Privacy in Motion: Implementing Differential Privacy for User Motion in VR

RUOXI SUN, CSIRO's Data61, Australia
HANWEN WANG, The University of Adelaide, Australia
MINHUI XUE, CSIRO's Data61, Australia
HSIANG-TING CHEN, The University of Adelaide, Australia

The rising adoption of immersive environments presents a significant challenge in balancing service providers' desire to collect user behaviour data with users' privacy concerns. Striking a balance between data collection and privacy protection becomes crucial in this context. As these technologies become more integrated into everyday life, the need for robust and privacy-preserving technologies grows to ensure users' trust and confidence while enabling service enhancements and targeted advertising. Our research explores implementing differential privacy algorithms in VR applications to enable statistical analysis of 3D spatial motion data while protecting user anonymity and evaluating the balance between data utility and privacy. Two datasets were used to conduct the experiments. First is an indoor activities data with simulated agents (N = 7). The second is a public 3D motion capture dataset of users playing VR sport games (N = 16). We assessed the efficacy of DP on both the original 3D spatial data and its cumulative heat map representation. Experimental results reveal that our approach effectively preserves data utility (with threshold $RSE \leq 1$) while reducing the accuracy of the re-identification attack model from 93.89% to 48.03% (through window-slicing) and from 96.53% to 55.37% (through heat map conversion). This study underscores the utility of the DP algorithm in the context of 3D body motion data, highlighting broad applicability across diverse VR contexts while ensuring user anonymity.

ACM Reference Format:
Ruoxi Sun, Hanwen Wang, Minhui Xue, and Hsiang-Ting Chen. 2024. Privacy in Motion: Implementing Differential Privacy for User Motion in VR. 1, 1 (October 2024), 14 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The global VR market was valued at 28 billion US dollars in 2022 and is projected to grow at a compound annual growth rate (CAGR) of 13% from 2023 to 2030 [1]. Leading tech companies invest heavily in VR, with Meta introducing its cutting-edge VR headset, the Meta Quest Pro [3], and reports suggesting that Apple has a team of 3,000 employees dedicated to their upcoming VR headset [16]. Consumer interest in applications such as gaming, fitness, and social experiences has steadily grown over the past decade. Notably, during the COVID-19 pandemic [2], VR has played a pivotal role in driving innovation in fields like art, healthcare, and education.

As VR devices become more widely adopted, researchers express increasing concerns about privacy issues in many VR applications [6, 9, 19]. On one hand, VR technology is rapidly evolving, and VR device companies understandably seek to continuously monitor user behaviour data to improve user experiences and the performance of VR systems [23]. On the other hand, it can be argued that the privacy risks associated with VR applications are potentially more severe than those of mobile applications. This is due to the extensive collection of users' personal information by various input/output devices and sensors [4]. For example, the seemly standard data from VR headsets and controllers can inadvertently disclose users' biometric details, such as height and body shape [26]. Furthermore, the dynamic data captured by motion sensors can even unveil users' preferences and opinions towards virtual content, as evidenced by the analysis of eye-tracking data [14]. Moreover, recent studies have revealed that users can be identified with an accuracy exceeding 90% when compared to a database of over 50,000 individuals, based on just 100 seconds of motion

Authors' addresses: Ruoxi Sun, CSIRO's Data61, Australia; Hanwen Wang, The University of Adelaide, Australia; Minhui Xue, CSIRO's Data61, Australia; Hsiang-Ting Chen, The University of Adelaide, Australia.

recorded during VR gaming sessions [24]. Striking a delicate balance between data collection and privacy preservation is imperative to enable the ongoing enhancement of VR technologies while respecting users' privacy and security.

Differential privacy (DP) is a mathematical framework that provides a strong guarantee of privacy by allowing data to be analyzed without revealing sensitive information about any individual in the dataset [12]. DP has been applied across diverse domains, such as concealing demographic census data [15] and safeguarding the privacy of Uber drivers and riders during analysis [20]. However, there is limited research on the use of DP in VR applications. Nair *et al.* [13] proposed the pioneering concept of "VR Incognito Mode", which uses DP to obscure sensitive user data attributes, such as user height, wingspan, or room size. However, it is unclear how to apply DP on 3D body motion data, such as head or hand movement, which has been shown vulnerable to re-identification attacks [24, 26].

To address this knowledge gap, we present two simple yet effective approaches to apply DP mechanism on 3D body motion data from VR applications. Our goal is to safeguard user privacy by preventing re-identification attack while retaining valuable statistical information, such as the average head and hand movements of users. This data is vital for enhancing the gaming experience and gaining insights into user preferences in virtual social or shopping spaces. Our first approach involves the direct application of DP onto the 3D body motion data while our second approach transforms the spatial data into 2D heat maps before applying DP. We evaluated the effectiveness of our privacy protection method using two VR datasets. The first dataset emulates indoor activities collected by the VirtualHome simulator [27], while the second dataset captures user motion in a VR sports game [21]. The experimental findings demonstrate that our method successfully maintains data utility (with an RMSE threshold set to 1) while diminishing the accuracy of the re-identification attack model from 93.89% to 48.03% (via window-slicing) and from 96.53% to 55.37% (through heat map conversion), indicating that heat map conversion is more effective.

Contribution

- We conduct experiments to apply Differential Privacy (DP) to 3D body motion data, aiming to protect user privacy while preserving data utility.
- We suggest a novel approach of transforming 3D body motion data into heat maps prior to applying DP, which enhances the efficacy of DP.
- We assess our method using both synthetic and real-world body motion datasets, specifically focusing on their resilience against re-identification attacks.

Our findings indicate that, despite the wealth of data being collected, user privacy can be preserved while still permitting data analysis for various purposes within an immersive environment. Given the rapid evolution of VR and sensor technologies, and the increasing collection of user behaviour data for analysis, there is a pressing need for more research dedicated to privacy-preserving approaches, such as DP.

2 RELATED WORK

Recent studies have revealed the ease with which attackers can identify [22, 25, 29–32, 40] and create profiles of VR users [28, 34] using just a few minutes of data streaming. Furthermore, these studies have highlighted that the extent and magnitude of data collection in VR surpass the capabilities of current internet platforms. The immersive nature of VR contributes to these vulnerabilities, as it can make users more susceptible to self-disclosure[33] and social engineering [5].

