

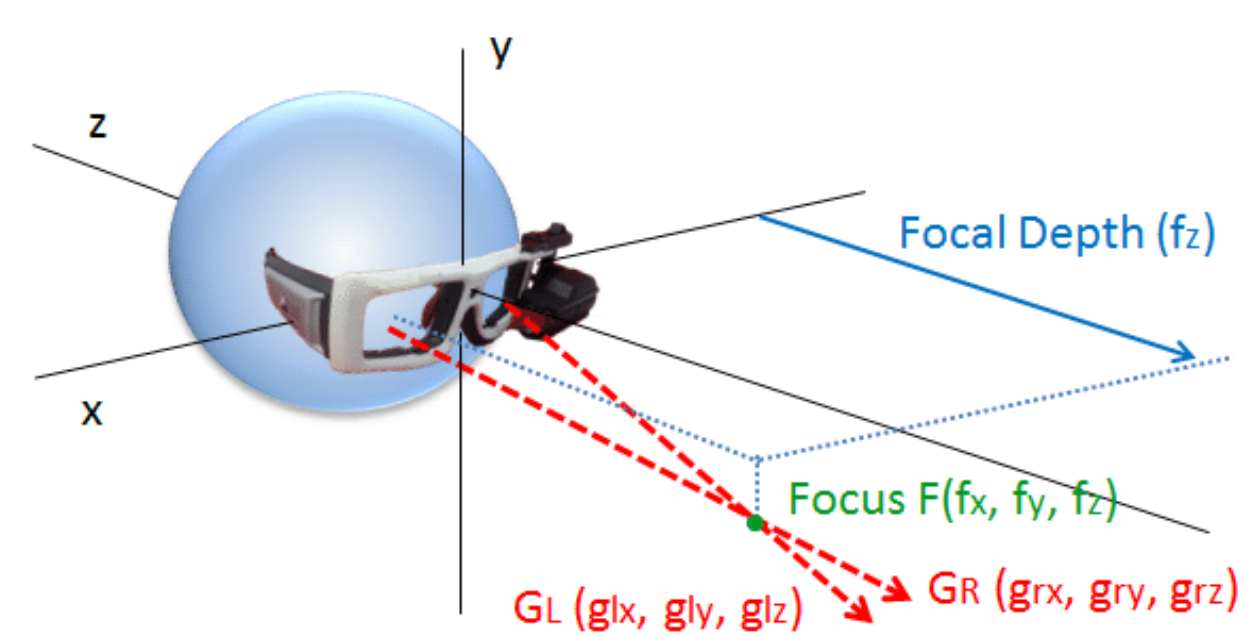
PeekXR: Understanding Privacy Leakages from Eye Gaze in Extended Reality

