VR ProfiLens: User Profiling Risks in Consumer Virtual Reality Apps

Ismat Jarin[†][§], Olivia Figueira[†], Yu Duan[†], Tu Le[‡] and Athina Markopoulou[†]
[†]University of California, Irvine
[‡]The University of Alabama
[§]Email: ijarin@uci.edu

Abstract*—Virtual reality (VR) platforms and apps collect users' sensor data, including motion, facial, eye, and hand data, in abstracted form. These data may expose users to unique privacy risks without their knowledge or meaningful awareness, yet the extent of these risks remains understudied. To address this gap, we propose VR ProfiLens, a framework to study user profiling based on VR sensor data and the resulting privacy risks across consumer VR apps. To systematically study this problem, we first develop a taxonomy rooted in CCPA definition of personal information and expanded it by sensor groups, apps, and threat contexts to identify user attributes at risk. Then, we conduct a user study in which we collect VR sensor data from *four* sensor groups from real users interacting with 10 popular consumer VR apps, followed by a survey. We design and apply an analysis pipeline to demonstrate the feasibility of inferring user attributes using these data. Our results demonstrate that user attributes, including sensitive personal information, have a moderately high to high risk (with up to $\sim 90\%$ F1 score) of being inferred from the abstracted sensor data. Through feature analysis, we further identify correlations among app groups and sensor groups in inferring user attributes. Our findings highlight risks to users, including privacy loss, tracking, targeted advertising, and safety threats. Finally, we discuss both design implications and regulatory recommendations to enhance transparency and better protect users' privacy in VR.

I. Introduction

Virtual reality (VR) provides immersive, interactive experiences for users across diverse apps, such as gaming, education and remote work [1]–[3]. As part of the broader Metaverse, which connects virtual, augmented, and mixed reality–also known as extended reality (XR) [4], the VR market continues to grow rapidly [5], driven by major platforms such as the Meta [6], SteamVR [7]. Though VR offers substantial benefits [1]–[3], its extensive data collection and immersive nature introduce unique privacy and security challenges for users.

User Privacy and Security in VR. VR apps collect diverse sets of sensor data that may contain users' biometrics or behavioral fingerprints. Compared to mobile and web platforms, users have far less control over their privacy decisions in VR [8]–[10]. Independent reviews of major VR platforms reveal weak security controls and vague privacy policies, limiting users' ability to make informed decisions regarding sharing their sensitive data [11], [12]. Meta, for example, discloses in their privacy policy that platforms and app developers can collect and use "abstracted" data derived from raw inputs [13], which may seem less privacy-sensitive. However, prior works show that sensor data[1] can uniquely identify users [15]–[17]. As the Metaverse incorporates advertising and marketing campaigns [18], sensor data can be repurposed for behavioral targeting. Additionally, AI agents capable of impersonating users or influencing user judgment and behavior [19] may further expand the attack surface for manipulation and identity misuse. These privacy concerns have escalated into lawsuits and enforcement actions targeting biometric data practices in immersive ecosystems, prompting stronger regulatory scrutiny and compliance expectations [20]–[23].

Problem Statement. Due to pervasive data collection and users' limited control over data sharing in VR, "abstracted" sensor data can be exploited for user profiling and other non-functional purposes. We define *user profiling* as inference of private user attributes [14], and we use the two terms interchangeably. Understanding the extent to which users can be profiled from "abstracted" sensor data across consumer VR apps[2], and the risks such profiling entails remains a critical yet understudied privacy problem.We aim to answer the following question, which is later expanded into six research questions in Section V: *to what extent can VR users be profiled using **only** "abstracted" sensor data across consumer VR apps, and how does this impact users' VR privacy and safety?*

Research Gaps. Recent studies show that "abstracted" sensor data enables unique identification [15]–[17] and user tracking across apps [17], [24]. However, user profiling using sensor data remains understudied, and existing studies exhibit several limitations. First, while prior work has proposed a VR user attribute taxonomy [14], their focus was VR literature only, which limits the taxonomy's scope. As a result, this taxonomy does not explain the privacy nor regulatory significance of user attributes, nor does it capture attributes relevant to broader threat scenarios such as targeted advertising, safety and harm,

[1] "Abstracted" sensor data refers to processed telemetry derived from raw sensor inputs (e.g., image, video), available to platforms and app developers [13], [14]. We use abstracted sensor data and sensor data interchangeably.

[2] Consumer VR apps are designed for naive purposes such as social interaction (e.g., a_1) or gaming (e.g., a_3), not for intentional attacks.

Symposium on Usable Security and Privacy (USEC) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-07-7
https://dx.doi.org/10.14722/usec.2026.23003
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

or app contexts. Rather than focusing on available VR data as a basis (i.e., bottom-up approach), we construct our taxonomy from privacy law and expand it with threat scenarios and app specific attributes. We subsequently analyze which attributes are currently applicable in the VR context (i.e., top-down approach), considering that other attributes included in the taxonomy may become relevant as VR ecosystem evolve. Second, prior works focused on profiling using a single sensor (i.e., body motion [25], [26]), leaving the risks associated with other sensors and multi-sensor combinations underexplored. Existing studies rely on custom adversarial app [25], [27] or a single consumer app (e.g., Beat Saber [28] [26]), limiting diversity of user activities. Moreover, prior work underexplores the privacy and safety implications of inferred attributes and offers limited user-centric, sensor- or app-specific mitigation and regulatory guidance.

Approach. To address prior research gaps, we develop VR ProfiLens, a framework for systematically investigating user profiling risks in consumer VR apps, as depicted in Figure 1. Overall, we make the following key contributions:

(1) VR User Profiling Taxonomy (Section III-D). We introduce a novel VR User Profiling Taxonomy that is rooted in privacy law, namely the California Consumer Privacy Act's (CCPA) definition of personal information [29], enabling systematic reasoning about privacy and regulatory relevance of user attributes. The taxonomy is further expanded across diverse threat scenarios, including targeted advertising, identity theft, and safety and harm, as well as prior literature related to VR profiling and app contexts, enabling us to identify and analyze user attributes across different threat scenarios and app groups. Our taxonomy enables us to analyze the relationships among user attributes, sensor groups, app groups, and threat scenarios, and we utilize superscripts (see Section III-D and Table I) to indicate each attribute's associated threats and legal origin for interpretability and traceability. Since we utilized a top-down approach in developing our taxonomy, it serves as a global taxonomy that can be further expanded and generalized following our methodology, for example, as new privacy laws, VR threats, and apps are introduced.

(2) Methodology for Investigating VR User Profiling (Sections III and IV). We design a methodology to investigate user profiling in VR, including a user study to collect users' data, practical threat model, an analysis pipeline that evaluates profiling from sensor data under multiple threat scenarios within multiple apps, examining both individual sensor and their combinations—an unexplored approach. Our methodology can be generalized to other platforms that collect similar sensor data and/or other apps aligned with our app groups.

(3) Empirical Evaluation of VR User Profiling (Section V). We apply our methodology to quantify the feasibility of inferring user attributes from abstracted sensor data across 10 consumer VR apps and to assess profiling risk under different settings. Further, our findings highlight how sensor and app groups influence user profiling risk.

(4) Design Implications and Mitigation Insights (Section VI). We discuss potential design implications for enhancing user's privacy in VR, including user-centered mitigation strategies tailored to both sensor and app groups, as well as regulatory and compliance recommendations.

Paper Outline. The rest of the paper is organized as follows: Section II discusses related work, Section III outlines our methodology, Section IV presents data collection and analysis pipeline, Section V details the outcomes of our experimental evaluation on user profiling, Section VI discuss the implications of our findings, and Section VII concludes our study.

II. Related Work

A. Privacy and Security Threats in VR

User Profiling. While VR sensor data has been widely studied for unique identification [15]–[17], [30], their influence for user profiling remains underexplored.Prior work demonstrates attribute inference from body motion and eye tracking, but is limited to age and gender [27]. Other works extracted 25 attributes by creating an adversarial VR game [25] or 40 user attributes using single-consumer app settings [26].

Other Privacy and Safety Threats. Prior studies have identified security and safety threats in VR, including attribute-driven risks. One potential threat is identity theft [31]–[34], raising concerns about whether avatars accurately represent their real-world users. Identity verification in sensitive settings (e.g., virtual courtrooms or age-restricted spaces) may rely on sensory attributes, can be exploited by attackers [33]. Studies have highlighted VR safety concerns, including virtual shock [35], harassment [36]–[40], cyberbullying, and discrimination [41],with heightened impact on youth (e.g., under 18), who are more vulnerable to harmful consequences from such experiences [42]. Attackers may gather user attributes to steer users toward unnecessary purchases [43], such as through targeted ads [18], and distressing shockvertisements [35], [43].

B. VR Taxonomies

Prior work proposed VR taxonomies but remained domain-specific. Garrido et al. [14] derived a taxonomy solely from VR literature, while legal-domain taxonomies grounded in the CCPA [29] focused narrowly on children's privacy [44].

III. Methodology

This section outlines our methodology for investigating user profiling, including VR sensor data and device (III-A) we studied, our selected VR apps and app groups (III-B), our threat model and threat scenarios (III-C), and the development of our VR User Profiling Taxonomy (III-D).

A. VR Devices and Sensors

VR platforms vary widely in software and hardware configurations. In this study, we focus on SteamVR, the leading VR gaming platform with over 7,000 applications [45] and millions of users [46]. We use the Meta Quest Pro for its comprehensive sensor suite, including body motion and eye gaze (also supported by older devices such as Quest

2), as well as hand joints and facial expression, which are increasingly supported by newer AR/VR devices [47], [48]. We explore the following *four* VR sensor groups: (1) body motion (BM) [49], [50], (2) eye gaze (EG) [51], [52], (3) hand joints (HJ) [53], [54], and (4) facial expression (FE) [55], [56]. These sensor groups are available to developers through the OpenXR APIs [57], which offer a common interface across different VR devices. We adopt the data structure definitions from the OpenXR standard [57]. Details regarding the sensor data structure are described in Appendix VII-A1.

B. VR Apps

1) App Selection: VR apps span multiple platforms, including SteamVR [7], Apple Vision Pro [47], Meta's Oculus VR [6], and HTC Viveport [58]. We select 10 apps from the top 100 apps on the SteamVR store [59], [60]. To ensure coverage, we include one to two of the most popular apps from each defined app group (see Section III-B2). We refer apps as $a_1, ..., a_{10}$ (see Appendix VII-A2).

2) App Groups: Seven app groups, as detailed in Appendix VII-A3 and Table IV, are defined based on similarities in user activities, predominantly representing BM, HJ, and user emotional (valence-arousal [61]) states induced by apps, namely FE.[3] The app groups are: Social (i.e., social activities, positive emotional state), Flight Simulation (i.e., flying aircraft, mostly negative emotion), Interactive Navigation (IN) (i.e., frequent user-object interactions, neutral emotional states), Knuckle-Walking (KW) (i.e., gorilla movement, positive emotional states), Rhythm (i.e., fast dance-like movements, mixed emotional states), and Shooting & Archery (i.e., shooting targets, mostly negative states). We group apps: (1) to generalize insights to other apps within the same group; (2) to support deeper investigations, such as identifying data collection patterns in VR (see Section III-B3) and building taxonomies (see Section III-D6); and (3) to provide design insights for privacy-preserving, usable defenses.

3) Sensor Data Collection Practices: We examined sensor data collection practices of 20 popular apps in Oculus Quest [6] and SteamVR [7]. We found that data collection practices and disclosures vary across platforms: Oculus provides more transparency and permission controls than SteamVR. Few app's data collection practices align with their functionality, while others collect more sensor data or lack privacy disclosures. Future VR apps may collect all sensor data to support richer, multiplayer interactions (see Appendix VII-A4).

C. Threat Model

1) Adversary Capabilities: The primary goal of VR ProfiLens adversaries is to infer private user attributes from sensor data. We consider app developers, companies, or third parties with equivalent permissions (e.g., Unity [62]), corresponding to app/client or server adversaries in prior work [14], [17]. Such adversaries may collect sensor data paired with available attributes (e.g., gender) as ground truth, train ML models, and then profile a *new set of users* using only sensor data at inference time (Section IV-C). Based on adversarial knowledge and sensor access, we define two types of adversary:

Single-Sensor Adversary. Our single-sensor adversary has access to only one sensor group as certain sensor groups may be unavailable due to data loss, limited availability for the third party, or selective sensor data sharing by the users.

Multi-Sensor Adversary. This adversary has access to multiple sensor groups, may use either a single sensor or a combination of sensors (e.g., BM, FE together) for attack. This adversary has been underexplored due to limited access to multi-sensor data. Prior work [27] combined eye and body data but focused on a narrow set of attributes (age and gender).

Both adversaries may leverage one or more user attributes to facilitate additional attacks described next.

2) Threat Scenarios: Our threat model examines potential threat scenarios driven by inferred attributes. It is motivated by recent work on security, privacy, and safety challenges in Metaverse [4], and subsequent studies on privacy risks [63], targeted advertising [35], identity theft [33], and safety and harm [64]. Our goal is not to present an exhaustive threat model, but to establish a flexible framework that can be expanded to incorporate new threats. While prior work studies user profiling [25], [26], it offers limited analysis of adversarial misuse and threat scenarios, while other studies on attribute-specific threats [11], [31], [36] do not demonstrate how such attributes can be inferred from implicit identifiers (i.e., sensor data). We therefore propose a practical threat model assuming adversaries exploit attributes inferred from sensor data to enable attacks aligned with threat scenarios, described next.

Honest-but-Curious Adversary. An honest-but-curious adversary [65] records a few minutes of sensor traces and could infer one or more private attributes (e.g., gender, health conditions) while the user remains anonymous and only shares sensor data. Revealing such information not only compromises individual privacy rights [66], [67], also undermines trust in VR apps and platforms [11]. The attributes inferable by this adversary in VR are detailed in Sections III-D5 and III-D6 and are shown in our VR User Profiling Taxonomy (Table I) marked by the superscript '5' or '6', or both (e.g., race^{4,5,6}).

Targeted Advertising. As discussed in Section II-A, targeted advertising is a growing concern in VR. According to Meta's VR advertising documentation [18], advertisers can utilize various user attributes to target advertisements, including location, age, gender, device identifiers, and interactions with Meta services. Alternatively, if advertisers can profile VR users with implicit identifiers (i.e., sensor data), allowing them to bypass advertising services and cut costs by targeting users directly. Targeted advertising in immersive environments may exploit user's vulnerabilities, leading to manipulative or harmful purchase [43]. Such attributes are discussed in Sections III-D2, III-D5, and III-D6, and are marked with the superscript '1' or '2' (or both) in Table I (e.g., chronic illness^{1,5,6}).

Identity Theft. With user's information, adversaries can initiate identity theft attack by impersonating a user's identity

[3] While our prior work [17] touched app-grouping, this study defines and develops a broader, more structured, and expandable categorization.

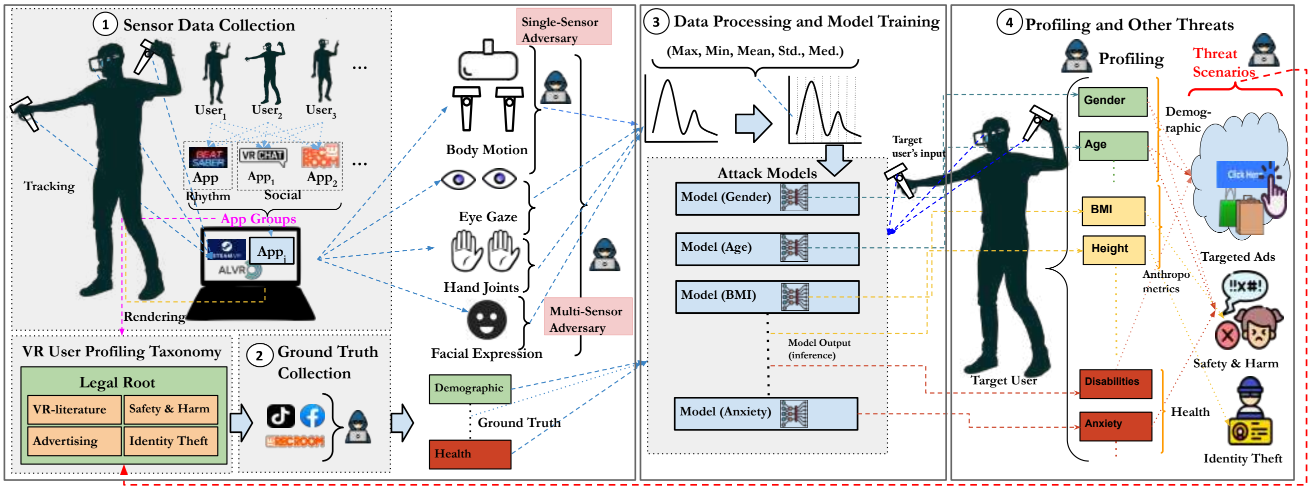


Fig. 1: **Overview of VR ProfiLens.** (1) **Sensor Data Collection using BehaVR [17] setup:** Each user interacts with 10 consumer apps using Quest Pro while *four* sensor groups are recorded; Single-Sensor Adversaries have access to one sensor group, and Multi-Sensor Adversaries have access to multiple sensor groups; we grouped apps based on similarities of activities and emotional states. (2) **Ground Truth Collection:** Ground truth collection from other platforms or apps which is guided by VR User Profiling Taxonomy. Our taxonomy is rooted in law and expanded by threat scenarios and app groups as indicated by arrows. (3) **Data Processing and Model Training**: Sensor Data processing, feature engineering, and inference attack model training using sensor data and ground truth. (4) **Profiling and Other Threats:** An adversary can take only VR sensor data as model input to infer user attributes. Next, they initiate further attacks aligned with threat scenarios in Section III-C2.

through bots to access secure or confidential areas. Identity theft may extend across digital platforms (e.g., Facebook [68]) and physical world, where attackers could misuse digital identities to compromise user's privacy and security. The attributes related to identity theft are discussed in Section III-D3 and marked by the superscript '3' in Table I (e.g., IPD^{3,5,6}).

