7-1-2023

A Literature Review on Privacy and Security in Virtual Reality and Augmented Reality

Yunus Gumbo

Liang Zhao

Xin Tian, et al.

A LITERATURE REVIEW ON PRIVACY AND SECURITY IN VIRTUAL REALITY AND AUGMENTED REALITY

Yunus Gumbo
Kennesaw State University
ygumbo@students.kennesaw.edu

Liang Zhao
Kennesaw State University
lzhao10@kennesaw.edu

Xin Tian
Kennesaw State University
xtian2@kennesaw.edu

Zhigang Li
Kennesaw State University
zli8@kennesaw.edu

Yuan Long
Georgia State University
ylong4@gsu.edu

ABSTRACT

As technologies become more advanced and powerful, the progression towards embracing virtual reality environments in our daily activities becomes more real, and subsequently, the boundaries between virtual and physical worlds are more in question. However, several issues continue to persist as the world around us changes – privacy and security. In this paper, we are going to analyze the newer virtual reality (VR) and augmented reality (AR) applications, the privacy risks associated with these environments, current solutions – their benefits and challenges as well as potential newer solutions which can be implemented to increase privacy protection. The intention of this paper is to generate a comprehensive literature review on this topic. In addition to that, to raise the awareness of proper protection and safeguarding of the virtual reality (VR) users' private information, but also improve the overall measures used to control privacy and security in these virtual environments.

Keywords

Virtual Reality, Augmented Reality, Privacy, Security

INTRODUCTION

There is an increased number of case studies, scientific research, and journals which have been published based on the inspiration regarding virtual reality, augmented reality and even, mixed reality. Metaverse and other similar platforms, have recently caused much awareness to privacy and security of end users, therefore, inspired so many scholars to revisit these sensitive subjects. The main objectives for this literature review paper are to answer few questions – first and foremost, does the current existing literature truly acknowledge and highlight privacy and security issues the society is currently facing? In addition to that, does the current literature address just these issues, or there are more concerns to other problems closely related to the privacy and security, and there are any proposed solutions to these problems? Furthermore, this literature review paper intends to serve as a public resource which comprehensively cover and reduce the gap between different journals, case studies, and research which pertains to the subject of privacy and security specifically in the virtual reality (VR) and augmented reality (AR) field. Therefore, the purpose of this literature review paper is to address those three questions concerning privacy and security in virtual reality and augmented reality, analyze and systematically synthesize all relevant journals, case studies and research from online trusted electronic databases and generate a comprehensive literature review which will provide valuable references to be used for other higher purposes such as development and implementation of different theoretical frameworks.

Virtual reality (VR) techniques offer users immersive experiences in a virtual environment (VE) where they can enjoy gaming, training, shopping, and social activities (Ling et al., 2019). In a nutshell, augmented reality (AR) is basically mixing the real world with digital content. AR is the real-time superposition of virtual information into the vision of the real world (Yang & Wang, 2020). With all the advantages which comes with the AR/VR, still the privacy concerns and questions remain real and open as wide range of new challenges regarding negative social experiences and interactions, such as harassment and privacy concerns in these growing immersive spaces (Maloney et al., 2020).

Just recently, Microsoft have shut down multiple AltspaceVR social hubs to combat privacy issues. This shows how serious privacy issues are when it comes to virtual reality environments, we use every day. In this article we will discuss why privacy should be focal point when it comes to VR/AR environments and why privacy by design should be taken seriously by manufacturers. This article will show that more privacy research is needed in VR/AR settings to make sure the people have the privacy they need, especially the most vulnerable ones.

Virtual reality has been adopted in plethora of applications and fields in today's world. There are different areas in which virtual reality is used extensively to improve performance or enhance the experience. Most businesses nowadays utilize 360 degrees view of the product in the market. Also, business virtual worlds are comprised of virtual tours, virtual meetings, and virtual trainings. Businesses embrace augmented reality and virtual reality technologies because it is very cost effective. Businesses can test products in early development by the use of VR/AR and hence reduce costs and lower business risks.

