A Proposal to Study Shoulder-Surfing Resistant Authentication for Augmented and Virtual Reality: Replication Study in the US

Naheem Noah
University of Denver
USA
naheem.noah@du.edu

Peter Mayer
University of Southern Denmark
Karlsruhe Institute of Technology
Germany
mayer@imada.sdu.dk

Sanchari Das
University of Denver
USA
sanchari.das@du.edu

ABSTRACT

In recent years, augmented and virtual reality (AR/VR) technologies have advanced significantly, becoming more accessible and practical for various industries and applications. However, new digital threats have emerged as AR/VR usage increases such as data exchange in shared spaces. Prior research on graphical authentication has proposed the *Things* scheme [21] and we plan to adapt this in the AR/VR domain. The scheme in combination with the private display available to users in AR/VR is resistant to shoulder-surfing attacks. Inspired by the work of Duezguen et al. [12], who conducted a user study applying the *Things* scheme in AR with 16 users in Germany, this short paper proposes a replication study that will implement the *Things* scheme in both AR and VR. We will recruit eligible participants for the in-lab study which will involve the use of HoloLens and Valve Index to test the *Things* scheme and we will evaluate the effectiveness of the scheme, the interaction modes for usability, and users' risk perception concerning security. Additionally, we will conduct a comparative analysis of cross-cultural disparities between the participants in Germany and in the USA.

CCS CONCEPTS

• **Security and privacy → Hardware-based security protocols**; **Information flow control**; **Software security engineering**; **Software security engineering**.

KEYWORDS

Augmented Reality, Virtual Reality, Graphical Authentication

ACM Reference Format:
Naheem Noah, Peter Mayer, and Sanchari Das. 2023. A Proposal to Study Shoulder-Surfing Resistant Authentication for Augmented and Virtual Reality: Replication Study in the US. In *Computer Supported Cooperative Work and Social Computing (CSCW '23 Companion), October 14–18, 2023, Minneapolis, MN, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3584931.3607007

CSCW '23 Companion, October 14–18, 2023, Minneapolis, MN, USA

ACM ISBN 979-8-4007-0129-0/23/10…$15.00
https://doi.org/10.1145/3584931.3607007

1 INTRODUCTION

In recent years, there has been significant progress in augmented and virtual reality (AR/VR) technology, with advancements in hardware, software, and applications [24]. These technologies have been widely adopted in various industries, including gaming, education, tourism, and advertising, to enhance user experiences and transform environments [22, 23, 35]. AR overlays digital information, such as images or text, onto the real-world environment, whereas VR creates immersive digital environments that simulate real-world experiences [1, 30]. However, the high level of adoption of AR/VR devices has led to the collection, processing, and transmission of sensitive data, and their use in shared spaces, introducing new security and privacy risks that require attention [2, 9].

On the other hand, recent advances in AR/VR technology have led to the development of various authentication mechanisms to enhance security. However, traditional authentication methods such as passwords are vulnerable to attacks such as interception or guessing and can lead to issues such as forgotten or lost passwords, resulting in the inability to access user accounts or data [25]. Biometric authentication has been proposed as a more secure alternative to passwords, as it can be difficult to spoof or replicate [38]. However, concerns remain regarding the accuracy and reliability of biometric authentication and privacy concerns regarding the collection and use of biometric data [33].

Authentication methods, such as hand gestures or eye tracking, have also been explored, but may not be reliable or accurate enough to provide strong security and can be uncomfortable or difficult for users to use [40]. Therefore, a secure and user-friendly authentication scheme that utilizes only the sensors of AR/VR HMDs and preserves user privacy is necessary, especially in shared spaces where security risks are heightened [41]. Although a knowledge-based authentication scheme has its limitations, yet a study conducted by Leo [17] found that users generally prefer knowledge-based authentication over biometric authentication, as they perceive it to be more privacy-preserving. Furthermore, the work of Zimmermann and Gerber informed that the most preferred authentication method by users is a knowledge-based scheme (password), despite the considerable cognitive load it places on users [43].

Along these lines, Mayer et al. [21] identified the *Things* scheme as one of the graphical authentication schemes that outperform text passwords in terms of memorability. Subsequently, Duezguen et al. [12] conducted a user study in Germany with 16 participants to evaluate the effectiveness of the *Things* scheme in the AR context.