Safety and Harm. VR users may experience harassment and safety threats, such as hate speech, violence, virtual crashing, and sexual harassment, based on attributes such as gender, race, and physical characteristics, as discussed in Section II-A. An adversary may infer those attributes from sensor data, even when users do not disclose them through their account or avatar choices (e.g., selecting an avatar of a different gender). VR can further deliver more immersive and targeted ads based on relevant attributes: for example, if a user's fear of heights is inferred, the adversary could deliver an immersive experience involving a virtual fall from a building [35] These attributes are included in our taxonomy (see Section III-D4) and marked by the superscript '4' in Table I (e.g., stress^{4,6}).

D. VR User Profiling Taxonomy

In this section, we discuss our VR User Profiling Taxonomy (Table I) and how it was developed. As discussed in Section II, prior work has identified various attributes that can be deduced from VR sensor data and user behaviors, but their taxonomies were limited to the VR context as they utilized a bottom-up approach in their development, namely starting from VR sensor data as a basis and analyzing related attributes. In order to develop a comprehensive and generalizable taxonomy that can enable the analysis of user profiling risk in VR in various contexts, we utilized a top-down approach instead. We present a new VR User Profiling Taxonomy that is rooted in the CCPA definition of personal information [29] (Section III-D1), which we further expand by incorporating attributes from advertising domains (Section III-D2), identity theft domains (Section III-D3), VR safety and harm literature (Section III-D4), and VR profiling literature (Section III-D5). We root our taxonomy in the CCPA definition of personal information, which specifies legally protected categories, and group all newly introduced attributes within these existing legal categories. The VR taxonomy [14] from prior work forms a subset of our taxonomy, as it is derived solely from VR literature. In contrast, by incorporating attributes from diverse sources beyond VR literature, our taxonomy is substantially more in-depth and encompasses various threat scenarios, which enables us to identify sensitive attributes that are shared among different threats. Our taxonomy serves as a global taxonomy as it includes a broad scope of attributes, and it can be further expanded following our methodology and generalized as new threats and app groups are introduced.

To develop our taxonomy, two researchers jointly decided on an approach and then independently worked to create the taxonomy. Once completed, discrepancies were discussed and resolved by consensus on the final taxonomy, presented in Table I. Next, we discuss the taxonomy development process, including incorporating attributes across sources (Sections III-D1-III-D5), and explain superscripts used in Table I.

1) Legal Domain Attributes: We began with the CCPA definition of personal information, which is defined as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[4] The definition includes 12 categories of personal information, such as identifiers, biometric information, geolocation data, and inferences. Following the category names and organization from the CCPA-based ontology in [44], we reorganized our table in a similar manner so that the categories were more specific to the attributes they contain, since some of the categories from the CCPA include subcategories. We maintained references to other laws and subdefinitions included in the CCPA text, such as the Family Educational Rights and Privacy Act (FERPA)[5], personal information described in subdivision (e) of Section 1798.80, and sensitive personal information in the CCPA, which are identified with the superscripts 'P', 'F', and 'S', respectively. We discuss more details in Appendix VII-A5.

2) Advertising Domain Attributes: Next, we incorporated attributes from advertising domains, namely the Interactive Advertising Bureau (IAB) Tech Lab Audience Taxonomy [69] and the Meta VR advertising documentation [18]. The IAB taxonomy attributes are grouped into three categories regarding user audiences that can be used for targeted advertising: demographics, purchase intent, and interests. For each demographics attributes, we added it to our taxonomy or marked the attributes that were already present in our taxonomy with a superscript '1', as shown in Table I. Purchase intent and interest categories already existed in our taxonomy, and these categories from the IAB taxonomy jointly contain over 1,400 attributes, which we leave out of the taxonomy due to space, except for a few attributes that are relevant to our study (e.g., caffeine or alcohol consumption). The Meta VR advertising documentation includes attributes that can be used for targeted advertising on Meta platforms, such as user location, age, gender and service interactions, which we incorporate into the corresponding taxonomy categories and mark with the superscript "2".

3) Identity Theft Attributes: Next, we studied attributes that could be misused for identity theft as described in Section III-C2. We utilized the California penal code regarding identity theft, which defines various attributes that may uniquely identify an individual and be misused for identity theft [70], [71]. Attributes include name, address, date of birth, unique biometric data, unique telecommunication data, and generally any "equivalent form of identification."[6] We incorporated these attributes and marked them with the superscript '3'.

4) Safety & Harm Literature Attributes: Next, we incorporated attributes that can be misused for harassment and endanger user's safety, as described in Section III-C2. We extracted attributes from prior VR literature on harassment, abuse, stalking, AI-driven harms, and shock advertising (i.e., "shockvertisements") that may incite fear, distress, or manipulation through targeted content or malware [35]–[40], [42], [64]. Identified attributes include demographic characteristics, avatar features revealing user identity, anxiety, and interests, among others, and we marked them with the superscript '4'.

5) VR Literature Attributes: Next, we analyzed attributes derived from prior VR literature [14], [26]. The taxonomy in [14] categorizes VR attributes based on a review of 75 privacy attack and defense studies, while [26], [72] identifies app-specific features in a single commercial app, *BeatSaber* [28]. We marked all related attributes with the superscript '5'.

6) VR User Profiling Attributes: In this step, we identify and expand attributes that can be captured from VR ecosystem (using multiple sensor data, app groups and threats). First, attributes derived from safety, harm, and VR literature (see Sections III-D4 and III-D5) are automatically included as they directly within the VR context. Next, we added more attributes related to each of all app groups (see Section III-B2), following a method used by [26], [72] for BeatSaber [28]. We expanded app-group specific attributes inspired by prior research [26], [72]. For example, in the social group, we added attributes such as social media usage and activity preference as they are relevant to our social apps' activities. We marked attributes associated with this step using the superscript '6'.

7) Final Attribute Selection for VR ProfiLens: Finally, we select a subset of attributes from our taxonomy to demonstrate user profiling risk. We consider both explicit and implicit attributes that are directly or indirectly mapped to our four sensor groups (HMD controllers, sensors, IMU, and observations) and app groups. Some attributes are (e.g., marital status, income) have correlation with other attributes, such as age or gender, which are inferable from sensor or behavioral data. Next, we excluded certain attributes based on our experimental setup. We omitted homogeneous user attributes, such as geolocation (i.e., participants were in the same location) as well as device and account related attributes (i.e., participants used the same device and account). We mark the final attributes in **bold text** in Table I, resulting in 48 attributes from 5 categories, namely Demographics, Health, Anthropometrics (included in the Biometrics category), Personal History, and User Interests and Behaviors. More details are in Appendix VII-B3 Table V.

IV. Experimental Setup

This section outlines our experimental setup and analysis pipeline, including sensor data collection from 10 consumer VR apps, user study protocol (IV-A), data processing (IV-B), model training for attribute inference (IV-C), and feature organization and analysis (IV-D) to support our evaluation.

A. *VR ProfiLens Dataset*

To study VR user profiling, we require users' sensor data and ground truth attributes. Thus, we conduct an IRB-approved user study with 20 participants, including VR sensor data collection followed by a survey. Participants were compensated at a $10/hour rate, and their data were stored using unique random IDs. We utilize the sensor dataset collected in our prior work [17] and augment it with more sensor data from the same participants across expanded app settings. Next, we will discuss our sensor data collection and survey procedures.

[4] CAL. CIV. Code § 1798.140(v)(1)
[5] 20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99
[6] CAL. PEN. Code § 530.55(b)

TABLE I: **VR User Profiling Taxonomy.** The taxonomy is developed from Legal, Advertising, Identity Theft, VR Safety/Harm, and VR User Profiling Literature domains and includes our Proposed VR User Profiling Attributes. The taxonomy is rooted in the CCPA definition of personal information [29]. Superscript values identify attributes that are included from other domains or legal texts (see Section III-D). Attributes in **bold text** are studied in this work. If all attributes within a category have the same superscripts, they are marked on the category.

Level 1	**Level 2**	**Level 3**	**Level 4**
Identifiers	Personal Identifiers	Name	Name[2,3,4,5,6,F], signature
		Linked Personal Identifiers[3]	Social security number[F,S], driver's license number[S], passport number[S], state identification card number[S], taxpayer identification number, US citizenship and immigration services-assigned number, birth or death certificate information (e.g., place of birth[F])
		Contact Information	Telephone numbers[2,3], postal/home address[2,3,4,F], email address[2,5,6]
		Reasonably Linkable Personal Identifiers	IP Address[5,6], unique personal identifier[3,4,5,6], Online identifier[3,4,5,6], aliases[3,4,5,6], unique pseudonym[3,4,5,6]
		User/Customer Numbers	Account name[2,4,5,6], customer number[3], insurance policy number[3] (e.g., health insurance), bank account number[3,S] (e.g., demand deposit, savings, checking account), credit card number[3,S], debit card number[S], student/school identification number[3,F], employee identification number[3], professional or occupation number[3]
		Login Information[3,S]	Account log-in, security or access code, password, or credentials
	Device Identifiers	Device Hardware Identifiers	Device identifier[2,3,5,6] (e.g., IMEI, MAC address), serial number[5,6]
		Device Software Identifiers	Cookies[5,6], beacons, pixel tags[2,6], mobile advertising identifiers[2], or similar technology[3]
		Device Information & Specifications[5,6]	Refresh rate, tracking rate, field of view, resolution, CPU/GPU power, CPU brand, logical cores, CPU speed, graphics card, system version, form factor, operating system, system memory, drive space, base stations
Personal Information	Personal Characteristics & History	Demographic Information[P]	**Race[4,5,6,S]**, color, **religion[4,5,6,S]**, **sex/gender[1,2,4,5,6]**, sexual orientation/preference[4,5,6], **marital status[1,2,5,6]**, military or veteran status, **ethnicity/national origin[4,5,6,S]**, language[1,2,5,6], ancestry, **age/date of birth[1,2,3,4,5,6,F]**
		Health Information	Medical conditions[4,P] (e.g., **illness/chronic illness[1,5,6], color blindness[1,5,6] close/distance vision and lenses[1,5,6]**, acuity[5,6], **motion sickness[4,6]**, substance/drug use[4,5,6], **sleepiness[5,6]**, dental care[1]), disability[4,P] (e.g., **mental disability[4,5,6]**, **physical disability[4,5,6]**, HIV/AIDS, cancer), genetic characteristics & information[P,S], medical history (e.g., medical leave[P], family care leave[P], pregnancy disability leave[P], retaliation for reporting patient abuse[P], vaccines[1]), physical health[4,5,6] (e.g., physical fitness[1,4,5,6], women's health[1], weight loss[1]), mental health[4,5,6] (e.g., **anxiety[4,6], stress[4,6], height phobia[4,6]**)
		Biometric Information[F,S]	**Anthropometric information** (e.g., **hand shape/length[3,5,6], face length[3,5,6], height[3,5,6], limb length[3,5,6] (arms, feet, etc.), interpupillary distance (IPD)[3,5,6], body measurements and relationships[3,5,6] (e.g., body ratios[3,5], wingspan[3,5,6], BMI[3,6]), weight[3,4,6], reaction time[3,5,6], physical characteristics or description[3,4,6]**), physiological characteristics[3,4,6] (e.g., heart rate, neural data[S]), biological characteristics[3], behavioral characteristics[3], DNA[3], imagery of the iris[3,4,5,6] (e.g., eye color), retina[3,4,5,6], fingerprint[3,6], face (e.g., facial features[3,5,6], facial movement[3,5,6], eye movement[3,4,5,6], faceprint[3,5,6]), hand[3,6], palm[3,6], and vein patterns[3,6], keystroke patterns/rhythms[3,6], biometric rhythms[3,4,5,6] (e.g., gestures[3,4,5,6], biometric movement[3,5,6]), gait patterns/rhythms[3,5,6], sleep, health, or exercise data that contain identifying information[3,6], voice recordings[3,4,5,6] (e.g., voiceprint[3], bone and air-borne vibrations[5])
		Personal History	Education information[1,5,6] (e.g., **education (highest level), academic interests**), employment information & History (e.g., employment role[1,6], employment sector/industry[1], employment status[1,5], working preference[1,6] (e.g., remote working), place of employment[3]), financial information (e.g., **income[1,5,6]**, wealth[5,6], personal level affluence or band[1], household income[1], monthly housing payment[1], median home value[1]), health insurance information, household data[1,6] (e.g., number of adults, children, individuals in household), citizenship or immigration status[S], union membership[S], family members' names[3,F] (e.g., mother's maiden name)
	Geolocation	Precise Geolocation[S]	Precise geolocation[2,4,5,6,S] (e.g., GPS location, postal/home address[2,3,4,F], coordinates (latitude, longitude))
		Coarse Geolocation	Coarse geolocation[1,2,4,5,6] (e.g., home location[1], country extension[1], region/state extension[1], city Extension[1], metro/DMA extension[1], zip or postal code extension[1])
	User Communications	Communications	Contents of mail, email, and text messages and conversations[2,5,6,S] (e.g., text content and semantic meaning, audio/speech content transcription)
		Internet Activity	Internet or other electronic network activity information[2,3,5,6], network bandwidth[2,3,5,6], network latency[2,3,5,6], browsing history, search history, unique electronic data including information identification number assigned to the person, address or routing code[3]
	User Interests & Behaviors	Purchasing Habits & Histories	Commercial information, records of personal property[1] (e.g., length of residence, single or multi generation household, household ownership, property type, urbanization), products or services purchased, obtained, or considered[1], other purchasing or consuming histories or tendencies[1]
		Sensor Data	Audio (e.g., user's voice[4,5,6], bystanders' voices[6]), electronic and thermal (e.g., physiological signals[5,6] (brain activity, electrothermal activity, skin galvanic response), IMU data[5,6] (device angular velocity, orientation, proper acceleration)), visual[4,5,6] (e.g., surrounding real-world space, physical objects, bystanders, room dimensions, play area), olfactory, or similar information
		App or Service Usage & Interaction	Information regarding a consumer's interaction with an internet website application, or advertisement[2,4,5,6] (e.g., user-app interactions[2,4,5,6], app name[5,6], app preferences[6], VR location[4,6], usage time[5,6], session info[5,6], digital presence[5,6] (e.g., avatars[4,5,6] and digital assets[5,6] (e.g., objects, currency, real estate)), user-to-user interaction[4,5,6], density of friendship[6], **social interaction[6]**, user-object interaction[6], field of view in VR[5,6], mobile device used[2,6])
		Inferences	Interests[1,2,4,5,6] (e.g., hobbies), preferences/predispositions[1,2,4,5,6] (e.g., **political orientation[1,4,5,6]**, background/experience (e.g., **musical instrument[1,5,6], dance[1,5,6], VR games [5,6], athletics/sports[1,4,5,6]), violence tolerance[1,4,6], working preferences (e.g., remote working)[6], organizational preferences[6], activity preference (e.g., indoor/outdoor)[6]**, travel preferences[2,6], clothing preferences[5] (e.g., lower/upper body clothing, footwear), characteristics & attitudes[5,6] (e.g., **introvert/extrovert[6], openness[6], conscientiousness[6], agreeableness[6]**), psychological trends (e.g., **emotions[4,5,6], emotional stability[6]**, cognitive processes[5,6], **attention/concentration[5,6]**, fear of death[4,6]), behavior (e.g., **handedness[5,6]**, physical preparation[5,6], drug consumption[4,5,6], **alcohol consumption[1,5,6], caffeine consumption[1,5,6], social media usage[4,6]**), aptitudes & abilities[5] (e.g., **reasoning & problem solving abilities[6], shooting experience[1,4,6]**, video game aptitude [4,6], intelligence[6])

Attribute Sources Legend:

1: IAB Advertising Audience Taxonomy
2: Meta VR Advertising Campaign
3: Identity Theft
4: VR Safety & Harm Threat Scenario
5: VR Literature
6: Proposed for VR User Profiling
P: Protected Classifications in CA
F: FERPA Definition of PII
S: Sensitive Personal Info. in CCPA

1) Sensor Data Collection: We collect the following four groups of sensor data, using the data collection setup from our prior work [17]: body motion (BM), eye gaze (EG), hand joint (HJ), and facial expressions (FE), recorded as time series. Each participant provided 5-6 minutes of data per sensor group per app, totaling to 3-4 hours per user for 10 apps, which required three months to collect for all participants. See Appendix VII-B1 for details.