Chuyang Peng, Mutahar Ali, Habiba Farrukh

Background

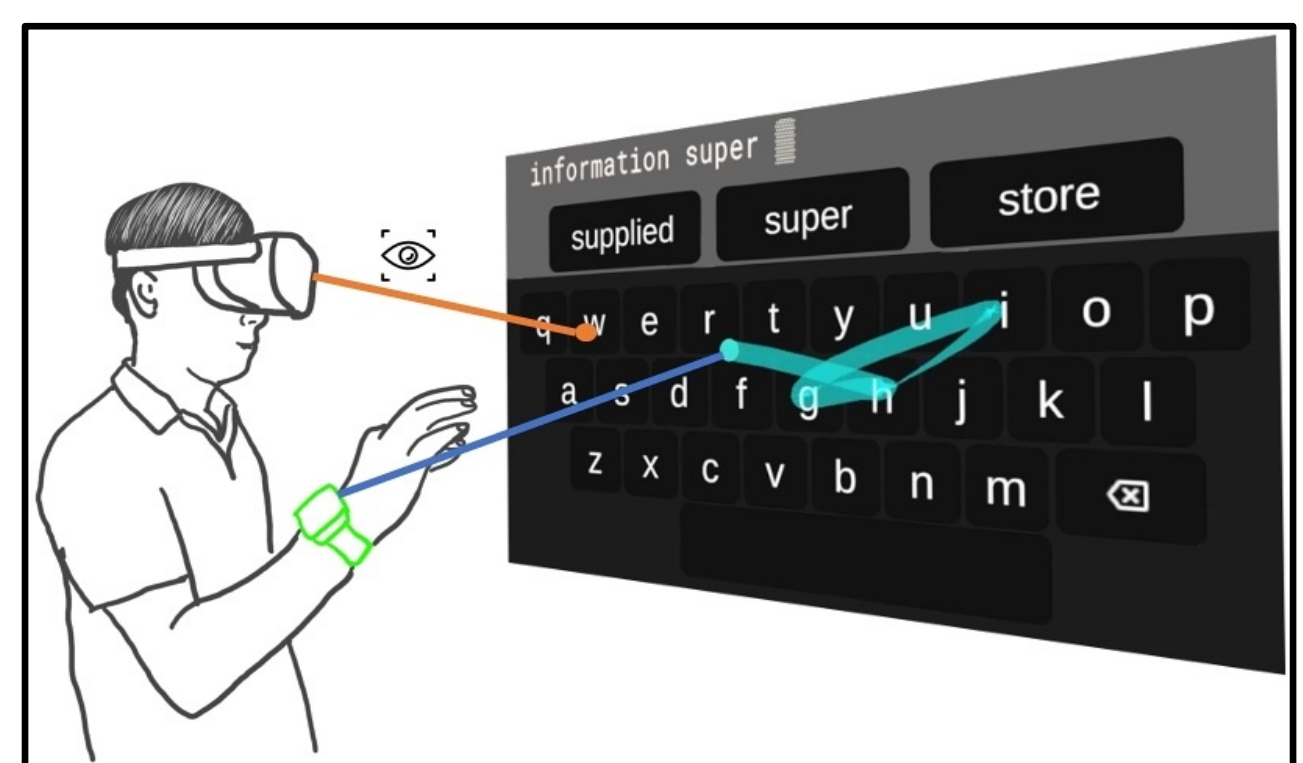
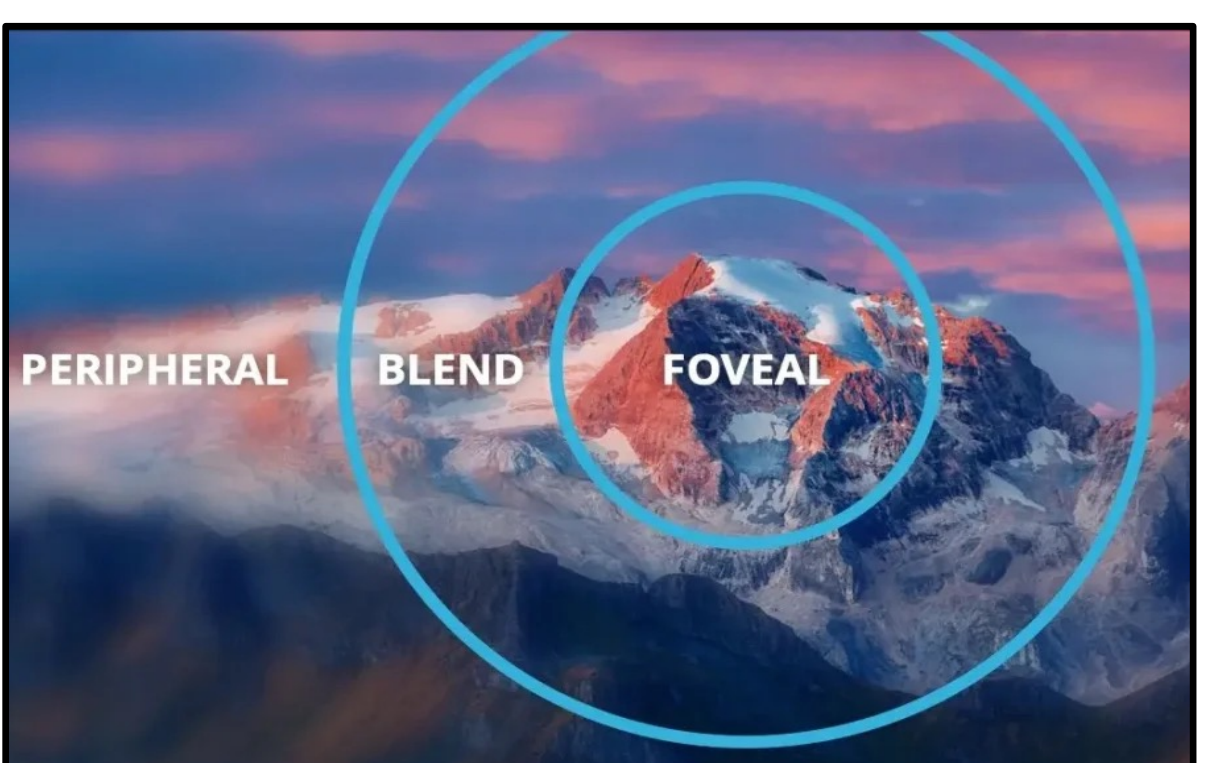
Eye tracking

