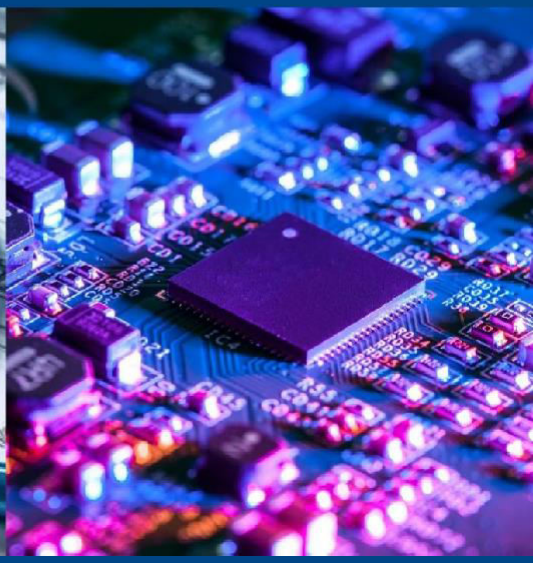
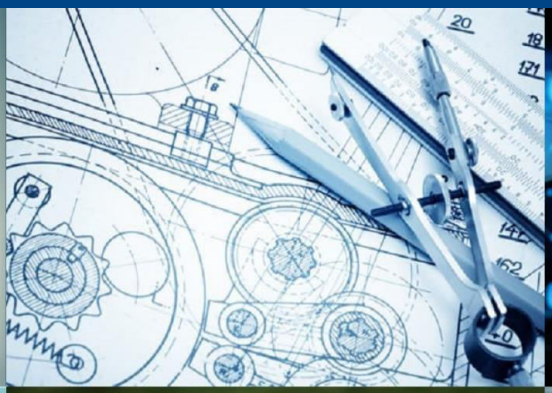
ISSN: 2582-7219

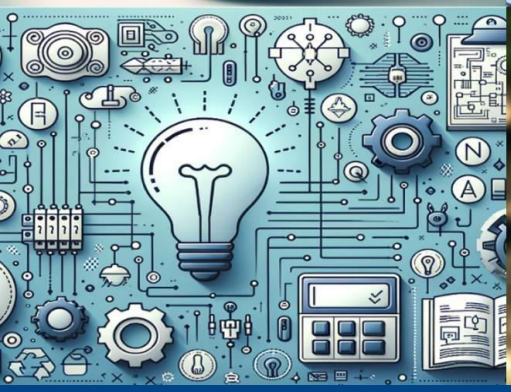




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 8, August 2025

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808054

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IMMERSIVE TECHNOLOGY SECURITY CHALLENGES: AN ANALYSIS OF VR AND AR VULNERABILITIES

Mrs.C.Kausalyadevi

Assistant Professor, Department of Computer Applications, Chevalier.T.Thomas Elizabeth College for Women, Sembium, Chennai, India

ABSTRACT: Virtual and augmented reality (VR/AR) systems face significant cybersecurity threats, including data theft, identity breaches, and network credential theft. As VR goggles function like IoT devices, they are as vulnerable as phones, tablets, and PCs. Cybercriminals can exploit security weaknesses, leading to hardware/software damage and personal data leaks. AR tools can aid cybersecurity by enabling real-time network monitoring and threat detection. However, research on VR security and privacy remains limited compared to its applications in gaming and entertainment. This study systematically reviews the literature on VR security concerns over the last 20 years, highlighting risks and potential countermeasures.

KEYWORDS: Cyber Security, Virtual Reality and Augmented Reality.

I. INTRODUCTION

Virtual reality is now available to the general public. Due to personal nature of which data had been collected from the users, VR users felt somewhat threatened by its privacy issues (Psychoula et al., 2018). VR encompasses applications on headsets FSB that allow the user FSB to navigate virtual FSB spaces. These devices collect personal data to a great extent from the users (Froehlich & Azhar, 2016) as a part of providing these experiences. Such information can be given by the users or derived from their historical data (Dick 2021). In a digital world, most of the behavioural patterns of users are logged and the various components of the VR world can be adjusted. Face book/ Oculus VR A case in point is Oculus VR of Face book. One component of a complicated system that needs careful security examination is virtual reality (VR) headsets. These headsets are susceptible to hacks since they are connected to content markets where users can download different programs. Vulnerabilities in apps, the marketplace, or even the VR devices themselves can be used by malicious actors. Additionally, virtual reality offers new avenues for exploitation for attackers. Reaching, nodding, stepping, and blinking are now all interpreted by virtual reality (VR) and augmented realities (AR) systems because to the development of metaverse technology, which was spearheaded by tech titans like Mark Zuckerberg. Immersion in gaming, socializing, business meetings, and even financial transactions are made possible by these interactions. However, protecting these environments from cyber dangers is crucial as VR and AR grow more ingrained in daily life.

