frontiers | Frontiers in Virtual Reality

TYPE Original Research
PUBLISHED 29 January 2024
DOI 10.3389/frvir.2024.1197547

OPEN ACCESS

EDITED BY
Kay Marie Stanney,
Design Interactive, United States

REVIEWED BY
David Murphy,
University College Cork, Ireland
Chutisant Kerdvibulvech,
National Institute of Development Administration, Thailand

*CORRESPONDENCE
Dilshani Kumarapeli,
kumarapeli.kumarapeli@pg.canterbury.ac.nz

RECEIVED 31 March 2023
ACCEPTED 03 January 2024
PUBLISHED 29 January 2024

CITATION
Kumarapeli D, Jung S and Lindeman RW (2024), Privacy threats of behaviour identity detection in VR.
Front. Virtual Real. 5:1197547.
doi: 10.3389/frvir.2024.1197547

Privacy threats of behaviour identity detection in VR

Dilshani Kumarapeli[1]*, Sungchul Jung[2] and Robert W. Lindeman[1]

[1]HIT Lab NZ, University of Canterbury, Christchurch, New Zealand, [2]Game Design and Development, Kennesaw State University, Georgia, GA, United States

This study explores the potential privacy risks associated with the use of behavioural data as an identification mechanism in immersive VR applications. With the advent of modern VR technology, tracking sensors are now able to provide a highly immersive experience with a high level of user agency, significantly increasing both the amount and richness of behavioural data being collected and recorded. However, there has been little research into the privacy risks of such approaches. In this work, we investigate the capability of machine learning algorithms to identify VR users across multiple sessions and activities, as well as their effectiveness when users deliberately change their behaviour to evade detection. We also examine how the physical characteristics of users impact the accuracy of these algorithms. Our results show that once a user is tracked in VR, they can be identified with 83% accuracy across multiple sessions of the same activity and with 80% accuracy when performing a different task. Even when users attempt to deliberately obfuscate their behaviour, they can still be recognised with 78% accuracy. These findings highlight the need for more robust technical measures to safeguard the behavioural privacy of VR users.

KEYWORDS

Virtual Reality (VR), behaviour capturing in VR, data privacy in virtual environments, behavioral biometrics, user profiling risks, ethical implications of VR, identity detection in VR, VR privacy threats

1 Introduction

In recent years, virtual reality (VR) has gained popularity in various fields, such as gaming, education, healthcare and security. However, accurately and reliably detecting users' identities in VR environments (e.g., for authentication) remains a key challenge in privacy and security in VR. To address this challenge, researchers have developed VR behaviour-based authentication systems that collect and analyse users' behavioural data, including movement patterns, eye gaze patterns and head movement patterns (Jones et al., 2021). While these systems are promising, they also come with privacy-related limitations and drawbacks, including the potential violation of user privacy (Adams et al., 2018; Falchuk et al., 2018).

Behavioural-based identity detection approaches train machine learning (ML) models to identify users based on their unique behavioural patterns (Yaremych and Persky, 2019; Miller et al., 2021; 2022a). This advancement eliminates the need for text input, providing a seamless and uninterrupted VR experience. However, using sensitive user behaviour data as a means of authentication carries inherent risks. The data is highly personal and can reveal a great deal of information about a user's habits, preferences and behaviours, potentially exposing them to privacy risks (Rafique and Cheung, 2020; Falk et al., 2021; Miller et al., 2022b). Unlike traditional authentication methods, users cannot easily change their behaviour patterns or revoke access to their behavioural data if it is leaked or

compromised. Hence, these behaviour profiles can be used maliciously to identify and track users across different platforms, leading to potential security breaches and privacy violations (Bailenson, 2018; Miller et al., 2020; Nair et al., 2022a; Giaretta, 2022). This could potentially have far-reaching consequences, such as exposing the user to targeted advertising, identity theft, or other forms of cybercrime (Egliston and Carter, 2021).

This paper investigates the nature of privacy risks in VR identity detection model design through six machine learning-based identity detection algorithms and a user study measuring identity detection accuracy using only participants' VR behavioural data. The study aims to gain a thorough understanding of the algorithms' characteristics and effectiveness, as well as explore how the physical characteristics of VR users affect identity detection accuracy. The study tests eight hypotheses under two research questions, providing insights into the balance of benefits and potential risks and ethical considerations of using sensitive user data for authentication in VR environments.

- RQ_1: How well can user behaviour data be used to identify particular users in VR?
  - H_{1_1}: Machine learning-based identity detection algorithms will be accurate when the training data and testing data are from the same task.
  - H_{1_2}: Machine learning-based identity detection algorithms will be accurate when the training data and testing data are from different tasks.
  - H_{1_3}: Machine learning-based identity detection algorithms will be accurate when the training data and testing data are from different tasks, and the user actively tries to thwart detection by changing their behaviour during the testing task.
- RQ_2: How does user appearance (e.g., skin tone, presence of facial hair) impact identity detection accuracy?
  - H_{2_1}: There is no significant influence of user gender on machine learning-based identity detection accuracy.
  - H_{2_2}: There is no significant influence of user skin tone on machine learning-based identity detection accuracy.
  - H_{2_3}: There is no significant influence of user hand dominance on machine learning-based identity detection accuracy.
  - H_{2_4}: There is no significant influence of user facial hair presence on machine learning-based identity detection accuracy.

The subsequent sections of this paper discuss related work, the study approach we utilised, the outcomes and the implications drawn from these results.

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.

2.1 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.

2.2 Awareness of privacy risks in behavioural identity

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 head-mounted 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). This demonstrates how

consumers may resist any interference that may scrutinise their behaviour. Nevertheless, according to Privacy International, an organisation working on protecting user privacy since 1990, case law demonstrates that even governments do not have the authority to violate people's right to privacy on a broad scale by collecting personally identifiable data[1].

2.3 Available solutions for behavioural identity privacy risks

Researchers have identified three categories of recommended solutions: i) providing adequate norms, principles and ethics to VR developers; ii) designing new behaviour-obfuscation technologies; and iii) utilizing user-knowledge-based authentication systems as a replacement for behaviour identification detection (De Guzman et al., 2020).

Many researchers and legal experts emphasise the significance of establishing rules and norms to govern data collection, storage and use while keeping ethical considerations in mind (Madary and Metzinger, 2016; Bailenson, 2018; Hosfelt, 2019; Satybaldy et al., 2020; Shadowen and Hosfelt, 2020). Most of the studies in this area stress the significance of taking action on the technological side, rather than waiting for rules and laws to arise, since the slow-moving regulatory structure struggles to keep up with the fast growth of technology (Prosser, 1960).

Another strategy to deal with this problem is to provide technical solutions for changing data to protect users' behavioural privacy. For example, David et al. reduced recognition accuracy by changing the eye gaze direction by a modest angle (David-John et al., 2021). Nair et al. suggested a technical framework to 'go incognito' in metaverse applications called "Meta Guard" (Nair et al., 2022b). This add-on allows users to hide their physical and geographical parameters like height, wingspan, geolocation and voice (Nair et al., 2022b). However, there is a severe lack of work being done to further explore this line of research.

Instead of employing behaviour detection, the final solution vector uses knowledge-based authentication techniques to authenticate the VR user (Yu et al., 2016). For example, by interacting with a 3D object, users may use the knowledge only they possess to authenticate the VR application (Mathis et al., 2021). This is basically the familiar PIN mechanism being applied more securely to meet the security requirements of VR applications. It has been suggested that these types of interactions are hard to guess by bystanders. Mohamad et al. discuss the trade-off between three different input methods used in knowledge-based authentication systems (Khamis et al., 2018). According to the comparison, using eye-gaze to enter a password takes the most time, but gives the highest level of security.