- Tracking where and how the eyes move to understand focus and attention.
- IR sensors and cameras in headsets are used to record gaze direction, fixation, and pupil movement.



Use cases for eye tracking

- Foveated rendering
- Gaze-based UI
- Enhanced avatar realism



Problem

Gaze data is sensitive

- Gaze is often subconscious, and the data it generates forms a continuous stream that can reveal how users think, feel, and behave.

Prior research

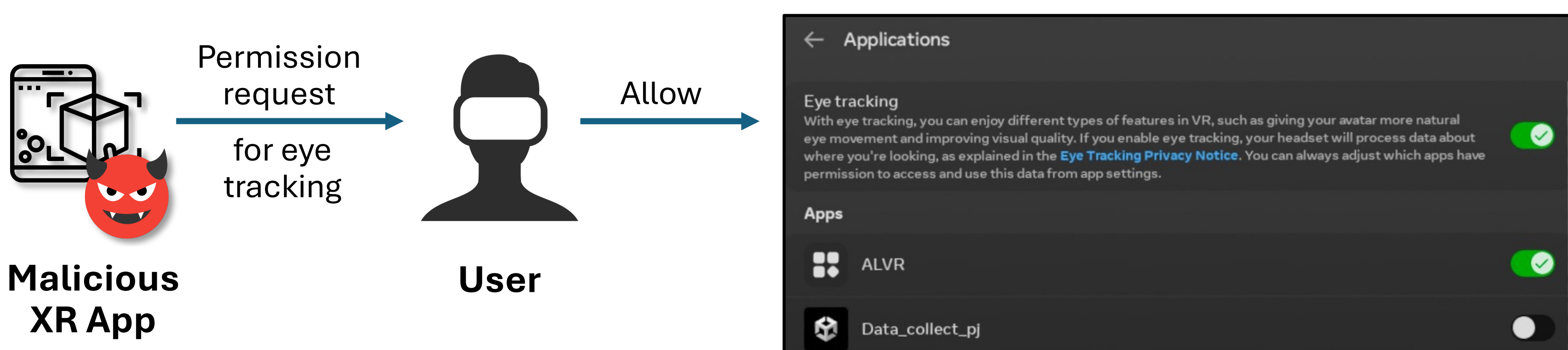
- Prior research has shown that gaze data can leak sensitive information, such as a victim's keystrokes on their touchscreen device, emotional states, and medical conditions.