In contrast to current Internet platforms, where users have options like Tor, VPNs, proxies, and incognito mode to protect against user tracking and profiling, there is a lack of equivalent and robust defense mechanisms to address the unique threats in VR. Existing literature provides a fragmented collection of privacy defenses that are still in the proof-of-concept stage, with limited application in commercial-grade solutions. Moreover, industry practices in the VR domain are not reassuring. Vulnerabilities in VR devices have been identified, some developers disregard their own privacy policies, and updates tend to prioritize increased data collection [35].

In our threat model, privacy breaches occur when attackers gather and infer sufficient information to consistently identify and extensively profile a user across multiple usage sessions in VR applications (referred to as tracking). Attackers achieve identification (*i*) by distinguishing the user from others in a unique manner and (*ii*) profiling users by associating unwarranted information with their characteristics, such as demographics, preferences, and browsing history [34].

For example, two primary entities pose threats to user privacy in this context: the developers of client-side applications running on VR devices (referred to as Application Adversaries [23]) and content creators (known as Content Adversaries [5]). Content adversaries have the ability to create immersive experiences that incorporate misleading, manipulative, and deceptive content. On the other hand, application adversaries can access input data through system APIs and manipulate the rendered frames and signals sent to VR devices, as well as the information streamed to external servers. While one server-side, server adversaries may have control over the external server. As a result, they possess the ability to manipulate and process the networked data they receive before streaming it to other users' devices in any desired manner.

We argue that without a well-designed privacy protection technique, users' privacy is threatened by both client-side and server-side adversaries. In other words, these adversaries have the capability to access users' private data and easily re-identify them.

3 USE CASES

Before diving into the methodology, we would like to introduce two use cases of our proposed privacy protection approach.

Case 1: VR Gaming. In VR gaming, the goal of privacy protection is to secure players' personal and sensitive information while providing a safe and enjoyable gaming experience. However, developers, such as gaming companies, often collect user data to analyze gameplay and enhance the gaming experience.

Consider a VR archery game where the objective is to hit the bull's eye. The bow is attached to the user's left hand, while the right hand draws the string, and arrows are loaded by moving the bow towards a virtual quiver. Developers may enhance the gaming experience by analyzing players' behaviour using body movement data collected from sensors on VR devices. This data can encompass eye tracking, hand controller positioning, and derived features like user height, reaction speed, and arm stability. Without adequate privacy protection, it could be possible to re-identify a specific user from this data. However, it's important to note that developers may not necessarily need precise body movement data from each user, as they are typically more interested in the average behaviour of all users.

Case 2: Virtual shopping mall. In another scenario, a virtual shopping mall provides an immersive and interactive environment, allowing shoppers to browse and purchase products from the comfort of their homes. This virtual environment closely mirrors a real shopping experience. Shoppers utilize VR headsets and controllers to navigate the mall, interact with objects, and even try on virtual clothing and accessories.

In this context, the company is interested in collecting spatial interaction data, such as movements within the virtual shopping mall or interactions with virtual shelves, to identify popular areas and modify the virtual environment to enhance user engagement. However, akin to the first use case, while this spatial interaction data is crucial for improving user experience, it could potentially be used to re-identify users, thus raising privacy concerns.

4 METHODOLOGY

In this section, we first introduce the background of differential privacy, followed by our method of applying differential privacy onto 3D body motion data through (*i*) window slicing and (*ii*) converting the data into heat maps. Our approach aims to safeguard data privacy while preserving its utility.

4.1 Background of Differential Privacy

Differential privacy [10, 11] is a formally recognized concept of privacy that can be mathematically validated for data releases, which has been widely used in data protection [38, 39]. Unlike k-anonymity, which is a property attributed to data, DP is a property attributed to algorithms. This implies that we can prove an algorithm's compliance with DP requirements. To assert that a dataset adheres to DP, we need to show that the algorithm used to generate it satisfies DP's principles..

Plain differential privacy. Formally, a mechanism $\mathcal{M} : \mathcal{D} \rightarrow \mathcal{R}$ with domain $\mathcal{D}$ and range $\mathcal{R}$ satisfies (plain) differential privacy if for all neighbouring datasets $d, d' \in \mathcal{D}$ and for all possible outputs $S \subseteq \mathcal{R}$ it have

$$Pr[\mathcal{M}(d) \in S] \leq e^{\epsilon} Pr[\mathcal{M}(d') \in S]. \tag{1}$$

Specifically, two datasets $d, d' \in \mathcal{D}$ are considered neighbours if they only vary in the information of a single individual. It's important to note that $\mathcal{M}$ is usually a randomised function, producing multiple possible outputs for the same input. As a result, the probability distribution describing its outputs is not a singular point distribution.

The crucial implication of this definition is that the output of $\mathcal{M}$ will remain largely unchanged, regardless of the inclusion or exclusion of any specific individual's data. In other words, the level of randomness incorporated into $\mathcal{M}$ should be sufficient to prevent an observed output from revealing whether the input was d or d'. For instance, if an individual data is present in d but not in d' an adversary would be unable to determine which of the two was the input to $\mathcal{M}$. As a result, the adversary would have no means of determining whether an individual's data was included in the input data, let alone obtaining any detailed information about that particular data.

The privacy parameter or privacy budget in the definition is denoted as ϵ. It serves as a control to adjust the "degree of privacy" provided by the mechanism. Smaller values of ϵ that should produce highly similar outputs for similar inputs, thereby offering stronger privacy protection. On the other hand, larger values of ϵ allow for greater variability in the outputs, resulting in reduced privacy.

Laplace mechanism. The most direct method to achieve DP is by incorporating random noise into the response. The primary challenge is to add enough noise to meet DP's requirements, while ensuring the answer remains meaningful and not excessively distorted. To streamline this process, the DP field has developed fundamental mechanisms that precisely outline the type and level of noise to be used.

Laplace mechanism [11] is a commonly used approach. Specifically, according to the Laplace mechanism, the following definition of $\mathcal{M}$ satisfies ϵ-differential privacy.

$$\mathcal{M}(d) = m(d) + Lap(\frac{s}{\epsilon}) \tag{2}$$

where s is the sensitivity of m which represents the amount of m's output changes when its input changes by 1 (recall the neighbouring datasets d and d'), and Lap denotes sampling from the Laplace distribution with centre 0 and scale $\frac{s}{\epsilon}$.

