# Knowledge-driven Biometric Authentication in Virtual Reality

**Florian Mathis**
University of Glasgow
Glasgow, United Kingdom
florian.mathis@glasgow.ac.uk

**Mohamed Khamis**
University of Glasgow
Glasgow, United Kingdom
mohamed.khamis@glasgow.ac.uk

**Hassan Ismail Fawaz**
University of Haute-Alsace
Mulhouse, France
hassan.ismail-fawaz@uha.fr


*CHI '20 Extended Abstracts*, April 25–30, 2020, Honolulu, HI, USA
ACM 978-1-4503-6819-3/20/04.
https://dx.doi.org/10.1145/3334480.3382799

## Abstract
With the increasing adoption of virtual reality (VR) in public spaces, protecting users from observation attacks is becoming essential to prevent attackers from accessing context-sensitive data or performing malicious payment transactions in VR. In this work, we propose *RubikBiom*, a knowledge-driven behavioural biometric authentication scheme for authentication in VR. We show that hand movement patterns performed during interactions with a knowledge-based authentication scheme (e.g., when entering a PIN) can be leveraged to establish an additional security layer. Based on a dataset gathered in a lab study with 23 participants, we show that knowledge-driven behavioural biometric authentication increases security in an unobtrusive way. We achieve an accuracy of up to 98.91% by applying a Fully Convolutional Network (FCN) on 32 authentications per subject. Our results pave the way for further investigations towards knowledge-driven behavioural biometric authentication in VR.

## Author Keywords
Authentication; Virtual Reality; Deep Learning

## CCS Concepts
**•Human-centered computing → Human computer interaction (HCI); •Security and privacy → Authentication;**

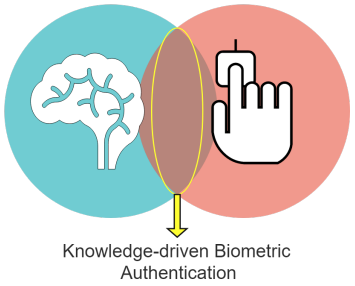


**Figure 1:** *RubikBiom* introduces knowledge-driven behavioural biometric authentication and leverages the concepts of **a)** knowledge-based authentication (e.g., entering a PIN) and **b)** biometric-based authentication (e.g., human movement patterns) by detecting human-behavioural movement patterns during users' authentications.

## Introduction

Virtual reality (VR) is becoming more and more popular due to its affordability and portability. Untethered head-mounted displays (HMDs) such as the Oculus Quest [32] contribute to an increasing interest in VR across a larger population. However, new interaction methods present opportunities for attackers as non-technology savvy users might be overwhelmed by such new technologies and underestimate possible threats.

This is crucial in situations where users have to authenticate to access confidential data or enter credentials such as PINs [20] to perform transactions. Users are often unaware of bystanders [10], especially whilst being immersed in VR [14, 27], who were shown to be able to infer the VR user's input (e.g., PINs) [14, 16, 40]. As researchers and practitioners in VR are very keen in creating immersive and mature technologies to increase users' experience and embed such novel technologies into our mundane life [18, 36], research to protect actual users against attacks (e.g., observation attacks, guessing attacks, or video attacks where attackers record and play back user's authentication [8, 15]) is still limited. *RubikBiom* protects users from such attacks even if attackers have access to the correct secret as it provides users with an additional security layer.

To our knowledge, *RubikBiom* is the first exploration into the use of knowledge-driven behavioural biometric authentication in VR (Fig. 1) in combination with deep learning (DL). *RubikBiom* makes successful attacks less common as an attacker has to **a)** derive the secret a user entered and **b)** precisely replicate the user's behaviour.

Our contribution is two-fold. First, we show that human behavioural biometrics collected during knowledge-driven natural asymmetrical bimanual cooperation [19] are promising for establishing an additional security layer in VR by applying state-of-the-art deep learning architectures for time series classification (TSC) [21]. Second, we propose knowledge-driven behavioural biometric authentication, a novel promising direction for authentication in VR.

