ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

Privacy threats of behaviour identification detection in VR

Lakshmeswari Chenngiri [1], Katta Bhagya Lakshmi [2], Jampala Guru Balaji[3], Abburi Sai Manikanta[4], Sangapuadikesava[5]

[1] Assistant Professor, Department of Computer Science Engineering, Chalapathi Institute of Engineering and Technology, Chalapathi Rd, Nagar, Lam, Guntur, Andhra Pradesh- 522034

[2,3,4,5] Students, Department of Computer Science Engineering, Chalapathi Institute of Engineering and Technology, Chalapathi Rd, Nagar, Lam, Guntur, Andhra Pradesh- 522034

Email id: lakshmi.chennagiri@gmail.com[1], bbhagyalakshmi552@gmail.com[2], gurubalajijampala@gmail.com[3], manikantas631@gmail.com[4], adikesava045@gmail.com [5]

Abstract

As Virtual Reality (VR) technology becomes increasingly integrated into entertainment, education, healthcare, and enterprise environments, it simultaneously introduces new and complex privacy challenges. This study examines privacy risks linked to the use of behavioral data for user identification in immersive virtual reality (VR) applications. With advancements in VR technology, tracking sensors now provide highly immersive experiences that capture extensive and nuanced behavioral data. However, limited research addresses the privacy implications of this data collection. In this work, we investigate the potential for machine learning algorithms to identify VR users across multiple sessions and activities and assess their effectiveness even when users alter their behavior to evade detection. Additionally, we explore how physical characteristics impact identification accuracy. Our findings reveal that users can be identified with 83% accuracy across repeated sessions of the same activity and 80% accuracy when performing different tasks, while attempts to mask behaviors still result in 78% accuracy. These results underscore the necessity for enhanced privacy measures to protect user behavior data in VR environments.

Keywords: Virtual Reality (VR), Behavioral data privacy, Identity detection in VR, User profiling risks

1.Introduction

Virtual Reality (VR) has transformed how users interact with digital content, offering deeply immersive experiences that blur the boundaries between the physical and virtual worlds. Through head-mounted displays, motion sensors, and eye-tracking systems, VR platforms continuously monitor user behaviors to enable natural and intuitive interactions. However, this rich behavioral data collection introduces serious privacy concerns, especially when these actions can be uniquely linked to individual users.

Behavioral identification in VR leverages subtle biometric signals—such as gait, body posture, eye movement, and interaction patterns—to recognize and authenticate users. While beneficial for personalization and security, these features are inherently difficult to anonymize. Unlike passwords or tokens, behavioral traits are persistent and often reveal sensitive information, including physical or mental health conditions, emotional states, and demographic attributes.

This persistent tracking increases the risk of surveillance, profiling, and potential misuse by third parties.

Current status of behavioural identity

systems in VR Many researchers have attempted to develop behavioural identity detection systems based on various behavioural biometrics. However, the most prevalent strategy is using head motions/head trajectory to uniquely identify a user (Rogers et al., 2015; Mustafa et al., 2018; Shen et al., 2019; Wang and Zhang, 2021). These techniques determine user head trajectories while performing an assigned or ordinary activity, and studies have demonstrated that VR users can be uniquely recognised with approximately 90% accuracy using head motions (Li et al., 2016; Quintero et al., 2021). Apart from this, many further experiments were carried out to develop robust authentication algorithms employing a mix of behavioural indicators, such as head motions, hand controller movements, blinking patterns and eye gaze (Revett, 2008; Kupin et al., 2019; Miller et al., 2020; Liebers et al., 2021; Miller et al., 2022a). The majority of these systems achieved remarkable accuracy (around 94%) by using basic classification approaches such as K-Nearest Neighbour (KNN), Random Forest Regression, Convolutional Neural Networks (CNN), Siamese Neural Networks and Support Vector Machines.

