International Journal of Core Engineering & Management

Volume-7, Issue-02, 2022 ISSN No: 2348-9510

AUGMENTED REALITY (AR) AND VIRTUAL REALITY (VR) SECURITY

Anvesh Gunuganti
maverickanvesh@gmail.com

Abstract

Technologies like Augmented Reality (AR) and Virtual Reality (VR) user engagement with digital and physical spaces for environments have revolutionized sectors ranging from health, education, and entertainment. AR adds digital information to the physical environment, while VR, on the other hand, places users in fully created digital environments. Implementing such extensive usage creates new issues of security where information, users' rights, and equipment trustworthiness need protection. This paper reviews AR and VR's security concerns on security threats, security models, and security standards. This research performs a literature review and systematic analysis of case studies in industrial and healthcare environments to determine the main security issues and reveal appropriate recommendations. This work indicates how IT managers should ensure security measures are properly taken, train users on security awareness, and follow regulatory norms. As for the recommendations for further studies and innovations, the focus is on constantly reassessing the potential threats.

Keywords: Augmented Reality, Virtual Reality, cybersecurity, data privacy, regulatory compliance

I. INTRODUCTION

Augmented Reality (AR) and Virtual Reality (VR) technologies have changed the manner in which users use them because there are new digital-added layers in the real world for AR, and there are newly created virtual environments for VR [1]. AR overlays digital information on top of the environment being viewed by the user, while VR puts the absorbers into virtual reality through accessories like helmets. Since these developing technologies are becoming more linked to different spheres of life, including healthcare, education, and entertainment, integration has great security consequences [2]. The security of the AR and VR systems should be maintained to protect the relevant data, users' interests, and the reliability of the used equipment from new threats in the cybersecurity field. This underlines the importance of appropriate security models to help ensure the appropriate use of AR/VR in various fields, ensuring security and efficiency.

1. Overview of Augmented Reality (AR) and Virtual Reality (VR)

Augmented Reality (AR) and Virtual Reality (VR) applications have developed swiftly across different industries and have been predicted to shift the world regarding experiences and uses. AR extends real-world environments by adding computer-generated imagery to a live view, while VR transports the user into an artificial environment. They are steadily applied to various business areas, including industrial manufacturing and health care, changing equipment control to patients' treatment [3]. Fig. 1 shows that AR augments physical space by integrating digital information into the real world, improving customer experiences in gaming and retail. Conversely, VR involves users in fully created environments using headsets that are more commonly used in gaming and simulators.

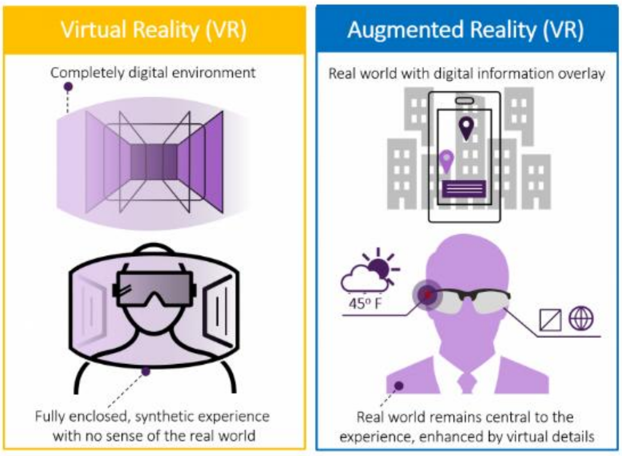
Virtual Reality (VR)
Completely digital environment
Fully enclosed, synthetic experience with no sense of the real world
Augmented Reality (VR)
Real world with digital information overlay
45° F
Real world remains central to the experience, enhanced by virtual details

Fig. 1. Augmented Reality (AR) and Virtual Reality (VR) [10]

2. Importance of Augmented Reality (AR) and Virtual Reality (VR)

Product integration of AR and VR provides unprecedented effects and, at the same time, creates unrevealed security problems [4]. In organizations, especially in the industries where equipment monitoring systems integrate AR and VR, security measures applied to data may help protect against cyber threats that could compromise vital processes. Likewise, in the healthcare area where AR and VR are applied for diagnostics, training, and treatment, it is crucial to ensure subject privacy and properly protect that data to respect the patient's right to privacy.