## Background and Related Work

*Knowledge-based Authentication in VR*

Existing approaches to improve authentication in VR rely on knowledge-based authentication such as entering a PIN or pattern [12, 15, 17, 40]. However, at the point where attackers derive entire secrets based on observations, they can access private data or make them publicly available. George et al. [17] investigated the direct transfer of well-established authentication schemes into VR. Their study showed that attackers could derive 18% of users' PINs and patterns through observations. Similarly, Yu et al. [40] highlighted that most people can guess the input from watching videos showing a user authenticating in VR.

*Behavioural Biometric Authentication in VR*

Recent research shows that it is possible to improve security of VR users by tracking users' movements when performing natural goal-oriented tasks in VR environments. For instance, Kupin et al. [25] showed that it is possible to authenticate users solely on throwing a ball within the virtual environment. In their pilot study they achieved a matching accuracy of up to 92.86%. Similarly, Yi et al. [39] leveraged head movement patterns for authentication in VR and achieved an authentication accuracy of 92%. However, Mustafa et al. [28] recommend to use such functionality as an added layer of security in security-sensitive VR applications as pure behavioural biometrics might not be feasible in a large scale setting. This is inline with findings from Pfeuffer et al. [29] who highlight the logarithmic decrease of accuracy with increasing group size, thus, making behavioural biometrics on its own not feasible for authentication in VR.

**Figure 2:** Users select their *RubikBiom* PIN by tapping with the dominant handheld controller on the cube that is attached to their non-dominant handheld controller.

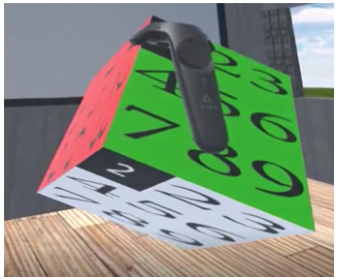

**Figure 3:** Participants entered the same set of PINs that were directly visualised on the cube using white digits on a black background.

Based on findings and lessons learnt from previous works [12, 15, 17, 25, 28, 29, 39, 40], we focus on the combination of a knowledge-based authentication scheme and corresponding human behavioural biometrics to increase security against observations. We apply DL on users' movement patterns during their knowledge-based authentication to make authentications more resistant to attacks (e.g., observation attacks, guessing attacks) in an unobtrusive way.

## Concept

To evaluate the suitability of human behavioural biometrics collected during knowledge-based authentication, we developed *RubikBiom*, a novel authentication scheme in VR (Fig. 2). *RubikBiom* is based on Guiard's kinematic chain model [19] that incorporates human asymmetrical bimanual cooperation. This means that user's non-dominant hand controls the pose of *RubikBiom* and user's dominant hand performs the pointing and selection. The benefits of applying Guiard's kinematic chain model are three-fold. It is **a)** a natural way of two-handed interaction [6, 22] and takes human skills into account that are already in place [22], **b)** adds complexity to observation attacks as attackers have to observe multiple interactions simultaneously [9], and **c)** allows leveraging human behavioural biometrics such as hand movements for authentication in VR. Users enter a 4-digit *RubikBiom* PIN by tapping on the corresponding digits and confirming the selection by pressing the HTC VIVE trigger button. Each PIN consists of 4 digit/surface combinations, e.g., 1 (green), 2 (white), 1 (red), 8 (white).

## User study

The aim of this study is to investigate the feasibility of human behavioural biometrics (e.g., hand movements) for knowledge-driven authentication in VR and to collect these for the following evaluation.

*Demographics*

We collected hand movements from 23 participants (13 females, 10 males) aged between 18 and 54 years ($\mu$=27.65, $\sigma$=8.26) within a lab study. Participants were recruited via internal university mailing lists. Most of them were students or staff members with a technical background. Half of our participants (52%) used VR at least once.