2.Related work

The most critical task in digital application security is to allow access to only legitimate users. These authentication approaches have evolved through several paradigms over the years, progressing from passwords and personal identification numbers (PIN), to biometric, characteristics like fingerprints, iris scans and face scans (Pishva, 2007). The latest trend in authentication security is to use behavioural biometrics (Liebers et al., 2021). Researchers in various disciplines are developing methods for using behavioural biometrics such as gait, keystrokes, EEG signals and voice as authentication techniques (Revett, 2008). The VR industry is also embracing these behavioural identity detection techniques, since they have natural access to many behavioural biometrics. However, this behavioural data analysis comes with several concealed privacy threats (Rathgeb and Uhl, 2011; Bailenson, 2018). This section discusses the present state-of-the-art of behavioural identity detection systems, their potential privacy problems and possible solutions to these problems according to the available literature. Even though discussions about the privacy risks associated with behavioural cue tracking have not reached the expected degree, some recent papers have emphasised the hidden risks of these systems. Bailenson (Bailenson, 2018) noted the possibilities of utilising behavioural tracking data to produce millions of records in a short period of time to forecast a user's mental and physical health status as a major wake-up call about these nonverbal behavioural data-related privacy risks. Hosfelt et al. discussed how eye and gaze tracking can be issues not only for headmounted display (HMD) based systems but also for web-based mixed reality applications (Hosfelt and Shadowen, 2020). Even though many users still do not take privacy protection seriously, several studies have shown that users want to protect their privacy when they know their movements are being tracked (Solove, 2007). Gordon et al. describe how people adjust their behaviour when they realise a prediction algorithm is attempting to forecast their actions (Gordon et al., 2021).

3. Methodology

A total of 159 participants, recruited from an online platform (Prolific.com), were used in this study. The mean age of the participants was 37.60 years, and of the 159 that responded, 102 of them indicated that their biological sex was male. The present study utilized a 'bring-your-own-device' approach, recruiting participants that owned VR devices and were willing to use them as part of an online research study. All participants were asked to complete a prescreening survey to determine eligibility including being located within the United States, owning a VR headset, having used a VR headset at least once before, being fluent in English, and having normal or corrected-to-normal vision. Based on the prescreen survey, 464 responses were eligible for the main study, with the types of VR devices reported by those that owned a system being Meta Quest 2 (N = 149), Oculus Quest 2 (N = 128), Meta Quest 3 (N = 54), Oculus Rift (N = 50), other (N = 33), HTC Vive (N = 16), Oculus Rift S (N = 14), Valve Index (N = 9), HTC Vive Pro (N = 4), HP Reverb G2 (N = 2), HTC Vive Focus Plus (N = 2), HTC Vive Pro 2 (N = 2), and HTC Vive Focus 3 (N = 1). Eligible participants were invited to complete the main study and informed of the nature of the task (i.e., they would be shown simulated fires). Participants were then randomly assigned to either the VE or screen conditions.

Privacy Threats and Risks

- User Re-identification: Even in anonymized environments, behavioral data such as head movement or walking patterns can uniquely identify users. This makes de-anonymization attacks highly feasible, especially when combined with external datasets.
- Profiling and Inference Attacks: VR data can reveal sensitive attributes such as gender, age, mood, cognitive ability, and health conditions. Malicious actors or data brokers may exploit this for profiling, targeted advertising, or discrimination.
- Surveillance and Data Leakage: Persistent tracking enables long-term surveillance, where user behavior can be continuously monitored, stored, and analyzed. Insecure storage or transmission of this data may also result in leaks or unauthorized access.
- Consent and Transparency Challenges: Many users are unaware of what behavioral data is being collected or how it is used. The immersive experience of VR often lacks visible interfaces for consent management or data control.

Artificial Intelligence Security

The rapid advancement of technology has made artificial intelligence (AI) increasingly capable of identifying and classifying potential cyber threats. These threats can then be communicated to relevant personnel for prompt action. Nevertheless, due to the black box (i.e., a system to which the user interacts through its external parameters without any or limited knowledge of what happens inside it) characteristics of AI and the identification of certain cyber-attacks can present significant challenges.