3 Methods

We collected sensor-based behavioural data (e.g., eye-gaze, head/hand movements) while participants recited and rephrased two bedtime stories. This section goes over the software and hardware resources we used, the procedures we followed, and our data collection. This study was approved by the Human Research Ethics Committee of the University of Canterbury, New Zealand, under the approval reference HREC 2022/31/LR-PS.

TABLE 1 Collected data types.

Behavioural data category	Physical appearance data
Eye Gaze	Skin Tone
Eye Movement	Dominant Hand
Lip movement	Presence of any Facial Hair
Hand Movement	
Head Movement	

3.1 Participants

Before recruiting participants, we conducted an *a priori* power analysis. We decided to use "Large" using Cohen's criteria (effect size = 0.8, alpha value = 0.05) and the projected sample size needed was 40 participants. We recruited 40 participants (Male: 18, Female: 21, Demi-Boy: 1) from the university campus (Age: $M = 28.2$, $SD = 7.46$). All participants were 18 years or older and had normal or corrected-to-normal vision. We provided hard copies of the Fitzpatrick scale and guide to participants to match and determine their skin tone (Fitzpatrick, 1975).

3.2 Study design

To investigate our research questions, we used a 2x1 within-subjects experimental design, with one independent variable "Task" with two levels "Reading" and "Speaking." We automatically logged 73 behavioural data points under five categories and collected three self reported physical appearance data points. Finally, users reported the strategies used to hide behavioural identity in the final task at the end of the study session using a Qualtrics questionnaire. Table 1 summarises all the data types we have collected throughout the experiment.

3.2.1 Task

Figure 1 shows the procedural flow on the study day. After an introduction and attaining informed consent, we had participants calibrate the eye tracker according to their eyesight using the built-in eye calibration feature of the VR headset. Refer to section 3.3 for eye-tracking device specifications. Our system was intentionally designed to require only simple interaction in a neutral setting. In addition, before starting the experiment, participants were given an introduction, including a briefing on the VR hand controllers and clear instructions on how to use them effectively throughout the session. Participants were also informed that data would only be collected between the START and STOP commands. We then asked participants to read two short bedtime stories in VR, each 7 minutes long, while

1 https://www.privacyinternational.org/learning-resources/guide-litigating-identity-systems

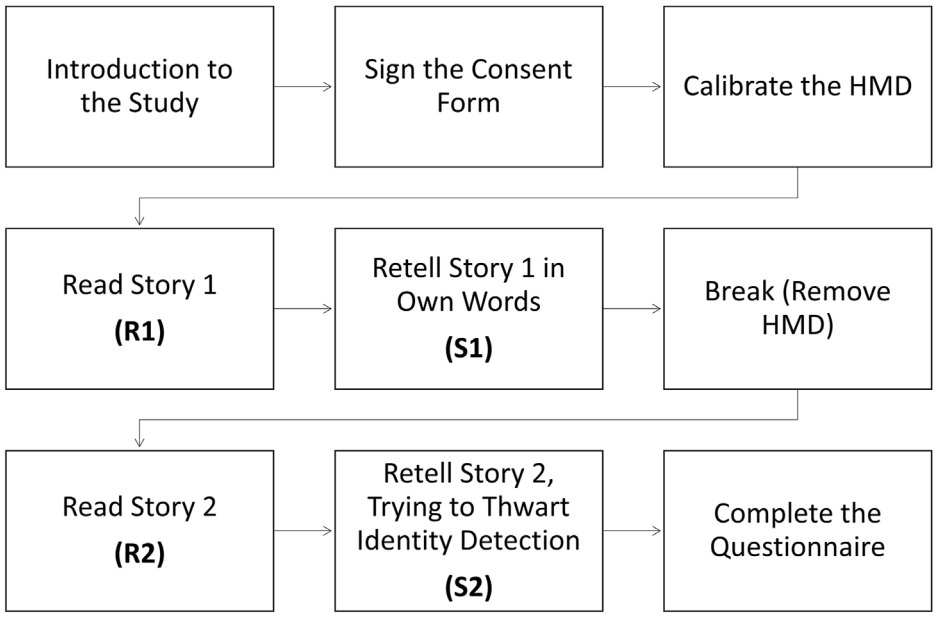

FIGURE 1
Experimental procedure.

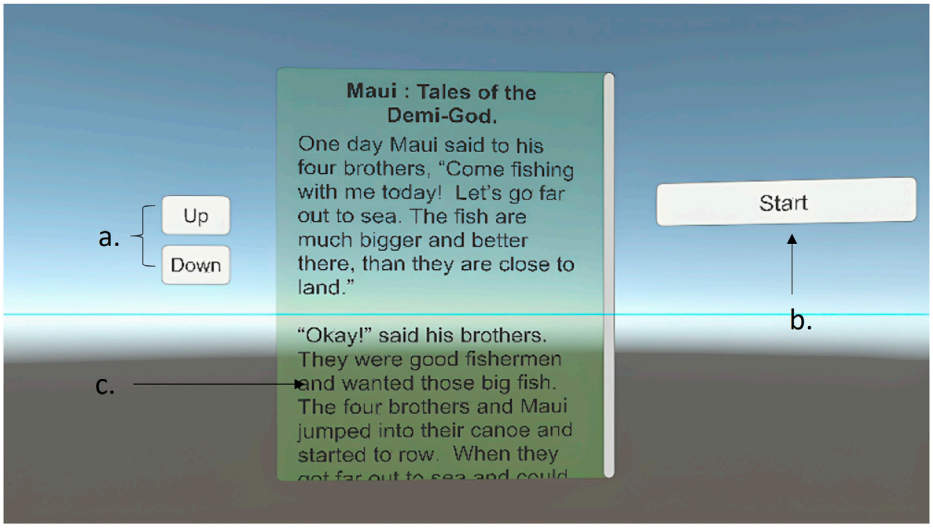

FIGURE 2
The Story Reading Interface. **(A)** The "Up" and "Down" buttons helped to scroll through the story. **(B)** The "Start" button toggled into a "Stop" button once started. **(C)** The story reading interface could be controlled using "Up" and "Down" buttons. Reproduced from Kumarapeli et al. (2023); with permission from IEEE.

holding two hand controllers (see Figure 2) to navigate through the story interface. The selected stories were traditional bedtime stories without offensive content for any ethnic or religious group (First story: "Maui, the tale of demi-god", Second story: "The Gift of the Magi"). For each story, we had them perform two steps. Once the participant pressed the "Start" button (which became a "Stop" button once pressed), a first story recitation task (**R1**) was started, a reading dialogue showed up on the screen in VR, and the participant started to read with their voice loudly. During the reading, the participant used the "Up" and "Down" buttons to scroll through the reading dialogue. When the participant completed reading, they pressed the "Stop" button and finished the **R1**. We collected the behavioural data only during the interval when the participant pressed the "Start" button until they pressed the "Stop" button. They repeated this procedure three more times, once where they were asked to rephrase the same story in their

TABLE 2 Parameters used for the classification algorithms.

Classification model	Parameters used
Fine Tree	Maximum number of splits: 100
	Split criterion: Gini's diversity index
	Surrogate decisions splits: Off
Medium KNN	Number of neighbours: 10
	Distance metric: Euclidean
	Distance weight: Equal
	Standardize data: True
Bagged Trees	Ensemble method: Bag
	Learner type: Decision Tree
	Maximum number of splits: 1,208,207
	Number of layers: 30
Single-layer Neural Network	Number of fully connected layers: 1
	First layer size: 25
	Activation: ReLu
	Iteration limit: 1,000
	Standardize data: True
Bilayered Neural Network	Number of fully connected layers: 2
	First layer size: 10
	Second layer size: 10
	Activation: ReLu
	Iteration limit: 1,000
	Standardize data: True
Fully Convolutional Neural Network	Same parameters and the architecture used in Fawaz et al
	with an input size of 73 (Fawaz et al., 2018)

own words (a story rephrasing task **(S1)**), another recitation task with a different story **(R2)**, and finally a story rephrasing task where they were asked to re-tell the second story while attempting to thwart the behavioural identification algorithm **(S2)**. Each above-mentioned stage was allotted 3–4 min based on individual reading and speaking speed. Hence, between the stages, participants were given a minimum of 10 min as washout periods to minimize carryover effects.

