Issues in Information Systems
Volume 23, Issue 2, pp. 185-192, 2022

DOI: https://doi.org/10.48009/2_iis_2022_125

Security and privacy in virtual reality: A literature review

Shalaka Kulal, *Kennesaw State University, skulal@students.kennesaw.edu*
Zhigang Li, *Kennesaw State University, zli8@kennesaw.edu*
Xin Tian, *Kennesaw State University, xtian2@kennesaw.edu*

Abstract

Virtual reality (VR) is gaining popularity and is used for various purposes such as gaming, social media, and training. Consequently, privacy and security issues have arisen with the increasing popularity of VR devices. However, compared to other types of research, such as virtual reality in gaming and entertainment, research on virtual reality's security and privacy issues is still limited. In this paper, we conducted a systematic literature review of research studies published in the past two decades on the topic of security and privacy issues associated with virtual reality environments. By looking at the latest developments in VR security and privacy, this article highlights these risks and examines the different approaches to privacy and security that have been proposed for VR. We also discuss further challenges and directions for VR privacy and security.

Keywords: virtual reality, privacy, security

Introduction

Virtual reality (VR), sometimes also called as "Virtual Environment" in the computer industry, is a 3D model presented in real-time, integrated with an immersive display that allows for direct manipulation and real-time interaction with the model world (Mazuryk & Gervautz, 1999). It lets you navigate a virtual world, sense it, see it through different angles or change it (Zheng et al., 1998). The idea of virtual reality started back in the 1930s as a science fiction story, which then evolved into an arcade-style theatre cabinet in the 1950s (Druck, 2006). The first interactive head-mounted display system was developed in 1970 by Ivan Sutherland and his team at the University of Utah (Frenkel & Sutherland, 1989). Yet despite all these inventions, there was never a term that captured the entire field. The actual name was put forth in the late 1980s by Jaron Lanier (Schroeder, 1993). Since then, the research in VR has developed rapidly. For instance, NASA used a VR simulator to train the astronauts (Loftin & Kenney, 1995), VR was the subject of multiple movies (Druck, 2006), and there were various inventions, such as Sega's VR and VR1 glasses, Nintendo virtual boy, and Oculus.

Virtual reality is now accessible to the public. Because of the personal nature of the collected data from the users, VR users perceived some danger in its privacy issues (Psychoula et al., 2018). VR includes applications on headsets that allow users to navigate virtual spaces. As a part of providing these experiences, these devices collect personal data to a great extent from the users (Froehlich & Azhar, 2016). This information may be provided by the users or generated from their previous information (Dick, 2021). In a virtual environment, many of the user behaviors can be tracked, and the elements in the VR environment can be modified. Oculus VR by Facebook highlights this privacy risk. When users agree to the Terms and Conditions to use Oculus VR, they are giving Facebook permission to collect and share private data such

as physical movements and GPS locations (Bagheri, 2016). Another major risk is information security because it is not protected in all virtual environments, as it is not encrypted (Korolov, 2014). Facebook has frequently been in the news for its data privacy and security issues. As part of its effort to reposition itself as a creator of a new digital world called the "Metaverse" (Dwoskin, 2021), when Facebook changed its official name to Meta, Mark Zuckerberg said, "The company plans to focus on the next wave of computing: a virtual universe where people will roam freely as avatars, attending virtual business meetings, shopping in virtual stores and socializing at virtual get-togethers" (Isaac, 2021). In his attempt to build this universe, he supports an approach for privacy and security from day one as he said, "With all the novel technologies that are being developed, everyone who's building for the metaverse should be focused on building responsibly from the beginning" (Vanian, 2021). With all these developments and a rise in VR technologies, there has been an increase in threats. Thus, we aim to conduct a detailed literature review to assess the current research on privacy and security in VR to help bring more attention to the issues and provide guidance to future research.

Methodology

This study adopted Cooper's five steps of the systematic literature review to ensure the quality of this paper. These five stages are (1) research question, (2) data collection, (3) data evaluation, (4) data analysis, and (5) interpretation and presentation of results (Cooper, 1998).