Despite the efficacy and accuracy of AI in identifying threats, the lack of transparency in the decision-making process can make it difficult to comprehend the basis for certain classifications. The Generative Adversarial Networks (GANs) attack is one of the most commonly used attack models that targets black box systems The GAN model comprises a pair of networks, where one generates data and the other determines whether the output is authentic or counterfeit. The two networks continuously interact in this manner until the first network reliably produces content that can deceive the other

Artificial intelligence (AI) in MR is crucial for enhancing user interactions by dynamically adjusting digital elements based on real-world inputs. However, MR's dependency on AI-driven contextual recognition, object identification, and behavioral prediction exposes it to additional security risks. AI models in MR must process vast amounts of personal data in real time, making them vulnerable to attacks that exploit model weaknesses, such as adversarial attacks.

Digital Twins Security

The advent of the Metaverse has brought a proliferation of digital services that collect, transmit, process, govern, and store user data. However, this process also poses significant risks to user privacy, particularly with the inclusion of digital twins. The latter may compromise sensitive user information such as location, habits, and living styles throughout the lifecycle of these digital services.

To facilitate immersive interactions with digital twins in the Metaverse, it is imperative to conduct comprehensive data collection procedures. These procedures encompass acquiring personal information, behavioral data, and user preferences. It is of utmost importance to ensure the privacy of these data to prevent unauthorized access or misuse by third parties.

Also, the effective creation and rendering of avatars and virtual environments in Metaverse services necessitate the aggregation and processing of voluminous data collected from the human body and its surrounding environment. However, this undertaking carries the potential for sensitive information to be exposed. Specifically, centralizing the private data of different users for training personalized avatar appearance models challenges user privacy and contravenes extant regulations such as the General Data Protection Regulation (GDPR). Besides that, due to the ability of avatars to reflect the behavior patterns, preferences, habits, and activities of their real-life counterparts, attackers can exploit this similarity to collect the digital footprints of avatars and create accurate user profiles that enable them to carry out illicit activities, posing a significant threat to the security and privacy of users. As such, it is imperative to safeguard users' data privacy and security in the Metaverse

4.Results

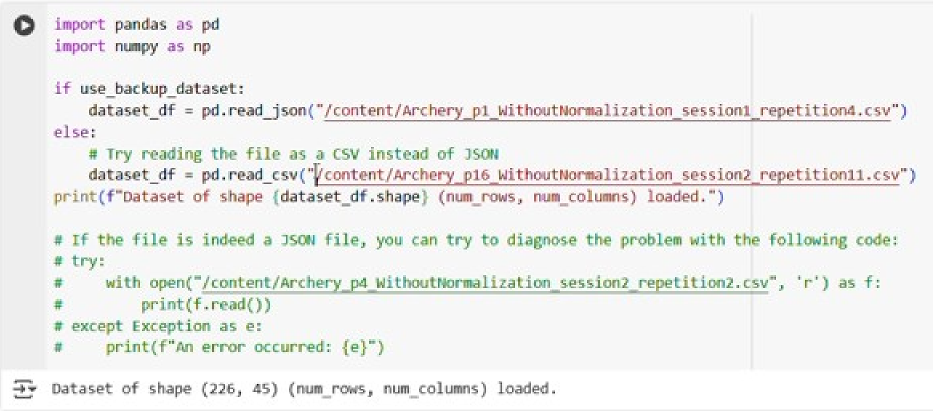
Participants completed up to five actions during the sequence of video simulations. The most frequent initial action was 'investigate' (0.47) followed by 'protect' (0.31), 'call 911' (0.18), and 'delay' (0.04; see Table 2 for transition probabilities). The three most frequently observed actions sequences were 'protect + call 911' followed by 'investigate + engage + engage' and 'investigate + protect + call 911'

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

Table: Transition probabilities from one action (row) to another (column).