II. LITERATURE REVIEW

Since virtual reality is entirely manufactured, nothing in it exists in the actual world. A person's identity, the veracity of a situation, and whether a place is safe to visit can all be inferred from a variety of signs that they display. All components can be manipulated and simulated realistically thanks to virtual reality. Though their encounter is fake, the user may have the best of intentions. Consider an entity operating a virtual bank where digital transactions are being conducted. The money being transferred is authentic, but how can one ascertain the legitimacy of the transaction record, bank, or teller? Unfortunately, there is no way to make a firm decision. This important cybersecurity issue still hasn't been resolved.

Augmented reality (AR) visualization could be useful for complicated security data, such as network topologies, threat landscapes, and system designs. This will make it simpler for security analysts to spot patterns, connections, and possible weaknesses, which will lead to better security protocols and lower risk. The dependability of the content could

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

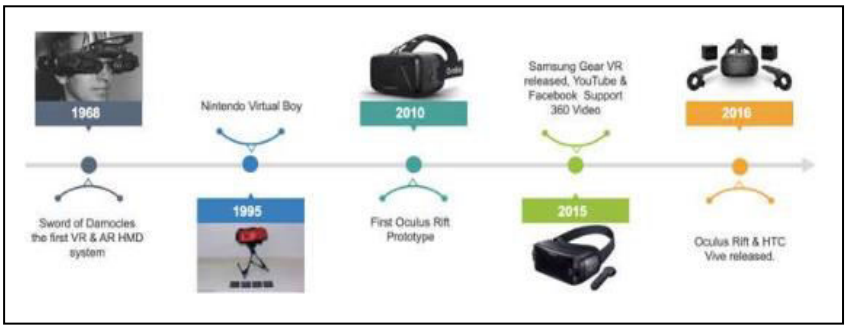
International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

be threatened by several cyberattacks, regardless of the source's legitimacy. This group comprises sniffers, spoofing, and data manipulation.

Although cybersecurity and augmented reality (AR) have been around for a while, they have significantly advanced and expanded in the last few years.

The corporate, industrial, tourism, academic, and social spheres—including the gaming, entertainment, and communication sectors—are where these technologies are most frequently found, though they have a wide range of potential uses. Everyone acknowledges the importance of these technologies to the global initiative known as Industry 4.0, which seeks to spark a fourth industrial revolution. They are also some of the most important technological developments of the last century. Offering clients vital information in a virtual setting is one of the most important uses of Augmented Reality (AR), while many other businesses also use it. The realism and immersion of virtual and augmented reality experiences will increase. It is hoped that this will increase their use and involvement. However, it also increases the risk they face. Known as "deepfakes," machine learning technology make it possible to create synthetic identities by manipulating voice and video to seem real. In the event that a hacker manages to access motion-tracking data from a virtual reality headset, they may potentially create a digital replica. After that, they can place this over someone else's VR experience—like an immersive business meeting—to initiate a social engineering attack.



III. METHODOLOGY

a. Use of tools and techniques

The study examined the benefits of incorporating cybersecurity within augmented and virtual reality environments. This perspective asserts that understanding arises from concrete, measurable experiences. In this framework, a positivist perspective relies on evidence and adopts a methodical approach. Qualitative metrics like system performance, success rate of integration, and rate of errors play a role in addressing the issue. Positivism is a framework that depends on measurement and logical reasoning, asserting that knowledge emerges from impartial and quantifiable observations of activities, actions, or reactions. According to positivism, if something cannot be measured in this manner, it cannot be known with certainty. Scientific knowledge is based on the collection of data that is acquired without the influence of theory or values through observation.

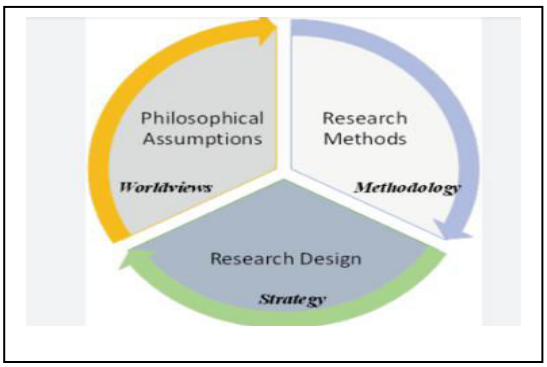


FIGURE 2: POSITIVISM PHILOSOPHY

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

b. Data Collection

Data Collecting concept papers and research papers about privacy and security in virtual reality was the aim of the data collection process. The following databases were chosen to locate relevant articles: Google Scholar, IEEE Explore, ACM Digital Library, Sage Journal, Wiley, Web of Science, and Springer. The literature review included articles published between 2000 and February 2022.

c. Data Analysis

After gathering the data, we carried out a comprehensive qualitative thematic analysis. The data was analyzed and visualized using statistical techniques. Descriptive statistics have historically been effective in revealing hidden trends and patterns. To find connections and assess assumptions based on the literature, inferential techniques were applied. Many themes have been identified from the qualitative data. Every person was thoroughly examined in order to identify trends, anomalies, and reoccurring issues.