*Data Collection*

During each authentication, we capture feature information regarding the Cartesian values ($x$,$y$,$z$) and Unity's Quaternion (i.e., rotations in 3D space) [33] of users' dominant (DH) and non-dominant hand (N-DH).

*Procedure*

We introduced participants to *RubikBiom* and ran training sessions before actually tracking their movements. Participants then entered 12 *RubikBiom* PINs. All participants entered the same set of *RubikBiom* PINs four times each (4 repetitions$\times$12 PINs = 48 authentications). We highlighted the PINs the participants have to enter directly on *RubikBiom* (Fig. 3). Participants were compensated by £8.

*Apparatus*

We used Unity C# for the implementation of *RubikBiom* and data collection. As head-mounted display, we used an HTC VIVE ($2160 \times 1200$ px) and SteamVR Plugin for controller communication. For applying the deep learning architecture, we built upon Ismail Fawaz et al.'s implementation [21] using Keras 2.2.4 [7] based on the TensorFlow backend.

*Data Processing*

In total, we collected human behavioural biometrics from 23 participants who performed 48 trials each, making it a total of 1104 authentications. We pre-processed our dataset and splitted it into a training (36 authentications, 75%) and a test dataset (12 authentications, 25%) for each user [24].

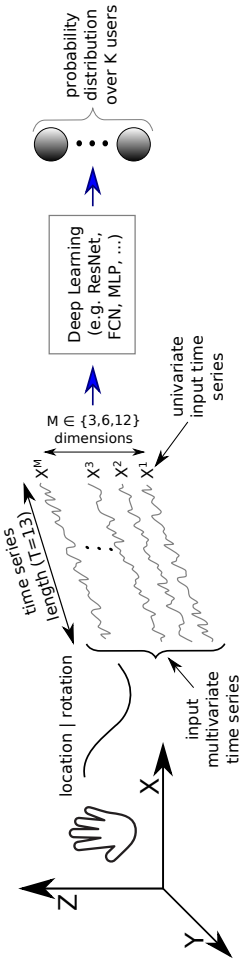


**Figure 4:** In *RubikBiom*, we experimented with $M$ = 3, 6, and 12 features and with a time series length of 13 time stamps$\times$50 ms each time stamp = 0.65 s.

| | | Top-1 Accuracy | | | | | |
|---|---|---|---|---|---|---|---|
| **Feature** | **Dimensions** | **MLP** | **FCN** | **ResNet** | **Encoder** | **MCDCNN** | **Time-CNN** |
| **DH Rotation** | 3 | 59.42% | **83.33%** | **83.33%** | 51.45% | *64.86%* | 51.09% |
| **DH Position** | 3 | 48.55% | *89.13%* | **89.86%** | 40.94% | 68.48% | 51.81% |
| **N-DH Rotation** | 3 | 44.93% | *73.19%* | **75.00%** | 31.16% | 45.29% | 48.19% |
| **N-DH Position** | 3 | 64.13% | **96.01%** | *93.84%* | 59.06% | 81.16% | 60.15% |
| **DH Position + Rotation** | 6 | 88.04% | **97.10%** | *95.65%* | 78.99% | 90.94% | 81.52% |
| **N-DH Position + Rotation** | 6 | 89.86% | **97.82%** | *97.10%* | 84.42% | 92.03% | 79.35% |
| **DH Rotation + N-DH Rotation** | 6 | 70.29% | *94.57%* | **96.01%** | 67.39% | 78.26% | 68.84% |
| **DH Position + N-DH Position** | 6 | 85.15% | **98.19%** | *97.46%* | 72.10% | 92.03% | 53.99% |
| **DH/N-DH Position + Rotation** | 12 | 92.39% | **98.91%** | *98.55%* | 88.41% | 93.84% | 90.58% |
| | **Mean Accuracy** | 71.42% | **92.03%** | *91.87%* | 63.77% | 78.54% | 65.05% |

**Table 1:** We calculated the top-1 classification accuracies. A Fully Convolutional Network (FCN) and a Residual Neural Network (ResNet) achieved the highest accuracies with 98.91% and 98.55%, respectively. **Bold** and *italic* denote category 1st and 2nd best, respectively.

