Geometry-Aware Local Differential Privacy with Temporal Unlinkability for Human Activity Recognition

Yujin Cha
chayuj0@snu.ac.kr
Seoul National University
Seoul, Republic of Korea

1 MOTIVATION

Human Activity Recognition (HAR) using smartphone and wearable IMU (Inertial Measurement Unit) data is foundational to many modern applications, from fitness tracking to personalized health monitoring. These services rely on collecting and processing large volumes of movement data from users, which often entails uploading windowed sensor features to a cloud server for model training or analytics.

However, this data collection pipeline presents two core privacy risks. First, individual sensor windows can reveal fine-grained details about users' movements, behaviors, and environments. The less addressed, and equally critical, second issue is that the sequence and timing of activity windows can allow a server to reconstruct daily routines, exposing sensitive behaviors such as commute schedules or personal habits.

The current wearable devices implement privacy measures such as encryption, anonymization, and server-side differential privacy. However, all these methods assume the server itself is trustworthy. There lies the core problem: a compromised or curious log server has both the means and the incentive to exploit sequential uploads and reconstruct a user's entire daily routine. Given the highly personal nature of movement data, this is a profound privacy failure.

2 RESEARCH PROBLEM

We begin by defining sensitive information categories within current wearable IMU-based HAR pipelines. The following categories correspond to different temporal scopes:

(1) **window-level privacy.** Each individual IMU window is processed into feature vectors (e.g., mean, variance, frequency components), and then transmitted to the server for training. These fine-grained feature vectors may reveal aspects of user behavior or context. Therefore, any server receiving the data must not be able to recover the precise movements from a single transmitted window.
(2) **routine-level privacy.** The sequence of individual windows and their data form continuous activity traces. If these traces are linkable across sessions, the server can infer sensitive routines of the user. The acquired routines can expose daily commutes, frequently-visited locations, exercise habits, or unique patterns to the person. This exposure enables user re-identification via behavior profiling, which is significant concern if the compromised server already possesses vast auxiliary data about the user's life.

Therefore, the privacy layers for both levels are necessary to achieve meaningful user protection. The current safeguard methods are insufficient because they do not protect all layers. Our goal is to design a unified, client-side privacy pipeline that successfully addresses both window-level and routine-level privacy requirements. The resulting data stream is directly consumable by existing, un-modified HAR models, while minimizing utility loss.

3 EXISTING SOLUTIONS AND THEIR LIMITATIONS

A variety of privacy-preserving strategies have been proposed for collecting and analyzing sensor data in HAR systems. Early efforts focus on **Anonymization** and de-identification on user data. However, research has shown that behavioral or sensor traces are often unique enough that it is possible to link or re-identify the data provider after standard anonymization techniques [3].

Server-side Differential Privacy (DP) has been widely adopted, adding noise to aggregated statistics or model updates [1]. While this protects group statistics, it requires trusting the server to implement DP correctly and does not address privacy risks from the server itself.

Recent development has shown that **Federated Learning**, which trains the model on device and share only model updates with the server, has a lot of promise for HAR. However, the practicality is limited by challenges such as significant on-device computation and communication costs [2]. Furthermore, privacy vulnerabilities from linkable updates or metadata still remain.

One research, possibly closest to our work, applies **Local Differential Privacy** on-device to sensor data such as heart rate streams. It noises prominent points on the stream, letting the server to reconstruct the signals from the perturbed data [4]. However, this method focuses on value privacy for single-attribute streams (like heart rate) and does not address multi-dimensional IMU features or the routine-level unlinkability needed for HAR classification.

To our knowledge, no existing approach covers both per-window and routine-level privacy while remaining efficient on small-resource mobile devices.

4 THE APPROACH

We combine two lightweight and complementary privacy mechanisms to address both window-level and routine-level privacy requirements.

Threat model. We assume a compromised server that observes perturbed feature windows, coarse timestamps, and metadata such as arrival order or counts.

1. Geometry-Aware LDP. This mechanism will ensure individual feature vectors reveal minimal information about the user's precise activity, even if the server is compromised. First, we extract standard multi-dimensional feature windows from IMU streams, such

as mean, variance, or frequency components. Unlike the previous work with LDP, we will not use naive ℓ_∞ clipping. Rather, we first implement geometry-aware clipping per feature to bound sensitivity, then apply Laplace LDP per feature, according to those bounds. In this work, we will evaluate the following three geometry-aware clipping techniques: (i) per-feature quantile box, (ii) ℓ_2 clipping on grouped features, and (iii) a fast approximate minimum enclosing ball, comparing the resultant utility loss and accuracy.