High frequency, high fidelity, high risk

- Modern XR headsets capture highly granular eye tracking data (including gaze direction, fixation points, pupil dilation) at a high frequency (e.g., up to 90 Hz for Quest Pro).

Can eye gaze data be used to infer a user's activities in an immersive environment, when the content itself is hidden from an adversary?

Threat Model



Access

- The adversary only has access to eye tracking data.
- The adversary cannot access video, audio, user inputs, or screen buffers.

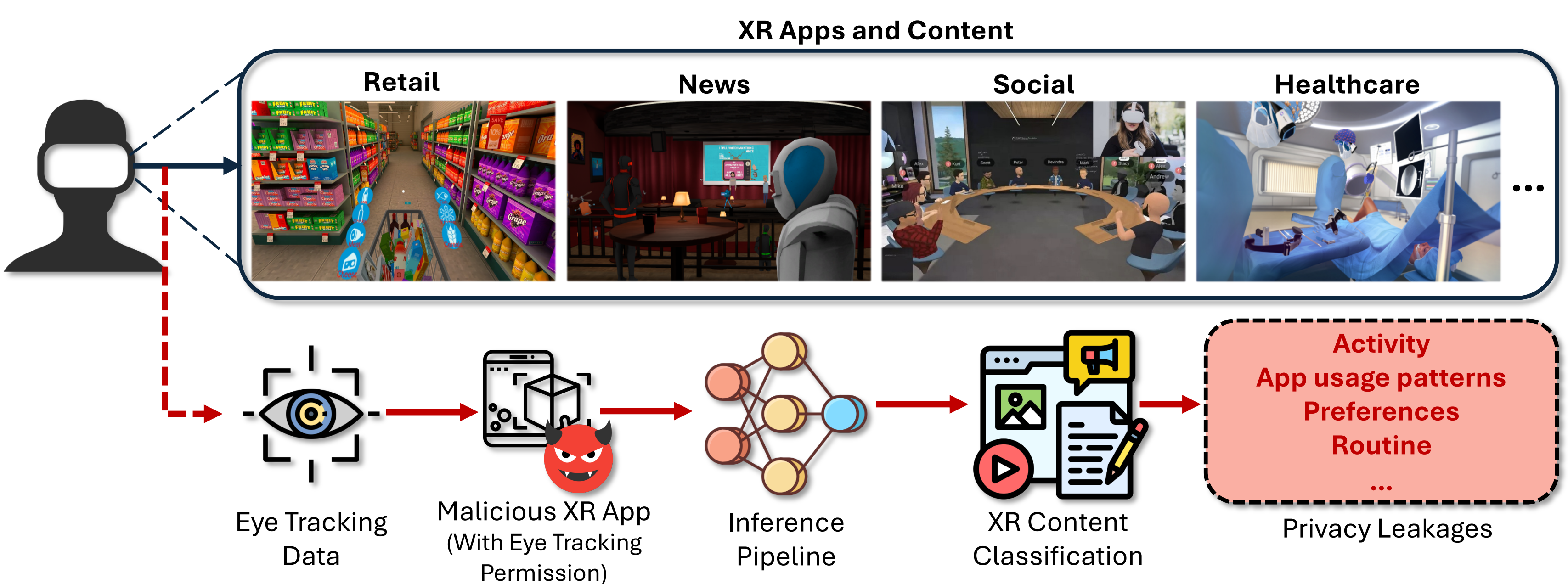
Goal

- To infer what content the user is viewing or which application they're using.