Augmented Reality (AR) and Virtual Reality (VR) have been at the forefront of technological innovation, revolutionizing industries by offering immersive and interactive experiences [5]. These immersive technologies provide unique opportunities for businesses to connect with their customers, optimize operational efficiency, and enhance employee training. Fig. 2 demonstrates the future outlook with AR and VR in revolutionizing experiences and applications across different sectors. It may depict their integration into various industries such as gaming, education, healthcare, and manufacturing. The figure illustrates how AR enhances real-world environments with digital overlays while VR immerses users in simulated environments.

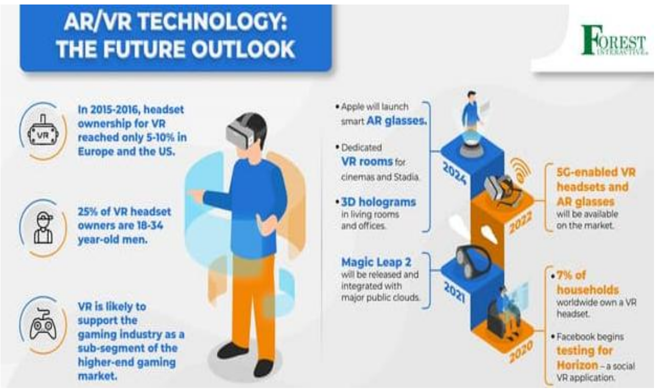
AR/VR TECHNOLOGY: THE FUTURE OUTLOOK
FOREST INTERACTIVE
VR
In 2015-2016, headset ownership for VR reached only 5-10% in Europe and the US.
25% of VR headset owners are 18-34 year-old men.
VR is likely to support the gaming industry as a sub-segment of the higher-end gaming market.
• Apple will launch smart AR glasses.
• Dedicated VR rooms for cinemas and Stadia.
• 3D holograms in living rooms and offices.
2024
5G-enabled VR headsets and AR glasses will be available on the market.
2022
Magic Leap 2 will be released and integrated with major public clouds.
2021
• 7% of households worldwide own a VR headset.
• Facebook begins testing for Horizon – a social VR application.
2020

Fig. 2. The Future Outlook with AR & VR [11]

3. Research Objectives and Scope

This study aims to establish the safety concerns in AR and VR in industries and healthcare facilities. Specifically, it explores measures to ensure the security of AR and VR systems in industries. It analyzes the privacy and security consequences of adopting AR and VR technologies in industries.

4. Research Questions

A. How can AR and VR systems in industrial settings, like those in equipment monitoring, be protected from cyber threats and ensure data integrity?

B. What are the privacy and security implications of deploying AR and VR technologies in healthcare settings?

II. LITERATURE REVIEW

This literature review aims to offer an updated perspective on the state of AR and VR security, threats, opportunities, and applications across industries. They are only relevant to understand these dynamics to move forward with the patterns of the secure adoption of such technologies and to reduce the risks implicit in such innovative technologies.

1. Current State of AR and VR Security

AR and VR technologies are recognized to have been receiving much attention and finding their uses in various fields of work and daily life. Still, their security is not immune to threats and vulnerabilities [6]. Current research and industry practices emphasize the following aspects:

- Security Frameworks and Standards**:** Implementing effective strategies in introducing security features to prevent cybercrimes involving AR and VR systems. These frameworks consist of preventions like authenticating users, granting permissions, protecting the contents from the effects of cyber threats through encryption, and using proper methods and communication channels [14].

- Vulnerability Assessments: Various potential risks have been identified with AR and VR, for example, data leakage, accessing other people's information without their consent, and exposure to malware optimized for these immersive systems.
- Regulatory Compliance: It remains important to note that the privacy of the patient data is paramount in any healthcare application and that the system should adhere to data protection policies such as GDPR, HIPAA, etc. The regulation of operational data is also among the challenges that industrial sectors face. In Fig. 3, AR and VR's potential impact on healthcare is evident in its transformative effects on training, treatment, and patient care. AR adds richness to learning through digital augmentations of paper media, and VR offers practice environments and home-based therapy for patients. Above all, both technologies regarding surgery increase the accuracy of operations, facilitate postoperative physical therapy, provide therapeutic means to alleviate anxiety, and provide patients with thorough information regarding their respective illnesses. Such developments clearly explain the evolution of the AR and VR systems as important tools in improving the education and treatment of healthcare and, overall, the patient's experience.