2) Survey Protocol: Participants also completed a survey[7], which collected user attributes derived from our taxonomy (see Section III-D7), as listed next, serving as the ground truth for model training. The survey included the following:

- *Demographics:* Participants were asked demographic questions based on the US Census [73] (e.g., gender, age).
- *Personal History:* Participants were asked questions relevant to their personal history (e.g., income).
- *Anthropometrics:* Participants either voluntarily visited the lab, where the lead researcher collected anthropometric attributes (e.g., height, IPD), or they were self-reported.
- *Health:* Participants answered questions regarding their mental and physical health status, disabilities and other VR-relevant health factors, such as fear of heights for flight apps.
- *User Interests and Behaviors:* Participants were asked about their general behaviors, interests, and attributes relevant to each app group, such as social media usage (related to social apps) and organizational preferences (related to IN apps).

3) Dataset Summary and Size: Our final dataset links each user's sensor data with their ground truth survey responses. Thus, it includes 20 participants, each with four sensor groups across 10 apps (from seven app groups) and 48 ground-truth attributes (from five categories), as identified in Section III-D7. Overall, it contains 200 data records (20 for 10 apps) per attribute, thus 200 × 48 records for all participants across all attributes. More details regarding participants' statistics and attributes are discussed in Table V and Appendix VII-B3.

B. Data Processing and Feature Engineering

We process users' raw sensor streams (i.e., sensor data collected over time, discussed in Section IV-A1) into 1-second blocks and summarize each reading using five statistics, yielding feature vectors for BM, EG, HJ, and FE that follow the OpenXR standard [57]. This results in 165 BM, 46 EG, 1,820 HJ, and 320 FE features per block for downstream model training. Additional details are provided in Appendix VII-C.

C. Inference Attack Models

1) Ground Truth Selection: We initially considered all 48 attributes identified in Section III-D7 and collected corresponding user responses through our survey. We then removed attributes with non-discriminative responses (e.g., no reports of physical disabilities), consistent with prior work [26]. Next, we excluded attributes with limited responses (e.g., most users did not disclose their IPD) and those that were highly correlated or produced duplicate responses. Finally, we selected 29 attributes as the ground truth for model training and inference, as listed in Table V in Appendix VII-B3 (marked with ✓).

2) Model Selection and Training: We formulate inference tasks as either categorical classification (e.g., gender) or continuous regression (e.g., height), depending on the attribute. We choose two types of ML models: classification for categorical (e.g., gender) and regression for continuous (e.g., height) attributes. We explore Random Forest (RF) [74], Gradient Boosting (XGB) [75], Light GBM (LGB) [76], and Support Vector Machine (SVM) [77] for classification. After our initial analysis, we choose RF and LGB based on performance, which also align with our objective to conduct feature analysis. For the regression, we explore Linear Regression (LR) [78] and Random Forest Regression (RFR) [79]. Based on our empirical analysis on model performance, we select RFR. We evaluated acceptable error margins (±5 cm, ±5 lb, ± 2.5 cm , ±0.5 cm for height, weight, hand, and face length respectively).

Our attack classifier design follows our threat model and participant response distribution; details are provided in Appendix VII-B4. We train multiple attack models, one per attribute for each sensor group and combinations of multiple sensor groups. This includes single-sensor models, which have one model per attribute (e.g., gender) per sensor group (e.g., BM) for the single-sensor adversary, and multi-sensor models, which have one model per attribute per sensor combination (e.g., BM and FE) for the multi-sensor adversary (see Section III-C1); e.g., BM gender inference model is trained on the BM sensor with gender serving as the ground truth.

3) Inference: Finally, we evaluate the feasibility of user profiling using 5-fold cross-validation, ensuring that users in the test fold are never present in the corresponding training folds. We report average performance to minimize bias from particular user subsets. While the participant count is limited, each user contributes multiple samples across apps, enabling per-sample evaluation under a strict user-disjoint setting. We report our final results per-sample basis (1s per chunk) rather than per user to reduce bias.

D. Feature Organization and Analysis

1) Feature Importance and Ranking: We evaluate feature importance for each attribute-inference model using information gain [80]. Then, we rank features as either high importance (HI), medium high importance (MH), medium importance (MI), or low importance (LI) by extracting three elbow points [81] per attribute per app group, based on sorted importance scores. These elbow points mark where feature scores sharply decline, serving as thresholds for ranking.

2) Feature Interpretation: Features from sensor groups are important for describing user actions. Prior works focused on a single attribute (e.g., identification [15]–[17]) or did not analyze features (e.g., [25], [26]), thus used ad hoc feature sets. Our study contains multiple dimensions (e.g., attribute vs. app vs. sensor group), requiring a more systematic and automated method. We provide an automated pipeline that enhances the interpretability of sensor-derived features. Details can be found in Appendix VII-C3, Tables VI (BM), VII (FE), and VIII (HJ).

[7] Our survey questionnaire is available at https://osf.io/wnue5/?view_only=004315c37a9d471fb9cfe2dbee62018e.

V. Evaluation

This section details our experimental evaluation on user profiling, including our evaluation metrics (V-A), research questions that guide our evaluation and discussion (V-B), and attribute inference results for our adversarial settings (e.g., sensor groups, app groups, adversaries) (V-C-V-F).

A. Evaluation Metrics

We evaluate our results using two evaluation metrics:

Attack Performance. We adopt F1 score metric to measure the performance of the inference attack models.

Risk Assessment. Leveraging industry and NIST practices [82]–[84], we map F1 scores into four risk levels to interpret profiling risk: High/Very High Risk (F1=80-100%, purple), Moderately High Risk (F1=70-80%, orange), Moderate Risk (F1=50-70%, blue), and Low Risk ($F1 < 50\%$, gray), as detailed in Appendix VII-D1. Colors indicate associated risk levels in our result tables (e.g., Table II). Additionally, we assume each attribute's risk level maps into its corresponding threat scenarios; e.g., if gender^{1,2,4,5,6} inference via BM yields an F1 of 85%, placing gender^{1,2,4,5,6} at high-risk level and, users sharing BM are likely at high risk for associated threats (e.g., targeted advertising, safety/harm; see Section III-C2) as indicated by the attribute's superscripts in Table I.

B. Research Questions

We evaluate the experimental results by answering the following Research Questions (RQs):

- RQ1. How well users can be profiled using *only* VR sensor data? (Section V-C)
- RQ2. What are the top features for profiling? (Section V-D)
- RQ3. How can user attributes be inferred from sensor data across different VR app groups? (Section V-E)
- RQ4. How do combinations of different sensor groups expose personal attributes? (Section V-F)

Moreover, we include an in-depth discussion in Section VI that addresses the following:

- RQ5. How does revealing one or multiple attributes place users at risk across different threat scenarios? (Section VI-A)
- RQ6. What are the design and regulatory implications of our findings, and how can these insights support service providers and lawmakers in designing safer VR experiences for users? (Sections VI-B and VI-C)

C. Quantifying Profiling Risks (RQ1)

We evaluate the effectiveness of attribute inferences using VR sensor data by answering **RQ1**. Details are in Table II (BM), Appendix VII-D2 Tables IX (FE), X (EG), and XI (HJ).

Attributes from demographics, anthropometrics, and health, are inferred with moderately high to high F1 across all sensor groups. Demographic attributes, such as gender^{1,2,4,5,6}, age^{1,2,3,4,5,6,F}, and ethnicity^{4,5,6,S}, are inferred with moderately high (70–80%) to high (80–100%) F1 using BM, FE, and HJ. HJ and BM exhibit the strongest overall performance; e.g., for gender^{1,2,4,5,6}, HJ achieves an F1 of 73–87% and BM 65–94%, and for age^{1,2,3,4,5,6,F} and ethnicity^{4,5,6,S}, 71–85% and 70–73%, respectively, across most app-groups. FE provides high performance on ethnicity^{4,5,6,S} (78–86%) and age^{1,2,3,4,5,6,F} (71–88%), but moderate to moderately high for gender^{1,2,4,5,6} (68–78%). Alternatively, attribute inferences based on EG show low to moderate adversarial risks (49–60%).

For anthropometrics, BM provides high F1 across app groups (70–100%), particularly for height^{3,5,6}, weight^{3,4,6}, and reaction time^{3,5,6}, and moderate/moderate-high for BMI^{3,6} (60–80%). FE performs well for face length (65–80%) but yields lower F1 for other attributes. HJ shows moderate to low performance, and EG yields the lowest. Health attributes show moderately high to high risk for BM and HJ (e.g., 80% for physical fitness^{1,4,5,6} and stress^{4,6}, and 70–85% for anxiety^{4,7,8} and height phobia^{4,6}), depending on the app groups. FE performs better in stress^{4,6} (85–94%) and anxiety^{4,7,8} (70–85%), but moderate for height phobia^{4,6} (55–73%).

BM provides high F1 for user behavior and interests; e.g., for organized versus unorganized^{6} (84–95%) and emotional stability^{6} (70–79%). FE provides high F1 for organized behavior^{6} (76–97%) and openness^{6} (73–84%). For attributes such as violence tolerance and emotional stability, FE provides high to moderately high F1 (74–86%), depending on the app groups. HJ demonstrates moderately high F1 for concentration$^{3,\ 6}$ (75–82%), violence tolerance$^{1,\ 4,\ 6}$ (70–81%), shooting experiences^{1,4,6} (70–79%), and moderate in others.

Key Takeaway 1

Observations: BM and HJ provide high F1 across demographic, health and behavioral attributes, while FE for mental-health attributes. Overall, results show that a substantial set of private user attributes can be inferred with high F1 (80-100%) from sensor data.

Implications: VR sensor data enables substantial user profiling. Profiling risk is sensor-dependent rather than uniform. Therefore, users privacy protections must be sensor-specific, with users control per sensor group.

D. Feature Analysis (RQ2)

Next, we analyze features for attributes with high and moderately high-risk, prioritizing those most likely to be exposed and most in need of mitigation. For BM (see Figures 2 and 3, Appendix VII-D2), demographic (e.g., gender^{1,2,4,5,6}, ethnicity^{4,5,6,S}) and health attributes (e.g., BMI^{3,6}, physical fitness^{1,4,5,6}) that provide high F1 for social, archery, shooting, and rhythm have max standing height as the high importance (HI) feature. Additional features such as sitting/standing statistics, controller span (analogous to wingspan), and left–right head position also emerge as important. For physical fitness^{1,4,5,6}, head and controller rotations are identified as medium-high to high importance features, particularly in physically demanding app groups (e.g., archery, rhythm). For mental health attributes such as stress^{4,6} and anxiety^{4,7,8}, high-performing app groups (flight, social, archery) primarily rely on dynamic motion features—head and controller rotations

TABLE II: **User Profiling Using BM Sensor Data Across 7 App Groups.** The color code, designed to be color-blind friendly [85], represents four risk levels based on F1: High/Very High Risk (F1=80-100%, purple), Moderate-High Risk (F1=70-80%, orange), Moderate Risk (F1=50-70%, light-blue), and Low Risk ($F1 < 50\%$, gray) as per V-A. Attribute superscripts indicate associated threats according to our threat scenarios (see Section III-C2) and taxonomy (see Section III-D6).

Attribute Groups	Attributes	App Groups						
		Social	Flight	Shooting	Rhythm	IN	KW	Archery
Demographics	Gender^{1,2,4,5,6}	85	65	90	94	75	78	92
	Age^{1,2,3,4,5,6,F}	68	70	70	68	67	63	70
	Ethnicity^{4,5,6,S}	70	71	58	51	70	62	73
	Marital status^{1,2,5,6}	58	52	54	55	63	55	42
Anthropometrics	Height^{3,5,6}	80	44	90	100	52	69	90
	Reaction Time^{3,5,6}	85	90	90	95	97	85	90
	Face Length^{3,5,6}	58	40	40	56	52	49	61
	Arm Length^{3,5,6}	75	45	66	71	70	50	49
	Weight^{3,4,6}	75	46	80	72	73	69	75
	BMI^{3,6}	70	60	73	65	81	73	61
Health	Close / Distance vision and lenses^{1,5,6}	58	61	53	60	60	51	65
	Physical fitness^{1,4,5,6}	80	65	71	86	70	80	86
	Anxiety^{4,6}	85	87	65	71	72	67	70
	Stress^{4,6}	88	90	89	81	83	86	87
	Height phobia^{4,6}	70	81	62	59	81	74	72
	Motion sickness^{4,6}	45	60	45	48	60	70	55
User Interests & Behaviors	Problem Solving Abilities^{6}	74	62	55	42	43	78	79
	Alcohol consumption^{1,5,6}	64	71	59	59	59	60	62
	VR Experience^{5,6}	77	73	65	77	66	74	78
	Activity preference^{6}	59	70	53	60	69	53	65
	Shooting Experiences^{1,4,6}	81	68	78	86	68	75	82
	Caffeinated item consumption^{1,5,6}	69	77	65	71	66	58	72
	Concentration^{3,6}	73	72	49.5	48	70	60	72
	Violence tolerance^{1,4,6}	74	70	42	67	70	70	70
	Introvert/Extrovert^{6}	55	65	45	45	61	47.5	55
	Organized/Unorganized^{6}	88	95	90	88	92	70	80
	Social media usage^{4,6}	75	60	80	90	70	71	90
	Openness^{6}	68	71	70	68	67	65	62
	Emotional Stability^{6}	76	74	53	74	78	66	75

and forward–backward movement—rather than static user-specific measurements. Similar trends are observed for HJ (Appendix VII-D2, Figure 5). Demographic inference primarily depends on hand positional features, while mental health and behavioral attributes rely more on hand joint rotations (e.g., height phobia^{4,6}). In contrast, physical fitness^{1,4,5,6} is inferred using a combination of physical measurements and movement-based features, that encode physical biometrics.

For FE (see Figure 4 in Appendix VII-D2) we observe demographic attributes such as age^{1,2,3,4,5,6,F} and gender^{1,2,4,5,6} show feature importance relevant to app groups. App groups involving social interactions (e.g., social, KW) predominantly contribute features related to positive or low-arousal negative emotions (e.g., surprise, disgust, happy), compared to features linked to non-emotional expressions or high-arousal negative emotions. In contrast, app groups where users may experience negative emotions (e.g., shooting) show high importance for features associated with negative emotions (fear, anger, or disgust). Across most app groups, important non-emotional features include jaw sideways, lip suck, and chin raiser, indicating older vs. younger users exhibit distinct facial feature around chin, jaw and lip. Behavioral and mental health attributes show variety of feature important for different app groups; e.g., for social apps, disgust and surprise are top features for stress^{4,6}.

Key Takeaway 2

Observations: Demographics and anthropometric attributes stem from sensor measurements, whereas mental health and behavioral attributes stem from emotion- and movement-based features.
Implications: Since each attribute category is driven by a specific set of features (e.g., measurements for demographic), suppressing those features can reduce profiling risk across multiple attributes.

E. Profiling Across App Groups (RQ3)

Next, we examine the relationship between user attributes and app groups (i.e., app activities and emotional states; Section III-B2), drawing from Table II (BM) and Appendix VII-D2 Tables IX (FE), X (EG), and XI (HJ). Several app groups yield higher attack performance for specific attributes using BM, HJ, and FE. For example, social, shooting, and archery apps achieve high F1 for gender^{1,2,4,5,6} (70–90%), age^{1,2,3,4,5,6,F}, and ethnicity^{4,5,6,S} (65–90%) across sensor groups. For *demographics*, attack performance varies by app group: using BM and HJ, gender^{1,2,4,5,6} reaches high risk levels (80–100%) in social, rhythm, and shooting/archery apps, but remains low in flight, KW, and IN. As shown in Section V-D, body measurements such as height^{3,5,6} and hand span are key for inferring gender. however, flight, IN, and KW involve seated or tilt-walking interactions (e.g., gorilla-style), which obscure true measurements and reduce inference performance.

Alternatively, *anthropometrics* such as height^{3,5,6}, weight^{3,4,6}, and BMI^{3,6} achieve moderate to high F1 across most app groups using BM, with lower performance in flight, KW, and IN (44–69%), where true physical measurements are less exposed. Physical fitness^{1,4,5,6} and mental health attributes (anxiety^{4,7,8}, stress^{4,6}, height phobia^{4,6}) reach high to very high F1 (70–100%) in social, flight (mental health only), archery, KW, and rhythm apps, where activity-driven body motions reveal health signals;e.g., HJ infers height phobia with high F1 in flight (85%) and KW (77%). FE performs poorly for physical fitness (45–65%) but moderately for mental health attributes, with limited variation across apps. For *user interests and behaviors*, BM achieves moderately high performance (70–79%) when aligned with app context; e.g., shooting experience^{1,4,6} reaches high F1 in shooting (81%), rhythm (86%), and archery (82%) apps, where movements resemble shooting actions.