RELATED WORKS

There are significant previous efforts which have been done by different people in this domain, however it is slightly difficult to find previous works or related research which cover both, the privacy and security aspects of the virtual reality environment. De Guzman et al. (2020) wrote one of the most comprehensive privacy and security approaches in mixed reality – which in a way covers virtual reality and augmented reality. This literature survey explored general privacy and security properties along with their corresponding threats and discussed in length each property. The literature derived privacy and security properties from three models and combined them to have an overarching model from which can be referred or qualify different approaches (both defensive and offensive strategies) (De Guzman et al., 2020).

In a separate case study conducted by Chen et al. (2018), which intended to bring awareness of potential privacy and security breaches from seemingly innocuous VR and AR technologies by deploying custom AR system based on Samsung Gear VR and ZED (Chen et al., 2018) which generated video feed from the ZED camera and sent to Gear VR app installed on a smartphone. Real Time Streaming Protocol (RSTP) was the protocol used for the delivery of multimedia data between a client and a server. It was proven that while pretending to be playing, an attacker can capture videos from a victim password input via touch screen. The study used depth and distance information provided by the stereo camera to reconstruct the attack scene and recover victim's password. Shockingly the experiment demonstrated the success rate of 90% for numerical passwords when the distance from the victim is 1.5 meters and reasonably good success rate achieved within 2.5 meters.

The paper written by Valluripally et al. (2020), titled "Attack Trees for privacy and security in Social Virtual Reality Learning Environments" is yet another well-written paper in the virtual reality domain which relates to privacy and security in Virtual Reality and Augmented Reality domain. Most critical applications utilize Virtual Reality Learning Environments (VRLE) such as military and public safety training, therefore privacy and security is of the outmost importance. This paper enforced on the important design principles, such as hardening, diversity and principle of least privilege to help enhance the resilience of social VRLEs. Through experiments carried out in this case study, it was demonstrated that the attack tree modeling had effectiveness with a reduction of 26% in probability of loss of integrity (security) and 80% in privacy leakage (privacy) in before and after scenarios pertaining to the adoption of the design principles (Valluripally et al., 2020).

METHODOLOGY

Search Strategy

The literature review utilizes and systematically analyzes robust online educational databases, and facilities provided by different online library systems which house extensive collection of electronic books and exclusive access to the repository of research and case studies, and journals. The databases such as Google Scholar, IEEE electronic (IEEE Xplore) library and ACM Digital Library were used extensively. We are concerned with newer, emerging technologies, the cross-sectional time horizon was limited to the past 10 years.

We have two screening steps. In the first screening step, the key search term was ("virtual reality" OR "augmented reality" OR "AR" OR "VR") AND ("privacy" OR "security"). We then apply the second screening step on the filtered papers, with key search term "concern" AND "threats" AND "solutions".

Eligibility Criteria

We applied the following criteria for accumulating the articles: 1) Available in full text 2) Written in English 3) Related to privacy and security in VR/AR 4) Peer-reviewed conference and journal 5) Published after 2012.

The following exclusion criteria are used to scan and filter the articles: 1) No books/chapters 2) No concerns in the privacy or security 3) No threats from privacy or security 4) No solutions for privacy or security.

Study Selection Results

The search yielded 120 potentially relevant articles and screened in addition to the original search. Figure 1 shows the PRIMSA flow chart of the search process and the number of inclusion and exclusion.