Approximate differential privacy. In this study, we employ the notion of approximate differential privacy, also called (ϵ, δ)-differential privacy, which is commonly used in machine learning and defined as below.

A randomized mechanism $\mathcal{M} : \mathcal{D} \rightarrow \mathcal{R}$ with a domain $\mathcal{D}$ and a range $\mathcal{R}$ achieves (ϵ, δ)-differential privacy if, for any pair of neighbouring inputs d and $d' \in \mathcal{D}$ and for any subset of outputs $S \subseteq \mathcal{R}$, the following condition is satisfied:

$$Pr[\mathcal{M}(d) \in S] \leq e^{\epsilon} Pr[\mathcal{M}(d') \in S] + \delta \tag{3}$$

where the privacy parameter δ represents the "failure probability" associated with the definition. With a probability of $1 - \delta$, the privacy guarantee provided is equivalent to pure differential privacy, while with a probability of δ, no guarantee is provided. In other words, with a probability of $1 - \delta$, we have the inequality $\frac{Pr[\mathcal{M}(d) \in S]}{Pr[\mathcal{M}(d')]} \leq e^{\epsilon}$. Due to this, it is typically required for δ to be very small, usually less than or equal to $\frac{1}{n^2}$, where n represents the size of the dataset.

4.2 Preparing Body Motion Data for DP

Outliers Dropping and Sequence Alignment. Due to individual differences among participants and varying temporal lengths of 3D body motion data, we initially remove outliers and temporally align the sequences. Data falling outside three standard deviations are considered outliers and are removed from the dataset. We use the Dynamic Time Warping (DTW) method to align sequences, thereby preserving their distinct features. Specifically, we employ a function from the 'DTAIdistance' library [8] to find values corresponding to the time length of the longest sequence and implement dynamic alignment using our user-defined function.

Window Slicing. Window slicing is a prevalent technique for training machine learning models on time series spatial data, operating on a rolling window with a predefined size, denoted as n, and a step size, denoted as m. This method iterates through each user's data recording, generating new samples at each step. We use a window size of $N = 10$ and the step size of $M = 1$ for our training and validation set for the evaluation.

From an adversary's perspective, the application of the window slicing technique involves a majority vote among the labels of all sliced windows. This approach is frequently used as it enables the attack model to identify temporal patterns and dependencies within the data, and potentially minimize noise or inaccuracies in the prediction.

Heat Map Conversion. Alongside window slicing, we explore transforming the 3D body motion data into heat maps. This approach is frequently employed in the visualization of spatial data and consequently helps to preserve the utility of the data.

Our proposed method comprises a series of steps. Initially, we calculate the range of data values on each axis, such as the X axis, represented by $[X_{max}, X_{min}]$. Subsequently, we define the resolution of the heat map as r, which determines the number of data points along each axis. By having r data points on each axis, the total number of data points in a heat map becomes $r \times r$. For each sample $x \in X$, we determine its position within the heat map using Equation 4. The "ceil" function, denoted as "$\lceil\ \rceil$", is applied to round each sample's position to the nearest integer, ensuring its placement within the heat map grid.

$$x_h = \lceil \frac{x - X_{min}}{X_{max} - X_{min}} * r \rceil \tag{4}$$

The value of each data point in the heat map is the number of samples that fall into the corresponding grid position. This provides a measure of the density or frequency of occurrences at that specific location. Lastly, to ensure consistency and comparability, we normalize the data values in the heat map to fall within the range of $[0, 1]$. This step facilitates a standardized representation of the data across various heat maps.

Heat map utility: one disadvantage of converting body motion data into heat maps is the loss of temporal information, limiting the analysis to spatial movement tracing and frequency information alone. However, as described in the use cases earlier, the omission of temporal data when sharing with vendors or third-parties have little impact the data utility. This is particularly true in scenarios such as virtual homes or virtual shopping, where the primary focus for application vendors may be recording movement traces and identifying the most frequently visited places by users. Similarly, in VR scenarios involving natural interactions like playing virtual archery, vendors may only need to collect users' average movement traces to analyse user behaviours and enhance the user experience of VR applications. Hence, for these common use cases, heat maps provide sufficient information to vendors or third-parties.

4.3 Applying DP on Body Motion Data with Utility Preserved

We then apply different privacy mechanism onto both the original motion data and the converted heat maps. To compare, we also conduct experiments applying DP on data with window slicing.

Differential privacy tool package. In this study, we utilize the IBM differential privacy library, Diffprivlib[1] [17], which offers a unified codebase and modular design making it particularly suitable for researchers conducting experiments and implementing DP models. Specifically, we use Diffprivlib's implementation of the Laplace mechanisms, initially proposed by Dwork *et al.* [11]. This implementation also supports (relaxed) (ϵ, δ)-differential privacy [18]. We leverage these mechanisms to apply differential privacy to our data, ensuring privacy protection while retaining valuable information.

Utility preserving. Often referred to as the *privacy parameter* or *privacy budget*, ϵ represents the maximum permissible deviation between queries executed on two neighboring databases (d and d'), where $d,\ d' \in \mathcal{D}$ differ by only one data change (i.e., the addition or removal of a single entry, as per Equation 1). More specifically, when ϵ is smaller, outputs generated for similar inputs must be very alike, thereby providing higher levels of privacy. On the other hand, when ϵ is larger, the outputs can exhibit greater dissimilarity, which leads to reduced privacy. Essentially, a smaller ϵ implies that more noise must be added to adequately protect the dataset's privacy.

While our primary objective is to utilize the Laplace mechanism to introduce noise and prevent the re-identification of individuals in the dataset, we also need to consider the balance between privacy protection and data utility as described in Section 3. To achieve this, we introduce a data utility threshold to control the level of noise added through the application of differential privacy. This threshold helps us avoid excessive noise that could potentially compromise the usefulness of the data while still ensuring an acceptable level of privacy.