Research Question

This paper aims to answer the following research question by analyzing data collected from electronic databases.

- What are the concerns and issues related to security and privacy in VR environments?

This article addresses the primary methodical review to assess the security and privacy concerns with the nature of human involvement in virtual reality.

Data Collection

The purpose of the data collection process was to collect concept papers and research papers related to Privacy and Security in Virtual Reality. The databases selected to find the articles related to the topic consist of Google Scholar, IEEE Explore, ACM Digital Library, Sage Journal, Wiley, Web of Science, and Springer. Articles from 2000 to February 2022 were collected for the literature review.

Combinations of search strings used to collect the articles are given below:

- "Privacy" and "Virtual Reality"
- "Security" and "Virtual Reality"
- "Privacy" and "Security" and "Virtual Reality"
- "Privacy" and "VR"
- "Security" and "VR"
- "Privacy" and "Security" and "VR"

Data Evaluation

The articles were selected based on the inclusion and exclusion criteria shown in Table 1.

Table 1. Inclusion and Exclusion Criteria

Inclusion	Exclusion
2000 – February 2022	Published before 2000
Peer-reviewed scholarly journals and conference papers	Magazines or news articles
Written in English	Other languages
Full-text available	Abstracts only
Related to privacy and/or security in VR	Not related to privacy and/or security in VR

Considering all the criteria in table 1, we conducted a search in different databases. The search results for them are shown in table 2.

Table 2. Search Results from different databases

Keywords	Databases (Since 2000)					
	Google Scholar		IEEE Explore		ACM	
	Results Returned	Articles Selected	Results Returned	Articles Selected	Results Returned	Articles Selected
"Privacy" and "Virtual Reality"	26	15	5	5	3	2
"Security" and "Virtual Reality"	48	8	15	6	8	3
"Privacy" and "Security" and "Virtual Reality"	10	7	2	2	3	0
"Privacy" and "VR"	11	3	1	1	2	0
"Security" and "VR"	28	4	2	0	2	0
"Privacy" and "Security" and "VR"	1	0	0	0	2	0

Table 2 shows the results returned from three databases and the articles that were selected based on their relevancy. We also searched other databases, including Sage Journal, Wiley, Web of Science, and Springer. Out of those, three of the databases returned 0 search results. Although database Wiley returned a few results for all the combinations, they were not selected because of their irrelevancy. After carefully examining the articles, a total of 14 research papers were collected from the electronic databases using the combination of research keywords. Articles that are not relevant, or do not answer the research questions were eliminated.

Data Analysis

The first step that went into the data analysis was to properly code the studies so that we could derive answers to the research questions from the collected articles. The following are some representations of the data.

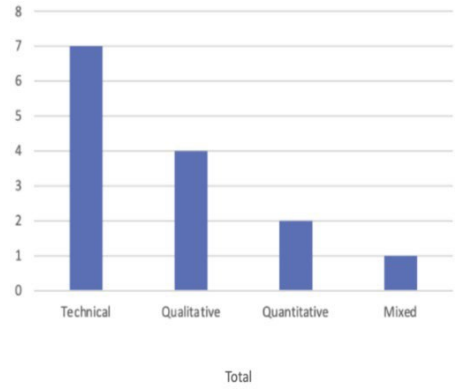

Fig 1. Count of Methodologies

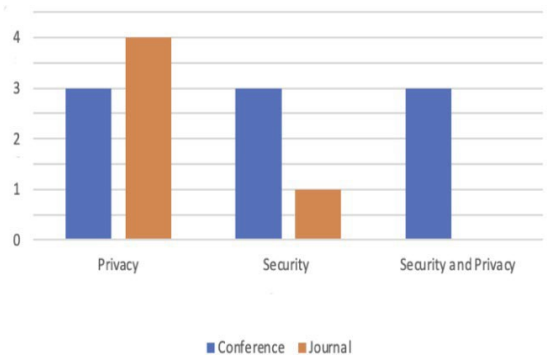

Fig 2. Number of Articles by Venues and Topics

In the above analysis, Fig 1 shows that half of the articles collected are related to the development of specific technical solutions for the VR environment. The rest of the articles are user studies using qualitative, quantitative, or mixed methods for their research design. Fig 2 is the representation of the type of articles for different topics. The analysis shows that more privacy-related articles have been published in conferences and journals. Out of the 14 articles, four articles are related to the general applications of VR. Two articles are specific to virtual social environments, and two articles are specific to virtual learning environments. The remaining articles are related to different domains, such as music, robotics, restaurant services, risk management, and authentication.