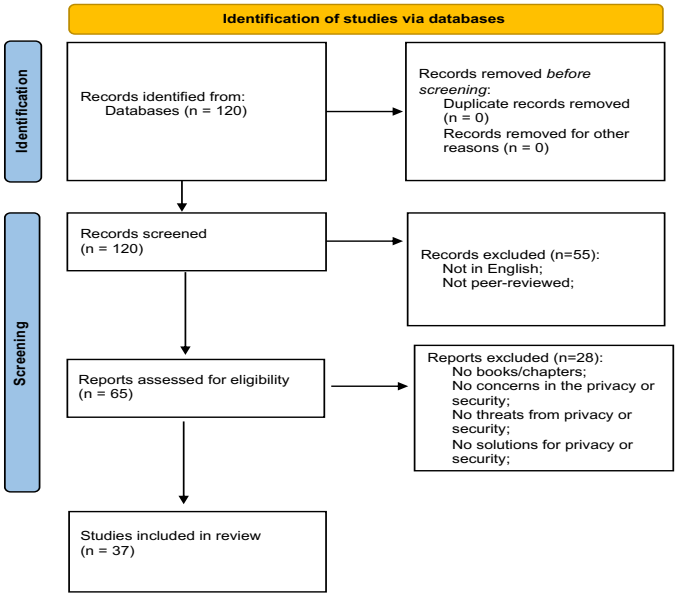

Figure 1: The Prisma Search Process

RESEARCH FINDINGS

Solutions and limitations. Currently there are several mitigation techniques which are used to counter privacy and security risks discussed earlier. These mitigation approaches are successful in a certain degree but not always a comprehensive and complete solution to the existing privacy concerns since they may or may not completely resolve some of the privacy concerns and may as well have limitations in its application which raise challenges. Often, these privacy and security mitigation techniques must be deployed in combination to have maximum effect. In this section we are going to discuss existing privacy mitigating solutions, and limitations associated with them.

Regardless of the data type risks concerns, mitigating approaches are similar in its nature, therefore, one or more mitigation technique can help protect one or more risk types. For instance, observable data allowed virtual reality environments to construct immersive experience unique to the end-user thus allow them to have customized experience based on their preferences. The collection of private information such as digital communications and in-app or in-world interactions may lead to privacy exposure. And one mitigation technique for observable data is disclosure and user consent. However, observed data, and computed data can also be protected using strong and well-designed disclosure agreements and user consent forms. However, even though these are also good approaches to privacy and security in AR/VR environments, we will only discuss them shortly and focus the attention of this paper in technical aspect of privacy and security mitigation techniques which can dramatically improve the privacy and security issues.

Technical mitigation techniques which help enhance privacy and security issues can be categorized in different ways depending on the perspective and analysis of the author, however, we are going to discuss these mitigation techniques in categories based on what they perform – such as data manipulation (altering data), data protection (shielding data) and privacy and security enhancement in systems and architecture. Table 1 below is going to provide an overview of these technologies (Fintech Edge Special Report, 2021).

Altering Data	Shielding Data	Systems and Architecture
Anonymization	Encryption	Multi-party Computation
Pseudonymization	Homomorphic Encryption	Data Dispersion
Differential Privacy	Privacy Enhanced Hardware	Management Interfaces
Synthetic Data		Digital Identity

*These categories are based on the authors' analysis of the PET space. The authors acknowledge that there are multiple ways to group these technologies, techniques, and processes.

Table 1. Overview of Security Technologies Implement Privacy (Fintech Edge Special Report, 2021)

Altering Data. Some researchers have proven the fact that personal identifying information can be protected using k-Anonymization and Pseudo-id, especially for the AR/VR environment utilizing location-based services (LBS). One of the

critical and core application in virtualization is location tracking, thus, most devices are equipped with GPRS capabilities. Location Determination Technology (LDT), such as Cell-ID, A-GPS, EOTD, etc. gives the location information which consist of X-Y co-ordinates (Aryan & Singh, 2010), which allows providers to be able to offer several very useful value-added services to their users, which in turn helps them to gain customer loyalty and helps them increase profitability.