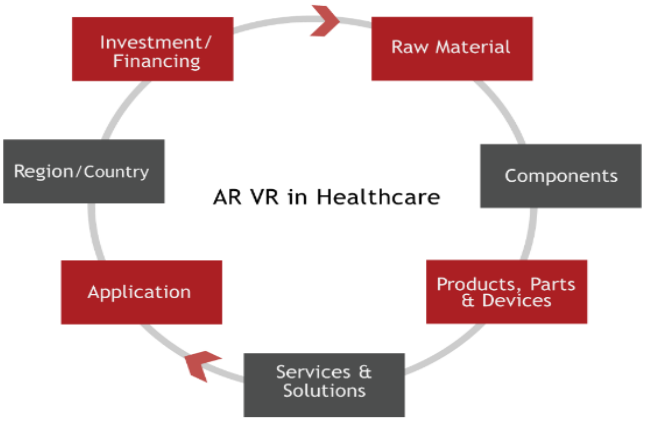

Fig. 3. AR and VR are transforming healthcare [12]

2. Key Challenges and Concerns

Despite their transformative potential, AR and VR technologies pose several security challenges:

- Data Integrity and Privacy: Data entry, exit accuracy, and customer information privacy are the main concerns. In an organizational environment, security breaches are more devastating by causing operational disruption in industrial facilities, whereas in medical facilities, disclosure of patients' privacy violates confidentiality [7].
- Cybersecurity Threats: It should be noted that viruses, malware, phishing, DoS attacks, etc., are some of the threats that are not unique to AR and VR

systems. These systems can increase risk across networks and devices as they are closely connected.

- User Authentication: User authentication and access control techniques in a system becoming compromised by unauthorized users are critical and must be safeguarded [8]. In Fig. 4, two distinct domains are depicted: the physical world, including the physical manifestation of elements such as machines and people involved in the production of goods, and the cyber world, which consists of software entities such as services, modules, and algorithms. Information technology interlinks with and configures the physical environment to regulate production processes digitally .

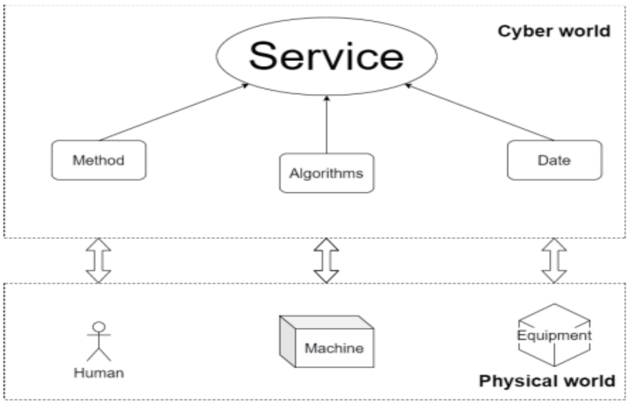

Fig. 4. Monitoring system scheme [1]

3. Technological and Applications

AR and VR technologies are revolutionizing various sectors:

- Industrial Applications: AR helps to improve equipment control, service, and simulation in industrial areas by displaying information and guidelines on the scenes. VR training enhances the workers' training and sets safety measures [15].
- Healthcare Applications: Applying AR in healthcare, doctors use it in medical training, simulations of surgeries, physical therapy, and telemedicine. Such technologies create engaging learning environments while improving the accuracy of surgical operations, provided that strong measures are taken to protect users' data privacy [9].
- Emerging Trends: Apart from the four main industries, AR and VR are steadily entering such fields as education, retail, architecture, and entertainment, causing new security risks and perspectives [10].
- Virtual assistant: The virtual assistant entity comprises five layers: Device-level and application-level components [16]. At the same time, the former collects the operating data of machines and sends it to a server for analysis; the latter informs a server about users' actions and receives information from

the server upon users' requests to the virtual assistant. The virtual assistant entity is shown in Fig. 5. The picture shows that the entity consists of 5 layers.