COMMON THREATS IN AR AND VR	PERCENTAGE
Latency problem	8%
Observation attacks for graphical pin 2d	15%
Confidentiality, integrity, availability(CIA)	15%
Privacy concerns	15%
Data theft	16%
Security, privacy and saftey(SPS)	31%

Table 2.1 Shows Analysis of Common AR and VR Threats: Threat Percentage Distribution

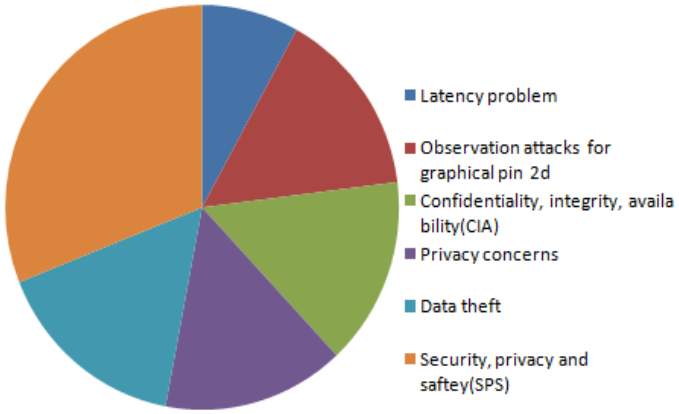


Figure 2.2: Threats in AR AND VR

d. Screening for inclusion

Although AR/VR is still a relatively new technology, as the underlying technology advances and a wider range of users encounter it for the first time, new opportunities for its application in equality and inclusion initiatives are coming to light. Using AR/VR as an empathy tool, modifying its wide range of features to accommodate users with disabilities, and removing obstacles brought on by physical distance to unite communities and improve face-to-face interactions across locations are the three main ways that AR/VR can support larger equity and inclusion initiatives.

e. Ethical evaluation

Ethical integrity was given top priority throughout the paper. In order to reduce the possibility of plagiarism claims when utilizing secondary data, the study made sure that all significant sources were properly acknowledged. To ensure the content remained confidential, we were guaranteed not to use any unapproved or non-public data. No changes were

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

made to the data used in the study to make it more consistent with the story. In order to maintain objectivity, we have declared any possible conflicts of interest that might have affected our research.

IV. FINDING AND ANALYSIS

Both augmented reality and cyber-security have been around for a while, but their recent growth and improvement have been nothing short of spectacular. These advancements have the potential to be applied in a wide range of fields, including business, industry, tourism, academia, and society. These developments may also have a beneficial effect on other industries, such as communication, gaming, and entertainment. There is a global movement called Industry 4.0 that aims to usher in a fourth industrial revolution, and everyone agrees that these technologies are essential to the movement. As some of the most revolutionary technological accomplishments of this century, they also rank highly among the most significant innovations.

To refine the skills required to protect a large cyber-physical system from a sophisticated cyberattack. Systems for attack prediction, reaction generation, and malicious actor strategic behavior modeling will be made possible by this. In order to ensure that cybersecurity students learn the necessary material in their lessons, the authors developed the scenario model. This model also includes a significant amount of serious game scenario aspects. The way the context-aware system interacts with the teacher, the student, and the program itself during the course of study is explained in the second part of the statement. These discussions center on the program's modules and their individual objectives.

A lack of cybersecurity experts and employees with the required training could result in a data leak. In this framework, companies look for efficient training methods to raise awareness and teach their staff about cybersecurity. Thisroblem can be resolved by combining gamified learning and training platforms with augmented and virtual reality technologies. These AR and VR-based educational resources allow students to engage with them in a dynamic, lifelike setting.

Cybersecurity experts may create training simulations that are very comparable to the real thing by utilizing augmented reality (AR). Trainees can gain practical experience and improve their threat identification and mitigation skills by simulating cyberattacks in authentic scenarios. This improves their skills, perception, and preparedness to handle actual cyber security problems. Although they enable users to see their immediate surroundings, cameras are essential parts of augmented reality headsets, but they also present security risks. Since the introduction of the Google Glass prototype in 2013, which garnered a lot of attention before being abandoned in 2015, privacy and security concerns have taken center stage.