One of the privacy protection models is non-cooperative model, techniques like pseudo-anonymity, where false dummies and landmark objects are used by the user itself to hide the location. It is very simple in design but very vulnerable to attacks (Aryan & Singh, 2010). The other model is centralized Trusted Third Party (TTP) model, in this case anonymizing the location of the user, requesting the service with the anonymized location, and returning the result to the user etc., is done by a TTP. The downside is that there is a performance bottle neck experienced when the number of requests TTP gets is higher that the number of requests TTP can store and process. Even though this is a major drawback in terms of performance, in terms of privacy, this model is very efficient. One other model which can be used to hide sensitive information such as location is peer to peer cooperative model, in this model, to achieve privacy, several users try to cooperate and compute their location or hide their location information in a distributed manner using cryptographic measures such as Oblivious Transfer (OT) or certificates to prove the trust worthiness (Aryan & Singh, 2010).

K-anonymity was introduced to address the question of "how a data holder can release its private data" which guarantees that the individual subjects of the data cannot be identified, while the data remain useful. The concept of personalized k-anonymization operates in a way that each user can specify their need anonymization level, since privacy of every user might change. Pseudo-ids can be used to drawbacks of personalized k-anonymization and utilized Hybrid Location Privacy Algorithm (HLPA) (Aryan & Singh, 2010).

Even though challenging, anonymization is also used in facial attributes obfuscation. Research by Li et al. (2021), shows that by anonymization is used by a robust model which modify the original end user's face without destroying the existing data distribution. The method is used to remove all the identification information and then generate a highly realistic face (Li et al., 2021). To satisfy the identity-preserving requirement, concept of soft biometric privacy is introduced and then develop a face mixing approach to conceal the gender attribute while preserving the recognition utility. The facial attributes such as gender, age, and race are preserved using different techniques such as Face De-identification and Face Manipulation. Evaluation metrics such as LPIPS Distance – used to measure the similarities between the generated images and original images, FD Distance – which calculates the distance between the distribution of real images and the generated images, and Human Preference – which is used to compare the realism and faithfulness of generated images, validate the quality of new images.

Shielding Data. Apart from the efforts to alter the data so that unintended access cannot lead to inference and eventually identify a person, another effort to secure data at-rest or in transit is by utilizing mitigation techniques which help protecting or shielding the data completely – in a way that even when the data is accessible, still will not be meaningful to a naked eye. AR/VR technologies present tremendous privacy risks. The devices that provide individuals with enhanced immersive experiences contain several sensors that continuously collecting data when in use, and transmit telemetry data of the user, such as body and eye movements. Unfortunately, functional AR/VR technology is inherently dependent on the device tracking of the end-user body movement using a collection of sensors to track close to 90 movements per second, which equates to documenting approximately two-million body-movement recordings during a 20-minute VR session (Kohnke, 2020). Clearly, with this magnitude of data at risk, privacy prevention techniques must be applied.

Research by Hu et al. (2021) introduced a split-process framework for augmented reality, with the goal of providing end users more control over application usage of their camera frames, and the information derived from them (Hu et al., 2021). The research answers the question: How do we protect users from surreptitious collection of visual data while maintaining usable visual computing for AR applications? Which in theory the correct approach is to protect visual privacy by processing camera frames into privacy-preserving visual features and only give apps access to those features or a region of the camera frame define by users. The research introduced LensCap, an application development framework built on top of split-process access control.

Another way to address data shielding is using encryption. Cryptography is one of many ways to make sure that confidentiality, authentication, integrity, availability, and identification of user data can be maintained as well as privacy and security of data can be provided to the end-user. Encryption on the other hand is the process of converting normal data or plaintext to something incomprehensible or cipher-text by applying mathematical transformations or formulae – these mathematical transformations or formulae used for encryption processes are called algorithms (Bhanot & Hans, 2015). Driven by the advances in mobile computing, and increasing demand for more immersive visual experiences, near-eye 3D display technology is in the center of virtual reality and augmented reality applications. The good news is application scenarios of these technologies such as metasurface in holographic 3D imaging have demonstrated that encryption is possible (Guo et al., 2021).