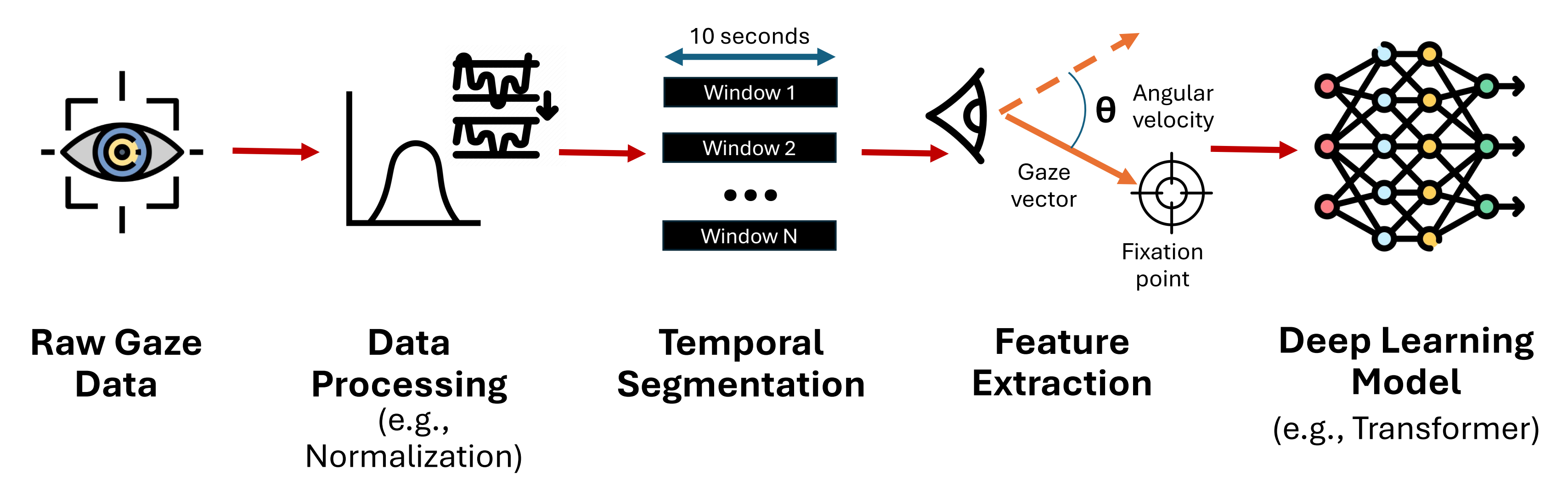


Avatar eye sync app
(Requires eye tracking permission)