2. Routine Unlinkability via Shifting Uploads Time. The second mechanism is implemented after individual feature vector perturbation, and it removes the server's ability to track routines. On the device, consecutive feature windows are grouped into activity *bouts* with change-point detection. For each bout, we locally shuffle the window order randomly, and device pseudonyms are rotated as well. The absolute timestamps are then replaced by a perturbed, coarse-grained bout start time. Only this calculated start time and the relative intra-bout duration are reported to the server.

Contributions.

(i) A geometry-aware LDP mechanism tailored to multidimensional IMU features.
(ii) A temporal unlinkability layer that preserves per-window model compatibility.
(iii) An evaluation that couples standard utility metrics with adversarial linkage (AUC / Top-1) under realistic attacks.

5 EXPECTED TECHNICAL CHALLENGES AND POSSIBLE SOLUTION

Utility-Privacy Tradeoff. Applying LDP inevitably introduces noise that may degrade HAR model accuracy, particularly for subtle activities or minority classes, as observed in prior LDP work [4]. However, we expect the accuracy to increase with the geometry-aware clipping methods, as they are adaptive to per-feature sensitivity. By exploring various geometry shapes, we will identify the optimal model configuration.

Reliable and Lightweight Bout Detection. For the Routine Unlinkability mechanism, finding a segmentation approach that is computationally efficient yet reliable against the noisy, LDP-perturbed data is a challenge. We plan to implement both lightweight bout detection using smoothed majority voting and simple change-point detection, then evaluate how each approach's segmentation errors affect unlinkability and utility.

Defense Against Temporal Linkability. Even with the Routine Unlinkability mechanism, a server could still be able to re-link sessions using time bins, activity n-grams, or statistical fingerprints. We will empirically test privacy by simulating such linkage attacks and measuring adversarial AUC. We will also perform ablation studies to identify the most effective parameter settings that balance privacy and utility.

Resource Constraints. All processing must be practical for battery-powered, resource-constrained devices. Thus, we will profile runtime and battery usage to ensure feasibility.

6 EVALUATION STRATEGY

We will empirically evaluate our approach using the UCI HAR dataset as the primary benchmark, with subject-wise splits (train, validation, test) to assess model generalization. We will use two representative models: Logistic Regression (lightweight baseline) and a small 1D-CNN (lightweight deep model, $\leq$ 100k parameters). Our evaluation will proceed across four privacy settings: (0) No Privacy (Baseline), (1) Geometry-Aware LDP only, (2) Routine Unlinkability only, and (3) Our Full Pipeline (LDP + Unlinkability).

6.1 Utility Metrics

Classification performance will be measured by overall accuracy, macro-F1 score, and per-class confusion matrices. We will systematically sweep the privacy budget parameter $\varepsilon \in \{0.2, 0.5, 1, 2, 4, 8\}$ and report the resulting privacy-utility trade-off curves.

6.2 Privacy Metrics

We will quantify temporal unlinkability by simulating an adversarial server attempting to re-link activity sessions based on available metadata: time bins, activity n-grams, and simple statistical patterns. We will report Area Under the ROC Curve (AUC) and the Top-1 linkage accuracy for the adversary. A lower AUC will confirm the effectiveness of our unlinkability layer.

6.3 Ablation and Parameter Selection

We will conduct ablation studies on our two core mechanisms and key parameters such as LDP clipping bounds and time bin sizes to identify the most effective configuration.

6.4 Overhead Analysis

We will profile the computational cost of the on-device processing. To maximize the project focus, we will analyze the per-window runtime and CPU utilization using a desktop proxy with software-throttled emulation.

REFERENCES

[1] Martín Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. 2016. Deep Learning with Differential Privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. 308–318. https://doi.org/10.1145/2976749.2978318
[2] Ons Aouedi, Antonio Sacco, Latif U. Khan, Duc C. Nguyen, and Mohsen Guizani. 2024. Federated Learning for Human Activity Recognition: Overview, Advances, and Challenges. *IEEE Open Journal of the Communications Society* 5 (2024), 7341–7367. https://doi.org/10.1109/OJCOMS.2024.3484228
[3] Yves-Alexandre de Montjoye, César Hidalgo, Michel Verleysen, and Vincent D. Blondel. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Sci. Rep.* 3 (2013), 1376. Issue 1. https://doi.org/10.1038/srep01376
[4] Zhangbing Li, Baichuan Wang, Jinsheng Li, Yi Hua, and Shaobo Zhang. 2022. Local differential privacy protection for wearable device data. *PLOS ONE* 17 (2022), e0272766. Issue 8. https://doi.org/10.1371/journal.pone.0272766