Specifically, we can establish the data utility threshold empirically using quantitative or qualitative metrics, or a combination of both. For instance, in the case of a heat map, a qualitative threshold could be defined as "the heat map, after applying differential privacy, should still provide clear visibility of the users' movement traces". Based on this qualitative threshold, we can further determine a quantitative threshold, such as "the Relative Squared Error (RSE)

[1]https://github.com/IBM/differential-privacy-library

between the heat maps before and after applying differential privacy should be lower than t". In our study, we identify the optimal privacy budgets as the largest ϵ value that produce the output below an acceptable utility threshold, based on the ϵ-RSE chart.

5 EXPERIMENT SETUP

In this section, we introduce the datasets, user identification models, and the evaluation metrics used in our study.

5.1 Datasets

VirtualHome dataset. A technique for simulating household activities using programs, employing sequences of atomic actions and interactions as a higher-level representation of complex tasks, was introduced by Puig *et al.* [27]. The proposed simulator, VirtualHome[2], empowers users to generate a comprehensive dataset of activity videos with detailed ground-truth information, facilitating the training and evaluation of video understanding models. An example of an agent is watching TV which is generated by the simulator and demonstrated in Figure 1(a). In our study, we use some interaction sequences as the simulator input and select all existed agents as the interacted subjects. Then, we utilize the simulator to generating interacted videos and 3D spatial interacted data of virtual agents performing kinds of tasks in household scenarios (*i.e.,* 7 agents acting 852 tasks) and collect the data as our experimental dataset. For example, in one scenario, multiple agents' activities can be generated using the following description: "Go to watch TV on the couch. Turn the TV off and grab the coffee pot. Put the coffee pot on the table and go turn the light on" [27]. We collect the motion data of the agents from their starting points to the TV, then to the table, and finally to the light switch. Figure 1(b) illustrates that the movement track of agent male 1 in a 3D space. Since the head is the center of the body and has more actions than other body parts, the position of data collection is the head of each agent. After that, the results of the heat map conversion method is utilized on interacted motion data, which is shown in Figure 1(c). In this scenario, we define the data utility as 'the average motion trace of multiple users', which could be collected by the app vendor or third-parties for further data analysis.

Body Movement dataset. Liebers *et al.* [21] conducted a laboratory study involving 16 participants to investigate the accuracy of user identification. The researchers simulated two task-driven scenarios using common VR games, *i.e.,* Bowling and Archery. In these VR games, users engage in natural interactions with the game, based on their spatial movement. An illustration of the Archery game to generate Body Movement dataset is demonstrated in Figure 2(a). Spatial motion data was collected using a consumer-grade head-mounted display (HMD) and hand-held controllers. Specifically, the data recording includes Euler Angles, timestamps, and motion stages as extended data features. These features are set into distinct experimental groups to investigate their impact on identification accuracy. Furthermore, researchers have introduced a novel normalization technique which is aimed at adjusting the height and arm length ratios between users and virtual players. This adjustment is also a part of the experimental setup. In this study, researchers argue that implementing the proposed height-normalization approach on spatial motion data only would generally increase the identification rate. In our research, we adopt their dataset[3] and particularly extract the users' motion data after body normalization applied. Figure 2(b) shows an example of body movement data in a 3D space; also, the heat map converted results are shown in Figure 2 (c).

[2]The simulator is available at https://github.com/xavierpuigf/virtualhome_unity.
[3]The dataset is available at https://www.hci.wiwi.uni-due.de/en/publikationen/understanding-user-identification-in-virtual-reality-through-behavioural-biometrics-and-the-effect-of-body-normalization/.

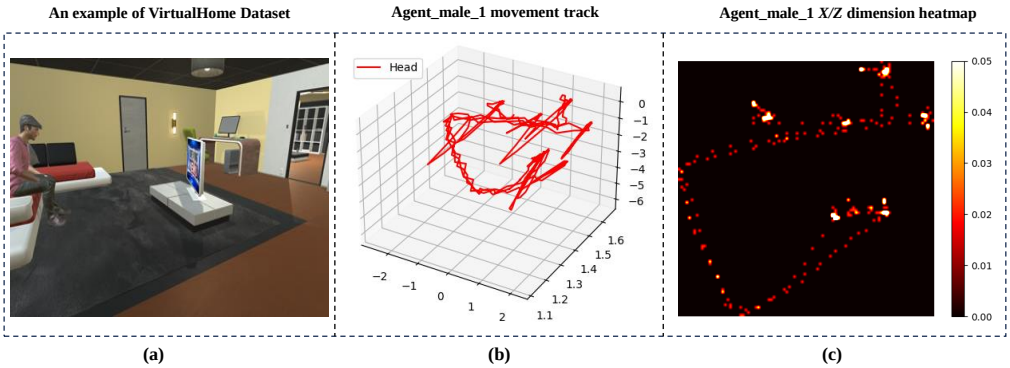

Fig. 1. A visualization of one sample in VirtualHome dataset [21]: (a) the virtual environment, (b) an illustration of movement track, and (c) the heat map conversion.

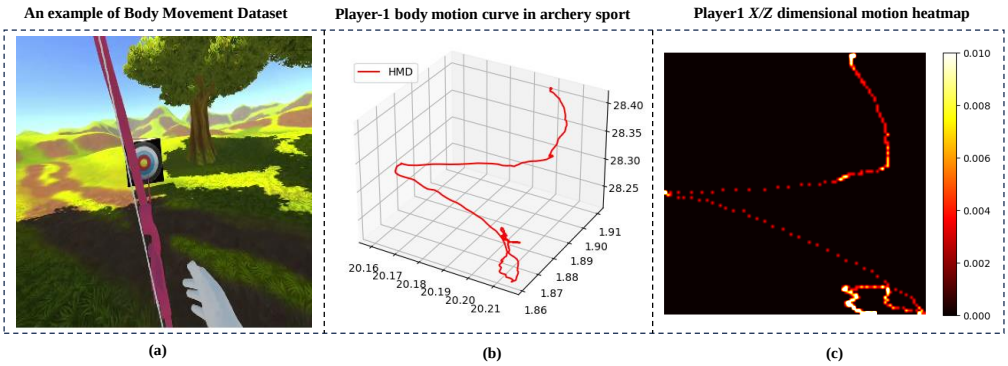

Fig. 2. A visualisation of one sample in Body Movement dataset [21]: (a) the virtual environment, (b) an illustration of movement track, and (c) the heat map conversion.