Results

Privacy

The privacy-related articles refer to the protection issues in the information gathered through social VR applications. The articles specifically discussed the types of information users disclose, to whom they reveal this information, and their privacy concerns regarding self-disclosure in social VR applications. Maloney et al. (2020) conducted semi-structured interviews with 30 candidates. They found three patterns for self-disclosure of personal information based on familiarity, anonymity, and open sharing. They also found that the participants have conflicting viewpoints concerning privacy and self-disclosure. To have a realistic experience on VR platforms, users' physical-associated information is required. Their personal information and data, such as online interaction, avatars or the virtual representation of people, eye tracking, hand tracking, and head movement, are exposed in applications (O'Brolcháin et al., 2016). These data can potentially be used to identify an individual and infer additional information. Dick (2021) suggested that this issue can be solved using a combination of encryption technology, transparency in the disclosure of user data, and law enforcement that protects their privacy and autonomy.

In separate studies, Hwang et al. (2012) and Men and Zhao (2021) used VR technology to study different patterns in people's privacy. Hwang et al. (2012) provided an experiment that examined people's reactions to their privacy while waiting in a Restaurant. The authors used a VR restaurant for the study. A total of 61 students participated in this survey experiment, and the impact of crowding in the waiting area in the restaurant was analyzed. Men and Zhao (2021) used VR to produce music with a focus on providing sonic privacy through augmented acoustic attenuation. A total of 42 students participated in the questionnaire and interview. The subjects created music in shared places and private places in a collaborative music tool using

VR and shared their experience regarding sonic privacy in both environments. Both studies showed that positive and negative emotions are induced in public places.

In other articles, researchers discussed the privacy issues associated with VR platforms in general. Adams et al. (2018) conducted a survey with 20 developers and users on their perceptions of risks in VR and how they are addressing those risks. Trimananda et al. (2022) developed a methodology for collecting, analyzing, and comparing privacy policies on Oculus VR and compared them to mobile and other applications. Peng et al. (2021) pointed out privacy issues associated with mobile edge computing and proposed a privacy-aware computation offloading method for VR environments.

Security

Two research teams (Gulhane et al., 2019; Valluripally et al., 2020) proposed frameworks that utilize attack trees to calculate a risk score for security and privacy threats. They discussed VR learning environments, risk assessment framework, human information safety, headsets, security attacks due to unauthorized access, privacy attacks, and vulnerability in security and privacy. Their approaches provide realistic insights into risks associated with the system component vulnerabilities to inform VRLE (Virtual Reality Learning Environment) policy management to mitigate risks. They also found that some security principles are more effective than others. However, combining them can result in a more effective mitigation mechanism.

In addition to security frameworks, other researchers proposed different methods for hiding information in the VR environment. For example, Djaghloul and Jessel (2019) presented a method for watermarking 3D objects and hiding various types of information in virtual reality environments. The research team evaluated the performance of the method and concluded that this method allows a high level of robustness to prevent attacks with unlimited watermarking but shows some weaknesses in some topological attacks. Another research team (Klubsuwan & Mungsing, 2008) presented the design and algorithm for multiple keys and messages embedding in 3D Video GIS, based on the steganography concept. They have enhanced the security of the information through this method by sampling pixel comparison.

Mathis et al. (2020) implemented an authentication scheme for the VR environment named RubikAuth. The team discussed the use of RubikAuth in securing authentication in VR, the experiences of users using it, and its limitations. They also debated the use of authentication in realistic threat models that ensure optimal conditions for the attacker and compared pointing using eye gaze, head pose, and controller tapping.