Cultural differences can affect the perceived usability of technology, as found in studies conducted by Noiwan et al. [26] and

Carrascosa et al. [8]. Therefore, it is essential to conduct a cross-cultural analysis to ensure that the technology is designed and implemented in a way that aligns with users' needs, values, and culture. Hence, building upon the prior work in Germany [12], we propose a replication study with 32 participants to evaluate the *Things* authentication scheme in the USA. By comparing the results from these two WEIRD (Western, Educated, Industrialized, Rich, and Democratic) countries, we can explore the influence of cultural factors, specifically privacy perceptions, on the acceptance and effectiveness of the authentication scheme [10, 24, 39]. With this, we aim to contribute to the development of a secure and usable authentication scheme for AR/VR devices. that can be used in various social and cultural contexts, ensuring secure user authentication and verification of sensitive data.

2 RELATED WORKS

Our research aims to develop a robust authentication scheme for AR/VR devices that is resistant to shoulder-surfing attacks and eliminates the need for external devices when using head-mounted displays (HMDs). In this study, we build upon previous research on authentication schemes to create an improved approach.

2.1 Graphical Authentication

Graphical authentication schemes are a type of knowledge-based authentication that relies on visual information instead of text [31]. Prior research shows that graphical authentication schemes can be more resistant to shoulder-surfing attacks than alphanumeric passwords [15]. Unlike alphanumeric passwords, graphical authentication passwords don't require users to enter characters in sequence, making them less vulnerable to shoulder-surfing attacks [36].

One of the most widely deployed graphical authentication schemes is the Android lock screen pattern. Despite its wide use, it does not offer higher shoulder-surfing resistance than PINs [4, 16, 42]. This limitation has prompted researchers to explore new implementations of graphical authentication schemes that offer improved security and usability. One such implementation is the PassMatrix scheme proposed by Sun et al. [34] for Android devices. In this scheme, users choose one square per image for a sequence of images to act as their password. They recorded an accuracy of 93.33% and an average of only 1.64 attempts required for users to successfully log into the system using PassMatrix. Our work focuses on a less widely known graphical authentication scheme, which, however, has more favorable properties in terms of shoulder-surfing resistance: the *Things* scheme. Firstly, the *Things* scheme is based on recognition instead of recall, i.e., users only have to recognize their password images among distractors instead of freely recalling them. This is cognitively a much easier task [37], which also leads to higher memorability of the passwords in this scheme [21] when compared to traditional text passwords and other graphical schemes. Secondly, the scheme can be easily hardened against shoulder-surfing even in non-AR/VR contexts by applying portfolio authentication approaches [3, 20]. In the AR/VR context, the private display allows to further strengthen this shoulder-surfing resistance from opportunistic attackers to other attacker types.

2.2 Authentication in AR/VR

AR/VR enable users to interact with virtual environments in a natural and intuitive way, utilizing controllers, gestures, hand movement, and spatial navigation [24, 25]. Without proper authentication measures in AR/VR, there is a risk of unauthorized access, data breaches, and other security threats. Authentication methods in AR/VR have evolved from traditional methods like pins or passwords to capture user data such as head and hand movement data (e.g., Bhalla et al. [5]) and iris and periocular data (e.g., Boutros et al. [6]). For example, Rogers et al. [29] conducted a study where users were asked to view rapidly changing images of numbers and letters on the AR/VR headset display. By capturing the users' blink and head movements, they achieved an impressive Balanced Accuracy Rate (BAC) of 94.4% and a low False Acceptance Ratio (FAR) of 0.5%. Similarly, Schneegass et al. [32] introduced SkullConduct, which leverages bone conduction of sound through the user's skull for authentication and achieved a remarkable accuracy of 97.0% with an Equal Error Rate (EER) of 6.9%. However, these approaches raise concerns regarding security and privacy due to the need for extensive data collection and tracking. In the *Things* scheme, the user's response is collected using available input options like pointing or gazing, reducing dependence on external hardware for data collection and tracking. In our implementation, we will use the finger tap functionality on HoloLens for the AR implementation and controllers available on Valve Index for VR implementation.