We block-randomised the order of the authentications to reduce variance and overfitting [3]. Our multivariate time series (MTS) test dataset is a holdout dataset as we did not use it for training. The data follows a natural temporal ordering as it depicts human movements over time. This represents a TSC problem that has been considered as one of the most challenging problems in data mining [11, 37]. Similar to recognising human activity where the concept of TSC is widely applied [34], we classify users based on their hand movements during authentications.

We structured our data in a way that each instance depicts one dimension (e.g., x-value of the DH position) for each time stamp (Fig. 4). We adopted the six most promising state-of-the-art DL architectures [21] for our TSC problem and trained 9 datasets $\times$ 6 DL architectures = 54 models. Our aim is to enhance the security of authentications in VR by distinguishing the user's behaviour from that of attackers when entering identical PINs. We used the hyperparameters for deep learning architectures provided by Ismail Fawaz et al. [21] in their public repository (Table 2).

*Metrics*

Similar to previous work [29], we report top-1 classification accuracies (i.e., number of correct classifications divided by the total number). All our datasets are balanced as the number of authentications is the same for each class (user). An architecture that predicts the outcome solely based on random guesses would achieve an accuracy of 4.35% (1 out of 23 users).

## Results

Table 1 shows the top-1 classification accuracies of the six deep learning architectures that we applied on our multivariate datasets. A Fully Convolutional Network (FCN) [35] achieved overall the best accuracy (98.91%) and achieved the highest accuracy when leveraging users' dominant hand position + rotation together with users' non-dominant hand position + rotation. Increasing the number of dimensions results in more accurate results, and thus, avoids false negatives. Note that false negatives can only happen in *RubikBiom* when a user entered the correct PIN in a step before.

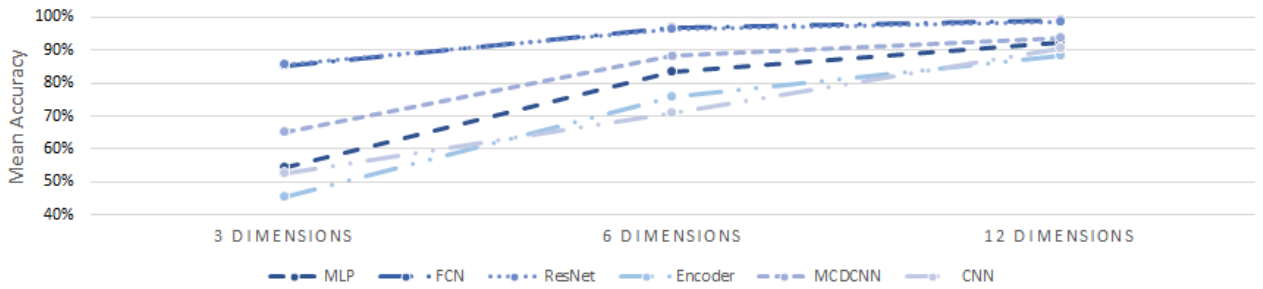


**Figure 5:** The classification accuracies represent a direct variation. The number of dimensions we use to train our models varies directly with the classification accuracy. This suggests that leveraging more dimensions results in higher classification accuracies. The graph depicts the direct variation across all DL architectures. All reported accuracies are mean values of clustered accuracies in Table 1.

| **Architecture** | **Optimizer** |
|---|---|
| MLP | AdaDelta |
| FCN | Adam |
| ResNet | Adam |
| Encoder | Adam |
| MCDCNN | SGD |
| Time-CNN | Adam |
| **Loss** | **Epochs\|LR** |
| Entropy | 5000\|1.0 |
| Entropy | 2000\|0.001 |
| Entropy | 1500\|0.001 |
| Entropy | 100\|0.00001 |
| Entropy | 200\|0.01 |
| MSE | 2000\|0.001 |

**Table 2:** Hyperparameters for the deep learning approaches used in our study.

When training a model on one feature (e.g., DH rotation) we achieved accuracies between 31.20% and 89.86% whereas two features (e.g, DH position and rotation) resulted in accuracies of 67.40% to 98.19%. Leveraging four features (e.g., DH + N-DH position and rotation) resulted in even higher accuracies of 88.41% to 98.91%. Figure 5 shows these increases of accuracies that follow a direct variation.