5.2 User Identification Attack Models

As described in Section 4, we explore two approaches for applying differential privacy to 3D body motion data. In concrete, we process the data with two different techniques (*i.e.,* window-slicing and converting into heat map). Then we conduct user identification attacks using two distinct models based on the features of the processed data. Specifically, following the experimental setup in datasets and recent studies [21, 27], we apply a Recurrent Neural Network (RNN) models on window-slicing data and Convolutional Neural Network (CNN) models on heat map data, respectively.

LSTM on window-slicing data. The LSTM model consists of three Long Short-Term Memory layers, and each layer has one hundred units. The activation function is selected as the default 'sigmoid'. Other hyper-parameters are set as: 200 epochs, Adam optimizer, and 1e-4 learning rate. Additionally, a majority voting is applied to determine the prediction label a sample. Specifically, according to the labels predicted on all sub-samples (a sample could be sliced into several sub-samples during window-slicing), the most frequent label is assigned as the final predicted label. Due to the

specificity of the dataset, which includes repetitions over two days, we divided the data into two parts: the motion data from the first day is set as the training set, while the data from the second day is set as the testing set. The advantage of splitting the dataset by date is that it helps avoid high repeatability between each sub-sample after window-slicing pre-processing.

CNN on heat map data. We establish a CNN network with two convolution layers and three full connection layer. In each convolution layer, there is a pooling layer. In the first two full connection layers, we add a drop layer with 0.5 dropping rate. For each layer, we use 'ReLU' as the activation function. The output of the model is a n-dimension vector, where n is the number of users in the dataset. The model is trained on 80% of the samples and tested on the remaining 20% samples.

5.3 Evaluation Metrics

In our study, we evaluate whether a privacy-enhancing approach is capable of safeguarding users' privacy while maintaining sufficient data utility. We use the following two metrics in experiments.

Relative squared error (RSE). To measure and control the error introduced by differential privacy, we utilize relative squared error (RSE) to calculate the average squared difference between the original data and the DP-enhanced data. The output value of RSE is expressed in terms of ratio. Specifically, as formalized in Equation 5, RSE calculates the relative squared error, which normalizes the total squared error (*i.e.,* MSE) and normalizes it by the square of the difference between the actual and the mean of the data.

$$RSE = \frac{1}{n} \frac{\sum_{i=1}^{n} (x_i - \hat{x}_i)^2}{\sum_{i=1}^{n} (x_i - \bar{x}_i)^2}, \tag{5}$$

where x_i is a data point from spatial data or a heat map, $\bar{x}_i$ is the mean of all data points, and $\hat{x}_i$ is the corresponding data point after applying DP. A RSE value can range from 0 to 1. A good model should have a value close to 0 while a model with a value greater than 1 is not reasonable.

The reason we use RSE as the error matric is because it is less influenced by the total data volume, compared to Mean Squared Error (MSE). Specifically, for window-slicing data, we directly compute two motion average curves between the temporal dimension and each dimension of feature, both before and after applying DP (*i.e.,* calculating the average curve by x-dimension data of the headset and time stamp); for heat map data, we calculate RSE between two 100*100 images.

Specifically, we use RSE as a quantitative threshold of data utility, to ensure that the data is still usable after applying DP onto it. The threshold of RSE will further determine the privacy budget ϵ which controls how much noise would be added to the data. For example, we can select the Relative Squared Error (RSE) threshold according to the specific utility scenario. A default threshold could be set at 1, and the smallest value of ϵ that can meet this threshold will be chosen for different privacy settings. For convenience in practice, we round up the value of ϵ to an integer. For example, if a chosen value of ϵ is 6.4, it will be rounded up to $\epsilon = 7$.

Identification accuracy. To evaluate the data privacy performance against user identification attacks, we utilize identification accuracy as the metric. As illustrated in Equation 6, the attack accuracy is defined as the number of user classifications the attack model correctly predicts divided by the total number of predictions made. Specifically, a lower identification accuracy indicates higher robustness of data privacy. If the accuracy of a user identification attack falls below that of random guessing (*i.e.,* below 50% in a binary classification), we classify the attack as failed and consider the data privacy to be robust.

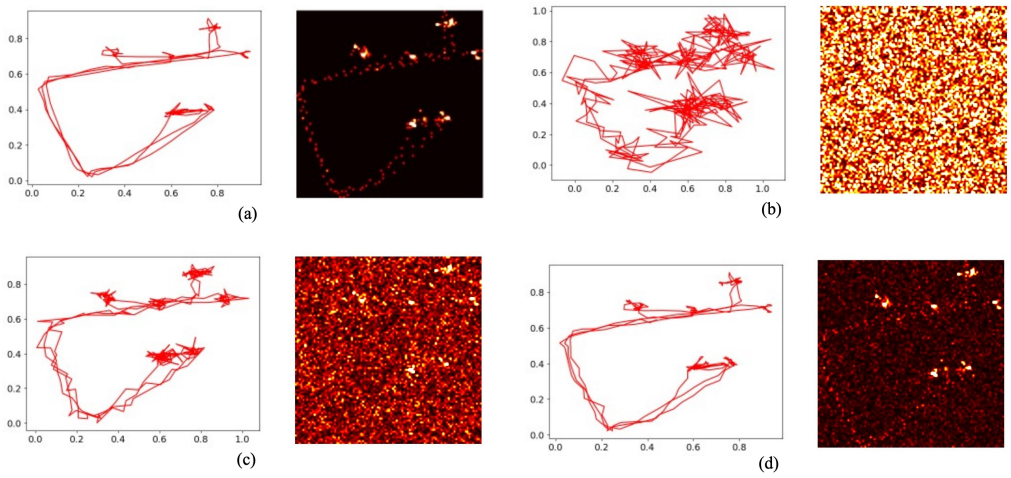

Fig. 3. Qualitative evaluation of data utility (an example from VirtualHome dataset). (a) original data and corresponding heat map; (b-d) data visualization after applying Laplace differential privacy with $\epsilon = 1, 3, 10$, respectively. Higher privacy budgets introduce less noise into the data. To maintain the data utility, a privacy budget higher than 3 should be selected, since when $\epsilon = 3$ the noise level is still high.

$$Identification\ Accuracy = \frac{Number\ of\ correct\ predictions}{Total\ number\ of\ predictions} \tag{6}$$

6 EXPERIMENTAL RESULTS

In this section, we present the experimental results of the data utility evaluation and the performance of our approach in protecting privacy against user identification attacks.