The *Things* graphical authentication scheme offers a unique approach to AR/VR authentication, providing both security and user-friendliness. The scheme involves assigning users a password consisting of five randomly generated images, which they are required to memorize. During the authentication process, users are presented with a sequence of images displayed either on a virtual grid or on virtual objects within a 3D environment. Their task is to select the specific set of images that matches their password. One of the notable advantages of using the *Things* scheme in AR/VR authentication is its potential to enhance the user's sense of presence and immersion in the virtual environment. By incorporating graphical elements that align with the virtual context, such as images related to the virtual world or the user's personal preferences, the authentication experience becomes more integrated and seamless with the overall virtual experience. Our work makes a significant contribution by introducing a cutting-edge shoulder-surfing authentication scheme specifically designed for AR/VR environments, ensuring both enhanced security and seamless usability.

3 RESEARCH METHODOLOGY

To implement a cross-cultural study in the United States, this research replicates the work of Duezguen et al. [12] and expands upon it. The study is approved by the Institutional Review Board (IRB) and adheres to ethical guidelines.

3.1 Participants Recruitment

We will actively recruit study participants by utilizing targeted advertising on social media networks and mailing lists. Our approach will involve using e-flyers that provide comprehensive information about the study requirements. We are specifically interested in individuals aged 18 years and above, who currently reside in the United

States and are able to attend the study in person at the designated location. To streamline the recruitment process, the e-flyer will include a link to an online pre-screening survey.

3.2 Pre-screening Survey

We aim to ensure that our study adheres to ethical guidelines and protects the privacy and confidentiality of participants. To achieve this, we have designed a pre-screening survey that serves as the primary tool for participant recruitment. The survey will collect key demographic information, such as age, gender, and educational level, and will screen potential participants based on the eligibility criteria. The pre-screening survey has been expanded from the prior works of Rajivan et al. [28] on expertise evaluation.

3.3 In-lab Study

We will conduct a study involving 32 participants, who will be randomly assigned into two groups: AR and VR, with 16 participants in each group. Participants will be briefed about the study upon check-in and provided with a laptop to complete an online survey using Qualtrics. The survey will collect information about their previous experience with AR/VR HMDs, their willingness to use them in the future, and their experience with authentication on HMDs.

After completing the survey, participants will be provided with either a HoloLens or Valve Index, depending on their group. The HMD will be adjusted for their eyes, and the instructor will guide the participant through the tasks by sharing the HMD's user interface on a monitor. Participants will undergo a brief training session called HoloLens Tips [1] or Steam VR Tutorial [2] to familiarize themselves with the HMD's interaction methods for HoloLens and Valve Index, respectively, which will only cover gesture control since the *Things* scheme requires only gesture interaction.

After the training, participants will test the *Things* scheme. The process begins with the participants entering their usernames by scanning a QR code using the camera integrated into the head-mounted display (HMD) instead of using a virtual keyboard. This approach was chosen to alleviate the cumbersome process of typing in the username, ensuring a smoother and more efficient user experience. Once the participant confirms their entered username, our system generates a set of five randomly generated and unique images to serve as the participant's password. We randomly generate the password for the participants as opposed to them selecting preferred images based on the work of Davis et al. [11], where they found through their graphical authentication scheme that the set of images selected by users is influenced by the first image they select and the set of images selected can be easily guessed by an attacker. To authenticate, participants will be shown five grids with 16 images each, and they must select the image that corresponds to their password for each grid. Upon selecting the final image, participants will confirm their input and receive feedback on whether their authentication was successful or not. Participants will repeat this process two more times with shuffled image grids. Following the authentication process, participants will complete an evaluation survey, including the System Usability Scale [18] and questions on perceived usability and security.

In order to evaluate the resistance of the *Things* authentication scheme to shoulder-surfing attacks, a comprehensive experiment will be conducted involving participants who will assume the role of attackers. These attackers will have the opportunity to observe an expert user as they go through the authentication process, using pre-recorded videos of the user. The experiment will consist of three rounds, during which the attackers will closely observe the expert user's authentication procedure and attempt to mimic it. The pre-recorded videos will be captured using a camera array, similar to the approach used by Aviv et al. [4], which allows for multiple angles and viewpoints to be recorded, accurately emulating the shared spaces typically associated with AR/VR HMDs. The purpose of this experiment is to assess the scheme's ability to withstand shoulder-surfing attacks, where an attacker tries to gain unauthorized access by observing and replicating the authentication process.

At any point during the study, participants may choose to withdraw, and their data will be deleted upon withdrawal. Biometric data, such as iris data collected by the HoloLens or Valve Index, will be deleted after the experiment and will not be evaluated. The HMDs will be used offline, and there will be no data exchange with Microsoft servers or third-party providers. All data captured by the HMD will be erased after the experiment. The maximum duration of the experiment for each user will be 30 minutes.