We added this last step **(S2)**) to test the robustness of the trained models. Anomaly-based Intrusion Detection Systems (AIDS) are designed to detect and respond to unusual or suspicious activity (Khraisat et al., 2019). Hence, one of the apparent ways to thwart these behaviour-based identity detections is through altered behaviour. We specially added this task to learn how immune these models are to deliberate user behaviour thwarts.

3.2.2 Measures

In order to address both research questions, we collected two types of data in our study. The first type was behavioural data from the virtual device sensors. This data was used to train the classification models that we propose. The second type of data we collected was physical appearance data, which was obtained through self-reported questionnaires. This data provided valuable insights into the demographics and physical characteristics of the users, which helped to understand the robustness of these ML classification models. By analyzing both types of data together, we hoped to be able to gain a more comprehensive understanding of the nature of behaviour identity detection systems.

3.2.2.1 Behavioural data collection

Seventy-three data points were collected from each participant while performing the four tasks described in section 3.2.1. All the data were collected while the participants were seated. All the data were written to separate CSV files under a randomly assigned user ID to maintain user anonymity. We collected 15 eye-movement data points, three gaze-direction data points, 37 lip-, jaw- and tongue-movement data points, 15 hand-movement data points and six head-movement data points. A detailed list of all the features is provided as supporting material.

The researcher gave a brief overview to participants about behaviour-based identity detection systems before starting the **S2** task. This included details of current state-of-art behaviour-based identity detection systems, their accuracy, features used and potential harm to users. The researcher answered participants' questions.

3.2.2.2 Physical appearance data collection

A questionnaire collected information about the participant's self-reported physical appearance. Using the same questionnaire,

TABLE 3 Training and testing accuracies for the classification models.

Model name	R1 accuracy	R2 accuracy	S1 accuracy	S2 accuracy
Fine Tree	92.7	41.7	60.1	46.6
Medium KNN	99.9	86.6	76.8	54.9
Bagged Trees (BT)	100.0	55.0	71.1	56.1
Single-layer Neural Network (SNN)	100.0	82.7	79.4	59.9
Bilayered Neural Network (BNN)	100.0	74.9	68.2	48.4
Fully Convolutional Neural Network (FCNN)	100.0	77.0	79.32	77.56

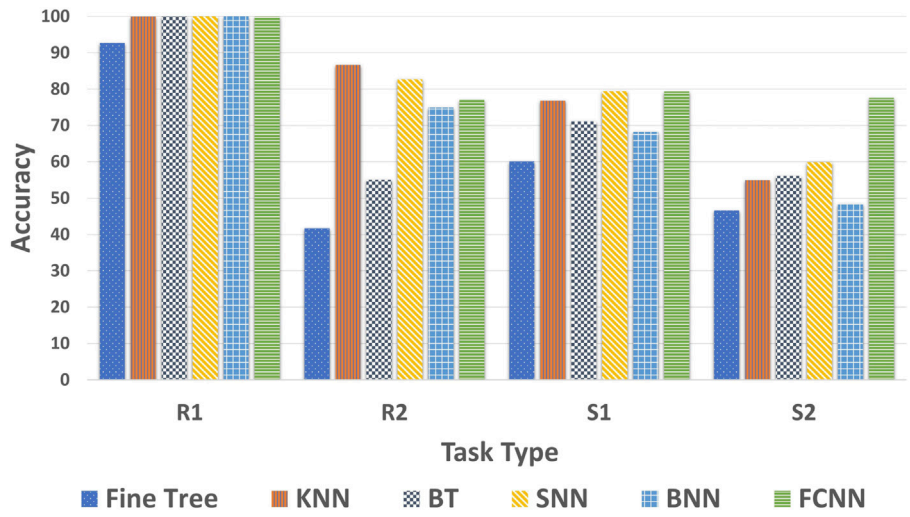

FIGURE 3
Accuracy comparison for each task using the different classification models.

TABLE 4 Accuracy change by changing behaviour.

Accuracy change (S1 accuracy - S2 accuracy)	No. of participants
less than 0 (accuracy increase)	9
0–20	14
21–40	9
41–60	3
61–80	2
81–100	3

participants also reported their behaviour-hiding strategies for **S2**. In summary, we collected essential demographic data, including self-reported Skin Tone (using Fitzpatrick Scale), Dominant Hand (Left/Right), Facial Hair (Yes/No), and Identity Detection Prevention Strategy (Text-input) (Fitzpatrick, 1975).

3.3 System design

We used an HTC Vive Pro Eye VR headset[2] with a Vive facial tracker[3] and SRanipal Eye and Facial tracking SDK version 1.3.3.0 to access sensor-based behavioural data. All the data were recorded at a 60 Hz frequency using the device's frame rate. A computer with an i7-12700H 12th Gen CPU with 32 GB RAM and NVIDIA GeForce RTX 3080 GPU was used to drive the VR device. We ran the behaviour detection algorithm on a computer with an i7-11800H 11th Gen CPU with 32 GB RAM and NVIDIA GeForce RTX 3070 GPU. We trained and tested the algorithm using the Matlab classification app Version-9.11.0.1873467 (R2021b) Update 3.

3.3.1 Identity detection model design

We selected six state-of-art classification models routinely used in behavioural identity detection algorithms. Then we used Keras from Tensorflow Version 2.11.0[4] to create a Fully Convolutional Neural Network (FCNN) and Matlab version 9.11.0.1873467 (R2021b) Update 3[5] classification app to train five other classification models to classify the 40 participants based on the 73 behavioural data points collected during the four tasks described in Section 3.4. We selected the six classification models used most frequently in previous behavioural identity detection systems described in Section 2.1: Fine Tree (Quinlan, 1986), Medium KNN (Altman, 1992), Bagged Trees (Kuhn and Johnson, 2016), Single-layer Neural Network (SNN) (Schmidhuber, 2015), Bilayered Neural Network (BNN) (Schmidhuber, 2015) and Fully Convolutional Neural Network (FCNN) (Fawaz et al., 2018). The classification algorithms were defined using the parameters listed in Table 2, and each model was trained using the **R1** dataset. The dataset was first collected and cleaned up before it was used to train the models. The accuracy was then tested against the other three datasets (**R2**, **S1**, **S2**).