6.1 Data Utility Evaluation

We first evaluate the data utility through both qualitative and quantitative manners.

Qualitative data utility. As previously described in Section 4 and 5, we first evaluate the data utility through a qualitative method. This involves ensuring that the movement traces are still clear and recognizable to the human eyes after adding differential privacy noise. We demonstrate the data utility by plotting the original spatial data in x/z space, along with its corresponding heat map.

Specifically, to compare the data utility in different ϵ settings, we randomly select two samples from each dataset and plot their spatial data and corresponding heat maps, as shown in (Figure 3(a) and Figure 4(a)). Then compare with data with differential privacy applied. This is done for ϵ settings of 1, 3, and 10, as shown in Figure 3(b-d) and Figure 4(b-d). From the experimental results, it is evident that higher privacy budgets (*e.g.*, when $\epsilon = 3$ and 10) introduce less noise into the data, which is expected as higher privacy budgets are applied.

Here we note that, in practice, the purpose of conducting qualitative utility evaluation is to obtain an approximate proper range of ϵ, to saving computational cost in the quantitative utility control, since a proper utility threshold may lead to selecting a very large or small ϵ in specific cases. For example, an ϵ value in the range of 3 to 10 provides sufficient data utility in VirtualHome dataset, while an ϵ value less than 3 introduces too much noise, making it difficult to recognize the body movements or the visiting trace in the virtual home.

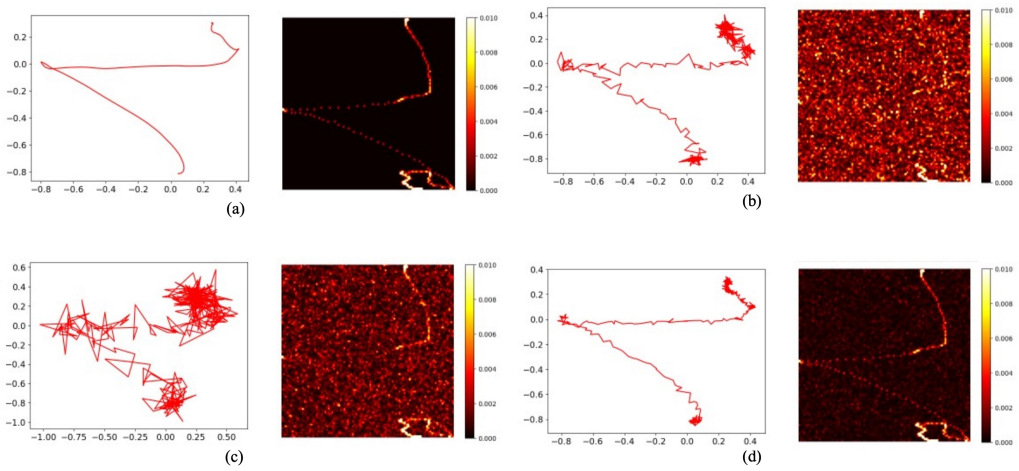

Fig. 4. Qualitative evaluation of data utility (an example from Body Movement dataset). (a) original data and corresponding heat map; (b-d) data visualization after applying Laplace differential privacy with $\epsilon = 1, 3, 10$, respectively. Higher privacy budgets introduce less noise into the data. To maintain the data utility, a privacy budget around 3 could be selected, since when $\epsilon = 3$ the noise level is acceptable and a stronger privacy protection can be pursued.

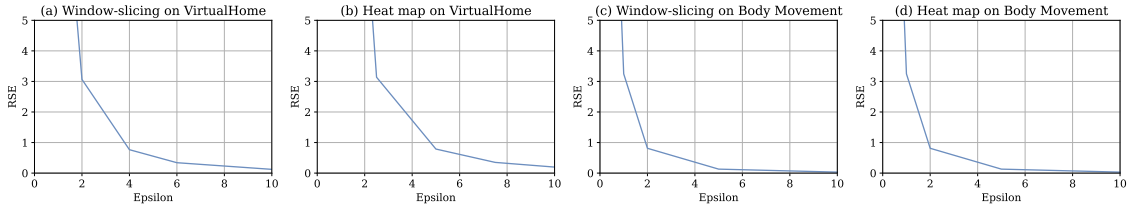

Fig. 5. RSE between the original data and the differential privacy-enhanced data with various ϵ settings. The query is the averaged user visiting trace.

Quantitative data utility controlling. Based on the qualitative results, we further determine the data utility using RMSE thresholds. In Figure 5, we present the RMSE between the original data and the differential privacy-enhanced data with various ϵ settings. Specifically, we vary the values of ϵ from 1 to 10 with a step size of 1. It can be observed that the RMSE decreases as ϵ increases. Moreover, there is an elbow point in the RSE-ϵ curve, indicating that an appropriate RSE threshold could be chosen near this point. In this region, increasing ϵ has less impact on the MSE, allowing us to select a privacy budget that is sufficiently tight.

According to Section 4, we selected a threshold of $RMSE \leq 1$ near the elbow point for our experiments, which led to different values of ϵ being chosen (*i.e.,* $\epsilon = 4$ for window-slicing data and $\epsilon = 7$ for heat map data). This difference arises because, when applying differential privacy to heat maps, perturbations are introduced to all points in the heat map (in our case, 100*100 points); whereas differential privacy applied to window-sliced data only introduces noise to individual time series data points, resulting in a smaller amount of noise being added with the same privacy budget, compared to the heat map case.

Table 1. Privacy enhancement against user identification attack.

Methods	Models	User Identification Accuracy					
		Original	Privacy Enhanced with Differential Privacy				
			$\epsilon = 0.5$	$\epsilon = 1$	$\epsilon = 2$	$\epsilon = 5$	ϵ controlled by utility threshold
Window-slicing	LSTM	93.89%	27.15	36.51	53.07	75.91	48.03%
Heat map	CNN	96.53%	14.09	24.83	63.09	87.92	55.37%

6.2 Privacy Performance against User Identification Attacks

We further evaluate the privacy protection performance of applying differential privacy to window-slicing data and its corresponding heat map. We conduct user identification attacks on the original data and privacy-enhanced data using various privacy budget settings (*i.e.,* $\epsilon = 1, 3, 10$), as well as an ϵ value selected based on the data utility threshold determined in the previous experiments.