Consent to participate in the study will be obtained during the pre-screening survey, which will include a clear explanation of the study's purpose and data processing, as well as contact information for the researcher. Participants who are interested in participating in future studies have the option to provide their email addresses within the survey to facilitate ongoing research in a particular area. To protect the privacy and confidentiality of study participants, any documents or materials collected during the study that contains identifying information will be de-identified following completion. User data will be stored in the organization's protected server, which complies with the General Data Protection Regulation (GDPR) and US state laws.

3.4 Scheme Evaluation

To evaluate the effectiveness of the scheme, we will measure the Accuracy Score by dividing the number of correctly authenticated instances by the total number of authentication attempts. We will assess the efficiency of the scheme by measuring the average Authentication Time, starting from the initiation of the authentication attempt until the system provides a response indicating whether the attempt was successful or not. Furthermore, we will measure the Authentication Workload; the mental workload required for a user to complete the authentication process by asking users to rate their perceived workload using the NASA Task Load Index (TLX). Additionally, we will assess Memorability by tracking the number of users who can successfully remember and use their authentication credentials over an extended period. To evaluate the resistance to shoulder-surfing attack, the attack success rate will be measured.

The satisfaction level of participants will be measured using the System Usability Scale (SUS), which evaluates users' subjective reactions to using the scheme [27]. To assess the user's risk perception,

[1] https://www.microsoft.com/en-us/p/hololens-tips/9pd4cxkklc47
[2] https://steamcommunity.com/sharedfiles/filedetails/?l=german%5C&id=1731528266

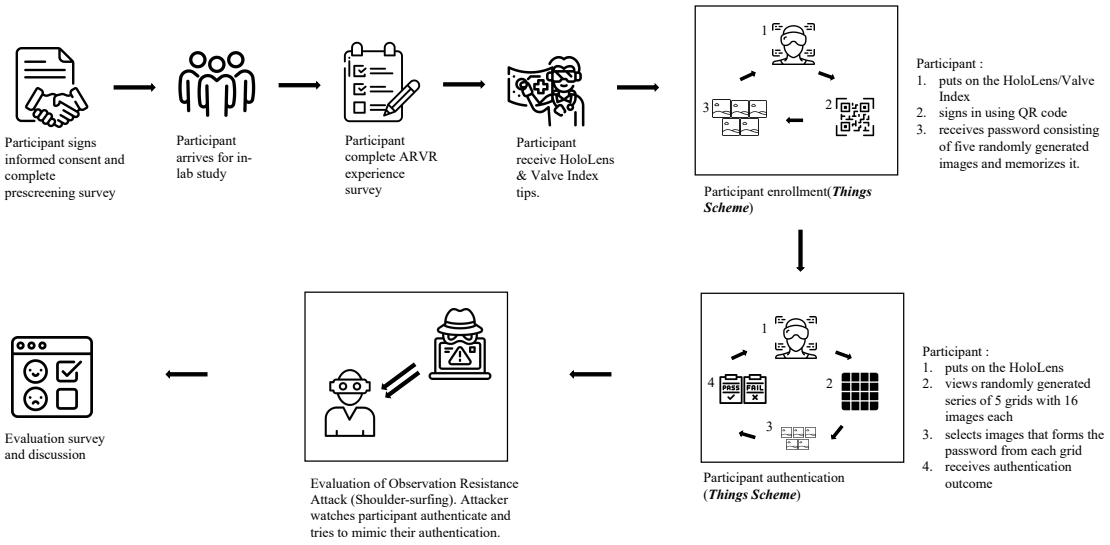

Figure 1: Illustration of the study protocol to evaluate the usability and security of the proposed *Things* scheme in both AR and VR in the USA.

we will adapt scales proposed by Fischhoff et al. [14] and Liang and Xue [19] in our study. The risk perception metric comprises nine characteristics of the risk, including voluntariness, immediacy, knowledge of the exposed, knowledge of experts, control, newness, common dread, chronic-catastrophic, and severity. This framework has been used in four decades to explain perceptions of technical security risks [7] and insider threats [13]. Through open-ended questions and structured interviews, we will encourage participants to express their thoughts, opinions, and suggestions regarding the usability, security, and overall user experience of the authentication scheme. This qualitative data will provide rich and nuanced insights into the strengths and limitations of the system, allowing us to better understand the users' perspectives and tailor future enhancements accordingly.