Even though some of the behavioural identity detection approaches used Siamese neural networks to identify users uniquely, we did not use the above model in our work as Siamese networks are not well-suited for identifying non-uniform behaviours due to their design philosophy of comparing the similarity of two inputs (Miller et al., 2021; 2022a). The network accomplishes this by encoding the inputs into a feature representation and then comparing the distance between these representations. This approach is effective when the inputs are

2 https://www.vive.com/nz/product/vive-pro-eye/overview/

3 https://www.vive.com/us/accessory/facial-tracker/

4 https://www.tensorflow.org/versions/r2.11/api_docs/python/tf

5 https://au.mathworks.com/products/matlab.html

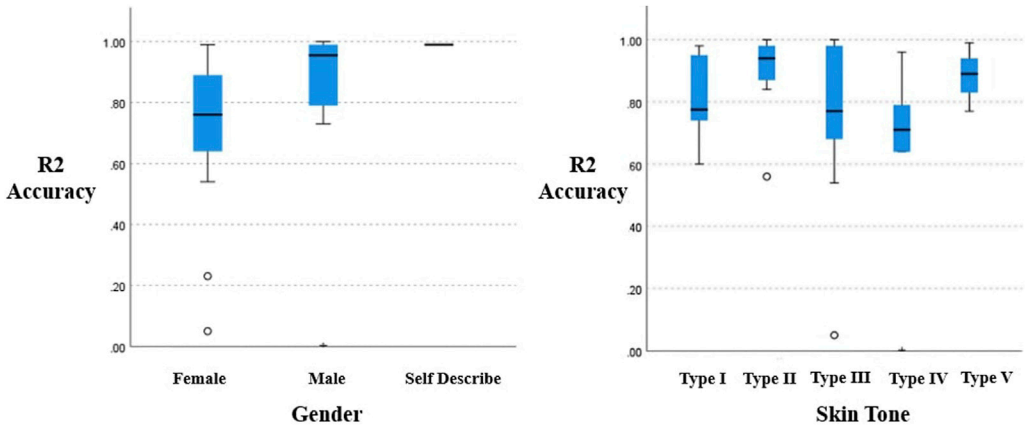

FIGURE 4
Independent-Samples Kruskal–Wallis Test for (left) H_{2_1} and (right) H_{2_2}. The graph on the right shows skin tone categories categorized according to the Fitzpatrick skin tone scale.

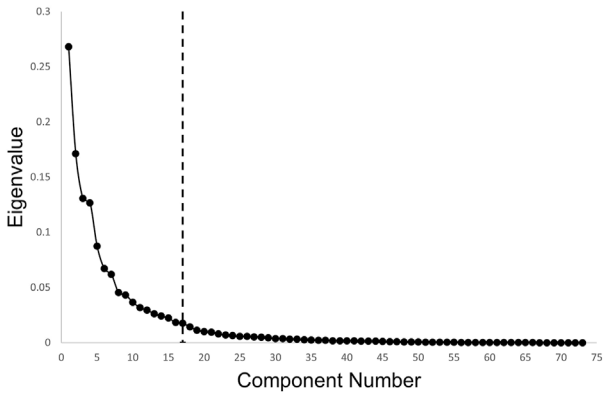

FIGURE 5
Scree Plot for Behaviour Identity Features: From the scree plot, it can be observed that 17 features are sufficient to explain 90% of the variance in the dataset, indicating that these features contain the most important information for the analysis.

similar in nature, and the differences between them are relatively small. However, when dealing with non-uniform tasks like reading or speaking, the inputs can exhibit significant differences and variations, leading to suboptimal results when using a Siamese network. Hence, we have excluded Siamense networks from our work.

3.3.2 Data processing protocol

By comparing the classification accuracy of all four datasets, we selected the model that got the largest number of highest scores as the best model for behavioural identity detection from the above-mentioned models. The accuracy of the chosen model was then used to test RQ_2.

3.4 Procedure

We conducted the study in a room isolated from visual or audio distractions. When the participants arrived, we gave them a consent form explaining the study and its purpose. Once they agreed to participate and signed the consent form, we asked them to wear the VR headset. Before starting the session, we calibrated the eye-tracker and inter-pupillary distance. The hand controller's trigger button was used to interact with the VR system. The researcher then briefed the participants on interacting with the system and introduced them to the hand controller buttons. After the participants felt confident controlling the scrolling of the example story dialogue with the two buttons ("Up" and "Down") in VR, they clicked the "Start" button and began **R1** with an actual story.

Then, we asked participants to retell the story in their own words after pressing the "Start" button again. The **R2** stage was also similar to the **R1** stage but with a different story. Finally, before starting **S2**, we described the nature of identity-detection algorithms and instructed the participant to retell the story while attempting to thwart the detection by adopting any strategy they wanted. Participants were given 10-min breaks between the above stages, and mints were provided. After the break, we verbally confirmed the participant's physical health condition regarding cybersickness before advancing to the next stage. Participants answered the questionnaire using a tablet computer when they finished the session and received a $20 gift card as a token of appreciation.

4 Results

4.1 Identity detection accuracy

Before we tested the dataset, we completed training the identity-detection models using the classification algorithms described in Section 3.3.1 with the **R1** dataset. With the trained models, we tested the **R2**, **S1** and **S2** datasets, and we provide each classification model's training and testing accuracy in Table 3. The results indicate that FCNN and SNN show the highest accuracy in **R2**, **S1**, and **S2** (see Figure 3). Accuracy for the **R1** dataset (training dataset) varied from 92.7% to 100%. The trained models classified the **R2** dataset with accuracy ranging from 41.7% to 86.6%, the **S1** dataset with accuracy ranging from 60.1% to 79.4% and the **S2**

TABLE 5 Feature Types Accounting for 90% of the Variance According to the Principal Component Analysis: The ranking of the features in descending order of importance is crucial information because it provides insights into the underlying structure of the dataset. The most important features at the top of the list are the ones that contribute the most to the variability in the dataset, while the less important features towards the bottom of the list have a smaller impact.

Ranking	Feature name	Ranking	Feature name
1	Eye_Left_Blink	10	Eye_Right_Down
2	Eye_Right_Blink	11	Head_position_Z
3	Right_controller_position_X	12	Eye_Left_Down
4	Right_controller_position_Z	13	Eye_Left_Squeeze
5	Right_controller_position_Y	14	Eye_Right_Squeeze
6	Jaw_Open	15	Left_controller_position_X
7	Left_controller_position_Z	16	Mouth_Smile_Right
8	Tongue_LongStep1	17	Eye_Left_Left
9	Head_position_X		

dataset from 46.5% to 77.56%. Since SNN showed the most consistent accuracy for all the tasks among all the models tested, we selected SNN as the best-performing model for behavioural identity detection in our research.

4.1.1 Accuracy during behavioural change

We analysed how people controlled their behaviour identity detection rate by changing the behaviour at a single user level. The accuracy difference between **S1** and **S2** tasks is shown in Table 4. Participants reported that they intentionally tried to change blinking patterns, mouth movements, hand gestures, and eye-ball movements, compared to their normal behaviour. Our results indicate that 12.5% of the participants reported a more than 60% accuracy decline.

4.2 Impact of personal attributes

We selected SNN as a reference baseline to investigate the impact of the user's appearance on identity detection accuracy (RQ_2), since SNN produced the best overall testing results for all four tasks (see section 4.1). We analysed the hypotheses for RQ_2 using IBM SPSS Statistics software version 28.0.1.1(15). Before we ran the statistics, we conducted a Shapiro-Wilk test to confirm the normality of the SNN classification results for each user with the **R2** dataset. Since all datasets failed to pass the normality test ($p < 0.001$), we conducted a non-parametric Kruskal–Wallis test.

4.2.1 Gender impact

We tested hypothesis H_{2_1} with the **R2** dataset. First, we conducted an independent-samples Kruskal–Wallis test, which showed that participant gender affected the accuracy of the behavioural identity detection algorithm, $H(2) = 9.798$, $p = 0.007$ (Figure 4(left)). Hence, we rejected the null hypothesis. Males ($Mdn = 0.9550$) were more detectable by these algorithms than females ($Mdn = 0.76$). We then conducted a pairwise comparison to find the group with a significant difference. Only the group Female-Male was reported as significant ($p < 0.50$). Here the significance values have been adjusted by Bonferroni correction for multiple tests.