## Lessons Learnt and Discussion

Following a knowledge-driven behavioural biometric approach for user authentication in VR yielded promising results with classification accuracies up to 98.91% (N=23). This is noticeably higher than in previous works with a matching accuracy of 92.86% (N=14) [25] and 63.55% (N=22) [29]. This highlights the security benefits of applying DL on human behavioural biometrics collected during knowldge-driven authentication where a user enters their 4-digit PIN on *RubikBiom* (Figure 2). As shown in Table 1 and Fig. 5, multi-feature datasets (e.g., DH Position + Rotation) result in more accurate top-1 classification accuracies compared to single-feature datasets (e.g., DH position).

*The Future of Authentication in VR*

Previous research transferred knowledge-based authentication schemes into VR [15, 16, 40] or leveraged head movements [2, 28], hand movements [2, 25, 29], or gait signatures [31] for authentication in VR. In the case of behavioural biometric authentication [2, 25, 28, 29, 31], the direction is quite clear as researchers try to eliminate explicit authentication. This is mainly attributed to the fact that authentication is a secondary task users have to go through (e.g., unlocking a device) before being able to perform a main task (e.g., interacting in VR) [30]. However, it has been argued that behaviour biometrics should be used to enhance knowledge-based schemes for VR rather than replace them [28, 29], especially because behaviour might not be unique for a large group size.

Although using fingerprints for authentication found its application (e.g., to unlock a smart phone), they remain a challenge as they cannot be changed and there are fears about how this data could be abused [13, 26]. Following a knowledge-driven behavioural biometric authentication approach as presented with *RubikBiom* protects users from

**Acknowledgements**
We thank all participants for taking part in the study. This publication was supported by the University of Edinburgh and the University of Glasgow jointly funded PhD studentships, and by the Royal Society of Edinburgh (award number 65040).

**Access to the data**
Interested in getting access to the (anonymised) material and implementation? Please get in touch with the authors.

attackers in a seamless and unobtrusive way in different contexts. Note that fingerprints, facial recognition, or voice patterns might not work in situations where users are exposed to high humidity, different lighting conditions, or noisy environments [1, 4, 5]. For these reasons, it is important to investigate the potential of knowledge-driven behavioural biometric authentication. In particular, future authentication systems could leverage additional metrics (e.g., eye movements) to expand the input space for authentication in VR.

*Adaptive Authentication*
*RubikBiom*'s aim is to make authentication more secure against attacks (e.g., observation attacks, guessing attacks, video attacks) by introducing an additional human behavioural security layer. However, protecting users with an additional security layer may affect usability. Previous research highlighted the importance of incorporating contextual factors such as different environments and/or human factors when designing and developing authentication schemes [23]. A knowledge-driven behavioural biometric authentication scheme such as *RubikBiom* can deactivate the additional behavioural biometric security layer easily in a context where observation attacks might not occur as frequent as in public spaces (e.g., at home). This raises further interesting questions, for instance: in which contexts do users prefer such an additional security layer?

In future work we plan to investigate long-term usage of knowledge-driven biometric authentication schemes to investigate users' usage of such a system and investigate how a knowledge-driven biometric approach affects usability and security in a real-world use case with multiple authentications over time. We believe that knowledge-driven biometric authentication systems are promising for future adaptive authentication schemes that contribute to more secure systems without negatively affecting users' experience.

## Limitations

Our results are based on a user study that incorporates *RubikBiom* and requires two-hand interactions. Two-handed interaction might not be suitable for users with motor disabilities. To work towards hands-free interactions that are accessible for a larger population, alternative knowledge-driven biometric authentication schemes could train models based on eye or head movements.