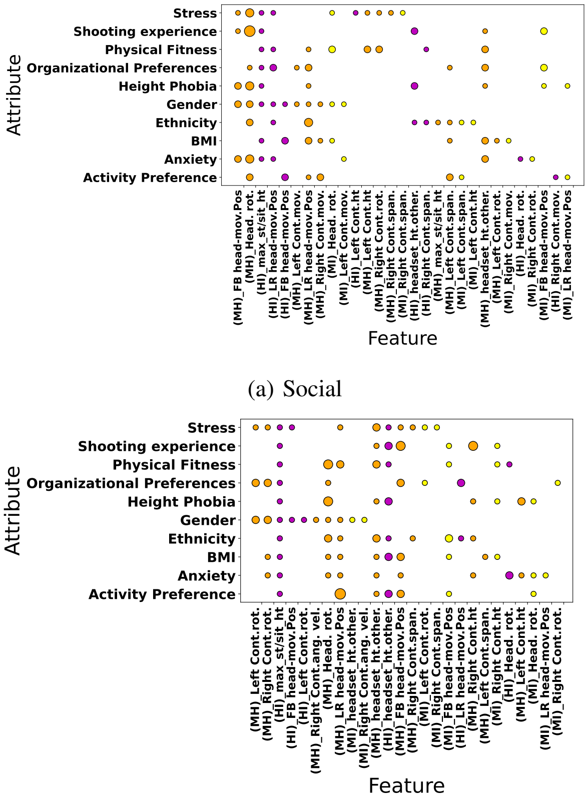
Key Takeaway 3

Observations: App groups influence user profiling risk, as app-specific contexts and user interactions expose certain attributes more strongly than others.
Implications: Profiling risk is influenced by app groups: different apps influence different attribute exposures. Thus, defenses must consider *which attributes are exposed in which apps* rather than applying a uniform policy across apps.

F. Multi-Sensor Adversary (RQ4)

We present the evaluation results of the multi-sensor adversary settings (see Section III-C1) to address **RQ4**. Our multi-sensor analysis is scoped as a proof-of-concept and evaluates a representative subset of sensor group combinations based on the realistic scenarios (details are below). We acknowledge that additional adversarial combinations are possible, and our methodology readily extends to explore them in future work.

1) BM and FE: Realistic adversaries for this setting include: (1) apps that use BM and FE together for functionality purposes (e.g., social apps) with user-granted permissions, and (2) third-party apps (e.g., ALVR [86]) that record both BM and FE without permission. The performance for *demographic* attributes, such as age^{1,2,3,4,5,6,F} and gender^{1,2,4,5,6} remains similar for some app groups (e.g., social), but improves for others (e.g., KW and IN)–raising their adversarial risk from medium-high to high (see Table XII). As discussed in Sections V-C and V-D, BM loosely provides users' measurements (e.g., height) for KW, IN, which are crucial to infer gender, combining BM with FE enhances accuracy in those app groups. For anthropometrics, performance remains unchanged, since facial features lack users' body measurements and vice versa. We also observe an 8–30% performance increase for height phobia, motion sickness, and interest/behavior attributes (e.g., violence tolerance). Another observation is, attack improvements further depend on app groups: violence tolerance increases in shooting, KW, and archery apps with fear-inducing activities.



(a) Social

(b) Archery

Fig. 2: **Feature Analysis on BM for Social and Archery App Groups.** The Y-axis lists attributes and the X-axis shows top features. Color encodes feature importance: HI (high, pink), MH (medium-high, orange), MI (medium, yellow).

2) BM, FE, and EG: In this setting, the attack risk remains high, comparable to the BM+FE adversary with only a slight increase (2–5%) in some groups (see Table XIII). Since EG is the weakest sensor group and BM+FE already yields strong performance, adding EG does not significantly improve results.

Key Takeaway 4

Observations: Multi-sensor adversary (BM+FE) elevates risk for health and several demographics (e.g., gender, age) from moderate to high (8–30%), while anthropometrics remain unchanged. Adding EG yields marginal gains (2–5%), indicating limited contribution.
Implications: Combining sensor groups amplifies profiling risk, highlighting the necessity of multi-sensor access protections to mitigate high-risk outcomes.

VI. Discussion

This section discusses the implications of our findings (see Section V) for users' privacy risks (VI-A), guided by **RQ5**, and both design (VI-B) and regulatory (VI-C) implications, guided by **RQ6**. We also discuss limitations and future directions (VI-D) as well as ethical considerations (VI-E).

A. Potential User Risks in Consumer VR Apps (RQ5)

1) Feasibility of User Profiling: We now revisit our central question: is it possible to profile users using *only* sensor data from non-adversarial, consumer VR apps? We demonstrate that BM, FE, and HJ enable moderately high to high F1 for multiple attributes (see Table II and Appendix Tables IX-XIII). Our feature analysis suggests that adversaries can infer one or more attributes even from a subset of sensor data: for example, in the social app group, adversaries can infer gender, physical fitness, and BMI using only height, left-right head movement, and other vertical headset statistics, which consistently rank as top features across these attributes (see Figure 2a).

2) User Attributes vs. Threat Scenarios: Compared to prior works [25], [26], we study data collected from multiple consumer VR apps, capturing a more realistic VR ecosystem used by millions of users, including vulnerable populations [87], [88]. Our findings highlight serious risks to users: a wide range of attributes, including sensitive demographic, health, and behavioral information were inferred with high F1 (70–100%). Exposure of one or a combination of multiple attributes can pose various threats to users (see Section III-D). For example, height phobia^{4,6}, anxiety^{4,6}, and stress^{4,6} achieve up to 81–90% F1 using BM in several app groups (e.g., flight, KW, archery). A user who shares BM with those apps could be exposed to safety threats (e.g., virtual shock) with high risk, according to our risk level described in Section V-A, and as indicated by superscripts '4' and '6' (see Section III-C2). Exposure of age^{1,2,3,4,5,6} and gender^{1,2,4,5,6} can put users at risk of targeted advertising (e.g., especially if combined with user interests and behavioral data), identity theft (e.g., if combined with other unique identifiers, such as their name and anthropometric data), and safety concerns, such as harassment or cyberbullying in VR for vulnerable groups, which can be more extreme when age and gender are known [42].

3) Threats Involving Anthropometrics: Anthropometric data poses privacy and security risks, as it can enable real-world or virtual identity theft: an adversary could infer a user's measurements, such as height^{3,5,6}, face length^{3,5,6}, and arm length^{3,5,6}, as well as attributes like age^{1,2,3,4,5,6}, from sensor data, enabling the replication of a user's digital identity in the virtual world. As discussed in Section V, our results show that users sharing BM, FE, or HJ data have moderately high to high adversarial risk (70–100% F1) for these attacks.

4) User Risks Across Multiple Apps: The attacks, discussed in Section VI-A1-VI-A3, can be more extreme, as users can be identified across different apps [17], [24] and different settings within an app [17]. Thus, an attacker can track users across apps and settings, aggregate inferred attributes, and launch profiling-based attacks across multiple apps.

B. Design Implications (RQ6)

The varying strengths of sensor data across different apps in inferring sensitive user attributes highlight the necessity of sensor- and app-specific privacy protections for users. We will discuss design implications next, considering both usability and risk mitigation tradeoffs.

1) User Awareness: Users often share sensor data without recognizing the privacy risks [89] as such sharing feels routine and harmless rather than an explicit or suspicious request that would raise concern. Moreover, marginalized users often conceal attributes (e.g., gender, age, body measurements) to avoid potential harm, even while choosing avatars [90]. We recommend that service providers (e.g., Meta) raise awareness by clearly communicating risk levels across attributes w.r.t. sensor and app groups as shown in VR ProfiLens, such as through a simple risk dashboard or by sending quick alerts when multiple sensors are active together, since combining multiple sensor data raises profiling risk.

2) Sensor Permission Design: Another potential defense is to turn off the sharing of certain sensor groups based on associated risks. Users should be able to independently enable or disable each type of sensor data across VR platforms. Modern VR platforms (e.g., Oculus) provide permission checks for FE, EG, and HJ [8], [13], [91], whereas others (e.g., SteamVR) still lack equivalent controls for sensor data access (see Section III-B3). Platforms should also clearly disclose the purpose of collecting sensor data, ensuring it aligns with the functionality of the app group. Currently, these purposes are often vague [8]; for example, the purpose of facial data collection in Meta Horizon Workstation, an IN app (see Section III-B3). A major challenge is the lack of granularity in data-sharing choices, which can significantly limit usability. For example, if users do not share FE sensor data in social apps, it may reduce social interaction quality based on facial expression.

3) Obfuscation-Based Design: A more granular defense approach would be to obfuscate sensor data (e.g., with local differential privacy (LDP) [92]), allowing users to share data without fully disabling sensors. Guided by VR ProfiLens's feature analysis, obfuscation can target the most important features for inferring sensitive attributes, thereby reducing adversarial risks. A more fine-grained approach is to target top features that affect multiple attributes. For example, for BM, the height feature is of high to medium-high importance for inferring gender and physical fitness. Obfuscating height can help lower the risk of exposing all three attributes and relevant threats (e.g., safety). The main challenge is to find the best privacy-usability trade-off while obfuscating attributes.

4) Privacy Assistance Agent: VR platforms could integrate a privacy-assistance agent (e.g., AI agent) to help users manage privacy decisions in real time. Guided by our findings, this agent may (i) provide permission nudges or suggestions and/or (ii) automatically predict and configure permission choices on the user's behalf, as is done in other domains [93], [94]. The agent can analyze the risk level associated with each sensor group in each app and scenario (e.g., private vs. public virtual space) and suggest or take actions, such as turning off sensor access or enabling privacy-preserving sharing (e.g., recommending or selecting noise levels based on users' privacy choices). This automation would reduce cognitive burden, enabling privacy and usability.

C. Regulatory Implications and Recommendations (RQ6)

1) Implications for Compliance: VR devices from different companies can vary widely in their sensor permission options (see Section III-B3). Permissions are only meaningful if users have real choices, as opposed to forcing access to all sensors in order to use an app. The CCPA definition of personal information [29] (i.e., foundation for our VR User Profiling Taxonomy) classifies biometric information as "sensitive personal information", which affords it special protections. Meta discloses that Meta and third parties are able to access "abstracted" sensor data, not raw sensor data [13]. We consider that "abstracted" sensor data aligns with CCPA's definition of biometric information, and we demonstrate its risks for user profiling. Depending on VR providers' interpretation of "abstracted" sensor data, they may skirt associated protections for biometric information, endangering users' privacy.

2) Regulatory Recommendations: We recommend that lawmakers and regulators scrutinize VR providers' privacy policies regarding their definitions of sensor data to better align law with practice. We urge lawmakers and regulators to pay special attention to vulnerable attributes we have identified through the development of our VR User Profiling Taxonomy and analysis of threat scenarios (see Sections III-D and III-C2). Regulations should mandate that VR providers only collect sensor data that is required for functionality. Further, regulations should require granular, opt-in sensor permissions and obfuscation-based privacy options for sensor data among VR devices. CCPA regulations already enforce strict privacy rights for vulnerable groups (e.g., consumers under 16 years old) and for sensitive personal information [66], and thus we recommend similar protections be required for VR and other devices that are able to collect sensitive biometric data.

D. Limitations and Future Directions

1) User Study Size: A limitation of our study is the number of participants (see Section IV-A). Our goal was to evaluate profiling across multiple apps, sensors, and attributes, thus we relied on an in-person user study, resulting in a sample size comparable to prior in-person VR studies (e.g., [25], [27], [30], [95]) but with more app and sensor coverage.

Recruitment was challenging, as participation required multi-hour gameplay across 10 apps and a follow-up survey. Some attributes in the survey were self-reported, which may introduce bias. Our attack classifier design (Section IV-C2) is guided by our threat model and participant distribution. Due to the limited participant pool, we could not exhaustively evaluate all adversarial capabilities; e.g., the absence of participants under 18 prevents demonstrating child–adult age gating, even though such inference aligns some attackers objective. While these limitations may constrain generalizability, we hope our work offers new insights by expanding the problem space across sensors, apps, and attributes. We hope our method and released artifact[8] enable future work with more users, additional apps, and new threat scenarios.

2) Design Defense Tools: As discussed in Sections VI-B and VI-C, future directions include designing defenses, such as AI agents to assist users with privacy decisions, sensor data permissions, more granular privacy-preserving options by platforms, and the enforcement of data minimization through regulation. Future defenses should be evaluated through user studies to ensure acceptable privacy–usability tradeoffs.

E. Ethical Considerations

We conducted an IRB-approved user study with careful attention to ethical considerations. We select apps to align with our IRB risk minimization protocol [96], such as excluding horror or violence genres that may cause psychological harm or distress to users. Participation in our study was voluntary, allowing participants to opt out at any time. Participants provided informed consent through a written consent form prior to participation. Our data was stored in a secure, password-protected database, and access was restricted to the lead researcher and only used for research purposes.

Personal attributes in our study were selected using our methodology and ethical considerations, with collection limited to attributes necessary for the study. Attributes were derived from prior VR literature [14], [26], [72] as part of our taxonomy development (see Section III-D), which identifies both explicit and implicit attributes, linked directly or indirectly to sensor/behavioral signals. Additionally, given the sensitivity of the survey content, all questions were optional and included a "Prefer not to answer" response. No personally identifiable information (e.g., name, email) was collected. Responses were identified using random unique IDs. Our reported results are not linked to any individual, and our experiments do not cause harm to the participants.

VII. Conclusion

We present VR ProfiLens, a framework for identifying and analyzing user profiling risks in Virtual Reality using "abstracted" sensor data. To the best of our knowledge, VR ProfiLens is the first holistic demonstration of VR user profiling by (1) developing an expandable and systematic VR User Profiling Taxonomy, (2) designing a methodology to examine profiling across sensor and app groups via a user study, (3) demonstrating profiling feasibility through empirical evaluation, and (4) providing both user-centered design and regulatory recommendations based on our findings. Additionally, our app groupings, threat model, and taxonomy are designed to be expandable, allowing new apps, emerging threats, and new attributes to be incorporated. Overall, our results demonstrated the adversarial feasibility of inferring user attributes using "abstracted" sensor data, underscoring the need for user-centered privacy protections and regulatory attention to improve users' privacy and safety in VR.

[8] VR ProfiLens source code is publicly available at https://github.com/UCI-Networking-Group/VR-Profilens.git.

Acknowledgments

This work was supported by the National Science Foundation under award numbers 1956393 and 1900654 and a gift from the Noyce Initiative. We also gratefully acknowledge that Ismat Jarin was partially supported by the ESET Women in Cybersecurity Scholarship, and Olivia Figueira was partially supported by the UCI ICS Steckler Family Endowed Fellowship and the ARCS and Danaher Foundation Scholar Award. We would like to thank Rahmadi Trimananda for his feedback on the initial version of this work. We thank the anonymous USEC reviewers for their constructive feedback, which helped improve this paper. The authors used OpenAI's ChatGPT [97] for minor editing, including correcting typos, improving grammar, and paraphrasing.

References

[1] Meta, "Meta for Education with virtual reality," https://forwork.meta.com/meta-for-education/, 2025.

[2] Meta, "Bring your teams together in Meta Horizon Workrooms," https://www.meta.com/work/workrooms/?utm_source=www.usenix.org&utm_medium=oculusredirect, 2025.

[3] Meta, "Watch shows, teams and streams in your own immersive theater," https://www.meta.com/quest/entertainment/?srsltid=AfmBOoqvCkxwIus14GHXILh_R3iXVQ_sGDbueLRFuzm15tqWJRnK9nvn, 2025.

[4] F. Roesner and T. Kohno, "Security and privacy in the metaverse," *IEEE Secur. Priv.*, vol. 22, no. 1, pp. 7–9, 2024. [Online]. Available: https://doi.org/10.1109/MSEC.2023.3333989

[5] M. Intelligence, "Virtual Reality (VR) Market Size & Share Analysis - Growth Trends And Forecast (2025 - 2030) Source: https://www.mordorintelligence.com/industry-reports/virtual-reality-market," https://www.mordorintelligence.com/industry-reports/virtual-reality-market, 2025.

[6] Meta, "Meta Quest Store," https://www.oculus.com/experiences/quest/, 2023.

[7] Valve, "SteamVR," https://store.steampowered.com/app/250820/SteamVR/, 2025.

[8] K. Cheng, M. Sim, T. Kohno, and F. Roesner, "User comprehension and comfort with eye-tracking and hand-tracking permissions in augmented reality," in *15th Symposium on Usable Security and Privacy (USEC 2025)*, San Diego, CA, USA, Feb 2025. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/usec25-5.pdf

[9] T. Hunter, "Surveillance will follow us into 'the metaverse,' and our bodies could be its new data source," https://www.washingtonpost.com/technology/2022/01/13/privacy-vr-metaverse/, 2022.

[10] K. Opsahl, "Come Back with a Warrant for my Virtual House," https://www.eff.org/deeplinks/2020/10/come-back-warrant-my-virtual-house, 2020.

[11] A. S. B., A. Agrawal, Y. Yao, Y. Zou, and A. Das, ""what are they gonna do with my data?": Privacy expectations, concerns, and behaviors in virtual reality," *Proc. Priv. Enhancing Technol.*, vol. 2025, no. 1, pp. 58–77, 2025. [Online]. Available: https://doi.org/10.56553/popets-2025-0005

[12] Y. Zhan, Y. Meng, L. Zhou, Y. Xiong, X. Zhang, L. Ma, G. Chen, Q. Pei, and H. Zhu, "Vpvet: Vetting privacy policies of virtual reality apps," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, 2024, pp. 1746–1760.

[13] M. Inc., "Supplemental Meta Platforms Technologies Privacy Policy," https://www.meta.com/legal/privacy-policy/, October 2025.

[14] G. Garrido, V. Nair, and D. Song, "Sok: Data privacy in virtual reality," in *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2023.

[15] M. R. Miller, F. Herrera, H. Jun, J. A. Landay, and J. N. Bailenson, "Personal Identifiability of User Tracking Data During Observation of 360-degree VR Video," *Scientific Reports*, vol. 10, no. 1, pp. 1–10, 2020.