PeekXR



Inference Pipeline



Feasibility Study

7 content categories

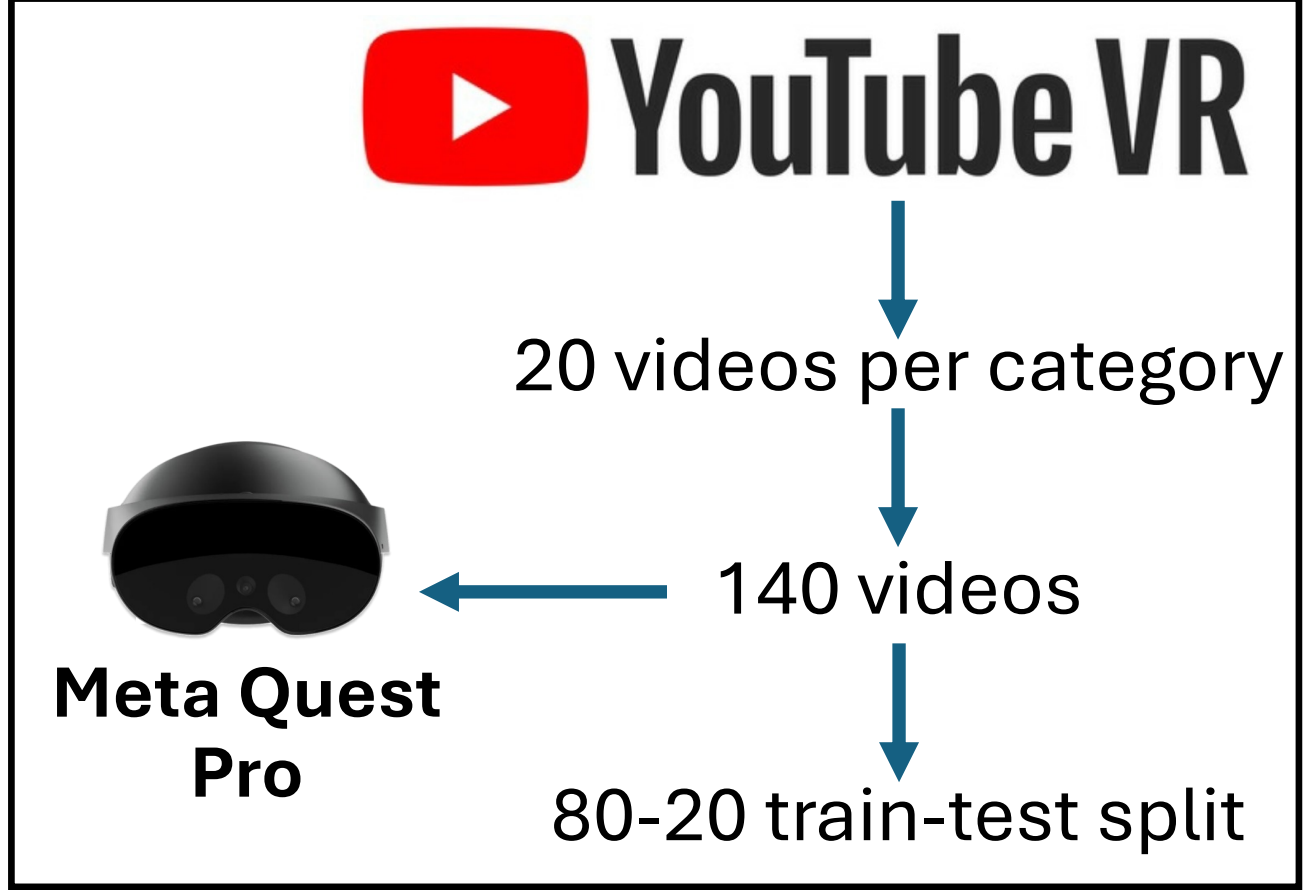
- Fashion
- Podcasts
- Gaming
- Movies
- Music
- Sports
- News

User study

- Users watched VR videos on Meta Quest Pro across 7 different genres.
- Eye tracking data sampled at 72Hz.

Results

- PeekXR successfully classified content with 75% accuracy using only gaze data from unseen videos.
- Accurate even with short 4-second gaze sequences.



Takeaways

Gaze as a behavioral fingerprint

- Gaze data leaks rich semantic information.
- Gaze patterns alone reveal what users are viewing.

Gaze data needs protection

- Gaze data should be treated a first-class privacy concern and deserves the same protections as camera, GPS, and mic data.

Future Work

Application fingerprinting

- Move beyond video classification to app fingerprinting and activity inference for more users.
- We hypothesize apps have unique gaze signatures.

Multimodal attacks

- Combine gaze with other sensor data (e.g., head and hand tracking) for more complex inference attacks.

Protecting gaze data

- Develop methods to protect gaze data while preserving functionality, such as using differential privacy or gaze obfuscation.

1. Berkovsky et al. 2019. Detecting personality traits using eye-tracking data. ACM CHI Conference on Human Factors in Computing Systems.
2. Chen et al. 2018. Eytell: Video-assisted touchscreen keystroke inference from eye movements. IEEE Symposium on Security and Privacy.
3. Wang et al. 2024. GAZEexploit: Remote Keystroke Inference Attack by Gaze Estimation from Avatar Views in VR/MR Devices. ACM SIGSAC Conference on Computer and Communications Security.
4. Wang et al. Follow my eye: Using gaze to supervise computer-aided diagnosis. 2022. In IEEE Transactions on Medical Imaging.