Moreover, we experimented with a time series length of 13 time stamps$\times$50 ms each time stamp = 0.65 s. Higher frequencies might affect architectures' performance and result in even higher classification accuracies [38]. Yet, leveraging longer time series for user classification implies that we have to rely on longer authentication times. Authentication is perceived to be a secondary task and should therefore be fast and effortless [30]. Follow-up work could experiment with different time series lengths to study its effect on classification accuracy.

## Conclusion

In this paper, we introduced *RubikBiom*, a knowledge-driven biometric authentication scheme for user authentication in VR. We collected human behavioural biometrics from 23 participants and applied current state-of-the-art deep learning architectures for time series classification. We trained 56 models on nine different features and six deep learning architectures. We found that a Fully Convolutional Network (FCN) is the most accurate architecture with a classification accuracy of up to 98.91%. Our results provide first insights into applying deep learning for time series classification within the context of authentication in VR. We conclude that the use of human behavioural biometrics greatly enhances the security in a seamless and unobtrusive way and introduces a new direction for future authentication schemes in VR.

## REFERENCES


[1] Israa Alsaadi. 2015. Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review. *International Journal of Scientific  Technology Research* Volume 4 (12 2015).

[2] Ajit Ashwin, Kohlgade Baneerjee Natasha, and Banerjee Sean. 2019. Combining Pairwise Feature Matches from Device Trajectories for Biometric Authentication in Virtual Reality Environments. (2019).

[3] Yoshua Bengio. 2012. *Practical Recommendations for Gradient-Based Training of Deep Architectures*. Springer Berlin Heidelberg, Berlin, Heidelberg, 437–478. DOI: http://dx.doi.org/10.1007/978-3-642-35289-8_26

[4] Rasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. (2015). DOI: http://dx.doi.org/10.14722/usec.2015.23003

[5] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov, Minkyu Choi, and others. 2009. Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology* 2, 3 (2009), 13–28.

[6] William Buxton and Brad Myers. 1986. A Study in Two-handed Input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '86)*. ACM, New York, NY, USA, 321–326. DOI: http://dx.doi.org/10.1145/22627.22390

[7] François Chollet and others. 2015. Keras. https://keras.io. (2015).

[8] Sauvik Das, David Lu, Taehoon Lee, Joanne Lo, and Jason I. Hong. 2019. The Memory Palace: Exploring Visual-Spatial Paths for Strong, Memorable, Infrequent Authentication. In *Proceedings of the 32Nd Annual ACM Symposium on User Interface Software and Technology (UIST '19)*. ACM, New York, NY, USA, 1109–1121. DOI: http://dx.doi.org/10.1145/3332165.3347917

[9] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now You See Me, Now You Don'T: Protecting Smartphone Authentication from Shoulder Surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2937–2946. DOI: http://dx.doi.org/10.1145/2556288.2557097

[10] Malin Eiband, Mohamed Khamis, Emanuel Von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 4254–4265. DOI: http://dx.doi.org/10.1145/3025453.3025636

[11] Philippe Esling and Carlos Agon. 2012. Time-series Data Mining. *ACM Comput. Surv.* 45, 1, Article 12 (Dec. 2012), 34 pages. DOI: http://dx.doi.org/10.1145/2379776.2379788

[12] Markus Funk, Karola Marky, Iori Mizutani, Mareike Kritzler, Simon Mayer, and Florian Michahelles. 2019. LookUnlock: Using Spatial-Targets for User-Authentication on HMDs. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19)*. ACM, New York, NY, USA, Article LBW0114, 6 pages. DOI: http://dx.doi.org/10.1145/3290607.3312959

[13] Simson Garfinkel and Heather Richter Lipford. 2014. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust* 5, 2 (2014), 1–124. DOI:http://dx.doi.org/10.2200/S00594ED1V01Y201408SPT011