From | To	Call 911	Delay	Engage	Investigate	Protect
Call 911	0	0.19	0.21	0.08	0.52
Delay	0.1	0	0.05	0.1	0.75
Engage	0.12	0.02	0.73	0	0.14
Investigate	0.15	0.04	0.51	0	0.31
Protect	1	0	0	0	0

To focus on the impact of fire cues and view on action responses, a multinomial logistic regression analyzed the initial action selected across conditions. The response ‘Investigate’ was set as the baseline category, with participants selecting ‘Delay’ as the initial action dropped from analysis due to low response rates (retained N = 152). Significant effects were observed for smoke and view conditions. For thick smoke, ‘Protect’ and ‘Call 911’ were more frequently selected compared to thin smoke; z = 4.61, $p < 0.001$, z = 3.23, $p = 0.001$, respectively. For the screen condition, ‘Protect’ and ‘Call 911’ were more frequently selected compared to the VR condition; z = 2.14, $p = 0.032$ and z = 2.64, $p = 0.008$, respectively This supported the hypothesis that the selection of actions taken during the decision-making task would vary by viewing condition and by fire characteristics, specifically smoke.

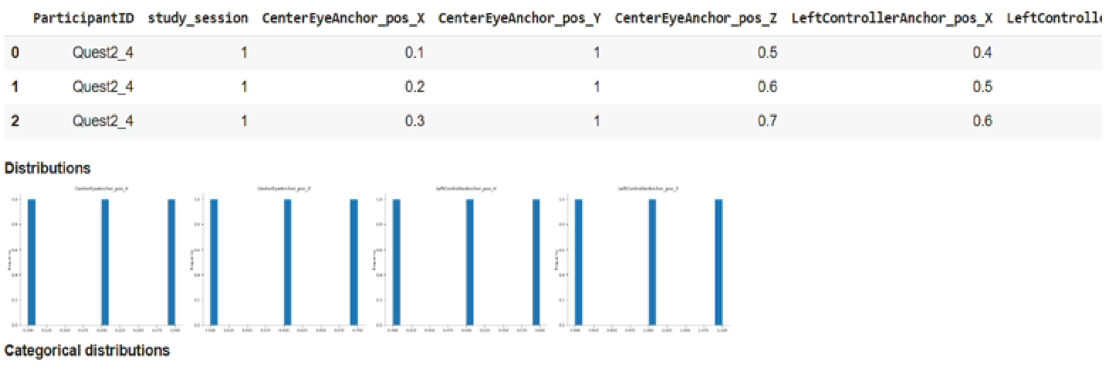


```
import pandas as pd
import numpy as np

if use_backup_dataset:
    dataset_df = pd.read_json("/content/Archery_p1_WithoutNormalization_session1_repetition4.csv")
else:
    # Try reading the file as a CSV instead of JSON
    dataset_df = pd.read_csv("/content/Archery_p16_WithoutNormalization_session2_repetition11.csv")
print(f"Dataset of shape {dataset_df.shape} (num_rows, num_columns) loaded.")

# If the file is indeed a JSON file, you can try to diagnose the problem with the following code:
# try:
#     with open("/content/Archery_p4_WithoutNormalization_session2_repetition2.csv", 'r') as f:
#         print(f.read())
# except Exception as e:
#     print(f"An error occurred: {e}")
```

