



IoT Network Traffic Analysis for User Behavior Mapping and Adaptive Privacy Risk Mitigation

T.D. Dissanayake¹, S.A.D.S. Fernando¹, J. Duwarahavidyan¹, W.M.T.H. Bandara¹, K.L.K. Sudheera^{1}*

¹ Department of Electrical and Information Engineering, Faculty of Engineering,
University of Ruhuna, Sri Lanka

**Corresponding author: kushan@eie.ruh.ac.lk*

The recent rise of Internet of Things (IoT) devices has raised significant concerns about user privacy, as these devices may unknowingly expose sensitive information to third parties. Since smart devices continuously communicate over a network, they generate unique traffic patterns that can be passively captured by an attacker without the user's knowledge. Although this traffic is encrypted, it can still reveal device identities and user behaviors within the environment. This study investigates how network traffic can be analyzed to identify specific IoT devices and how detected device triggers can be mapped to meaningful user actions under realistic deployment conditions. Accordingly, we propose a novel four-stage methodology to address this challenge. First, we introduce a Retrieval-Augmented Generation (RAG) based device fingerprinting approach that supports open-set recognition and enables identification of previously unseen devices. Second, we implement a hybrid device trigger detection method that combines a rule-based system with a Long Short-Term Memory (LSTM) approach to improve reliability under practical constraints. Third, sequences of detected triggers are mapped to user behaviors using a prompt-engineered Large Language Model (LLM) framework capable of inferring complex activities without reliance on fixed training datasets. Furthermore, we evaluate and propose privacy-preserving mitigation techniques that conceal genuine user behavior within realistic fake behaviors through adaptive traffic obfuscation, increasing attacker uncertainty rather than attempting to fully block inference. To support experimentation and evaluation, two practical testbeds are deployed for data collection and validation, and a user-friendly web application integrates the full pipeline into an accessible interface. Overall, this work provides practical insights into privacy risks in smart environments and demonstrates effective, deployable strategies for mitigating behavior inference from encrypted IoT traffic.

Keywords: Behavior inference, Device fingerprinting, Encrypted traffic analysis, IoT privacy, Passive sniffing