[14] Ceenu George, Philipp Janssen, David Heuss, and Florian Alt. 2019a. Should I Interrupt or Not?: Understanding Interruptions in Head-Mounted Display Settings. In *Proceedings of the 2019 on Designing Interactive Systems Conference*. ACM, 497–510. DOI: http://dx.doi.org/10.1145/3322276.3322363

[15] Ceenu George, Mohamed Khamis, Daniel Buschek, and Heinrich Hussmann. 2019b. Investigating the Third Dimension for Authentication in Immersive Virtual Reality and in the Real World. In *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. 277–285. DOI: http://dx.doi.org/10.1109/VR.2019.8797862

[16] Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. 2017a. Seamless and Secure VR: Adapting and Evaluating Established Authentication Systems for Virtual Reality. In *Network and Distributed System Security Symposium (NDSS 2017) (USEC '17)*. NDSS. DOI: http://dx.doi.org/10.14722/usec.2017.23028

[17] Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. 2017b. Seamless and Secure VR: Adapting and Evaluating Established Authentication Systems for Virtual Reality. In *Network and Distributed System Security Symposium (NDSS 2017) (USEC '17)*. NDSS. DOI: http://dx.doi.org/10.14722/usec.2017.23028

[18] Jan Gugenheimer, Christian Mai, Mark McGill, Julie Williamson, Frank Steinicke, and Ken Perlin. 2019. Challenges Using Head-Mounted Displays in Shared and Social Spaces. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19)*. ACM, New York, NY, USA, Article W19, 8 pages. DOI: http://dx.doi.org/10.1145/3290607.3299028

[19] Yves Guiard. 1987. Asymmetric Division of Labor in Human Skilled Bimanual Action. *Journal of Motor Behavior* 19, 4 (1987), 486–517. DOI:http://dx.doi.org/10.1080/00222895.1987.10735426 PMID: 15136274.

[20] INQUIRER.net. 2016. Alibaba launches full VR shopping experience with Buy+. (2016). https://technology.inquirer.net/56131/alibaba-launches-full-vr-shopping-experience-buy accessed 29 August 2019.

[21] Hassan Ismail Fawaz, Germain Forestier, Jonathan Weber, Lhassane Idoumghar, and Pierre-Alain Muller. 2019. Deep learning for time series classification: a review. *Data Mining and Knowledge Discovery* 33, 4 (01 Jul 2019), 917–963. DOI: http://dx.doi.org/10.1007/s10618-019-00619-1

[22] Paul Kabbash, William Buxton, and Abigail Sellen. 1994. Two-handed input in a compound task.. In *CHI*, Vol. 94. 417–423.

[23] Christina Katsini, Marios Belk, Christos Fidas, Nikolaos Avouris, and George Samaras. 2016. Security and Usability in Knowledge-based User Authentication: A Review. In *Proceedings of the 20th Pan-Hellenic Conference on Informatics (PCI '16)*. ACM, New York, NY, USA, Article 63, 6 pages. DOI: http://dx.doi.org/10.1145/3003733.3003764

[24] Abinaya Kumar, Aishwarya Radjesh, Sven Mayer, and Huy Viet Le. 2019. Improving the Input Accuracy of Touchscreens Using Deep Learning. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19)*. ACM, New York, NY, USA, Article LBW1514, 6 pages. DOI: http://dx.doi.org/10.1145/3290607.3312928

[25] Alexander Kupin, Benjamin Moeller, Yijun Jiang, Natasha Kholgade Banerjee, and Sean Banerjee. 2019. Task-Driven Biometric Authentication of Users in Virtual Reality (VR) Environments. In *MultiMedia Modeling*, Ioannis Kompatsiaris, Benoit Huet, Vasileios Mezaris, Cathal Gurrin, Wen-Huang Cheng, and Stefanos Vrochidis (Eds.). Springer International Publishing, Cham, 55–67. DOI: http://dx.doi.org/10.1007/978-3-030-05710-7_5