[16] V. Nair, W. Guo, J. Mattern, R. Wang, J. F. O'Brien, L. Rosenberg, and D. Song, "Unique identification of 50,000+ virtual reality users from head & hand motion data," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 895–910.

[17] I. Jarin, Y. Duan, R. Trimananda, H. Cui, S. Elmalaki, and A. Markopoulou, "Behavr: User identification based on vr sensor data," *Proceedings on Privacy Enhancing Technologies*, 2025.

[18] Meta Horizon, "Launching your first ad campaign," https://developers.meta.com/horizon/resources/launch-ad-campaign/, 2024.

[19] P. Fung, Y. Bachrach, A. Celikyilmaz, K. Chaudhuri, D. Chen, W. Chung, E. Dupoux, H. Jégou, A. Lazaric, A. Majumdar, A. Madotto, F. Meier, F. Metze, T. Moutakanni, J. Pino, B. Terver, J. Tighe, and J. Malik, "Embodied AI agents: Modeling the world," *CoRR*, vol. abs/2506.22355, 2025. [Online]. Available: https://doi.org/10.48550/arXiv.2506.22355

[20] Reuters Staff, "Meta platforms to pay $1.4 billion to settle texas lawsuit over facial recognition data," 2024.

[21] Federal Trade Commission, "Ftc biometric enforcement actions and facial recognition policy guidance," https://www.ftc.gov/legal-library/browse/cases-proceedings, 2025.

[22] Texas Office of Attorney General, "Texas attorney general announces $1.4 billion settlement with meta under the capture or use of biometric identifier act (cubi)," https://www.texasattorneygeneral.gov/, 2024.

[23] F. D. B. . R. LLP, "Ftc sends a reminder to facial recognition tech companies to do what they say and say what they do," 2025.

[24] L. Schach, C. Rack, R. P. McMahan, and M. E. Latoschik, "Motion-based user identification across xr and metaverse applications by deep classification and similarity learning," *arXiv preprint arXiv:2509.08539*, 2025.

[25] V. Nair, G. M. Garrido, D. Song, and J. F. O'Brien, "Exploring the Privacy Risks of Adversarial VR Game Design," in *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2023.

[26] V. Nair, C. Rack, W. Guo, R. Wang, S. Li, B. Huang, A. Cull, J. F. O'Brien, M. Latoschik, L. Rosenberg, and D. Song, " Inferring Private Personal Attributes of Virtual Reality Users from Ecologically Valid Head and Hand Motion Data ," in *2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. IEEE Computer Society, Mar. 2024, pp. 477–484. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/VRW62533.2024.00094

[27] P. P. Tricomi, F. Nenna, L. Pajola, M. Conti, and L. Gamberi, "You can't hide behind your headset: User profiling in augmented and virtual reality," vol. 11, 2023, pp. 9859–9875. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3240071

[28] B. Games, "Beat Saber," https://www.beatsaber.com/, 2025.

[29] California Legislative Information, "California Consumer Privacy Act of 2018, Definition of Personal Information," 2018, CAL. CIV. Code § 1798.140. [Online]. Available: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[30] R. Miller, N. K. Banerjee, and S. Banerjee, "Combining Real-world Constraints on User Behavior with Deep Neural Networks for Virtual Reality (VR) Biometrics," in *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. IEEE, 2022, pp. 409–418.

[31] J. Lin and M. E. Latoschik, "Digital body, identity and privacy in social virtual reality: A systematic review," *Frontiers in Virtual Reality*, vol. 3, p. 974652, 2022.

[32] B. Rowe and D. Wood, "Are home internet users willing to pay isps for improvements in cyber security?" in *Economics of information security and privacy III*. Springer, 2012, pp. 193–212.

[33] R. McAmis, B. Durak, M. Chase, K. Laine, F. Roesner, and T. Kohno, "Handling identity and fraud in the metaverse," *IEEE Security & Privacy*, vol. 23, no. 1, pp. 27–37, 2024.

[34] H. X. Qin, Y. Wang, and P. Hui, "Identity, crimes, and law enforcement in the metaverse," *Humanities and Social Sciences Communications*, vol. 12, no. 1, pp. 1–15, 2025.

[35] A. H. Mhaidli, S. Rajaram, S. Fidan, G. Herakovic, and F. Schaub, "Shockvertising, malware, and a lack of accountability: Exploring consumer risks of virtual reality advertisements and marketing experiences," *IEEE Secur. Priv.*, vol. 22, no. 1, pp. 43–52, 2024. [Online]. Available: https://doi.org/10.1109/MSEC.2023.3332105

[36] Q. Zheng, S. Xu, L. Wang, Y. Tang, R. C. Salvi, G. Freeman, and Y. Huang, "Understanding safety risks and safety design in social vr environments," *Proceedings of the ACM on Human-Computer Interaction*, vol. 7, no. CSCW1, pp. 1–37, 2023.

[37] S. Abhinaya, A. Sabir, and A. Das, "Enabling developers, protecting users: Investigating harassment and safety in {VR}," in *33rd USENIX Security Symposium (USENIX Security 24)*, 2024, pp. 6561–6578.

[38] G. Freeman, S. Zamanifard, D. Maloney, and D. Acena, “Disturbing the peace: Experiencing and mitigating emerging harassment in social virtual reality,” *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW1, pp. 1–30, 2022.

[39] K. Schulenberg, G. Freeman, L. Li, and C. Barwulor, “” creepy towards my avatar body, creepy towards my body”: How women experience and manage harassment risks in social virtual reality,” *Proceedings of the ACM on Human-Computer Interaction*, vol. 7, no. CSCW2, pp. 1–29, 2023.

[40] G. Freeman, J. Frommel, R. L. Mandryk, J. Gugenheimer, L. Li, and D. Johnson, “Novel approaches for understanding and mitigating emerging new harms in immersive and embodied virtual spaces: A workshop at CHI 2024,” in *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems, CHI EA 2024, Honolulu, HI, USA, May 11-16, 2024*, F. F. Mueller, P. Kyburz, J. R. Williamson, and C. Sas, Eds. ACM, 2024, pp. 483:1–483:7. [Online]. Available: https://doi.org/10.1145/3613905.3636288

[41] T. Zhang, Z. Ye, A. T. Mahdad, M. M. R. R. Akanda, C. Shi, Y. Wang, N. Saxena, and Y. Chen, “Facereader: Unobtrusively mining vital signs and vital sign embedded sensitive info via AR/VR motion sensors,” in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023, Copenhagen, Denmark, November 26-30, 2023*. ACM, 2023, pp. 446–459.

[42] S. Hinduja and J. W. Patchin, “Metaverse risks and harms among us youth: Experiences, gender differences, and prevention and response measures,” *new media & society*, p. 14614448241284413, 2024.

[43] A. H. Mhaidli and F. Schaub, “Identifying manipulative advertising techniques in xr through scenario construction,” in *Proceedings of the 2021 chi conference on human factors in computing systems*, 2021.

[44] O. Figueira, R. Trimananda, A. Markopoulou, and S. Jordan, “Diffaudit: Auditing privacy practices of online services for children and adolescents,” in *Proceedings of the 2024 ACM on Internet Measurement Conference*, ser. IMC ’24. New York, NY, USA: Association for Computing Machinery, 2024, p. 488–504. [Online]. Available: https://doi.org/10.1145/3646547.3688416

[45] Steam, “Virtual Reality Titles,” https://store.steampowered.com/vr, July 2025.

[46] R. A. Lee, “Steam Statistics 2025: Users, Revenue, Top Games & Trends,” https://sqmagazine.co.uk/steam-statistics/, September 2025.

[47] Apple Inc., “Apple vision pro,” https://www.apple.com/apple-vision-pro/, 2025.

[48] Meta, “Meta Quest 3,” https://www.meta.com/quest/quest-3/, 2023.

[49] Meta, “This is Meta Quest Pro,” https://www.meta.com/quest/quest-pro/tech-specs/, 2023.

[50] T. K. O. W. Group, “The openxr specification: § 2.16. coordinate system,” https://registry.khronos.org/OpenXR/specs/1.0/html/xrspec.html#coordinate-system, April 2023.

[51] Meta, “Eye tracking on Meta Quest Pro,” https://www.meta.com/help/quest/articles/getting-started/getting-started-with-quest-pro/eye-tracking/, 2023.

[52] T. K. O. W. Group, “The openxr specification: § 12.28. xr_ext_eye_gaze_interaction,” https://registry.khronos.org/OpenXR/specs/1.0/html/xrspec.html#XR_EXT_eye_gaze_interaction, April 2023.

[53] Meta, “Getting started with Hand Tracking on Meta Quest headsets,” https://www.meta.com/help/quest/articles/headsets-and-accessories/controllers-and-hand-tracking/hand-tracking-quest-2/, 2023.

[54] T. K. O. W. Group, “The openxr specification: § 12.30. xr_ext_hand_tracking,” https://registry.khronos.org/OpenXR/specs/1.0/html/xrspec.html#XR_EXT_hand_tracking, April 2023.

[55] Meta, “Use Natural Facial Expressions on Meta Quest Pro,” https://www.meta.com/help/quest/articles/getting-started/getting-started-with-quest-pro/facial-expressions/, 2023.

[56] T. K. O. W. Group, “The openxr specification: § 12.53.7. conventions of blend shapes,” https://registry.khronos.org/OpenXR/specs/1.0/html/xrspec.html#_conventions_of_blend_shapes, April 2023.

[57] ——, “The openxr specification,” https://registry.khronos.org/OpenXR/specs/1.0/html/xrspec.html, April 2023.

[58] HTC Corporation, “Viveport: Vr games, apps, & videos,” https://www.viveport.com/, 2025.

[59] SteamDB, “Most played VR games,” https://steamdb.info/charts/?tagid=21978, February 2025.

[60] Valve, “Steam Store,” https://store.steampowered.com/, 2023.

[61] N. S. Suhaimi, C. T. B. Yuan, J. Teo, and J. Mountstephens, “Modeling the affective space of 360 virtual reality videos based on arousal and valence for wearable eeg-based vr emotion classification,” in *2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA)*. IEEE, 2018, pp. 167–172.

[62] Unity, “Unity Analytics,” https://docs.unity.com/ugs/manual/analytics/manual/overview, April 2025.

[63] V. Nair, L. Rosenberg, J. F. O’Brien, and D. Song, “Truth in motion: The unprecedented risks and opportunities of extended reality motion data,” *IEEE Security & Privacy*, vol. 22, no. 1, pp. 24–32, 2023.

[64] J. O’Hagan, J. Gugenheimer, F. Mathis, J. Bonner, R. Jones, and M. McGill, “A viewpoint on the societal impact of everyday augmented reality and the need for perceptual human rights,” *IEEE Secur. Priv.*, vol. 22, no. 1, pp. 64–68, 2024. [Online]. Available: https://doi.org/10.1109/MSEC.2023.3333988

[65] A. Paverd, A. Martin, and I. Brown, “Modelling and automatically analysing privacy properties for honest-but-curious adversaries,” *Tech. Rep*, 2014.

[66] California Legislative Information, “California Consumer Privacy Act of 2018,” 2018, CAL. CIV. Code § 1798. [Online]. Available: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[67] European Union, “General Data Protection Regulation,” 2016, official Journal of the European Union, L 119, 4 May 2016, pp. 1-88. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[68] S. P. Velayudhan and M. S. B. Somasundaram, “Compromised account detection in online social networks: A survey,” *Concurrency and Computation: Practice and Experience*, vol. 31, no. 20, p. e5346, 2019.

[69] IAB Tech Lab, “Data transparency standard,” https://iabtechlab.com/standards/data-transparency/, 2024, primary IAB Tech Lab Contact for Data Transparency: Hillary Slattery, Director of Programmatic, Product, support@iabtechlab.com.

[70] California Legislative Information, “California Penal Code Part 1, Title 13, Chapter 8, Section 530.55,” 2021. [Online]. Available: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=530.55

[71] E. Harrel and A. Thompson, “Victims of Identity Theft, 2021,” https://bjs.ojp.gov/document/vit21.pdf, 2023, U.S. Department of Justice Office of Justice Programs Bureau of Justice Statistics.

[72] V. Nair, V. Radulov, and J. F. O’Brien, “Results of the 2023 census of beat saber users: Virtual reality gaming population insights and factors affecting virtual reality e-sports performance,” pp. 1–19, May 2023. [Online]. Available: http://graphics.berkeley.edu/papers/Nair-ROT-2023-05/

[73] U. S. C. Bureau, “2020 informational questionnaire,” 2020. [Online]. Available: https://www2.census.gov/programs-surveys/decennial/2020/technical-documentation/questionnaires-and-instructions/questionnaires/2020-informational-questionnaire.pdf

[74] L. Breiman, “Random forests,” *Machine learning*, vol. 45, no. 1, pp. 5–32, 2001.

[75] T. Chen and C. Guestrin, “Xgboost: A scalable tree boosting system,” in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM, 2016, pp. 785–794.

[76] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, and T. Liu, “Lightgbm: A highly efficient gradient boosting decision tree,” in *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, December 4-9, 2017, Long Beach, CA, USA*, 2017, pp. 3146–3154.

[77] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, “Estimating the support of a high-dimensional distribution,” *Neural computation*, vol. 13, no. 7, pp. 1443–1471, 2001.

[78] D. W. Hosmer, S. Lemeshow, and R. X. Sturdivant, *Applied Logistic Regression*. John Wiley & Sons, 2013.

[79] M. R. Segal, “Machine learning benchmarks and random forest regression,” 2004.

[80] B. Azhagusundari, A. S. Thanamani *et al.*, “Feature selection based on information gain,” *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 2, no. 2, pp. 18–21, 2013.

[81] C. Shi, B. Wei, S. Wei, W. Wang, H. Liu, and J. Liu, “A quantitative discriminant method of elbow point for the optimal number of clusters in clustering algorithm,” *EURASIP journal on wireless communications and networking*, vol. 2021, no. 1, p. 31, 2021.

[82] “F1 score in machine learning,” https://encord.com/blog/f1-score-in-machine-learning/, 2025.

[83] "Understanding and applying the f1 score," https://arize.com/blog-course/f1-score/, 2025.
[84] D. Maclean, "The nist risk management framework: Problems and recommendations," pp. 207–217, 2017.
[85] N. S. C. R. Corner, "Colorblind Safe Color Schemes," https://www.nceas.ucsb.edu/sites/default/files/2022-06/Colorblind%20Safe%20Color%20Schemes.pdf, 2022.
[86] ALVR, "ALVR - Air Light VR," https://github.com/alvr-org/alvr, 2023.
[87] Steam, "CHARTS OVERVIEW," https://store.steampowered.com/charts/, April 2023.
[88] N. Kumar, "Virtual reality statistics 2025: Users & trends," https://www.demandsage.com/virtual-reality-statistics/, 2025.
[89] H. Hadan, D. M. Wang, L. E. Nacke, and L. Zhang-Kennedy, "Privacy in immersive extended reality: Exploring user perceptions, concerns, and coping strategies," in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–24.
[90] M. Sim, B. Radka, E. Yoshikawa, F. Roesner, K. Hugenberg, and T. Kohno, "To reveal or conceal: Privacy and marginalization in avatars," *Proceedings on Privacy Enhancing Technologies*, 2025.
[91] S. Radway and D. Votipka, "Identifying new challenges in the oculus permissions framework," in *Proceedings of the Symposium On Usable Privacy and Security (SOUPS) 2023, Poster Session*. USENIX Association, 2023.
[92] C. Dwork, *Differential Privacy*. Berlin: Springer, 2006, tutorial presentation at the International Conference on Automata, Languages and Programming (ICALP).
[93] Y. Wu, K. Yang, F. Roesner, T. Kohno, N. Zhang, and U. Iqbal, "Towards automating data access permissions in ai agents," 2025.
[94] V. Morel, L. H. Iwaya, and S. Fischer-Hübner, "Ai-driven personalized privacy assistants: a systematic literature review," *IEEE Access*, 2025.
[95] J. Liebers, M. Abdelaziz, L. Mecke, A. Saad, J. Auda, U. Gruenefeld, F. Alt, and S. Schneegass, "Understanding User Identification in Virtual Reality through Behavioral Biometrics and the Effect of Body Normalization," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–11.
[96] U. F. Government, "§ 46.111 Criteria for IRB approval of research (eCFR)," https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-46/subpart-A/section-46.111, April 2023.
[97] OpenAI, "ChatGPT," https://chatgpt.com/, 2026.
[98] Unity, "Eye Gaze Interaction," https://docs.unity3d.com/Packages/com.unity.xr.openxr@1.0/manual/features/eyegazeinteraction.html, April 2023.
[99] T. K. O. W. Group, "The openxr specification: § 12.31.6. conventions of hand joints," https://registry.khronos.org/OpenXR/specs/1.0/html/xrspec.html#convention-of-hand-joints, April 2023.
[100] P. Ekman and W. V. Friesen, "Facial Action Coding System: Manual," 1978.
[101] S. Bouchard and G. Labonté-Chartrand, *Emotions and the emotional valence afforded by the virtual environment*. IntechOpen, 2011.
[102] P. Sykownik, L. Graf, C. Zils, and M. Masuch, "The most social platform ever? a survey about activities & motives of social vr users," in *2021 IEEE virtual reality and 3D user interfaces (VR)*. IEEE, 2021, pp. 546–554.
[103] M. T. Deighan, A. Ayobi, and A. A. O'Kane, "Social virtual reality as a mental health tool: how people use vrchat to support social connectedness and wellbeing," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023, pp. 1–13.
[104] G. S. Parnell, H. W. Conley, J. A. Jackson, L. J. Lehmkuhl, and J. M. Andrew, "Foundations 2025: A value model for evaluating future air and space forces," vol. 44, no. 10. INFORMS, 1998, pp. 1336–1350.
[105] V. Tanwar, V. Anand, P. Aggarwal, M. Kumar, and G. R. Kumar, "Revolutionizing military training: A comprehensive review of tactical and technical training through augmented reality, virtual reality, and haptics," pp. 1–5, 2024.
[106] B. Farnsworth, "Facial Action Coding System (FACS),A Visual Guidebook," https://imotions.com/blog/learning/research-fundamentals/facial-action-coding-system/, October 2022.
[107] S. Han, J. R. Riddell, and A. R. Piquero, "Anti-asian american hate crimes spike during the early stages of the covid-19 pandemic," *Journal of interpersonal violence*, vol. 38, no. 3-4, pp. 3513–3533, 2023.
[108] P. Christen, D. J. Hand, and N. Kirielle, "A review of the f-measure: its history, properties, criticism, and alternatives," *ACM Computing Surveys*, vol. 56, no. 3, pp. 1–24, 2023.