4.2.2 Personal appearance attribute impact

We tested hypotheses H_{2_2} (Skin Tone), H_{2_3} (Hand Dominance) and H_{2_4} (Facial Hair) with the **R2** dataset. First, we conducted an independent-samples Kruskal–Wallis test which showed that there was no significance impact over the behavioural identity detection accuracy from any of these variables (Skin Tone: $H(4) = 6.6657$, $p = 0.115$; Hand Dominance: $h(1) = 0.926$, $p = 0.336$; Facial Hair: $h(1) = 2.397$, $p = 0.122$). Hence, we accepted the null hypotheses for these variables. Figure 4(right) shows the independent-samples Kruskal–Wallis test results for the skin tone.

5 Discussion

In this section, we explain our findings from the user study, and whether they support our hypotheses, thus helping us address our research questions. We numbered our research questions and hypotheses, and represent each within the headings below. Please refer to the Introduction section for longer descriptions.

5.1 RQ_1: Can user behaviour data be used to identify particular users in VR?

5.1.1 Machine learning classification models can accurately identify VR users (H_{1_1})

In the **R1** dataset, all five models were able to achieve an accuracy greater than 92%. On the other hand, in the **R2** dataset, all five models achieved an accuracy greater than 41%, with the highest accuracy being 83%. Among all the models, the SNN had the highest overall accuracy, which is why we selected it as the best model for detecting behavioural identity. It is worth noting that five out of six models demonstrated better-than-chance accuracy in identifying a particular user.

Based on the results of our analysis, we concluded that these classification models are reliable for behavioural identity detection tasks and can perform well with data gathered across multiple sessions. Therefore, regardless of the application or session in which the behavioural identification data is collected, it can be

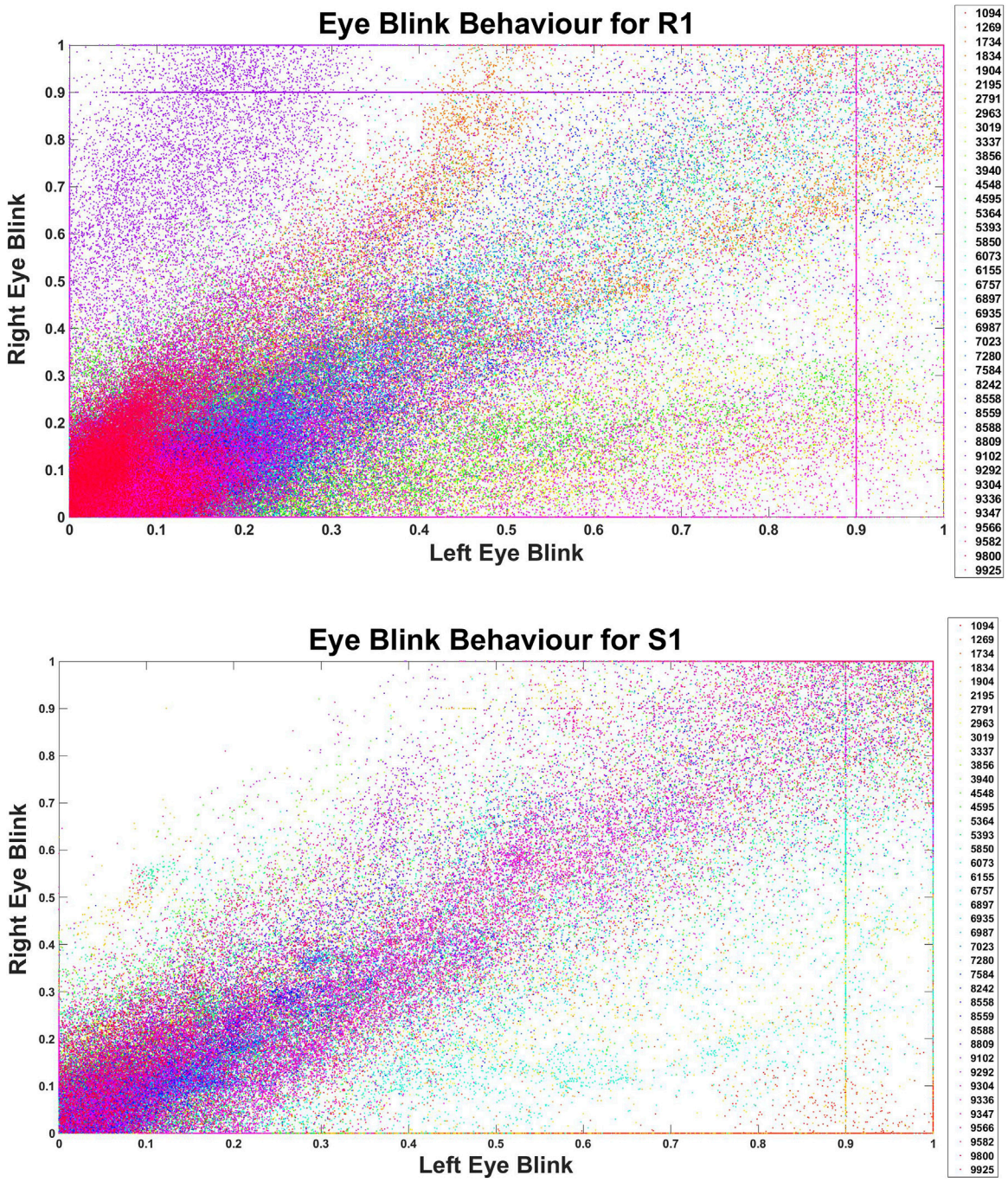

FIGURE 6
Eye Blinking Behaviour for Different Task Types: Each user was given a unique four-digit number generated randomly as the user ID during the study, and here, each user ID is represented with a different colour.

used to identify the user in the same type of activities routinely. We collected data with a frequency of 60Hz, and after training, only one data record was enough to identify a user. This means that a user could be identified with a minimum delay of 0.017 s. However, this time may vary depending on the HMD frequency and the identity detection logic used.

It is evident that once this identity detection model is trained, it can identify a user even with minimal VR exposure. Therefore, we conclude that identifying a person without significant delays is possible, especially with considerably greater data capture rates that are expected to be possible in the future.

5.1.2 Once trained, machine learning classification models are reusable for separate tasks (H_{1_2})

Using the **S1** dataset, we tested all six models. Surprisingly, all models successfully classified the dataset with greater than 60%