[26] Václav Matyáš and Zdeněk Říha. 2002. *Biometric Authentication — Security and Usability*. Springer US, Boston, MA, 227–239. DOI: http://dx.doi.org/10.1007/978-0-387-35612-9_17

[27] Mark McGill, Daniel Boland, Roderick Murray-Smith, and Stephen Brewster. 2015. A dose of reality: Overcoming usability challenges in vr head-mounted displays. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2143–2152. DOI: http://dx.doi.org/10.1145/2702123.2702382

[28] Tahrima Mustafa, Richard Matovu, Abdul Serwadda, and Nicholas Muirhead. 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 (IWSPA '18)*. ACM, New York, NY, USA, 23–30. DOI: http://dx.doi.org/10.1145/3180445.3180450

[29] 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)*. ACM, New York, NY, USA, Article 110, 12 pages. DOI: http://dx.doi.org/10.1145/3290605.3300340

[30] M. A. Sasse, S. Brostoff, and D. Weirich. 2001. Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal* 19, 3 (01 Jul 2001), 122–131. DOI: http://dx.doi.org/10.1023/A:1011902718709

[31] Y. Shen, H. Wen, C. Luo, W. Xu, T. Zhang, W. Hu, and D. Rus. 2019. GaitLock: Protect Virtual and Augmented Reality Headsets Using Gait. *IEEE Transactions on Dependable and Secure Computing* 16, 3 (May 2019), 484–497. DOI: http://dx.doi.org/10.1109/TDSC.2018.2800048

[32] Facebook Technologies. 2019a. Oculus Quest - All-in-One-VR. (2019). https://www.oculus.com/quest/

[33] Unity Technologies. 2019b. Quaternions in Unity 3D. (2019). https://docs.unity3d.com/Manual/QuaternionAndEulerRotationsInUnity.html

[34] Jindong Wang, Yiqiang Chen, Shuji Hao, Xiaohui Peng, and Lisha Hu. 2019. Deep learning for sensor-based activity recognition: A survey. *Pattern Recognition Letters* 119 (2019), 3 – 11. DOI: http://dx.doi.org/https://doi.org/10.1016/j.patrec.2018.02.010 Deep Learning for Pattern Recognition.

[35] Z. Wang, W. Yan, and T. Oates. 2017. Time series classification from scratch with deep neural networks: A strong baseline. In *2017 International Joint Conference on Neural Networks (IJCNN)*. 1578–1585. DOI: http://dx.doi.org/10.1109/IJCNN.2017.7966039

[36] Julie R. Williamson, Mark McGill, and Khari Outram. 2019. PlaneVR: Social Acceptability of Virtual Reality for Aeroplane Passengers. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, Article 80, 14 pages. DOI: http://dx.doi.org/10.1145/3290605.3300310

[37] QIANG YANG and XINDONG WU. 2006. 10 CHALLENGING PROBLEMS IN DATA MINING RESEARCH. *International Journal of Information Technology & Decision Making* 05, 04 (2006), 597–604. DOI: http://dx.doi.org/10.1142/S0219622006002258

[38] Shuochao Yao, Shaohan Hu, Yiran Zhao, Aston Zhang, and Tarek Abdelzaher. 2017. DeepSense: A Unified Deep Learning Framework for Time-Series Mobile Sensing Data Processing. In *Proceedings of the 26th International Conference on World Wide Web (WWW '17)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 351–360. DOI: http://dx.doi.org/10.1145/3038912.3052577

[39] S. Yi, Z. Qin, E. Novak, Y. Yin, and Q. Li. 2016. GlassGesture: Exploring head gesture interface of smart glasses. In *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*. 1–9. DOI: http://dx.doi.org/10.1109/INFOCOM.2016.7524542

[40] Z. Yu, H. Liang, C. Fleming, and K. L. Man. 2016. An exploration of usable authentication mechanisms for virtual reality systems. In *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*. 458–460. DOI: http://dx.doi.org/10.1109/APCCAS.2016.7804002