Title: Variational Autoencoders for Anomaly Detection in IoT Data

1. ABSTRACT

The Internet of Things (IoT) includes smart devices that collect and send data. Sometimes, these devices may send strange or incorrect data due to problems like faults or attacks. To keep the system working well, we need to find these unusual patterns (called **anomalies**) quickly.
In this project, we use a type of deep learning model called a **Variational Autoencoder (VAE)** to find such anomalies. We train the model using only the normal (correct) data. After learning, if the model has trouble recreating (reconstructing) a data point, it means the data might be abnormal.This method helps us **detect problems automatically**, even if we don't have examples of abnormal data. It's a smart and useful way to keep IoT systems safe and working properly.

2. Problem Statement

IoT devices, such as sensors, collect large amounts of data every day. Sometimes, things can go wrong like sensor malfunctions, sudden attacks, or unusual behavior. Finding these unusual activities (called **anomalies**) is important to keep the system working safely and correctly. In real life, we often **don't know what abnormal data looks like**, and manually labeling all data is difficult. Therefore, we need an intelligent method that can **learn what normal data looks like** and automatically detect anything different. This project solves the problem by using a **Variational Autoencoder (VAE)** — a deep learning model that learns from normal data and tells us if new incoming data is abnormal, based on its reconstruction accuracy.