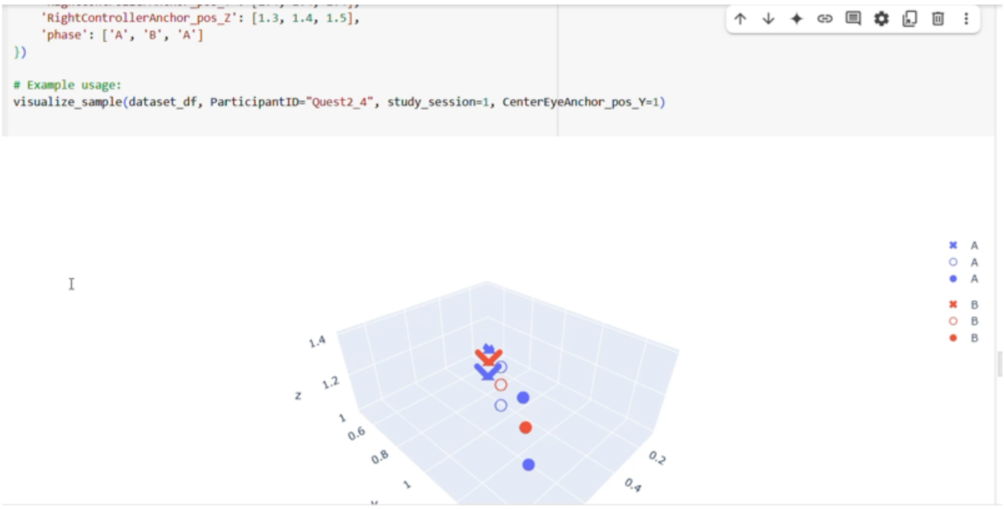
```
Dataset of shape (226, 45) (num_rows, num_columns) loaded.
```



	ParticipantID	study_session	CenterEyeAnchor_pos_X	CenterEyeAnchor_pos_Y	CenterEyeAnchor_pos_Z	LeftControllerAnchor_pos_X	LeftControll
0	Quest2_4	1	0.1	1	0.5	0.4	
1	Quest2_4	1	0.2	1	0.6	0.5	
2	Quest2_4	1	0.3	1	0.7	0.6	

Distributions

Categorical distributions



```
    'RightControllerAnchor_pos_Z': [1.3, 1.4, 1.5],
    'phase': ['A', 'B', 'A']
})

# Example usage:
visualize_sample(dataset_df, ParticipantID="Quest2_4", study_session=1, CenterEyeAnchor_pos_Y=1)
```

Conclusion

The fusion of behavioral analytics and immersive VR environments offers unprecedented opportunities for personalization and interactivity. However, it also opens the door to significant privacy risks that must be proactively addressed. As VR continues to grow, ensuring user privacy through responsible data practices, user empowerment, and strong security protocols is not optional—it is essential for the ethical development and acceptance of virtual reality technologies.

References:

1. Adams, D., Bah, A., Barwulor, C., Musaby, N., Pitkin, K., and Redmiles, E. M. (2018). Ethics emerging: the story of privacy and security perceptions in virtual reality. SOUPS@ USENIX Secur. Symp., 427–442. doi:10.13016/M2B853K5P
2. Altman, N. S. (1992). An introduction to kernel and nearest-neighbor nonparametric regression. Am. Statistician 46, 175–185.
3. Bailenson, J. (2018). Protecting nonverbal data tracked in virtual reality. JAMA Pediatr. 172, 905–906. doi:10.1001/jamapediatrics.2018.1909
4. David-John, B., Hosfelt, D., Butler, K., and Jain, E. (2021). A privacy-preserving approach to streaming eye-tracking data. IEEE Trans. Vis. Comput. Graph. 27, 2555–2565. doi:10.1109/tvcg.2021.3067787
5. De Guzman, J. A., Thilakarathna, K., and Seneviratne, A. (2020). Security and privacy approaches in mixed reality. ACM Comput. Surv. 52, 1–37. doi:10.1145/3359626
6. Egliston, B., and Carter, M. (2021). Critical questions for facebook's virtual reality: data, power and the metaverse. Internet Policy Rev. 10, 1–23. doi:10.14763/2021.4.1610
7. Falchuk, B., Loeb, S., and Neff, R. (2018). The social metaverse: battle for privacy. IEEE Technol. Soc. Mag. 37, 52–61. doi:10.1109/MTS.2018.2826060
8. Falk, B., Meng, Y., Zhan, Y., and Zhu, H. (2021). "Poster: reavatar: Virtual reality deanonymization attack through correlating movement signatures," in Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, New