We will compare the results of our AR study with the results of the previous study conducted in Germany. By examining the similarities and differences between these two studies, we can gain a better understanding of how cultural factors and privacy perceptions impact the evaluation of the authentication scheme in different contexts. Furthermore, we will compare the results of both our AR study and our VR study so we can explore the potential variations in user experiences, usability, and security between these two immersive technologies. Figure 1 presents an overview of the study protocol.

4 CONCLUSION

The growing usage of augmented and virtual reality (AR/VR) technologies has introduced new security threats, especially in shared environments where multiple users can access sensitive data and user account information. To address this concern, prior researchers have proposed the *Things* scheme as a secure authentication method for AR/VR devices. This scheme is resistant to shoulder-surfing attacks and can be used with the interaction methods provided by Head-Mounted Displays (HMDs). Although a user study was conducted on the *Things* scheme in AR with 16 users in Germany, it has not been tested with US users, and the scheme was previously only implemented for AR devices. In this paper, we propose an extension of the prior work by implementing the *Things* scheme in both AR and VR. Our study will evaluate the effectiveness of the scheme, the interaction modes for usability, and users' risk perception concerning security. Additionally, we will conduct a comparative analysis of cross-cultural disparities. This study aims to contribute to the development of a secure and user-friendly authentication scheme for AR/VR devices, especially in shared spaces.

ACKNOWLEDGMENTS

This work was supported by a research gift from Meta. We would also like to acknowledge the Inclusive Security and Privacy-focused Innovative Research in Information Technology (InSPIRIT) Lab at the University of Denver for supporting this work. This work was also supported by the Helmholtz Association (HGF) through the subtopic Engineering Secure Systems (ESS). Any opinions, findings, conclusions, or recommendations expressed in this material are solely those of the authors.

REFERENCES

[1] Charvi Agarwal and Narina Thakur. 2014. The evolution and future scope of augmented reality. *International Journal of Computer Science Issues (IJCSI)* 11, 6