Appendices

A. Details on Methodology

In this appendix, we elaborate on our methodology, as introduced in Section III, including the sensor data structure (VII-A1), VR apps we studied (VII-A2), VR app groups (VII-A3), sensor data collection practices (VII-A4), and the VR User Profiling Taxonomy (VII-A5).

1) Details on Sensor Data Structure: Among the sensor groups, Body Motion (BM) includes the position, rotation, angular and linear velocity of the two controllers, and only the position and rotation of the headset [50]. This group has been studied in prior works [15]–[17], [26]. Eye Gaze (EG) includes the position and rotation of both left and right eyes (7 values per eye), as specified by OpenXR [52], [98]. Hand Joints (HJ) consists of 26 articulated joints per hand, as defined by the OpenXR `XrHandJointEXT` structure [99] and include the position and rotation of each joint [54]. Finally, Facial Expression (FE) includes 64 facial expression elements tracked by the OpenXR standard, following the `XrFaceExpressionFB` structure [56]. These elements map to 31 Facial Action Units (AUs) in the FACS system [100], each representing a facial muscle movement.

2) More about VR Apps: The VR ProfiLens study is based on 10 apps selected from the SteamVR store [60], as listed in Table III and discussed in Section III-B. Starting from the top 100 apps listed under "Most Played VR Games" on Steam [59], we exclude apps based on user discomfort, such as horror or violent genres, in accordance with 45 CFR § 46.111(a)(1) to minimize participant risk [96].

3) Details on App groups: We define app groups based on similarities in activities, which mostly influence the BM and HJ sensor groups, and emotional (valence-arousal [61]) states, which mostly influence the FE sensor group as discussed in Section III-B2 and listed in Table IV. Details are as follows:

Social App Group. Social apps focus primarily on facilitating real-life social experiences through an enhanced sense of ownership over an avatar within a 3D environment, distinguishing them from traditional 2D text/image-based social media. Social apps facilitate various forms of social interactions [102] and contribute to social engagements [103]. Users engage in various activities within these apps, including walking, waving at friends, handshakes, conversations, and interacting with each other (e.g., hangouts). The emotional state associated with social apps is typically positive, as users are expected to be relaxed and happy while using them. The social apps in our study are a_1, RecRoom, and a_2, VRChat.

Flight Simulation App Group. Flight simulation primarily resembles flying an airplane, helicopter, or other flying vehicle. These apps can be used broadly in air force training [104], military education [105], and entertainment purposes. The app-specific activities can include but are not limited to holding a joystick, interacting with a control-panel and buttons, and looking at the surrounding environment to avoid possible crashes. The arousal/valence mostly tends to be negative (fear/stress) depending on the user, or there can be low

TABLE III: **List of 10 selected consumer VR apps ($a_1, ..., a_{10}$) for VR ProfiLens study and corresponding app activities.** See Section III-B and Appendix VII-A2 for app selection details.

App No.	App Title	App Activities
a_1	Rec Room	Explore welcome room or virtual recreation center; Users use bare hand for waiving or handshaking.
a_2	VRChat	Explore virtual scene by walking around; The user will wave or greet with bare hands.
a_3	DCS World Steam Edition	Fly a military aircraft: the user first control the aircraft with controllers and then with bare hands.
a_4	X-Plane 11	Fly a civilian aircraft and interact with the virtual objects with the controllers and with bare hands.
a_5	Job Simulator	Explore office-worker simulation; The user is to interact with a virtual office objects with controllers and then with bare hands.
a_6	Tabletop Simulator	Move chess pieces: first with the controllers and then with bare hands.
a_7	Gorilla Tag	Perform gorilla movement (walk like gorilla to explore the environment): first with the controllers, then with bare hands.
a_8	Beat Saber	Cut objects with light-sabers: with the controllers and then with bare hands.
a_9	No Man's Sky	Explore an unknown planet by teleporting; the user interacts with a laser gun (shoot targets) with controllers and then with bare hands.
a_{10}	Elven Assassin	Shoot arrows to monsters: with the controllers and then with bare hands.

TABLE IV: **Grouping apps ($a_1, ..., a_{10}$) listed in in Table III based on their similarity of activities and emotional states (arousal/valence [101]).** *Sensor Groups:* BM, EG, HJ, FE. *Emotional States:* LA = low arousal, HA = high arousal, PV = positive valence, NV = negative valence. Important sensors is based on our app grouping, where each sensor is relevant with app specific activities.

App Groups	App No.	Important Sensors	Scope	App-Specific Activities	Arousal/Valence
Social	a_1, a_2	BM, EG, FE, HJ	Social Media	Walking, waving, socializing and sightseeing	LA/PV, HA/PV
Flight Simulation	a_3, a_4	BM, HJ	Train./Education	Holding onto the airplane control stick, interacting with control panel/buttons in an airplane cockpit	LA/NV, HA/NV, LA/PV
Interactive Navigation	a_5, a_6	BM,HJ	Office/Entertainment	Grabbing, moving objects i.e., short time interaction with objects	Neutral, LA/PV, LA/NV
Knuckle-walking	a_7	BM, HJ, FE	Social Media	Walking using an open fist like a gorilla	LA/PV, HA/PV, LA/NV
Rhythm	a_8	BM, HJ	Entertainment	Dancing-like moves and cutting objects in quick pace	All
Shooting & Archery	a_9, a_{10}	BM, HJ	Train./Education.	Grabbing/holding a gun/arrow, aiming+shooting objects	LA/NV, HA/NV

arousal/positive valence (surprise). The flight apps in our study are a_3, DCS World Steam Edition, and a_4, X-Plane 11.

Interactive Navigation App Group. Interactive navigation apps refer to apps in which the user has frequent interaction with virtual objects using their hands, controllers, and/or eyes. The app-specific activities include but are not limited to grabbing, pressing/moving objects, interacting with virtual keyboard/virtual office objects, cooking, and playing chess. The arousal/valence should be neutral as users tends to concentrate on activities. The interactive navigation apps in our study are a_5, Job Simulator, and a_6, Tabletop Simulator.

Knuckle-Walking App Group. This group includes apps where players imitate gorilla-like locomotion, using hand and knuckle positions to walk and jump through the environment. Regarding the valence/arousal, it is similar to the social app group, as the app is multiplayer and people explore the environment and go on adventures together. However, this kind of app includes climbing and jumping from tall structures, and thus can induce negative arousal/valence as well. The knuckle-walking app in our study is a_7, Gorilla Tag.

Shooting App Group. The shooting group refers to apps that involve simulated shooting activities. This typically includes apps in which players engage in activities such as aiming at and hitting targets with firearms. The arousal/valence state is most likely to be negative, as it involves looking for targets or enemies and shooting at them, e.g., a_9, No Man's Sky.

Archery App Group. This app group simulates archery experiences, where users shoot at targets with bows and arrows, track targets with head movements, and looking around the environment. It has similarity as the shooting group, however, it requires users to hold a virtual bow and arrow, that is different than holding a virtual gun, resulting in distinct HJ/BM characteristics. The arousal/valence state is most likely to be negative as it involves shooting at targets/enemies, similarly to the shooting group, e.g., a_{10}, Elven Assassin.

4) Details on Sensor Data Collection Practices: We examine Oculus Quest [6] and SteamVR [7] apps data collection practices (introduced in Section III-B3). We selected 20 apps based on popularity and relevance to our app groups, then manually inspected their sensor data collection and privacy policies to determine stated purposes of use. We find that data-collection permissions vary across platforms. SteamVR [7] apps require no runtime permissions and offer no disclosure of sensor data collection in their privacy policies. For Oculus Store apps, social apps collect data from all four sensor groups to support realistic avatars, and their policies state that this data is used for app functionality under Meta's standard policy. Interactive navigation apps disclose collecting hand joint and body motion data, aligning with app-specific activities (see Section III-B2). However, apps like Virtual Desktop and Meta Horizon Workstation also mention facial and eye tracking data collection, which aligns less with purposes of their app groups. Notably, some interactive navigation apps (e.g., Job Simulator, Lost Recipes) either lack privacy disclosures or state that they collect data for advertising and share it with third parties. Flight and shooting apps collect both body-motion and voice data, whereas rhythm apps collect only body-motion. Specifically, apps such as Shuttle Commander and Pavlov VR disclose that they use collected data for marketing purposes. Shuttle Commander specifies that this usage is restricted to first-party marketing only.

5) Details on the VR User Profiling Taxonomy: In this section, we discuss further details regarding how we extracted and organized attributes and categories from the CCPA definition of personal information and included them in our taxonomy, as discussed in Section III-D1. Some of the categories within the

TABLE V: **Attributes Obtained from VR User Profiling Taxonomy for our VR ProfiLens Study.** The **Class:Statistics** column represents each class name along with its corresponding statistics. If an attribute is continuous in nature, we use regression and mark the **Class:Statistics** field as N/A. If two attributes are highly correlated and yield the same response, we mark the response as N/P. The **Selection** column indicates whether an attribute is selected (✓) or filtered out (✗), with the corresponding reason provided for exclusion.

Category	**Attribute**	**Class: Statistics**	**Selection**
Demographics	Sex/Gender[1,2,4,5,6]	male: 55%, female: 45%	✓
	Age / Date of Birth[1,2,3,4,5,6]	< 30 : 65%, ≥30: 35%, no-res.: 10%	✓
	Religion[4,5,6]	religious:25%,non-religious:65%,no-res:10%	✗: does not map
	Marital Status[1,2,5,6]	married:35%, unmarried:65%, no-res.:10%	✓
	Ethnicity/National Origin[4,5,6]	Asian:65%, others:35%	✓
	Race[4,5,6]	Asian:65%, others:35%	✗: Same response as Ethnicity
Personal History	Education (Highest Level)[1,5,6]	<graduate:0%, graduate:100%	✗: Non-Discriminative Response
	Academic Interests[1,5,6]	CS/EECS:100%	✗: Non-Discriminative Response
	Income (USD)[1,5,6]	≤40k:50%,>40k:50%	✗
Anthropometrics	Hand shape/length[3,5,6]	N/A	✓
	Face length[3,5,6]	N/A	✓
	Height[3,5,6]	N/A	✓
	Arms Length[3,5,6]	N/A	✓
	IPD[3,5,6]	respond:50%, non-res:50%	✗: Limited Response by users
	Wingspan[3,5,6]	respond:40%, non-res:60%	✗: Limited Response by users
	Weight[3,4,6]	N/A	✓
	BMI[3,6]	normal: 55%, overweight/obese: 45%	✓
Health	Physical Fitness[1,4,5,6]	fit:45%, unfit:45%, no-res.:10%	✓
	Illness (COVID)[1,5,6]	yes: 5%, no: 80%, no-res.:15%	✗: Limited Response by users
	Color blindness[1,5,6]	yes:0%, no:90%, no-res.:10%	✗: Non-Discriminative Response
	Close / Distance vision and lenses[1,5,6]	yes:35%, No:55% no-res.:5%	✓
	Mental disability[4,5,6]	yes:0%, no:100%	✗: Non-Discriminative Response
	Physical disability[4,5,6]	yes:0%, no:100%	✗: Non-Discriminative Response
	Anxiety[4,6]	yes:45%, no:55%	✓
	Stress[4,6]	yes: 65%, no:20%, no-res.:15%	✓
	Height phobia[4,6]	yes:45%, no:50%, non-res.:5%	✓
	Motion sickness[4,6]	yes:30%, no:65%, no-res.:5%	✓
	Sleepiness[5,6]	yes: 0%, no: 100%	✗: Non-Discriminative Response
Interests & Behaviors	Political orientation[1,4,5,6]	respond:50%, no-res.:50%	✗: Limited Response
	Musical instrument experience[1,5,6]	N/P	✗
	Dance experience[1,5,6]	N/P	✗
	VR experience[6]	experienced:45%, inexperienced:55%	✓
	Athletics/sports experience[1,4,5,6]	N/P	✗: high correlation w/ another class
	Shooting experience[1,4,6]	yes:45%, no:55%	✓
	Violence tolerance[1,4,6]	yes: 45%, no: 45%, no-res.:10%	✓
	Alcohol Consumption[1,5,6]	yes:30%,no/occasionally:60%, no-res.:10%	✓
	Caffeinated item consumption[1,5,6]	high: 35%, moderate:60%, no-res.:5%	✓
	Social media usage[4,6]	Active:60%, Inactive:40%	✓
	Attention / Concentration[5,6]	good: 65%, poor: 35%	✓
	Handedness[5,6]	left:0%, right:90%, no-res.:10%	✗: Non-Discriminative Response
	Problem Solving Abilities[6]	confident:70%, moderate:30%	✓
	Working Preferences (Remote Working)[6]	N/P	✗: high correlation w/ another class
	Organizational Preferences[6]	organized: 80%,unorganized:20%	✓
	Activity Preference (Indoor/Outdoor)[6]	indoor:50%,outdoor:50%	✓
	Introvert/Extrovert (Extraversion)[6]	Introvert:45%, Extrovert:50%, no-res.:5%	✓
	Openness[6]	open:60%, neutral:40%	✓
	Conscientiousness[6]	N/P	✗:high correlation w/ another class
	Emotional stability[6]	stable:50%, unstable:45%, no-res.0%	✓

CCPA definition include references to other CCPA definitions or legal texts, such as sensitive personal information, biometric information, personally identifiable information defined in the Family Educational Rights and Privacy Act (FERPA)[9], and personal information described in subdivision (e) of Section 1798.80. For such cases, we extracted all the attributes from those separate definitions and either moved them to other more specific categories due to contextual similarities (e.g., sensitive personal information in the CCPA includes precise geolocation, which we moved to the existing geolocation category) or removed them because the attribute already existed in another category (e.g., name and address appear in both the FERPA definition and the identifiers category, so we kept them only in the identifiers category as it is more specific). For all other categories in the CCPA definition of personal information that did not reference other definitions, we included the categories and their attributes as stated in the legal text.

[9] 20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99

TABLE VI: **Feature Interpretations of Body Motion (BM) Sensor Group.** Based on the OpenXR data structures [50].

Feature Interpretation	Actual Feature Name
Head rotation	Quatx Headset, Quaty Headset, Quatz Headset, Quatw Headset
LR (Left-Right) head-movement Pos	Position.x Max Headset, Position.x Min Headset, Position.x Mean Headset, Position.x Std Headset, Position.x Median Headset
Max standing/sitting height	Position.y Max Headset
FB (Forward-Backward) head-movement Pos	Position.z Headset
Headset height other stats.	Position.y (Min, Mean, Std, Median) Headset
Left Controller rotation	Quatx Left Controller, Quaty Left Controller, Quatz Left Controller, Quatw Left Controller
Left Controller span	Position.x Left Controller
Left Controller height	Position.y Left Controller
Left Controller movement	Position.z Left Controller
Left Controller linear velocity	Lin0 Left Controller, Lin1 Left Controller, Lin2 Left Controller
Left Controller angular velocity	Ang0 Left Controller, Ang1 Left Controller, Ang2 Left Controller
Right Controller rotation	Quatx Right Controller, Quaty Right Controller, Quatz Right Controller, Quatw Right Controller
Right Controller span	Position.x Max Right Controller, Position.x Min Right Controller, Position.x Mean Right Controller, Position.x Std Right Controller, Position.x Median Right Controller
Right Controller height	Position.y Right Controller
Right Controller movement	Position.z Right Controller
Right Controller linear velocity	Lin0 Right Controller, Lin1 Right Controller, Lin2 Right Controller
Right Controller angular velocity	Ang0 Right Controller, Ang1 Right Controller, Ang2 Right Controller

TABLE VII: **Feature Interpretations of Facial Expression (FE) Sensor Group.** Based on the OpenXR [56] feature indices and Facial Action Coding System (FACS) [106] system.