As shown in Table 1, the attack success rates experience a significant drop when differential privacy is applied. For instance, in the VirtualHome (Body Movement) dataset, the identification rate decreases in the range of from 41.16% to 45.86% (from 22.44% to 27.09%), compared to the baseline attack success rates when no privacy enhancement is applied.

7 DISCUSSION

Our findings demonstrate that DP can effectively mitigate the risk of re-identification attacks, while still preserving the utility of understanding average 3D body motion. This balance between privacy and utility is crucial in various applications. For instance, in gaming, understanding players' body motions can lead to enhancements in the gaming experience. Similarly, in a virtual shopping context, understanding shoppers' movements and interactions can help improve the virtual shopping experience. Thus, the application of DP not only ensures user privacy but also contributes to the refinement of user experiences in virtual environments.

Our result also suggest that the transformation of a user's 3D body motion data into heat maps can effectively enhance user privacy. When the same privacy budgets are assigned to both the raw 3D body motion data and the heat maps, the heat maps approach can incorporate more noise into the data, thereby increasing the level of privacy protection. Importantly, this increase in noise does not significantly compromise the utility of the data. This means that important patterns and trends within the data can still be identified, which is vital for analyzing user behaviour and improving virtual experiences.

8 LIMITATIONS AND FUTURE WORK

In this study, we utilized two VR application datasets to investigate user visiting tracing in virtual home scenarios and body movement in an interactive VR game. Although our choice of datasets is limited, we acknowledge the inherent limitations in terms of representing the entire scope of VR scenarios. It is important to note that the field of VR is vast and diverse, encompassing various applications and user interactions. Despite such limitation, we contend that our approach holds general applicability across a wide range of scenarios involving the collection of users' spatial data.

Another limitation of our study could be the number of attack models involved in the experiments. We acknowledge that there exist more complex models that could be used for user identification attacks. However, the primary goal of our study is to demonstrate that the application of differential privacy mechanisms can significantly reduce the

success rate of user identification attacks, thus enhancing user privacy. In future research, we aim to conduct more comprehensive investigations into how the complexity or structure of attack models can influence privacy protection. This includes exploring whether a more complex privacy protection method or a tighter privacy budget is necessary when facing stronger attack models.

Additionally, it is crucial to explore the delicate balance between data utility and privacy protection. For example, collecting the user's gait and other biosignals could help us assess attention [36, 37], predict VR sickness [7], or detect stress levels [40] for early intervention. Further studies can shed light on how to optimise this trade-off and develop strategies that effectively preserve data utility while ensuring robust privacy protection. By addressing these aspects, we can advance the understanding of privacy protection in the context of VR applications and offer valuable insights into the design of more resilient and efficient privacy-preserving mechanisms.

9 CONCLUSION

We present a research study focused on the application of DP to 3D body motion data within VR applications, with the goals of preserving both user privacy and data utility. We discussed and evaluated two potential use cases - VR gaming and virtual shopping - using both synthetic and real-world datasets. The results indicate that our proposed heat map method surpasses the direct application of DP. These findings underscore the viability of our approach and advocate for further research into privacy-preserving techniques that do not compromise data utility in VR.

REFERENCES

[1] 2021. Virtual Reality Market Size, Share & Trends Analysis Report. https://www.grandviewresearch.com/industry-analysis/virtual-realityvr-market.

[2] 2022. Immersive Media Technologies: The Acceleration of Augmented and Virtual Reality in the Wake of COVID-19. https://www.weforum.org/reports/immersive-media-technologies-the-acceleration-of-augmented-and-virtual-reality-in-the-wake-of-covid-19.

[3] 2022. Meta Connect 2022: Meta Quest Pro, More Social VR and a Look Into the Future. https://about.fb.com/news/2022/10/meta-quest-pro-social-vrconnect-2022/.

[4] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin, and Elissa M Redmiles. 2018. Ethics emerging: the story of privacy and security perceptions in virtual reality. In *SOUPS@ USENIX Security Symposium*. 427–442.

[5] Nadisha-Marie Aliman and Leon Kester. 2020. Malicious design in aivr, falsehood and cybersecurity-oriented immersive defenses. In *2020 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*. IEEE, 130–137.

[6] Lauren E Buck and Bobby Bodenheimer. 2021. Privacy and personal space: Addressing interactions and interaction data as a privacy concern. In *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. IEEE, 399–400.

[7] Carlos Alfredo Tirado Cortes, Chin-Teng Lin, Tien-Thong Nguyen Do, and Hsiang-Ting Chen. 2023. An EEG-based Experiment on VR Sickness and Postural Instability While Walking in Virtual Environments. In *IEEE Conference Virtual Reality and 3D User Interfaces (VR)*. 8.

[8] Wannes Meert; Kilian Hendrickx; Toon Van Craenendonck. 2020. wannesm/dtaidistance v2.0.0. *Zenodo* (2020).

[9] Jaybie A De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2019. Security and privacy approaches in mixed reality: A literature survey. *ACM Computing Surveys (CSUR)* 52, 6 (2019), 1–37.

[10] Cynthia Dwork. 2006. Differential privacy. In *Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II 33*. Springer, 1–12.

[11] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. 2006. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3*. Springer, 265–284.

[12] Cynthia Dwork, Aaron Roth, et al. 2014. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science* 9, 3–4 (2014), 211–407.

[13] Gonzalo Munilla Garrido, Vivekand Nair, and Dawn Song. 2023. Going Incognito in the Metaverse. *arXiv preprint arXiv:2301.05940* (2023).

[14] Thomas Germain. 2022. Meta's New Headset Will Track Your Eyes for Targeted Ads. https://gizmodo.com/meta-quest-pro-vr-headset-track-eyes-ads-facebook-1849654424.

[15] Ruobin Gong, Erica L. Groshen, and Salil Vadhan. 2022. Harnessing the Known Unknowns: Differential Privacy and the 2020 Census. *Harvard Data Science Review* (2022).