(2014), 59.
[2] Abrar Alismail, Esra Altulaihan, MM Hafizur Rahman, and Abu Sufian. 2022. A Systematic Literature Review on Cybersecurity Threats of Virtual Reality (VR) and Augmented Reality (AR). *Data Intelligence and Cognitive Informatics: Proceedings of ICDICI 2022* 1, 1 (2022), 761–774.
[3] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. 2005. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies* 63, 1 (2005), 128 – 152. http://eprints.gla.ac.uk/13858/
[4] Adam J. Aviv, John T. Davin, Flynn Wolf, and Ravi Kuber. 2017. Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference* (Orlando, FL, USA) *(ACSAC '17)*. Association for Computing Machinery, New York, NY, USA, 486–498. https://doi.org/10.1145/3134600.3134609
[5] Arman Bhalla, Ivo Sluganovic, Klaudia Krawiecka, and Ivan Martinovic. 2021. MoveAR: Continuous biometric authentication for augmented reality headsets. In *Proceedings of the 7th ACM on Cyber-Physical System Security Workshop*. Proceedings of the 7th ACM on Cyber-Physical System Security Workshop, New York, NY, USA, 41–52.
[6] Fadi Boutros, Naser Damer, Kiran Raja, Raghavendra Ramachandra, Florian Kirchbuchner, and Arjan Kuijper. 2020. Iris and periocular biometrics for head mounted displays: Segmentation, recognition, and synthetic data generation. *Image and Vision Computing* 104 (2020), 104007.
[7] L Jean Camp. 2009. Mental models of privacy and security. *IEEE Technology and society magazine* 28, 3 (2009), 37–46.
[8] Juan Miguel Carrascosa, Jakub Mikians, Ruben Cuevas, Vijay Erramilli, and Nikolaos Laoutaris. 2015. I always feel like somebody's watching me: measuring online behavioural advertising. In *Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies*. Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies, New York, NY, USA, 1–13.
[9] Song Chen, Zupei Li, Fabrizio Dangelo, Chao Gao, and Xinwen Fu. 2018. A case study of security and privacy threats from augmented reality (ar). In *2018 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2018 International Conference on Computing, Networking and Communications (ICNC), New York, NY, USA, 442–446.
[10] Sanchari Das, Andrew Dingman, and L. Jean Camp. 2018. Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key. In *Financial Cryptography and Data Security*, Sarah Meiklejohn and Kazue Sako (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 160–179.
[11] Darren Davis, Fabian Monrose, and Michael K Reiter. 2004. On user choice in graphical password schemes.. In *USENIX security symposium*, Vol. 13. USENIX security symposium, New York, NY, USA, 11–11.
[12] Reyhan Düzgün, Peter Mayer, and Melanie Volkamer. 2022. Shoulder-Surfing Resistant Authentication for Augmented Reality. In *Nordic Human-Computer Interaction Conference*. Nordic Human-Computer Interaction Conference, New York, NY, USA, 1–13.
[13] Fariborz Farahmand and Eugene H Spafford. 2013. Understanding insiders: An analysis of risk-taking behavior. *Information systems frontiers* 15 (2013), 5–15.
[14] Baruch Fischhoff, Paul Slovic, Sarah Lichtenstein, Stephen Read, and Barbara Combs. 1978. How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy sciences* 9 (1978), 127–152.
[15] Agata Kołakowska. 2013. A review of emotion recognition methods based on keystroke dynamics and mouse movements. In *2013 6th international conference on human system interactions (HSI)*. IEEE, 2013 6th international conference on human system interactions (HSI), New York, NY, USA, 548–555.
[16] Arash Habibi Lashkari, Samaneh Farmand, Dr Zakaria, Omar Bin, Dr Saleh, et al. 2009. Shoulder surfing attack in graphical password authentication. *arXiv preprint arXiv:0912.0951* 6, 2 (2009), 145–154.
[17] SP Leo Kumar. 2019. Knowledge-based expert system in manufacturing planning: state-of-the-art review. *International Journal of Production Research* 57, 15-16 (2019), 4766–4790.
[18] James R Lewis. 2018. The system usability scale: past, present, and future. *International Journal of Human–Computer Interaction* 34, 7 (2018), 577–590.
[19] Huigang Liang, Yajiong Lucky Xue, et al. 2010. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems* 11, 7 (2010), 1.
[20] Peter Mayer and Melanie Volkamer. 2015. Secure and Efficient Key Derivation in Portfolio Authentication Schemes Using Blakley Secret Sharing. In *Proceedings of the 31st Annual Computer Security Applications Conference* (Los Angeles, CA, USA) *(ACSAC '15)*. Association for Computing Machinery, New York, NY, USA, 431–440. https://doi.org/10.1145/2818000.2818043
[21] Peter Mayer, Melanie Volkamer, and Michaela Kauer. 2014. Authentication schemes-comparison and effective password spaces. In *Information Systems Security: 10th International Conference, ICISS 2014, Hyderabad, India, December 16-20, 2014, Proceedings 10*. Springer, Information Systems Security: 10th International Conference, ICISS 2014, Hyderabad, India, December 16-20, 2014, Proceedings 10, New York, NY, USA, 204–225.
[22] Luis Muñoz-Saavedra, Lourdes Miró-Amarante, and Manuel Domínguez-Morales. 2020. Augmented and virtual reality evolution and future tendency. *Applied sciences* 10, 1 (2020), 322.