Feature Interpretation	Element Number	Feature Interpretation	Element Number
Happy	[5], [6], [33], [34]	Surprise	[23], [24], [25], [58], [59], [60], [61]
Anger	[1], [2], [60], [61], [29], [30], [49], [50]	Contempt	[33], [11], [12]
Disgust	[56], [57], [31], [32], [52], [53]	Fear	[1], [2], [23], [24], [25], [29], [30], [31], [32], [43], [44], [58], [59], [60], [61]
Sadness	[23], [24], [1], [2], [31], [32]	NEFE: Cheek Puff	[3], [4]
NEFE: Cheek Suck	[7], [8]	NEFE: Chin Raiser	[9], [10]
NEFE: Eyes Closed	[13], [14]	NEFE: Eyes Look Down	[15], [16]
NEFE: Eyes Look Left	[17], [18]	NEFE: Eyes Look Right	[19], [20]
NEFE: Eyes Look Up	[21], [22]	NEFE: Jaw Sideways	[26], [27]
NEFE: Jaw Thrust	[28]	NEFE: Lip Funneler	[35], [36], [37], [38]
NEFE: Lip Pressor	[39], [40]	NEFE: Lip Pucker	[41], [42]
NEFE: Lip Suck	[45], [46], [47], [48]	NEFE: Lips Toward	[51]
NEFE: Mouth Stretch	[54], [55]	NEFE: Upper Lip Raiser	[62], [63]

TABLE VIII: **Feature Interpretations of Hand Joint (HJ) Sensor Group.** Based on the list of 26 joints in the `handData` data structure per OpenXR convention [54].

Feature Interpretation	Joint No. & Type	Feature Interpretation	Joint No. & Type
Palm (rotation/position)	[1] rotation/position	Wrist (rotation/position)	[2] rotation/position
Thumb Metacarpal (rotation/position)	[3] rotation/position	Thumb Proximal (rotation/position)	[4] rotation/position
Thumb Distal (rotation/position)	[5] rotation/position	Thumb Tip (rotation/position)	[6] rotation/position
Index Metacarpal (rotation/position)	[7] rotation/position	Index Proximal (rotation/position)	[8] rotation/position
Index Intermediate (rotation/position)	[9] rotation/position	Index Distal (rotation/position)	[10] rotation/position
Index Tip (rotation/position)	[11] rotation/position	Middle Metacarpal (rotation/position)	[12] rotation/position
Middle Proximal (rotation/position)	[13] rotation/position	Middle Intermediate (rotation/position)	[14] rotation/position
Middle Distal (rotation/position)	[15] rotation/position	Middle Tip (rotation/position)	[16] rotation/position
Ring Metacarpal (rotation/position)	[17] rotation/position	Ring Proximal (rotation/position)	[18] rotation/position
Ring Intermediate (rotation/position)	[19] rotation/position	Ring Distal (rotation/position)	[20] rotation/position
Ring Tip (rotation/position)	[21] rotation/position	Little Metacarpal (rotation/position)	[22] rotation/position
Little Proximal (rotation/position)	[23] rotation/position	Little Intermediate (rotation/position)	[24] rotation/position
Little Distal (rotation/position)	[25] rotation/position	Little Tip (rotation/position)	[26] rotation/position

B. *Details on Experimental Setup*

We elaborate on our experimental setup discussed in Section IV, including sensor data collection (VII-B1), survey protocol (VII-B2), and attributes and their statistics (VII-B3) here.

1) Sensor Data Collection: In the sensor data collection phase, each participant wore the Quest Pro and interacted with all 10 apps, first using controllers and then using bare hands. During app interaction, all sensor data (BM with controller, HJ without controller, FE, EG) are being collected using the set-up from [17]. This data collection setup employs the Meta VR device, called Quest Pro, and instruments parts of ALVR's source code that receives sensor data from the Quest Pro. Note that ALVR [86] is an open-source software that can run VR apps on a PC, and the sensor data sent from Quest Pro are received by ALVR as time series.

Our data collection process was based on real-world scenarios, minimizing control and bias created by a lab environment. For example, in social apps (a_1, a_2) users engage in multi-user environments (i.e., public rooms) where they can naturally interact with other users (e.g., waving, talking) and explore app environments (e.g., walking like humans or gorillas). Social apps support more immersive and realistic interactions than 2D platforms, so we focus on natural user activities driven by their in-app social environments.

2) Survey Protocol: Details on demographics, personal history, and anthropometric are discussed in Section IV-A2. Here, we focus on health and user interests/behavior as follows:

Health. Attributes were collected through a structured post-session survey response. Attributes such as chronic illness, motion sickness, stress, height phobia were derived from these responses, e.g., participants rated their physical fitness level and reported whether they experienced stress during our study.

User Interests & Behavior. Participants self-reported their interests, experiences, and personality traits. These included political orientation, prior VR experiences, among others; e.g., to gauge social media use, we asked how frequently participants engage with social media (e.g., Instagram).

3) Final Attributes: The demographic distributions of the participants are as follows: female is 9 (45%), male is 11 (55%). The age ranges is between 20-40 with a median age of 26 and mean age of ~ 28. The participants' heights range from 154–190 cm, with a median height of 174 cm and a mean

TABLE IX: **User Profiling Using FE across 7 App Groups.** The color code, designed to be color-blind friendly [85], represents four risk levels based on F1: High/Very High Risk (F1=80-100%, purple), Moderate-High Risk (F1=70-80%, orange), Moderate Risk (F1=50-70%, light-blue), and Low Risk ($F1 < 50\%$, gray) as per V-A. Attribute superscripts indicate associated threats according to our threat scenarios (see Section III-C2) and taxonomy (see Section III-D6).

Attribute Groups	**Attributes**	**App Groups**						
		Social	Flight	Shoot	Rhythm	IN	KW	Archery
Demographics	Gender^{1,2,4,5,6}	68	78	70	70	72	65	71
	Age^{1,2,3,4,5,6,F}	88	65	80	71	78	73	75
	Ethnicity^{4,5,6,S}	80	78	86	82	85	85	80
	Marital status^{1,2,5,6}	49	47	43	52	55	55	40
Anthropometrics	Height^{3,5,6}	60	48	45	57	32	30	68
	Reaction Time^{3,5,6}	70	60	70	90	80	80	80
	Face Length^{3,5,6}	65	56	70	75	80	71	75
	Arm Length^{3,5,6}	52	54	52	50	37	46	52
	Weight^{3,4,6}	39	46	45	30	45	40	35
	BMI^{3,6}	68	65	70	66	70	79	65
Health	Close / Distance vision and lenses^{1,5,6}	64	59	54	63	68	69	59
	Physical fitness^{1,4,5,6}	55	63	65	45	52	61	65
	Anxiety^{4,7,8}	78	71	70	82	78	70	65
	Stress^{4,6}	85	85	90	82	90	94	90
	Height phobia^{4,6}	61.5	65	73	62	59	57	55
	Motion sickness^{4,6}	45	50	47	45	45	55	40
User Interests & Behaviors	Problem Solving Abilities^{6}	48	48	42	40	49	44	53
	Alcohol consumption^{1,5,6}	68	69	67	70	78	67	62
	VR Experience^{5,6}	67	65	70	73	65	76	66
	Activity preference^{6}	53	48	63	43	50	32	58
	Shooting Experiences^{1,4,6}	66	74	76	69	73	79	75
	Caffeinated item consumption^{1,5,6}	75	66	64	77	75	79	69
	Concentration^{3,6}	46	45	55	40	45	55	45
	Violence tolerance^{1,4,6}	68	70	75	57	67	72	62
	Introvert/Extrovert^{6}	70	60	62	58	65	60	56
	Organized/Unorganized^{6}	82	90	81	97	92	76	80
	Social media usage^{4,6}	43	49	71	56	49	62	61
	Openness^{6}	80	73	74	84	73	81	80
	Emotional stability^{6}	68	71	86	65	76	68	69

of ~ 172 cm, weights range from 57–118 kg, with a median weight of 73.5 kg and a mean of ~ 74.6 kg. Among them, 11 (55%) of users have prior VR experiences, 9 (45%) was trained during our study by the authors. More details about user attributes and their statistics are shown in Table V.

4) Classification: As discussed in Section IV-C2, our attack classifier is designed to demonstrate adversarial capability, while aligning with the distribution of participant survey responses. Our attack classifier design is guided by adversarial goals defined in our threat model (see Section III-C), with each attribute mapped to relevant threat scenarios as indicated by its superscripts in the taxonomy. For example, *Sex/Gender* (Men 55%, Women 45%; superscripts ^{1,2,4,5,6}) is modeled as a binary classifier aligned with targeted advertising and profiling threats, where coarse gender inference is sufficient for advertiser-driven decision making (superscripts ^{1,2}). Similarly, *Ethnicity/National Origin* (Asian 65%, Others 35%; superscripts ^{4,5,6}) is modeled as Asian vs. Others, reflecting plausible adversarial goals such as discriminatory targeting or safety-and-harm risks (e.g., Asian hate crime [107] or harassment), corresponding to the safety and harm threat scenario (see Section III-C2).

Classifier granularity is further constrained by the participant distribution. For *age*, while adversaries may aim to infer child vs. adult (e.g., for age gating or regulatory evasion), our cohort contains no participants under 18. We therefore demonstrate a coarse age split (< 30 vs. ≥ 30), which is commonly used in advertising taxonomies [69] and remains meaningful for targeted advertising threats. These design choices reflect proof-of-concept demonstrations rather than exhaustive evaluation of all adversarial goals.

C. Data Processing and Feature Engineering

1) Sensor Data Processing: Sensor data is received as a time series, segmented into fixed 1-second intervals, referred to as blocks. We summarize the information in the time series of each block with a vector of five statistics, i.e., maximum, minimum, mean, standard deviation, and median. This summarization was originally proposed in [15] for body motion and was also used in [16], [17].

2) Feature Engineering: Each sensor group comprises multiple features, defined according to OpenXR standards [50] and further processed through our data processing pipeline (see Section VII-C1). There are 33 BM sensor readings, including

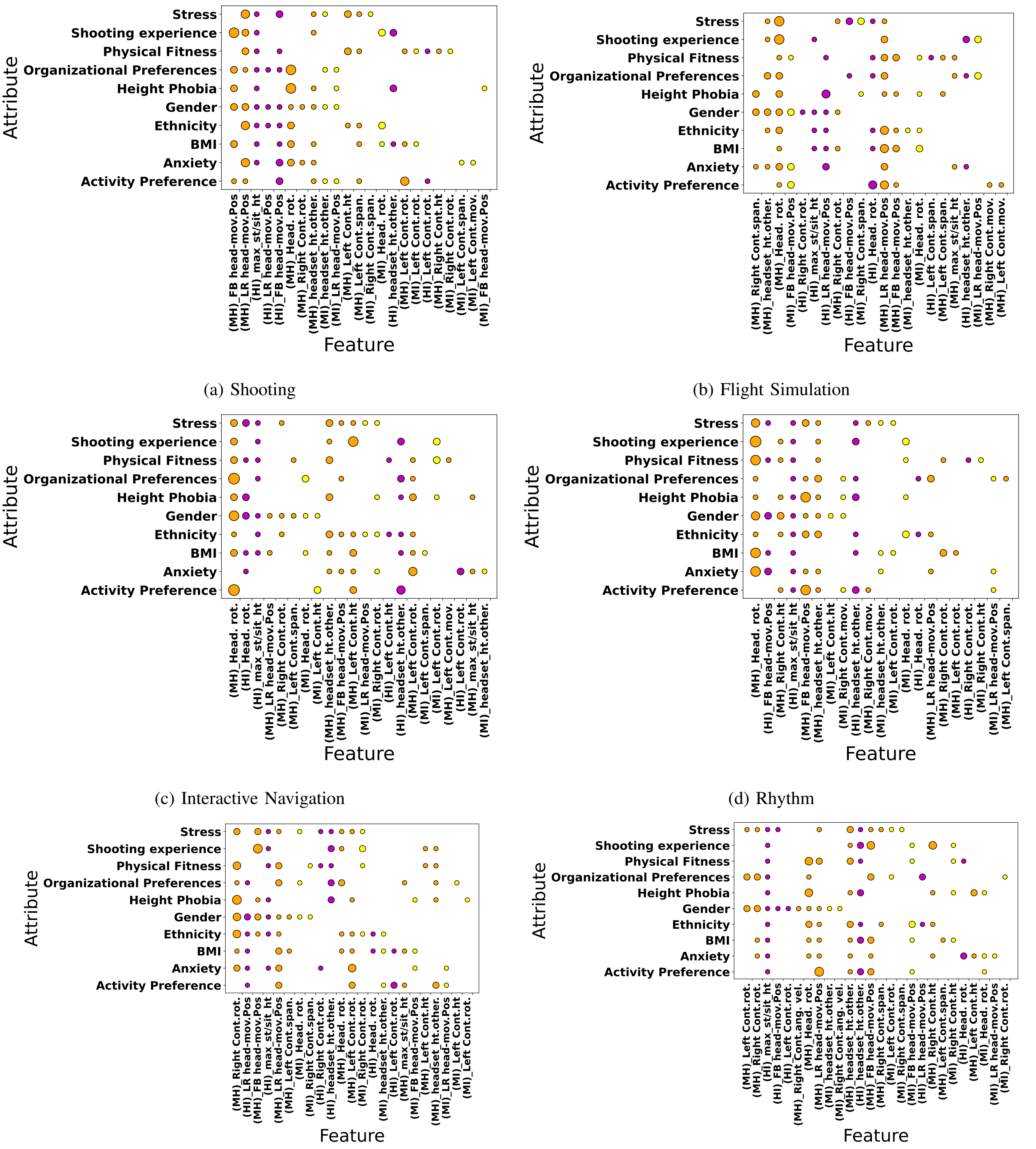
3 position and 4 rotation from controllers and the headset, and an additional 3 linear and 3 angular velocity readings for each controller. After the data processing , each sensor reading yields 5 statistics, resulting in 165 BM features per block. Similarly for EG, there are 7 readings (3 position and 4 rotation) for each eye, providing 46 features. For HJ, there are 182 readings per hand that describe 3 position and 4 rotation readings from each of 26 joints [54]. Finally, we have 364 sensor readings for 2 hands and 1820 features after data processing step. FE comprises 64 readings [56] to capture facial expression and emotions. We refer to each sensor reading as an "element" (See Appendix VII-C3, Table VII). After data processing, we obtain 320 features per block.

3) Feature Analysis and Interpretation: Here, we elaborate on our feature analysis and interpretation approaches, as discussed in Sections IV-B and IV-D. While prior works have applied ad hoc feature sets to support their evaluations, there is no standardized or reproducible process for transforming sensor group features into semantically coherent descriptors. Moreover, previous studies often focused on a single attribute (e.g., identification [15]–[17]) or did not provide any detailed analysis of the feature space [26]. Although such approaches may be suitable for domains with limited dimensionality, drawing conclusions across multiple dimensions (attribute vs. app vs. sensors) requires a more systematic and automated method. For BM, we recall our 165 features from Section VII-C2. We reorganized these 165 attributes into 17 interpretable features that are more suitable to capture users' app-specific activities and characteristics within the context of the BM. For example, the maximum positional features from the headset can be interpreted as the user's height. Detailed descriptions of raw features to interpretable features are described in Table VI. For the FE, we reorganized these 320 features into 24 interpretable features that are more suitable to capture users' app-specific emotion/valence state as well as facial expression within the context of the FE sensor group (see Table VII). For the HJ, we recall our 1820 features from Section VII-C2. We reorganized these 1820 features into 52 interpretable features as described in Table VIII.

D. Evaluations

1) More Detailed on Risk Assessments: As described in Section V-A, we rank user attributes by profiling risk using the F1 score, which jointly captures precision and recall and reflects adversarial inference strength. Our risk mapping follows industry ML evaluation practices (e.g., Encord [82], Arize [83]) and government risk assessment frameworks (e.g., NIST SP 800-30 and the NIST AI RMF [84]). Consistent across these sources, F1 scores of 80–100% indicate consistently reliable inference and are classified as High/Very High Risk, while F1 scores below 50% reflect unreliable inference and are classified as Low Risk. Although F1 scores above 70% are often considered strong in general ML practice [108], industry and NIST frameworks reserve the highest risk classification for performance above 80%. To avoid conflating emerging and consistently exploitable inference, we split the intermediate range: 50–70% is classified as Moderate Risk, and 70–80% as Moderately High Risk, capturing meaningful differences in adversarial capability.

2) Results: This appendix outlines additional results for user attribute inferences and feature analysis to support Section V. The inference results for single-sensor adversaries (FE, EG, and HJ) correspond to Tables IX, X, and XI, and for multi-sensor adversaries (BM and FE, and BM, FE, and EG) correspond to Tables XII and XIII. Feature analysis results for attributes with high or moderately high risk across each app group per sensor groups in Figure 3, 4 and 5 for BM, FE and HJ respectively.



(a) Shooting

(b) Flight Simulation

(c) Interactive Navigation

(d) Rhythm

(e) Knuckle Walking

(f) Archery

Fig. 3: **Feature Analysis for BM Group across Different App Groups.** Y-axis provides attribute names, X-axis represents corresponding top features for attribute inferences. Color code represents feature ranking: HI (high, pink), MH (medium-high, orange), MI (medium, yellow), while Circle size reflects feature frequency (i.e., larger circles, higher occurrences).

TABLE X: **User Profiling Using EG Sensor Data Across 7 App Groups.** (Color code representation similar as Table IX).