As a result of the amount of data gathered and shared, Vasylevska and Mortezapoor (2021) focused on data security issues. The article implies that integrating robots under ROS (Robot Operating System) poses a significant risk in terms of data security. In addition, using a robot for simulations in VR requires redundant data collection and sharing. This article creates awareness of data security challenges and some tracking solutions for these issues.

Adams et al. (2018) investigated end-user perceptions of VR risks and how developers consider and address those risks. They surveyed the VR privacy policies and studied the ethics of co-design by interviewing both VR users and developers on the issue. The survey showed that users raised privacy issues around headset producer reputation. Although they discussed more privacy, it has little mention of security. They concluded that there are more users than developers that raised security concerns.

Conclusion

Prior to 2010, there was not a popular, affordable VR device available on the market. Thus the quantity of research related to VR is limited due to the relatively high cost and the limitations of the hardware (Ivanova, 2018). We have gathered a comprehensive collection of security and privacy approaches in VR and related technologies. We analyzed different authentication schemes, methods for hiding information, privacy frameworks, and the privacy of people in social environments. We have identified that there has been more privacy-related research than security-related research. With the increased popularity of VR and the emphasis on cybersecurity, research on privacy and security-related issues in VR deserve more attention.

Limitations and Future Research

Compared to other types of research, such as virtual reality in gaming and entertainment, research on the security and privacy issues in virtual reality is still limited, as shown by the number of articles selected in this literature review. However, given the increased interest in VR research and its applications and the emphasis on cybersecurity awareness, new studies on the security and privacy issues in VR are likely to appear more often, and this deserves continuous attention from both researchers and VR developers. In addition, many companies have been developing VR applications, which will increase the likelihood of privacy and security-related issues.

References

Adams, D., Bah, A., Barwulor, C., Musabay, N., Pitkin, K., & Elissa Redmiles. (2018). Ethics emerging: The story of privacy and security perceptions in virtual reality. *Proceedings of the Fourteenth Symposium on Usable Privacy and Security*, 443–458. https://www.usenix.org/conference/soups2018/presentation/adams

Bagheri, R. (2016). Virtual reality: The real life consequences. *UC Davis Business Law Journal*, *17*(1), 101–120.

Cooper, H. (1998). *Synthesizing Research: A Guide for Literature Reviews* (3rd ed, pp. xii, 201). Sage Publications, Inc.

Dick, E. (2021). Balancing user privacy and innovation in augmented and virtual reality. *Information Technology & Innovation Foundation*. https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality

Djaghloul, H., & Jessel, J.-P. (2019). 3D objects based security in virtual and augmented reality systems. *International Journal of Virtual Reality*, *19*(2). https://doi.org/10.20870/IJVR.2019.19.2.2911

Druck, A. (2006). *When will virtual reality become a reality?* https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.363.2866&rep=rep1&type=pdf

Dwoskin, E. (2021). *Facebook is changing its name to Meta as it focuses on the virtual world*. The Washington Post. https://www.washingtonpost.com/technology/2021/10/28/facebook-meta-name-change/

Frenkel, K. A., & Sutherland, I. (1989). An interview with Ivan Sutherland. *Communications of the ACM*, *32*(6), 712–714. https://doi.org/10.1145/63526.63531

Froehlich, M. A., & Azhar, S. (2016). Investigating virtual reality headset applications in construction. *52nd ASC Annual International Conference Proceedings*. 52nd ASC Annual International Conference, Provo, UT. http://ascpro0.ascweb.org/archives/cd/2016/paper/CPRT195002016.pdf

Gulhane, A., Vyas, A., Mitra, R., Oruche, R., Hoefer, G., Valluripally, S., Calyam, P., & Hoque, K. A. (2019). Security, privacy and safety risk assessment for virtual reality learning environment applications. *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 1–9. https://doi.org/10.1109/CCNC.2019.8651847

Hwang, J., Yoon, S., & Bendle, L. J. (2012). Desired privacy and the impact of crowding on customer emotions and approach-avoidance responses: Waiting in a virtual reality restaurant. *International Journal of Contemporary Hospitality Management*, *24*(2), 224–250. https://doi.org/10.1108/09596111211206150

Isaac, M. (2021). Facebook renames itself Meta. *The NewYork Times*. https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html

Ivanova, A. V. (2018). VR & AR technologies: Opportunities and application obstacles. *Strategic Decisions & Risk Management*, *3*(108), 76–91.