[23] Anand Nayyar, Bandana Mahapatra, D Le, and G Suseendran. 2018. Virtual Reality (VR) & Augmented Reality (AR) technologies for tourism and hospitality industry. *International journal of engineering & technology* 7, 2.21 (2018), 156–160.
[24] Naheem Noah and Sanchari Das. 2021. Exploring evolution of augmented and virtual reality education space in 2020 through systematic literature review. *Computer Animation and Virtual Worlds* 32, 3-4 (2021), e2020.
[25] Naheem Noah, Sommer Shearer, and Sanchari Das. 2022. Security and privacy evaluation of popular augmented and virtual reality technologies. In *Proceedings of the 2022 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence, and Neural Engineering (IEEE MetroXRAINE 2022)*. Proceedings of the 2022 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence, and Neural Engineering (IEEE MetroXRAINE 2022), New York, NY, USA, 1.
[26] Supaporn Noiwan, Matthew Warren, Linda O'Conner, and Yvonne O'Connor. 2006. Cultural issues in information systems outsourcing: An empirical study. *Journal of Information Technology* 21, 3 (2006), 159–170.
[27] S Camille Peres, Tri Pham, and Ronald Phillips. 2013. Validation of the system usability scale (SUS) SUS in the wild. In *Proceedings of the human factors and ergonomics society annual meeting*, Vol. 57. SAGE Publications Sage CA: Los Angeles, CA, Proceedings of the human factors and ergonomics society annual meeting, New York, NY, USA, 192–196.
[28] Prashanth Rajivan, Pablo Moriano, Timothy Kelley, and L Jean Camp. 2017. Factors in an end user security expertise instrument. *Information & Computer Security* 25, 2 (2017), 190–205.
[29] Cynthia E Rogers, Alexander W Witt, Alexander D Solomon, and Krishna K Venkatasubramanian. 2015. An approach for user identification for head-mounted displays. In *Proceedings of the 2015 ACM International Symposium on Wearable Computers*. Proceedings of the 2015 ACM International Symposium on Wearable Computers, USA, 143–146.
[30] Joseph M Rosen, Hooman Soltanian, Richard J Redett, and Donald R Laub. 1996. Evolution of virtual reality [Medicine]. *IEEE Engineering in Medicine and Biology Magazine* 15, 2 (1996), 16–22.
[31] Harsh Kumar Sarohi and Farhat Ullah Khan. 2013. Graphical password authentication schemes: current status and key issues. *International Journal of Computer Science Issues (IJCSI)* 10, 2 Part 1 (2013), 437.
[32] Stefan Schneegass, Youssef Oualil, and Andreas Bulling. 2016. SkullConduct: Biometric user identification on eyewear computers using bone conduction through the skull. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, USA, 1379–1384.
[33] Sophie Stephenson, Bijeeta Pal, Stephen Fan, Earlence Fernandes, Yuhang Zhao, and Rahul Chatterjee. 2022. Sok: Authentication in augmented and virtual reality. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022 IEEE Symposium on Security and Privacy (SP), New York, NY, USA, 267–284.
[34] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh, and Chia-Yun Cheng. 2016. A shoulder surfing resistant graphical authentication system. *IEEE Transactions on Dependable and Secure Computing* 15, 2 (2016), 180–193.
[35] Zsolt Szalavári, Erik Eckstein, and Michael Gervautz. 1998. Collaborative gaming in augmented reality. In *Proceedings of the ACM symposium on Virtual reality software and technology*. Proceedings of the ACM symposium on Virtual reality software and technology, New York, NY, USA, 195–204.
[36] Furkan Tari, A Ant Ozok, and Stephen H Holden. 2006. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proceedings of the second symposium on Usable privacy and security*. Proceedings of the second symposium on Usable privacy and security, New York, NY, USA, 56–66.
[37] Barbara Tversky. 1973. Encoding Processes in Recognition and Recall. *Cognitive Psychology* 5, 3 (1973), 275 – 287. https://doi.org/10.1016/0010-0285(73)90037-6
[38] Vivek Veeraiah, K Ranjit Kumar, P Lalitha Kumari, Shahanawaj Ahamad, Rohit Bansal, and Ankur Gupta. 2022. Application of Biometric System to Enhance the Security in Virtual World. In *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*. IEEE, 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), New York, NY, USA, 719–723.
[39] Yang Wang. 2018. Inclusive security and privacy. *IEEE Security & Privacy* 16, 4 (2018), 82–87.
[40] Waqas Wazir, Hasan Ali Khattak, Ahmad Almogren, Mudassar Ali Khan, and Ikram Ud Din. 2020. Doodle-based authentication technique using augmented reality. *IEEE Access* 8 (2020), 4022–4034.
[41] Minrui Xu, Wei Chong Ng, Wei Yang Bryan Lim, Jiawen Kang, Zehui Xiong, Dusit Niyato, Qiang Yang, Xuemin Shen, and Chunyan Miao. 2023. A Full Dive Into Realizing the Edge-Enabled Metaverse: Visions, Enabling Technologies, and Challenges. *IEEE Communications Surveys & Tutorials* 25, 1 (2023), 656–700. https://doi.org/10.1109/COMST.2022.3221119

[42] Nur Haryani Zakaria, David Griffiths, Sacha Brostoff, and Jeff Yan. 2011. Shoulder surfing defence for recall-based graphical passwords. In *Proceedings of the seventh symposium on usable privacy and security*. Proceedings of the seventh symposium on usable privacy and security, New York, NY, USA, 1–12.

[43] Verena Zimmermann and Nina Gerber. 2020. The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies* 133 (2020), 26–44.

accepted 15 June 2023