Attribute Groups	Attributes	App Groups						
		Social	Flight	Shoot	Rhythm	IN	KW	Archery
Demographics	Gender[1,2,4,5,6]	63	62	62	66	55	61	58
	Age[1,2,3,4,5,6,F]	62	52	49	58	63	39	62
	Ethnicity[4,5,6,S]	42	53	69	58	62	61	47
	Marital status[1,2,5,6]	58	42	58	46	48	59	60
Anthropometrics	Height[3,5,6]	56	53	56	59	58	56	56
	Reaction Time[3,5,6]	45	50	40	56	44	57	52
	Face Length[3,5,6]	39	31	49	16	45	38	49
	Arm Length[3,5,6]	53	58	54	40	50	59	54
	Weight[3,4,6]	56	53	56	51	58	56	56
	BMI[3,6]	49	59	47	60	52	49	55
Health	Close / Distance vision and lenses[1,5,6]	53	55	48	45	68	57	48
	Physical fitness[1,4,5,6]	53	57	52	67	48	58	38
	Anxiety[4,7,8]	57	65	51	66	60	57	54
	Stress[4,6]	46	48	51	64	55	69	65
	Height phobia[4,6]	49	54	37	62	55	57	49
	Motion sickness[4,6]	47	48	45	42	54	54	50
User Interests & Behaviors	Problem Solving Abilities[6]	42	44	41	53	48	44	43
	Alcohol consumption[1,5,6]	52	50	52	63	45	43	40
	VR Experience[5,6]	38	54	48	59	49	64	52
	Activity preference[6]	44	59	47	61	55	45	33
	Shooting Experiences[1,4,6]	55	65	60	57	47	57	56
	Caffeinated item consumption[1,5,6]	59	41	39	49	45	58	52
	Concentration[3,6]	66	42	42	42	46	43	43
	Violence tolerance[1,4,6]	67	56	57	60	58	71	63
	Introvert/Extrovert[6]	60	53	45	53	70	57	55
	Organized/Unorganized[6]	52	48	61	66	50	57	55
	Social media usage[4,6]	48	46	42	46	48	48	41
	Openness[6]	62	58	60	56	52	47	36
	Emotional stability[6]	26	39	64	62	25	55	62

TABLE XI: **User Profiling Using HJ Sensor Data Across 7 App Groups.** (Color code representation similar as Table IX).

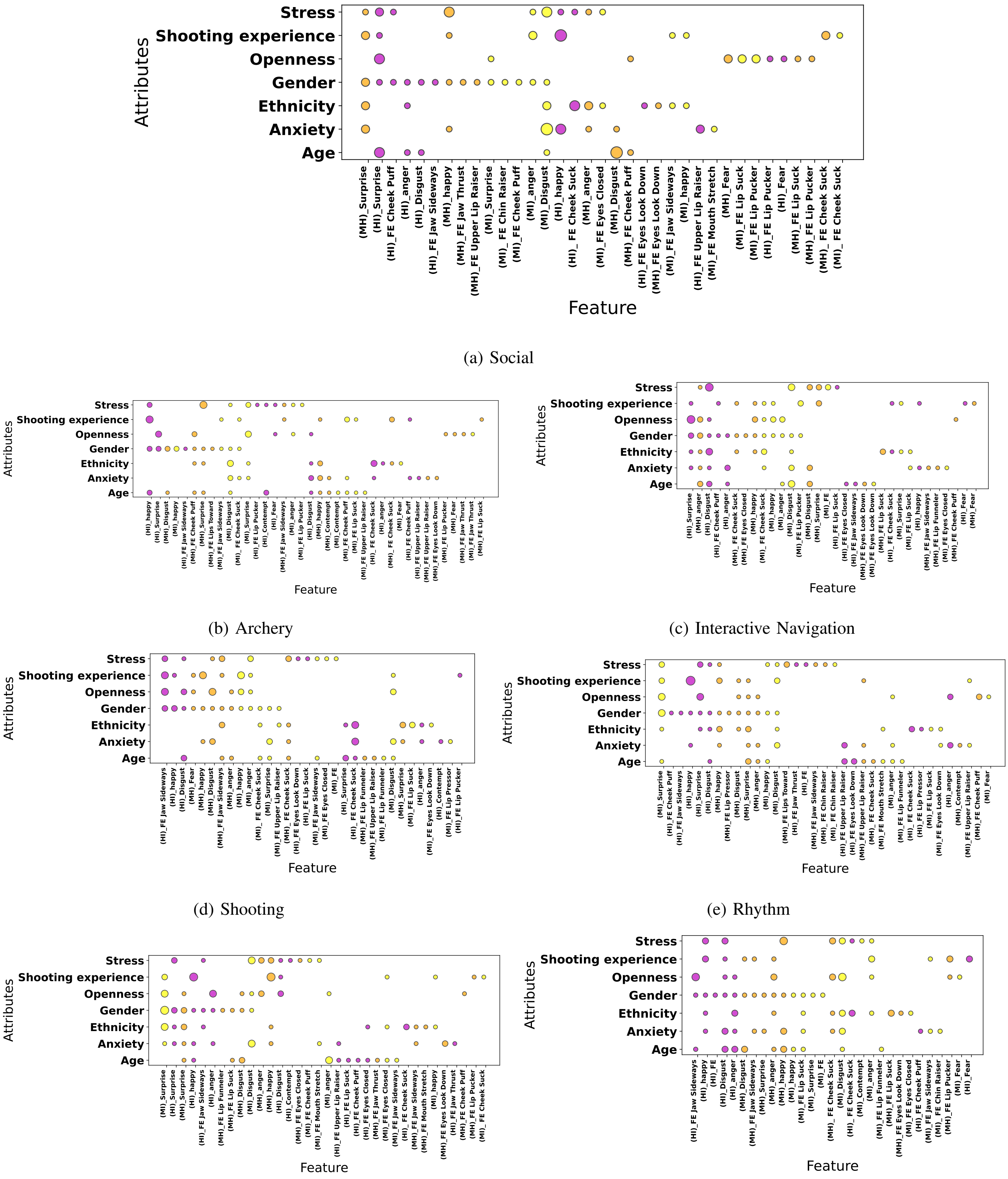
Attribute Groups	Attributes	App Groups						
		Social	Flight	Shoot	Rhythm	IN	KW	Archery
Demographics	Gender[1,2,4,5,6]	73	75	61	75	75	87	67
	Age[1,2,3,4,5,6,F]	63	73	83	73	75	75	70
	Ethnicity[4,5,6,S]	73	80	78	61	71	78	70
	Marital status[1,2,5,6]	78	67	82	52	64	79	68
Anthropometrics	Height[3,5,6]	60	51	76	55	55	68	55
	Reaction Time[3,5,6]	90	98	91	89	93	86	94
	Face Length[3,5,6]	57	55	57	44	20	36	38
	Arm Length[3,5,6]	49	38	56	71	56	67	50
	Weight[3,4,6]	62	58	56	55	62	74	68
	BMI[3,6]	63	74	67	66	77	61	56
Health	Close / Distance vision and lenses[1,5,6]	71	68	65	67	72	73	76
	Physical fitness[1,4,5,6]	79	82	72	63	75	77	76
	Anxiety[4,6]	80	82	54	78	77	75	81
	Stress[4,6]	85	90	79	75	85	72	88
	Height phobia[4,6]	68	85	65	67	65	77	70
	Motion sickness[4,6]	78	80	73	53	70	89	75
User Interests & Behaviors	Problem Solving Abilities[6]	62	76	76	59	75	69	82
	Alcohol consumption[1,5,6]	63	72	63	63	72	69	65
	VR Experience[5,6]	66	69	82	55	62	76	81
	Activity preference[6]	66	76	76	68	70	68	63
	Shooting Experiences[1,4,6]	76	72	77	69	74	83	71
	Caffeinated item consumption[1,5,6]	71	71	85	61	74	73	68
	Concentration[3,6]	75	80	69	59	76	71	79
	Violence tolerance[1,4,6]	70	81	55	77	66	71	78
	Introvert/Extrovert[6]	72	65	52	63	74	71	65
	Organized/Unorganized[6]	81	86	90	67	88	79	89
	Social media usage[4,6]	72	62	78	68	78	73	78
	Openness[6]	73	72	68	84	74	70	61
	Emotional stability[6]	75	77	66	73	76	70	76

TABLE XII: **User Profiling for Multi-Sensor (BM & FE) Adversary Across 7 App Groups.**

Attribute Groups	Attributes	App Groups						
		Social	Flight	Shoot	Rhythm	IN	KW	Archery
Demographics	Gender[1,2,4,5,6]	90	75	91	90	80	81	86
	Age[1,2,3,4,5,6,F]	78	71	84	80	80	74	71
	Ethnicity[4,5,6,S]	80	75	83	72	85	80	78
	Marital status[1,2,5,6]	57	54	70	63	67	65	69
Anthropometrics	Height[3,5,6]	80	49	90	100	52	70	90
	Reaction Time[3,5,6]	90	90	89	90	89	89	90
	Face Length[3,5,6]	65	56	70	75	80	71	75
	Arm Length[3,5,6]	68	39	60	65	65	61	75
	Weight[3,4,6]	75	48	40	72	73	70	75
	BMI[3,6]	72	73	78	68	70	76	70
Health	Close / Distance vision and lenses[1,5,6]	73	67	56	69	68	67	64
	Physical fitness[1,4,5,6]	89	76	87	80	78	80	95
	Anxiety[4,7,8]	83	75	63	80	65	80	66
	Stress[4,6]	84	87	88	93	88	85	95
	Height phobia[4,6]	78	80	76	63	68	77	75
	Motion sickness[4,6]	75	68	77	60	68	80	56
User Interests & Behaviors	Problem Solving Abilities[6]	48	48	42	48	49	84	81
	Alcohol consumption[1,5,6]	62	74	68	63	74	69	65
	VR Experience[5,6]	74	70	64	72	67	75	72
	Activity preference[6]	54	48	63	48	74	52	66
	Shooting Experiences[1,4,6]	68	75	76	68	77	78	86
	Caffeinated item consumption[1,5,6]	74	76	61	70	78	72	75
	Concentration[5,6]	75	65	74	57	80	69	85
	Violence tolerance[1,4,6]	84	66	77	60	73	75	70
	Introvert/Extrovert[6]	75	67	56	75	75	70	62
	Organized/Unorganized[6]	86	91	91	95	91	74	95
	Social media usage[4,6]	90	69	81	82	79	83	86
	Openness[6]	83	73	72	84	81	77	72
	Emotional stability[6]	82	77	85	81	83	88	75

TABLE XIII: **User Profiling for Multi-Sensor (BM, FE & EG) Adversary Across 7 App Groups.**

Attribute Groups	Attributes	App Groups						
		Social	Flight	Shoot	Rhythm	IN	KW	Archery
Demographics	Gender[1,2,4,5,6]	90	75	91	90	84	82	85
	Age[1,2,3,4,5,6,F]	80	70	85	80	80	77	71
	Ethnicity[4,5,6,S]	80	75	83	75	85	80	81
	Marital status[1,2,5,6]	58	53	71	69	65	70	64
Anthropometrics	Height[3,5,6]	80	49	90	100	52	70	90
	Reaction Time[3,5,6]	90	95	99	100	100	89	100
	Face Length[3,5,6]	65	56	70	75	80	71	75
	Arm Length[3,5,6]	68	39	60	65	65	61	75
	Weight[3,4,6]	75	48	40	72	73	70	75
	BMI[3,6]	72	73	78	68	70	76	70
Health	Close / Distance vision and lenses[1,5,6]	73	62	56	67	68	67	64
	Physical fitness[1,4,5,6]	53	57	52	67	48	58	38
	Anxiety[4,7,8]	76	79	76	68	66	77	73
	Stress[4,6]	89	86	93	84	91	86	91
	Height phobia[4,6]	70	75	71	69	66	66	78
	Motion sickness[4,6]	59	56	73	42	64	80	40
User Interests & Behaviors	Problem Solving Abilities[6]	81	61	66	65	72	52	63
	Alcohol consumption[1,5,6]	63	73	68	63	72	69	65
	VR Experience[5,6]	74	70	64	72	68	73	74
	Activity preference[6]	61	67	63	62	70	55	67
	Shooting Experiences[1,4,6]	73	76	73	79	77	86	75
	Caffeinated item consumption[1,5,6]	75	75	61	71	79	72	75
	Concentration[3,6]	68	67	72	60	68	77	85
	Violence tolerance[1,4,6]	69	68	58	57	70	75	68
	Introvert/Extrovert[6]	63	62	53	72	68	67	60
	Organized/Unorganized[6]	90	92	91	99	89	47	92
	Social media usage[4,6]	82	65	92	80	77	82	89
	Openness[6]	84	70	84	84	82	80	73
	Emotional stability[6]	80	80	84	83	82	88	75



(a) Social

(b) Archery

(c) Interactive Navigation

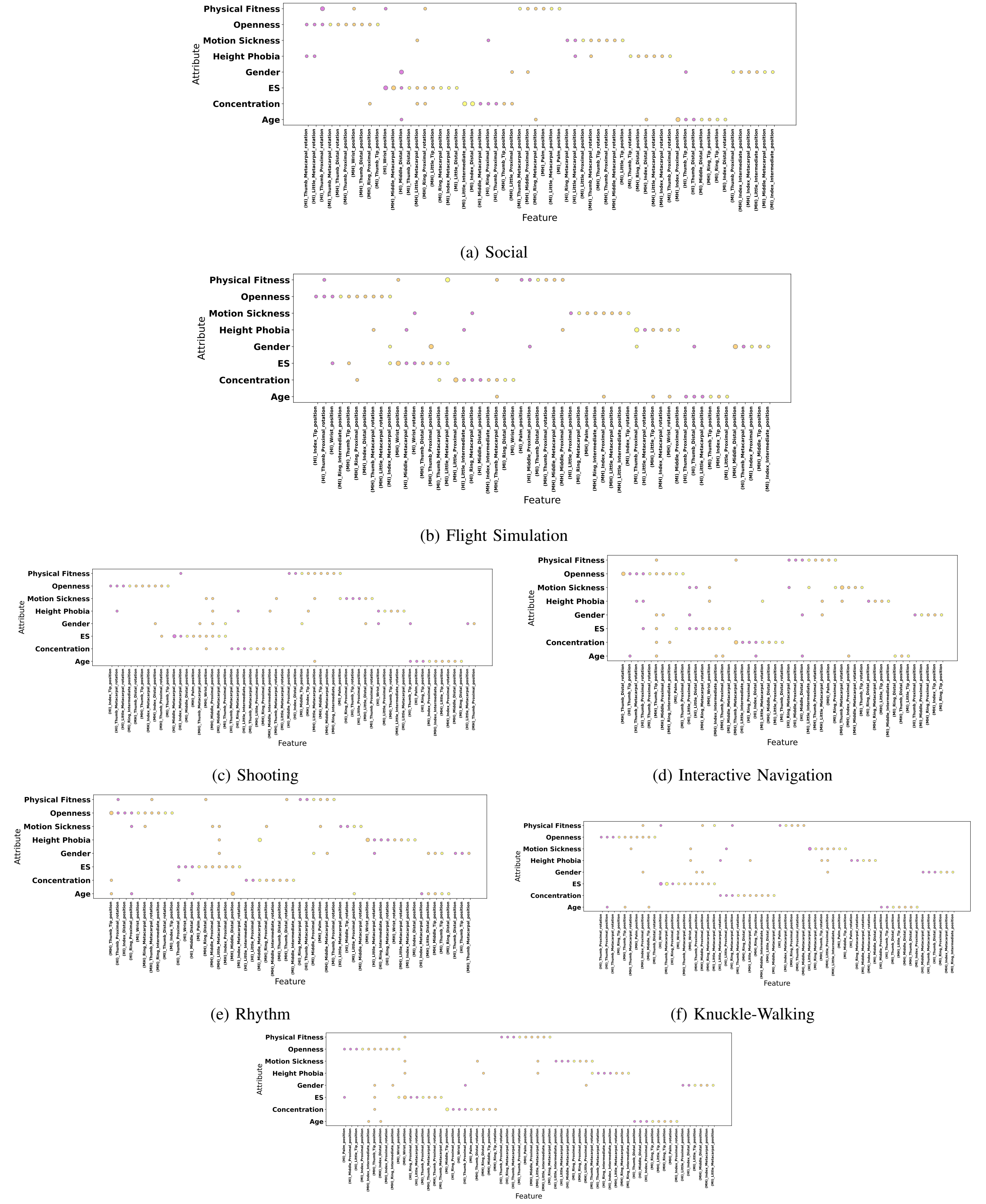
(d) Shooting

(e) Rhythm

(f) Knuckle-Walking

(g) Flight Simulation

Fig. 4: **Feature Analysis for FE Sensor Group Across Different App Groups.** Y-axis provides attribute names, and X-axis represents corresponding top features for attribute inferences. Color code represents feature importance ranking: HI (high, pink), MH (medium-high, orange), and MI (medium, yellow), while circle size reflects feature frequency (i.e., larger circles indicate higher occurrences).



(a) Social

(b) Flight Simulation

(c) Shooting

(d) Interactive Navigation

(e) Rhythm

(f) Knuckle-Walking

(g) Archery

Fig. 5: **Feature Analysis for HJ Sensor Group Across Different App Groups.** Y-axis provides attribute names, and X-axis represents corresponding top features for attribute inferences. Color code represents feature importance ranking: HI (high, pink), MH (medium-high, orange), and MI (medium, yellow).