Klubsuwan, K., & Mungsing, S. (2008). Digital data security and hiding on virtual reality VDO 3DGIS-Map. *2008 4th IEEE International Conference on Management of Innovation and Technology*, 548–553. https://doi.org/10.1109/ICMIT.2008.4654424

Korolov, M. (2014). *The Real Risks of Virtual Reality*. Risk Management Magazine. https://www.rmmagazine.com/articles/article/2014/10/01/-The-Real-Risks-of-Virtual-Reality-

Loftin, R. B., & Kenney, P. (1995). Training the Hubble space telescope flight team. *IEEE Computer Graphics and Applications*, *15*(5), 31–37. https://doi.org/10.1109/38.403825

Maloney, D., Zamanifard, S., & Freeman, G. (2020). Anonymity vs. familiarity: Self-disclosure and privacy in social virtual reality. *26th ACM Symposium on Virtual Reality Software and Technology*, 1–9. https://doi.org/10.1145/3385956.3418967

Mathis, F., Williamson, J., Vaniea, K., & Khamis, M. (2020). RubikAuth: Fast and secure authentication in virtual reality. *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–9. https://doi.org/10.1145/3334480.3382827

Mazuryk, T., & Gervautz, M. (1999). *History, Applications, Technology and Future*. https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.7849

Men, L., & Zhao, D. (2021). Designing privacy for collaborative music making in virtual reality. *Audio Mostly 2021*, 93–100. https://doi.org/10.1145/3478384.3478392

O'Brolcháin, F., Jacquemard, T., Monaghan, D., O'Connor, N., Novitzky, P., & Gordijn, B. (2016). The convergence of virtual reality and social networks: Threats to privacy and autonomy. *Science and Engineering Ethics*, *22*(1), 1–29. https://doi.org/10.1007/s11948-014-9621-1

Peng, K., Liu, P., & Huang, T. (2021). *A Privacy-aware computation offloading method for virtual reality application*. Woodstock'21: Symposium on the irreproducible science, Woodstock, NY.

Psychoula, I., Singh, D., Chen, L., Chen, F., Holzinger, A., & Ning, H. (2018). Users' privacy concerns in IoT based applications. *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, 1887–1894. https://doi.org/10.1109/SmartWorld.2018.00317

Schroeder, R. (1993). Virtual reality in the real world: History, applications and projections. *Futures*, *25*(9), 963–973. https://doi.org/10.1016/0016-3287(93)90062-X

Trimananda, R., Le, H., Cui, H., Ho, J. T., Shuba, A., & Markopoulou, A. (2022). *OVRSEEN: Auditing network traffic and privacy policies in Oculus VR*. USENIX Security Symposium 2022.

Valluripally, S., Gulhane, A., Mitra, R., Hoque, K. A., & Calyam, P. (2020). Attack trees for security and privacy in social virtual reality learning environments. *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, 1–9. https://doi.org/10.1109/CCNC46108.2020.9045724

Vanian, J. (2021). *Mark Zuckerberg's metaverse may be as privacy flawed as Facebook*. Fortune. https://fortune.com/2021/10/29/mark-zuckerberg-metaverse-privacy-facebook-meta/

Vasylevska, K., & Mortezapoor, S. (2021). *Safety and Security Challenges for Collaborative Robotics in VR*. USENIX Symposium on Usable Privacy and Security (SOUPS) 2021, Vancouver, B.C., Canada.

Zheng, J. M., Chan, K. W., & Gibson, I. (1998). Virtual reality. *IEEE Potentials*, *17*(2), 20–23. https://doi.org/10.1109/45.666641