Privacy Leakage Study and Protection for Virtual Reality Devices

RUTGERS
WINLAB | Wireless Information Network Laboratory

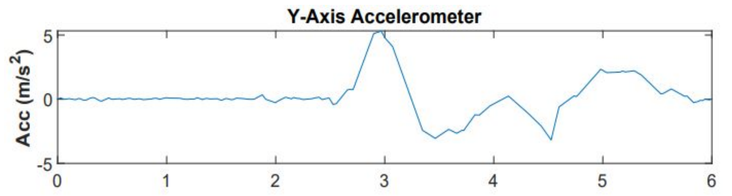
Team: Dirk Catpo Risco (MS), Brody Vallier (UG), Emily Yao (HS)
Project Advisor: Prof. Yingying (Jennifer) Chen
PhD Students as Mentors: Changming Li, Honglu Li, Tianfang Zhang

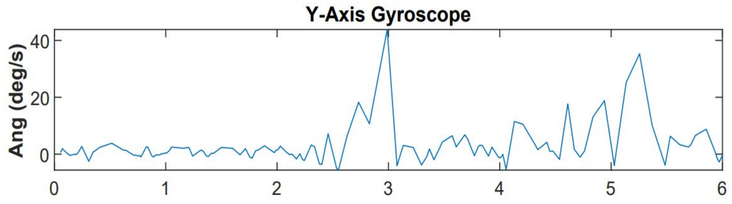
Motivation and Objectives

- Augmented Reality/Virtual Reality (AR/VR) technologies have been rapidly gaining popularity in recent years
- Motion sensor data encodes various types of the user's private information, such as activity information and preferences
- This project studies sensor data management in commercial AR/VR headsets and analyze the potential of private information leakage

Background

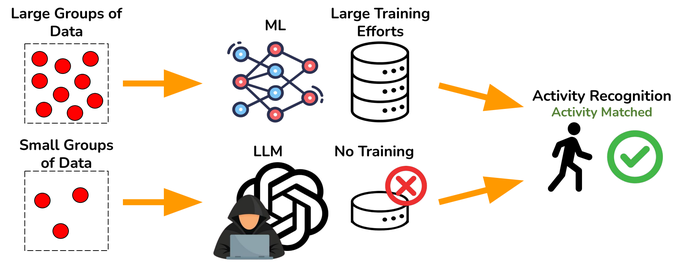
- User movements can be captured via built-in motion sensors (i.e., accelerometer and gyroscope) embedded in AR/VR headset and controllers
- Motion sensor recordings capture human motions in terms of linear acceleration and angles in a three-dimensional space





Decoding Privacy with AI

- Machine learning methods, such as Support Vector Machine (SVM), can learn to classify human activities by constructing support vectors to differentiate features of different classes
- Large Language Models (LLMs) have strong generalization capability in reasoning and inferring private activity information from motion sensor readings, without training efforts from the attacker

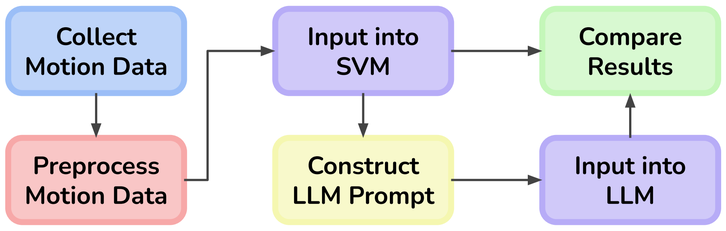


Methodology

- Utilizing SVM upon statistical features (e.g., mean, max, min, etc.) from motion sensor data to classify human activities
- Designing LLM prompts based on identified effective statistical features
  - Explaining the goal of the task and data types to be received
  - Expert knowledge about how to utilize the effective statistical features

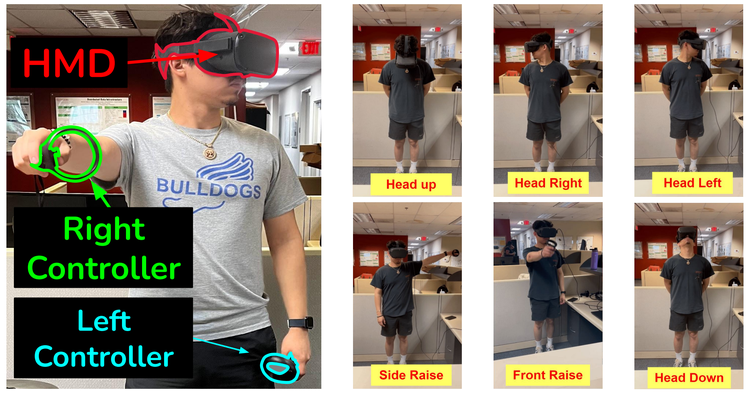
    1. **HMD Accelerometer**: Measures linear acceleration.
    Data: Time (s); x, y, and z-axis coordinates (m/s²).
    Interpretation: Acceleration values between -0.5 m/s² and 0.5 m/s² indicate the head is stable. Values below -0.5 m/s² and above 0.5 m/s² indicate head linear movement.
    2. **HMD Gyroscope**: Measures angular velocity.
    Data: Time (s); x, y, and z-axis coordinates (deg/s).
    Interpretation: Gyroscope values between -8 deg/s and 8 deg/s indicate the head is stable. Values below -8 deg/s and above 8 deg/s indicate head rotational movement.

  - Providing a response structure for results



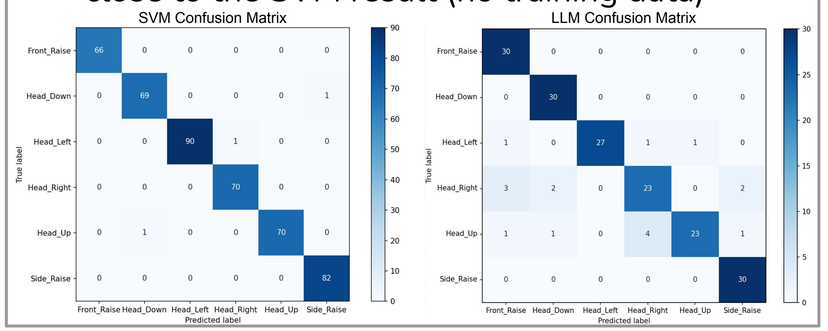
Experiment Setup

- Used Android Studio to develop an application to extract head-mounted display (HMD) and controller IMU data from Meta Quest
- Designed six motions (two head motions and four hand motions) for data collection
- Preprocessed and denoised data in MATLAB to create accurate waveforms and 3D graphs



Experiment Results

- Comparing accuracies between SVM and LLM
  - SVM test accuracy achieves 99.33%
  - LLM achieves an accuracy of 90.6% which is close to the SVM result (no training data)



Conclusion and Future Work

- We can achieve high activity inference accuracies with AI techniques (SVM and LLM)
- Our LLM test accuracy results could be improved with further fine-tuning the expert knowledge and the prompts for activity inference

References

[1] Xu, H., Han, L., Yang, Q., Li, M. and Srivastava, M., 2024, February. Penetrative AI: Making LLMs Comprehend the Physical World. In Proceedings of the 25th International Workshop on Mobile Computing Systems and Applications (pp. 1-7)
[2] Brownlee, J., 2018. 1D Convolutional Neural Network Models for Human Activity Recognition. Mach. Learn. Mastery, 26, p.2021.

Acknowledgement

We would like to thank our project advisor and mentors for their support and guidance throughout this project.

Scan for Project Website

WINLAB