V. CONCLUSION

Finally, when boundaries between the real and virtual worlds begin to melt, some hazards only become apparent. The potential of genuine physical harm from a virtual reality experience is significant, even though the risk of theft from a self-driving automobile is more evident. There have been reports that some people, especially those who use earlier VR headset models, get motion nausea from virtual reality (VR). The advent of better hardware has lessened this. Particularly with augmented reality (AR), consumers' physical security is at serious risk. We examined several authentication systems, information concealment techniques, privacy frameworks, and social environment privacy. Researchers have found that more research has been done on privacy than security.

REFERENCES

1. Adhikari, S., 2021. Intelligent Cyber Defense in 5G Augmented Aviation Cybersecurity Framework. In AIAA Scitech 2021 Forum (p. 0661). **https://arc.aiaa.org/doi/abs/10.2514/6.2021-0661**

2. Ahmet, E.F.E. and Isık, A., 2020. A general view of industry 4.0 revolution from cybersecurity perspective. International Journal of Intelligent Systems and Applications in Engineering, 8(1), pp.11-20. **https://ijisae.org/index.php/IJISAE/article/download/903/611**

3. Alnajim, A.M., Habib, S., Islam, M., AlRawashdeh, H.S. and Wasim, M., 2023. Exploring cybersecurity education and training techniques: a comprehensive review of traditional, virtual reality, and augmented reality approaches. Symmetry, 15(12), p.2175. **https://www.mdpi.com/2073-8994/15/12/2175**

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4. Alqahtani, H. and Kavakli-Thorne, M., 2020, February. Exploring factors affecting user's cybersecurity behaviour by using mobile augmented reality app (CybAR). In Proceedings of the 2020 12th International Conference on Computer and Automation Engineering (pp. 129-135). **https://dl.acm.org/doi/abs/10.1145/3384613.3384629**

5. Alqahtani, H. and Kavakli-Thorne, M., 2020. Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). Information, 11(2), p.121**.** **https://www.mdpi.com/2078-2489/11/2/121/htm**

6. Böhm, F., Dietz, M., Preindl, T. and Pernul, G., 2021. Augmented Reality and the Digital Twin: State-of-the-Art and Perspectives for Cybersecurity. Journal of Cybersecurity and Privacy, 1(3), pp.519-538. **https://www.mdpi.com/2624-800X/1/3/26/pdf**

7. Braun, V. and Clarke, V., 2019. Reflecting on reflexive thematic analysis. Qualitative research in sport, exercise and health, 11(4), pp.589-597. **https://doi.org/10.1080/2159676X.2019.1628806**

8. Burton, S.L., 2021. Artificial intelligence (AI) and augmented reality (AR): Disambiguated in the telemedicine/telehealth sphere. Scientific Bulletin, 26(1), pp.1-11. **https://sciendo.com/pdf/10.2478/bsaft-2021-0001**

9. Dimitrov, W., 2020. Analysis of the need for cyber security components in the study of advanced technologies. In INTED2020 Proceedings (pp. 5259- 5268). IATED. **https://library.iated.org/view/DIMITROV2020ANA**

10. Dissanayake, V.D., 2019. A review of Cyber security risks in an augmented reality world. University of Sri Lanka, Institute of Information Technology: Malabe, Sri Lanka. **https://www.researchgate.net/profile/Viraj-Dissanayake/publication/339941469_A_review_of_Cyber_security_risks_in_an_Augmented_reality_world/links/5e6e3c2a299bf12e23c8ba56/A-review-of-Cyber-security-risks-in-an-Augmented-reality-world.pdf**

11. Sundler, A.J., Lindberg, E., Nilsson, C. and Palmér, L., 2019. Qualitative thematic analysis based on descriptive phenomenology. Nursing open, 6(3), pp.733-739. **https://doi.org/10.1002/nop2.275**

12. Suri, H., 2020. Ethical considerations of conducting systematic reviews in educational research. Systematic reviews in educational research: Methodology, perspectives and application, pp.41-54. **https://doi.org/10.1007/978-3-658-27602-7**

13. Tai, Y., Wei, L., Zhou, H., Peng, J., Li, Q., Li, F., Zhang, J. and Shi, J., 2019. Augmented-reality-driven medical simulation platform for percutaneous nephrolithotomy with cybersecurity awareness. International Journal of Distributed Sensor Networks, 15(4), p.1550147719840173. **https://journals.sagepub.com/doi/full/10.1177/1550147719840173**

14. Park, Y.S., Konge, L. and Artino Jr, A.R., 2020. The positivism paradigm of research. Academic medicine, 95(5), pp.690-694. **https://doi.org/10.1097/ACM.0000000000003093**

15. Raybourn, E.M. and Trechter, R., 2018. Applying Model-Based Situational Awareness and Augmented Reality to Next-Generation Physical Security Systems. Cyber-Physical Systems Security, pp.331-344.**https://www.osti.gov/servlets/purl/1469093**

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com