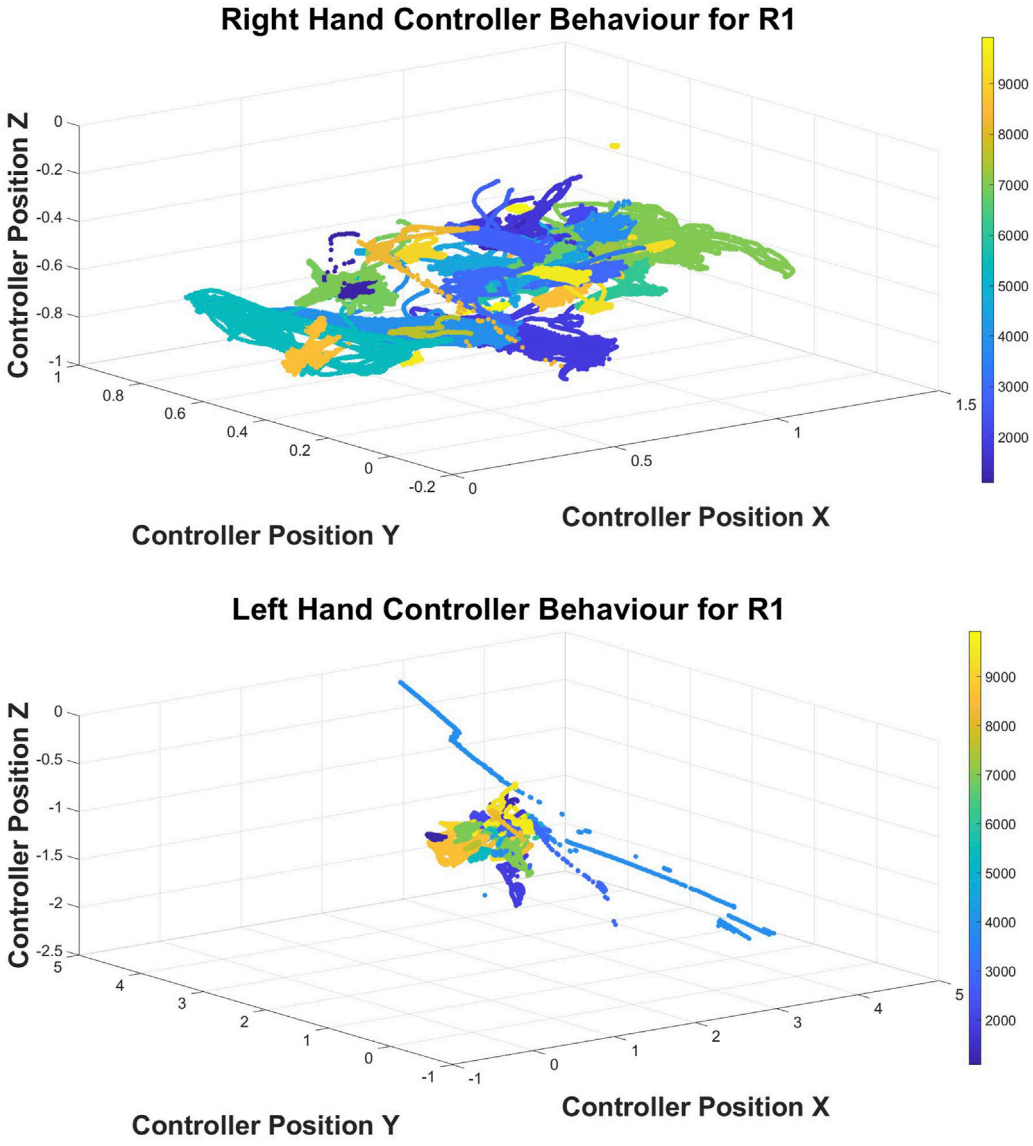

FIGURE 7
Left and Right Hand Controller Movement Behaviour for **R1**. As before, each user ID is represented with a different color.

accuracy, and SNN classified users with 80% accuracy. The notable accuracy of the SNN model suggests that once an identity profile, calibrated for a specific task, is established, it possesses the flexibility to be adaptively applied to other activities that exhibit similar levels of physical exertion. This adaptability underscores the potential of SNN models in dynamic environments where user tasks may vary yet share underlying behavioural patterns.

Further, the analysis of behavioural graphs, particularly as illustrated in Figure 6, is instrumental in elucidating the recognition of individuals across varying tasks. These graphs reveal that despite the distinctive nature of each task, a consistent pattern in user behaviour exists. This consistency is crucial as it forms the basis for behaviour detection algorithms, enabling them to identify users across different sessions and tasks effectively.

In-depth scrutiny of these behavioural patterns reveals that the algorithms are not merely capturing surface-level activity but are discerning subtler, consistent behavioural traits that are less apparent but equally significant. This insight is critical for refining the development of behaviour detection algorithms, ensuring they are sensitive to overt and covert user behaviour patterns.

In summary, the findings from this study provide substantial evidence that behaviour detection algorithms, particularly those based on SNN models, can identify users with high accuracy across a range of tasks. This capability is rooted in the algorithms' proficiency in detecting underlying behavioural consistencies, making them valuable tools in scenarios where accurate user recognition is imperative. The implications of these findings are profound, especially in the context of developing sophisticated models for behaviour tracking in virtual environments. Equally, these results raise concerns about the privacy risks when a user gives their permission to utilise

behavioural identity approaches for certain tasks in VR, as the resulting behavioural identity profile could also be used to accurately identify the user in other contexts and/or at other times. Hence, this field continually seeks to balance user privacy with the need for accurate data capture and avatar expressiveness.

5.1.3 Machine learning classification remains accurate, even when users intentionally change their behaviours (H_{1_3})

We evaluated the S2 dataset using six distinct classification methodologies in our empirical investigation. Remarkably, even the least performant model in this ensemble, the fine tree classifier, demonstrated a baseline accuracy of 47%. This observation underscores the inherent robustness of classification algorithms in behaviour analysis. The Fully Convolutional Neural Network (FCNN) exhibited the most noteworthy performance, which achieved an impressive accuracy of 77.56%. This high degree of accuracy highlights the advanced capabilities of neural network architectures in discerning nuanced behavioural patterns.

A pivotal aspect of our study involved assessing accuracy at the individual participant level. Here, it was observed that a mere 20% of participants could diminish the classification accuracy by a substantial margin of 40%. This finding indicates individuals' challenges in consciously altering their behavioural patterns to evade detection by sophisticated classification systems. Intriguingly, approximately 25% of participants exhibited higher accuracy rates than the S1 test, where natural behaviour was expected. This paradoxical outcome suggests a complex interplay between conscious behavioural modification and the inherent capability of classification algorithms to adapt or generalize from such modifications.

A comparative analysis of the behaviour feature graphs revealed a critical insight: the clusters of behaviour did not exhibit significant divergence, notwithstanding attempts by participants to modify their habitual behaviour. This observation suggests that more than superficial behavioural variations are required to substantially impair the efficacy of clustering algorithms, particularly those equipped with extensive feature sets.

Consequently, our findings underscore a significant challenge in virtual environments: most individuals need help to effectively shield themselves against behaviour-based classification models, even with awareness of the potential privacy threats posed by behaviour identity detection systems. This vulnerability is a technological issue and a fundamental concern regarding user privacy in virtual spaces.

The implications of our study are profound, emphasizing the urgent need for platform-level interventions to safeguard the privacy rights of users in virtual reality environments. Such measures are not merely advisable but essential, as they address a critical gap in user autonomy and privacy protection in the rapidly evolving domain of virtual reality.

5.2 RQ_2: Does the user's appearance impact identity detection accuracy?

5.2.1 Males are more identifiable than females (H_{2_1})

Our research indicates that when using the SNN model for behaviour-based identity detection algorithms with the above-mentioned parameters, the identification accuracy for males is higher than for females. Hence, our system suggests that females are slightly more protected against such privacy concerns arising from behavioural data within the given context. However, from the data we have collected, it is hard to provide a reasonable explanation for this gender-based disparity. Therefore, we recommend further research to explore this phenomenon and gain a better understanding of the underlying factors contributing to this disparity.

5.2.2 Skin tone does not affect behaviour identity detection accuracy (H_{2_2})

Because of differences in light reflectance wavelength, various skin tones react differently to different sensor types (Fallow et al., 2013). Therefore, we attempted to identify at least some skin types that might benefit from this difference against these behavioural identity detections. However, results show that, under the given conditions, skin tone does not influence the accuracy of these machine learning classification algorithms.

5.2.3 Dominant hand does not affect behaviour identity detection accuracy (H_{2_3})

We tested this hypothesis to find whether the behaviour changes that come with the dominant hand impact the user's behaviour identity detection. Nonetheless, the results reveal that, under the given conditions, the dominant hand of the VR user does not affect his or her identity detection accuracy.

However, when we study the behavioural clusters for the left hand and right hand, we can see more distinct behavioural clusters for the right hand than for the left hand. These graph patterns perfectly matched the dataset consistency, which included only five people who were left-hand dominant. Nevertheless, when these features are analysed with many other features, clustering algorithms can still identify users accurately.

