive global model. The updated model is distributed iteratively to participating devices, enabling consistent and synchronized anomaly detection while preserving data privacy. Anomalies in sleep patterns are identified by comparing local data with the learned patterns within the global model, leading to the early detection of sleep-related anomalies and potential underlying health issues(Humayun, Jhanjhi, & Almotilag, 2022; Humayun, Niazi, Jhanjhi, Alshayeb, & Mahmood, 2020).

To evaluate the performance of the proposed solution, a labeled dataset of sleep sessions is used, with precision and accuracy metrics employed to assess the anomaly detection system. The results demonstrate promising precision and accuracy rates, indicating the effectiveness of the distributed model for anomaly detection in sleep patterns. The study provides valuable insights into leveraging federated learning in IoT environments for early detection of sleep disorders and paves the way for future research to enhance the accuracy and efficiency of anomaly detection and explore applications in other domains beyond sleep pattern analysis.