Systems and Architecture. Since virtual reality and augmented reality function by consuming sensitive data from different sources and locations, secure multi-party computation (SMPC) can significantly help secure private sensitive information by deploying cryptographic technique that enables different parties (whether server/client architecture or peer-to-peer architecture) to carry out computational tasks using locally residing data and share the output rather than revealing private information over the network. Figure 2 illustrates the workflow of SMPC. Rather than having centrally massive computing device, by deploying low resource-intensive "nodes" will eliminate transfer of sensitive data, single point of failure, and significantly improve performance – since segregated computing is faster and less networking traffic is utilized. Data can be split among untrusted parties assuming that information can only be inferred when the distributed parts are combined, thus SMPC allows computation of data from two or more sources without necessarily knowing about the actual data each source has, and therefore enhance privacy and security of the personal identifying information. One good example is the virtual cloth try-on service used secret sharing and secure two-party computation. The anthropometric information of the user is split between the user's mobile device and the server, and are both encrypted (De Guzman et al., 2020).

To quickly explain how secret sharing or SMPC work, please refer to the following generic diagram (shown in Figure 2) which shows cryptographic technique using secure multi-party computation where two or more parties exchange secrets (1.1 and 1.3) to extract combined knowledge (1.2 and 1.4) without the need for divulging or decrypting each other's data share (De Guzman et al., 2020).

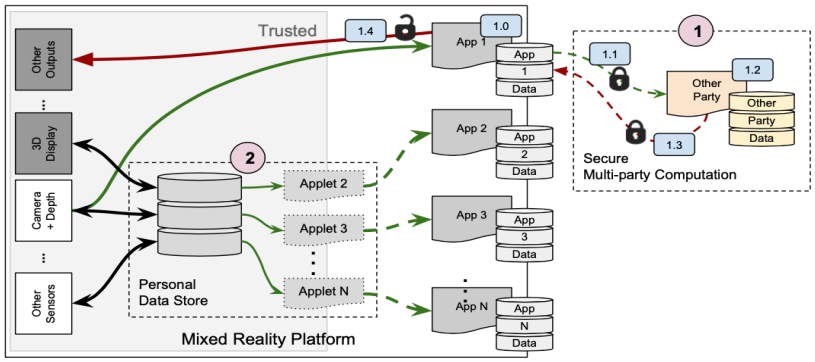

Figure 2. Cryptographic Technique Using Secure Multi-Party Computation (De Guzman et al., 2020)

Disclosure and User Consent Forms. Furthermore, there are other non-technical approaches to improve end-user decision making, there should be a better clarity and better "opt-in" mechanism in place to help end-users understand that by participating in AR/VR usage, permission to disclose users' confidential information to third parties depends on their decision to consent. Therefore, AR/VR privacy policies have some mechanism in place to make user accept these terms and conditions, before participating in AR/VR environments. However, there are still challenges such as AR/VR companies choose to construe an affirmative answer as consent to disclose personal information in accordance with its privacy policy and use this narrative to avoid liability. The authors in (Shaub, 2009) additional review of privacy policies offered by some AR/VR manufacturers clearly suggests that aggregate data collected by the device, such as the end-user financial state, transaction history and movement data, are shared with the manufacturer's business affiliates without further consent from the end-user (Kohnke, 2020). In most cases the issued disclosure and consent forms are more a formal right than a true protection, the main reason is that data subjects do not have time to read and understand the general terms of use or privacy policies of data controller (De & Metayer, 2018).

DISCUSSION

Privacy and security are mutually inclusive concepts in any domain. Some might even argue that one cannot exist without the other. In AR/VR environments, privacy concerns can be mitigated using multiple security approaches such as altering data and/or shielding the data completely. Data alteration helps preserve personal identifying information from being exposed in the first place, while data shielding deploy means which guarantees that data is completely not accessible to an unauthorized entity. It is important to note that privacy and security concerns in AR/VR are distinct, however they are closely related, and most times a solution or remedy for one might also resolve the other. Therefore, the general and collective view to these concerns is important.