5.2.4 Facial hair does not affect behaviour identity detection accuracy (H_{2_4})

We tested how these algorithms work when VR users have beards or moustaches. However, the results demonstrated that, under the given conditions, the presence of facial hair did not affect the accuracy of these algorithms.

Upon careful analysis of all the results, it is abundantly clear that VR stands to benefit significantly from technical solutions that empower users with proactive measures to protect their behavioural privacy. As such, we meticulously examined the data to identify the data points that exhibit the highest variance. Therefore, future research efforts should concentrate more on these data types when developing behavioural privacy solutions. Hence, to identify the component with the highest variance, we conducted a principal component analysis (PCA) on the entire dataset consisting of all 73 features. Figure 5 shows that 90% of the variance is included in 17 features from 73 features. Table 5 shows the 17 features with the highest variance according to the first component of the PCA. Figure 6 and 7 depict the patterns of behaviour of certain critical aspects for the four different tasks, **R1**, **R2**, **S1** and **S2**.

5.3 Implications

After training and testing our behavioural identity detection system, we have identified several implications related to the system discussed in this paper. The above findings illustrate that once a behavioural identity detection classifier is trained, it can be used to correctly identify that individual across various types of applications in VR, including other tasks with equivalent physical activity levels, for example, reading and speaking. Furthermore, user attempts to thwart these classifiers by altering their behaviour are largely ineffective. In our study, we found that behaviour classifiers are robust to common physical characteristics, such as facial hair, hand dominance, or skin tone, as they did not affect the performance of the classifiers.

Based on our results and observations, we conclude that the privacy risks invariably exceed the advantages of reliable behavioural user identification systems for VR user security purposes. Since these behaviour identity detection systems are bound to each user's habitual actions, removing the behavioural "digital finger print" is impossible if these identity data are compromised. Unfortunately, there are several gaps in the VR application process through which third parties may obtain this vital data (Nair et al., 2022a). Furthermore, at the beginning of the study, when we mentioned to the participants that their behaviours could be used to identify them uniquely, everyone was astonished at how damaging it could be to their privacy. This hints at how individuals might reject behavioural tracking if they knew what they were getting themselves into. Currently, it is presumed that users still do not understand the potential of the tracked behaviour data fully in the VR context, and there are insufficient policies or systems in place to prevent it. Thus, we conjecture that the privacy threats associated with these behaviour identity detections can be high in VR.

We firmly believe that if researchers, regulators and major tech firms do not take sufficient steps to shield VR users from potential behavioural privacy issues, the privacy threats associated with these behaviour identity detection approaches will plague many future VR users. Furthermore, protecting user privacy is not just a choice but an obligation that we, as researchers, must fulfill. Hence, we firmly believe that privacy is a fundamental right that should be respected rather than a mere privilege.

Finally, we wish to use these findings to emphasise the significance of developing new technical solutions to safeguard VR users from the privacy threats that could emerge from these behaviour identity detection approaches, even as these were initially intended to provide security for VR users as authentication systems.

6 Limitations and future works

The tasks we have selected have the same physical activity level. However, these results could change if the models were trained and tested with activities that require a different level of physical movement; for example, be trained with reading-activity behavioural data but tested with ball-throwing activity behavioural data. Also, we collected data for both sessions on the same day. Collecting data with a time gap of at least 3 days could decrease the accuracy of these models (Miller et al., 2021). One potential area for improvement in this study is the randomization of the two main tasks. While a washout time was given, randomizing the tasks would have further strengthened the study's design and reduced the likelihood of any confounding variables impacting the results. It has been identified that not recording the participant's prior experience level with VR is a limitation in our study. To gain a more comprehensive understanding of the results obtained, it would be beneficial to record this parameter.

As a constructive next step in this study, we aim to implement and test the effectiveness of behavioural privacy filters that give users more control over when and what behaviour data is shared with different applications. Consequently, we will explore how these filters can enhance or affect collaboration in immersive environments as well.

7 Conclusion

This paper examined the underlying privacy dangers that behavioural identity detection technologies in VR potentially pose. First, we demonstrated that even simple classification approaches could identify the participants with a high detection rate utilising behavioural features in VR. Following that, we investigated how reliably these trained classifiers can be used to identify the same person performing different tasks. The study then demonstrated how ineffective intentional user behaviour changes are to circumvent these classifiers. Then, we investigated the impact of the user's physical attributes on the classification of behavioural identity. Finally, we demonstrated the behavioural data types with the highest variance, which should be assigned a higher priority when creating behavioural privacy protection solutions such as behaviour filters. These findings highlight the importance of offering greater privacy protection tools for VR users to benefit both VR consumers and the VR industry. Also, while numerous models exist in the literature for detecting identity from user behaviour, our main objective in this study was not to reproduce and evaluate all of them. Instead, we focused on highlighting the potentially harmful capabilities of some of this field's most widely used models. Specifically, we sought to demonstrate the dangers these models pose to user privacy and underscore the importance of further research to mitigate these risks. To the best of our knowledge, this is the first study to investigate the link between user appearance and the accuracy of behaviour identity recognition through a formal user study. By presenting this information, we aim to provide a constructive approach towards developing effective privacy solutions, such as behaviour filters. We hope this knowledge will inspire innovative solutions prioritising user privacy while allowing for a positive, immersive experience.

Data availability statement

The datasets presented in this article are not readily available because the dataset is only available to the researchers involved in this study due to the ethics approval conditions. Requests to access the datasets should be directed to Dilshani Kumarapeli, kumarapeli.kumarapeli@pg.canterbury.ac.nz.

Ethics statement

The studies involving humans were approved by Human Research Ethics Committee, University of Canterbury, New Zealand. The studies were conducted in accordance with the local legislation and institutional requirements. The participants provided their written informed consent to participate in this study.

Author contributions

DK, SJ, and RL designed the study after analysing the current status of behaviour based identity detection in VR. DK was responsible for the implementation of the study, including data collection, analysis, and interpretation. SJ and RL provided input into the study design and methodology. All authors contributed to the article and approved the submitted version.

Funding

This research has been fully funded by Science for Technological Innovation funds.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Supplementary material

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/frvir.2024.1197547/full#supplementary-material

References

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

Altman, N. S. (1992). An introduction to kernel and nearest-neighbor nonparametric regression. *Am. Statistician* 46, 175–185. doi:10.1080/00031305.1992.10475879

Bailenson, J. (2018). Protecting nonverbal data tracked in virtual reality. *JAMA Pediatr.* 172, 905–906. doi:10.1001/jamapediatrics.2018.1909

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

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

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

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

Falk, B., Meng, Y., Zhan, Y., and Zhu, H. (2021). "Poster: reavatar: Virtual reality de-anonymization attack through correlating movement signatures," in Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, November, 2021, 2405–2407. doi:10.1145/3460120.3485345

Fallow, B. A., Tarumi, T., and Tanaka, H. (2013). Influence of skin type and wavelength on light wave reflectance. *J. Clin. Monit. Comput.* 27, 313–317. doi:10.1007/s10877-013-9436-7

Fawaz, H. I., Forestier, G., Weber, J., Idoumghar, L., and Muller, P.-A. (2018). "Transfer learning for time series classification," in 2018 IEEE international conference on big data (Big Data), Seattle, WA, USA, December, 2018, 1367–1376.

Fitzpatrick, T. (1975). Sun and skin. *J. de Med. Esthetique* 2, 33–34.

Giaretta, A. (2022). Security and privacy in virtual reality–a literature survey. https://arxiv.org/abs/2205.00208.

Gordon, J. R., Curran, M. T., Chuang, J., and Cheshire, C. (2021). "Covert embodied choice: decision-making and the limits of privacy under biometric surveillance," in Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, May, 2021. doi:10.1145/3411764.3445309

Hosfelt, D. (2019). Making ethical decisions for the immersive web. https://arxiv.org/abs/1905.06995.