[16] David Heaney. 2022. Apple Reportedly Has 3000 People Working On Its Upcoming Headset. https://uploadvr.com/apple-3000-staff-ar-vr-headset/.

[17] Naoise Holohan, Stefano Braghin, Pól Mac Aonghusa, and Killian Levacher. 2019. Diffprivlib: the IBM differential privacy library. *ArXiv e-prints* 1907.02444 [cs.CR] (July 2019).

[18] Naoise Holohan, Douglas J Leith, and Oliver Mason. 2015. Differential privacy in metric spaces: Numerical, categorical and functional data under the one roof. *Information Sciences* 305 (2015), 256–268.

[19] Jingdong Jia and Wenchao Chen. 2017. The ethical dilemmas of virtual reality application in entertainment. In *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, Vol. 1. IEEE, 696–699.

[20] Chuck Kapelke. 2021. Using differential privacy to harness big data and preserve privacy. https://www.brookings.edu/articles/using-differential-privacy-to-harness-big-data-and-preserve-privacy/.

[21] Jonathan Liebers, Mark Abdelaziz, Lukas Mecke, Alia Saad, Jonas Auda, Uwe Gruenefeld, Florian Alt, and Stefan Schneegass. 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*. 1–11.

[22] Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A Landay, and Jeremy N Bailenson. 2020. Personal identifiability of user tracking data during observation of 360-degree VR video. *Scientific Reports* 10, 1 (2020), 1–10.

[23] Vivek Nair, Gonzalo Munilla Garrido, and Dawn Song. 2022. Exploring the unprecedented privacy risks of the metaverse. *arXiv preprint arXiv:2207.13176* (2022).

[24] Vivek Nair, Wenbo Guo, Justus Mattern, Rui Wang, James F O'Brien, Louis Rosenberg, and Dawn Song. 2023. Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data. *arXiv preprint arXiv:2302.08927* (2023).

[25] Ilesanmi Olade, Charles Fleming, and Hai-Ning Liang. 2020. Biomove: Biometric user identification from human kinesiological movements for virtual reality systems. *Sensors* 20, 10 (2020), 2944.

[26] Ken Pfeuffer, Matthias J Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19, Paper 110)*. Association for Computing Machinery, New York, NY, USA, 1–12.

[27] Xavier Puig, Kevin Ra, Marko Boben, Jiaman Li, Tingwu Wang, Sanja Fidler, and Antonio Torralba. 2018. Virtualhome: Simulating household activities via programs. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 8494–8502.

[28] Cong Shi, Xiangyu Xu, Tianfang Zhang, Payton Walker, Yi Wu, Jian Liu, Nitesh Saxena, Yingying Chen, and Jiadi Yu. 2021. Face-Mic: inferring live speech and speaker identity via subtle facial dynamics captured by AR/VR motion sensors. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. 478–490.

[29] Zewei Shi, Ruoxi Sun, Jieshan Chen, Jiamou Sun, and Minhui Xue. 2024. The Invisible Game on the Internet: A Case Study of Decoding Deceptive Patterns. In *Companion Proceedings of the ACM Web Conference 2024*.

[30] Ruoxi Sun, Hanwen Wang, Minhui Xue, and Hsiang-Ting Chen. 2024. PPVR: A Privacy-Preserving Approach for User Behaviors in VR. In *2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. IEEE, 1055–1056.

[31] Ruoxi Sun, Minhui Xue, Gareth Tyson, Tian Dong, Shaofeng Li, Shuo Wang, Haojin Zhu, Seyit Camtepe, and Surya Nepal. 2023. Mate! Are You Really Aware? An Explainability-Guided Testing Framework for Robustness of Malware Detectors. In *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*.

[32] Ruoxi Sun, Minhui Xue, Gareth Tyson, Shuo Wang, Seyit Camtepe, and Surya Nepal. 2023. Not Seen, Not Heard in the Digital World! Measuring Privacy Practices in Children's Apps. In *Proceedings of the ACM Web Conference 2023*. 2166–2177.

[33] Philipp Sykownik, Divine Maloney, Guo Freeman, and Maic Masuch. 2022. Something personal from the Metaverse: Goals, topics, and contextual factors of self-disclosure in commercial social VR. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–17.

[34] Pier Paolo Tricomi, Federica Nenna, Luca Pajola, Mauro Conti, and Luciano Gamberi. 2023. You can't hide behind your headset: User profiling in augmented and virtual reality. *IEEE Access* 11 (2023), 9859–9875.

[35] Rahmadi Trimananda, Hieu Le, Hao Cui, Janice Tran Ho, Anastasia Shuba, and Athina Markopoulou. 2022. {OVRseen}: Auditing Network Traffic and Privacy Policies in Oculus {VR}. In *31st USENIX security symposium (USENIX security 22)*. 3789–3806.

[36] Renji Wu and Hsiang-Ting Chen. 2023. The Effect of Visual and Auditory Modality Mismatching between Distraction and Warning on Pedestrian Street Crossing Behavior. In *IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*. 8.

[37] Renjie Wu, Hu Wang, Feras Dayoub, and Hsiang-Ting Chen. 2023. Segment Beyond View: Handling Partially Missing Modality for Audio-Visual Semantic Segmentation. In *AAAI 2024*.

[38] Kai Zhang, Yanjun Zhang, Ruoxi Sun, Pei-Wei Tsai, Muneeb Ul Hassan, Xin Yuan, Minhui Xue, and Jinjun Chen. 2023. Bounded and Unbiased Composite Differential Privacy. *arXiv preprint arXiv:2311.02324* (2023).

[39] Yanjun Zhang, Ruoxi Sun, Liyue Shen, Guangdong Bai, Minhui Xue, Mark Huasong Meng, Xue Li, Ryan Ko, and Surya Nepal. 2024. Privacy-Preserving and Fairness-Aware Federated Learning for Critical Infrastructure Protection and Resilience. In *Proceedings of the ACM Web Conference 2024*.

[40] Howe Yuan Zhu, Hsiang-Ting Chen, and Chin-Teng Lin. 2021. The effects of virtual and physical elevation on physiological stress during virtual reality height exposure. *IEEE Transactions on Visualization and Computer Graphics* 29, 4 (2021), 1937–1950.