CONCLUSION

Augmented and virtual reality uses will continue to grow. Despite the usefulness of these environments, potential privacy and security risks will continue to be a significant problem. In this paper, much has been covered in terms of privacy and security

approaches and mitigations, however, more work in researching for better, more applicable measures must be investigated especially for the cloud-based AR/VR service environments. Cloud architecture brings a completely new challenges which current mitigation techniques might fall short. It will also be useful and very interesting research in the future to dive deep into the privacy and security regulations domain. This is another area which should be extensively researched in the future because there is so many loopholes and improvement which are strongly required to help technical aspects of privacy and security data protection.

It is crucial to note that, generally, the coexistence of privacy concepts and security technologies has become to be known over the years. Privacy usually generates a framework so that informed decision-making can be made as to what entity should legitimately be able to access and manipulate target information. While security mechanisms and technologies always change, the goal remains the same – all security mechanisms are designed for one purpose in mind, implementing privacy decisions and choices made. As a consequence, most times, when a privacy issue occurs, it is not necessarily that the privacy framework choices were wrong, rather, loopholes within the implementation of these choices has been found and exploited. This is the reason why security mechanisms were discussing today might not be the same in tomorrow or in few years from now.

REFERENCES

1. Aryan, A., & Singh, S. (2010). Protecting Location Privacy in Augmented Reality Using k-Anonymization and Pseudo-id. *International Conference on Computer & Communication Technology.*
2. Bhanot, R., & Hans, R. (2015). A Review and Comparative Analysis of Various Encryption Algorithms. *International Journal of Security and Its Applications, 9*(4), 289-306.
3. Chen, S., Li, Z., DAngelo, F., Gao, C., & Fu, X. (2018). A Case Study of Security and Privacy Threats from Augmented Reality (AR). *2018 International Conference on Computing, Networking and Communication (ICNC): Communication and Information Security Symposium.*
4. De Guzman, J., Thilakarathna, K., & Seneviratne, A. (2020). Security and Privacy Approaches in Mixed Reality: A Literature Survey. *52*(6), 1-37.
5. De, S. J., & Metayer, D. L. (2018). Privacy Risk Analysis to Enable Informed Privacy Settings. *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, (pp. 95-102).
6. Fintech Edge Special Report. (2021). *Privacy Enhancing Technologies: Categories, Use Cases, and Considerations.* Federal Reserve Bank of San Francisco.
7. Guo, X., Zhong, J., Li, B., Qi, S., Li, Y., Li, P., . . . Zhao, J. (2021). Full-Color Holographic Display and Encryption with Full-Polarization Degree of Freedom. *34*(3), 1-21.
8. Hu, J., Iosifescu, A., & LiKamWa, R. (2021). LensCap: Split-Process Framework for Fine-Grained Visual Privacy Control for Augmented Reality Apps. *Proceedings fo the 19th Annual International Conference on Mobile Systems, Applications, and Services.*
9. Kohnke, A. (2020). The Risk and Rewards of Enterprise Use of Augmented Reality and Virtual Reality. *ISACA Journal Dubai Compliance, 1*, 1-68.
10. Li, J., Han, L., Chen, R., Zhang, H., Han, B., Lili, W., & Cao, X. (2021). Identity-Preserving Face Anonymization via Adaptively Facial Attributes Obfuscation. *Multimedia Research and Recommendation.* China.
11. Ling, Z., Li, Z., Chen, C., Luo, J., Yu, W., & Fu, X. (2019). I Know What You Enter on Gear VR. *2019 IEEE Conference on Communications and Network Security (CNS)*, 241-249.
12. 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.
13. Shaub, S. (2009). User Privacy and Information Disclosure: The Need for Clarity in "Opt-in" Questions for. *Washington Journal of Law, Technology & Arts, 5*(4).
14. 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).*
15. Yang, Y., & Wang, R. (2020). LBS-Based Location Privacy Protection Mechanism in Augmented Reality. *2020 International Conference on Internet of Things and Intelligent Applications (ITIA)*, 1-6.