Hosfelt, D., and Shadowen, N. (2020). Privacy implications of eye tracking in mixed reality. https://arxiv.org/abs/2007.10235.

Jones, J. M., Duezguen, R., Mayer, P., Volkamer, M., and Das, S. (2021). "A literature review on virtual reality authentication," in *Human aspects of information security and assurance*. Editors S. Furnell, and N. Clarke (Cham, Germany: Springer International Publishing), 189–198.

Khamis, M., Trotter, L., Mäkelä, V., Zezschwitz, E. v., Le, J., Bulling, A., et al. (2018). Cueauth: comparing touch, mid-air gestures, and gaze for cue-based authentication on situated displays. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 1–22. doi:10.1145/3287052

Khraisat, A., Gondal, I., Vamplew, P., and Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity* 2, 20. doi:10.1186/s42400-019-0038-7

Kuhn, M., and Johnson, K. (2016). *Applied predictive modeling*. Berlin, Germany: Springer.

Kumarapeli, D., Jung, S., and Lindeman, R. W. (2023). "Privacy threats of behaviour identity detection in VR," in 2023 IEEE conference on virtual reality and 3D user interfaces abstracts and workshops (VRW), Shanghai, China, 861–862. doi:10.1109/VRW58643.2023.00273

Kupin, A., Moeller, B., Jiang, Y., Banerjee, N. K., and Banerjee, S. (2019). "Task-driven biometric authentication of users in virtual reality (vr) environments," in *MultiMedia modeling*. Editors I. Kompatsiaris, B. Huet, V. Mezaris, C. Gurrin, W.-H. Cheng, and S. Vrochidis (Cham, Germany: Springer International Publishing), 55–67.

Li, S., Ashok, A., Zhang, Y., Xu, C., Lindqvist, J., and Gruteser, M. (2016). "Whose move is it anyway? authenticating smart wearable devices using unique head movement patterns," in 2016 IEEE International Conference on Pervasive Computing and Communications (PerCom), Sydney, NSW, Australia, March, 2016, 1–9. doi:10.1109/PERCOM.2016.7456514

Liebers, J., Abdelaziz, M., Mecke, L., Saad, A., Auda, J., Gruenefeld, U., et al. (2021). "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, Yokohama Japan, May, 2021. doi:10.1145/3411764.3445528

Madary, M., and Metzinger, T. K. (2016). Real virtuality: a code of ethical conduct. recommendations for good scientific practice and the consumers of vr-technology. *Front. Robotics AI* 3, 3. doi:10.3389/frobt.2016.00003

Mathis, F., Williamson, J., Vaniea, K., and Khamis, M. (2021). Fast and secure authentication in virtual reality using coordinated 3d manipulation and pointing. *ACM Trans. Computer-Human Interact.* 28, 1–44. doi:10.1145/3428121

Miller, M. R., Herrera, F., Jun, H., Landay, J. A., and Bailenson, J. N. (2020). Personal identifiability of user tracking data during observation of 360-degree VR video. *Sci. Rep.* 10, 17404. doi:10.1038/s41598-020-74486-y

Miller, R., Banerjee, N. K., and Banerjee, S. (2021). "Using siamese neural networks to perform cross-system behavioral authentication in virtual reality," in 2021 IEEE Virtual Reality and 3D User Interfaces (VR), Lisboa, Portugal, March, 2021, 140–149. doi:10.1109/VR50410.2021.00035

Miller, R., Banerjee, N. K., and Banerjee, S. (2022a). "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), Christchurch, New Zealand, March, 2022, 409–418. doi:10.1109/VR51125.2022.00060

Miller, R., Banerjee, N. K., and Banerjee, S. (2022b). "Using external video to attack behavior-based security mechanisms in virtual reality (vr)," in 2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Christchurch, New Zealand, March, 2022, 684–685. doi:10.1109/VRW55335.2022.00193

Mustafa, T., Matovu, R., Serwadda, A., and Muirhead, N. (2018). "Unsure how to authenticate on your vr headset? come on, use your head," in Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics, Tempe AZ USA, March, 2018, 23–30. doi:10.1145/3180445.3180450

Nair, V., Garrido, G. M., and Song, D. (2022a). Exploring the unprecedented privacy risks of the metaverse. https://arxiv.org/abs/2207.13176.

Nair, V., Garrido, G. M., and Song, D. (2022b). Going incognito in the metaverse. https://arxiv.org/abs/2208.05604.

Pishva, D. (2007). Multi-factor authentication using spectral biometrics. *J. Jpn. Soc. Fuzzy Theory Intelligent Inf.* 19, 256–263. doi:10.3156/jsoft.19.256

Prosser, W. (1960). Privacy. *Calif. Law Rev.* 48, 383–389. doi:10.2307/3478805

Quinlan, J. R. (1986). Induction of decision trees. *Mach. Learn.* 1, 81–106. doi:10.1007/BF00116251

Quintero, L., Papapetrou, P., Hollmén, J., and Fors, U. (2021). "Effective classification of head motion trajectories in virtual reality using time-series methods," in 2021 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), Taichung, Taiwan, November, 2021, 38–46. doi:10.1109/AIVR52153.2021.00015

Rafique, M. U., and Cheung, S.-c. S. (2020). Tracking attacks on virtual reality systems. *IEEE Consum. Electron. Mag.* 9, 41–46. doi:10.1109/MCE.2019.2953741

Rathgeb, C., and Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J. Inf. Secur.* 2011, 3. doi:10.1186/1687-417X-2011-3

Revett, K. (2008). *Behavioral biometrics: a remote access approach*. Hoboken, New Jersey, United States: John Wiley & Sons.

Rogers, C. E., Witt, A. W., Solomon, A. D., and Venkatasubramanian, K. K. (2015). "An approach for user identification for head-mounted displays," in Proceedings of the 2015 ACM International Symposium on Wearable Computers, Osaka Japan, September, 2015, 143–146. doi:10.1145/2802083.2808391

Satybaldy, A., Nowostawski, M., and Ellingsen, J. (2020). *Self-sovereign identity systems*. Cham, Germany: Springer International Publishing, 447–461. doi:10.1007/978-3-030-42504-3_28

Schmidhuber, J. (2015). Deep learning in neural networks: an overview. *Neural Netw.* 61, 85–117. doi:10.1016/j.neunet.2014.09.003

Shadowen, N., and Hosfelt, D. (2020). Addressing the privacy implications of mixed reality: a regulatory approach. https://arxiv.org/abs/2007.10246.

Shen, Y., Wen, H., Luo, C., Xu, W., Zhang, T., Hu, W., et al. (2019). Gaitlock: protect virtual and augmented reality headsets using gait. *IEEE Trans. Dependable Secure Comput.* 16, 484–497. doi:10.1109/TDSC.2018.2800048

Solove, D. (2007). 'i've got nothing to hide' and other misunderstandings of privacy. *San. Diego Law Rev.* 44.

Wang, X., and Zhang, Y. (2021). "Nod to auth: fluent ar/vr authentication with user head-neck modeling," in Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama Japan, May, 2021. doi:10.1145/3411763.3451769

Yaremych, H. E., and Persky, S. (2019). Tracing physical behavior in virtual reality: a narrative review of applications to social psychology. *J. Exp. Soc. Psychol.* 85, 103845. doi:10.1016/j.jesp.2019.103845

Yu, Z., Liang, H.-N., Fleming, C., and Man, K. L. (2016). An exploration of useable authentication mechanisms for virtual reality systems. In 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS). Jeju, Korea (South), October, 2016, 458–460. doi:10.1109/APCCAS.2016.7804002