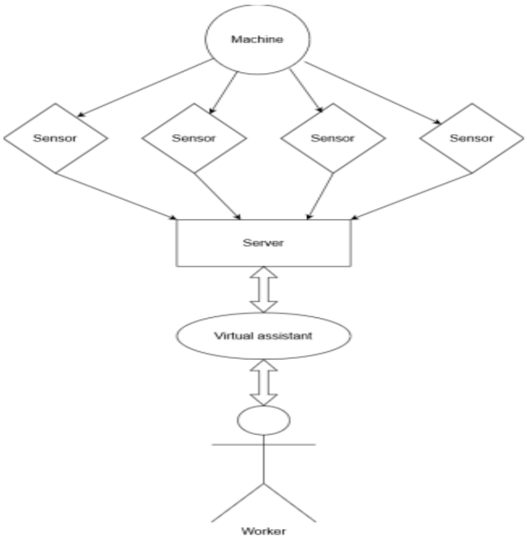

Fig. 5. Virtual assistant [1]

III. METHODOLOGY

In this study, the case study research approach is used systematically to examine the security issues arising from using Augmented Reality (AR) and Virtual Reality (VR) technologies. The cases are selected based on the book's focus: offering practical information on real-world applications and the security issues that various technologies encounter in different industries. This approach examines the security frameworks, threats, and safeguards used in several AR and VR applications.

1. Case Study Analysis

Two distinct case studies are analyzed to highlight the security challenges and strategies associated with AR and VR technologies:

- Case Study [1] - Industrial Sector Implementation: This paper focuses on using AR to manage equipment monitoring systems in the industrial setting. This calls for the safe conveyance of information and strong verification measures for operational safeguards. Potential risks include cyber issues threatening to compromise specific industrial processes and the kinds of information belonging to certain industries, and the study examines how certain security controls protect against these risks.
- Case Study [2] - Realization in the Healthcare: Area Based on the type and specific application, virtual reality technology is discussed regarding surgery rehearsals and patient treatment in the healthcare area. More specifically, the

points touched are the privacy factors proportional to the patient's identifiable information protection, safe telecommunication channel use, and compliance with health care policies or HIPAA. The difficulties described in the analysis are specifically relevant to healthcare, including maintaining the identity of information, using augmented and virtual reality in teaching and training, and therapy.

As a result of a comparative analysis of the two cases, it is possible to identify some common threats, which means that further threats, such as data leakage or unauthorized access, are described. This paper reviews current measures implemented in each sector regarding encryption techniques, access control measures, and compliance with best practices. The aspects extracted from these cases provide guidelines to improve the secure implementation and administration of AR and VR in various sectors, focusing on employing preventive security measures to ensure firms' compliance with legal requirements and minimize the impact of cyber threats.

IV. FINDINGS AND DISCUSSION

The findings highlight the dynamic nature of security risks in AR/VR solutions and the importance of their consideration by businesses across various industries. They furnish guideposts for the stakeholders to improve the security measures, minimize risks, and accrue the maximum profits from such engaging technologies without compromising the data authenticity and users' anonymity.

1. Analysis of Case Study Results

The cases presented in the paper identify the general and case-specific security risks and protective measures. In the industrial sector (Case Study 1), more critical issues are data authenticity during equipment monitoring and cyber-physical risks, which are solved using encodings and precise authentication. In healthcare (Case Study 2), privacy is paramount for users involved in VR applications, including simulating surgery and telemedicine, which is protected through patient information encryption. Effective security measures hinge on the following:

- Holistic Security Approach: These measures can be further incorporated into broad frameworks that include data encryption and complete authentication, along with specificity to the industry.
- User Awareness and Training: Training the users to minimize mistakes and maintain system security.
- Regulatory Compliance: Compliance with regulatory frameworks such as HIPAA and data protection regulations to mitigate legal exposure and enhance stakeholder confidence.
- Innovation vs. Security Balance: The challenge and the opportunity to balance innovative solutions with secure solutions that deal proactively with these vulnerabilities.

- Continuous Evaluation and Adaptation: This means continuously reviewing and fine-tuning the system and the measures against new threats.

V. CHALLENGES AND FUTURE DIRECTIONS

Organizational control of the future nature of AR and VR security concerns include the following: improving encryption for data assurance, merging biometric signatures, using behavioral analysis, adopting Blockchain for decentralization, and securing telecommunications. Eradicating these through partnership, policy adherence, and future studies is essential for better AR and VR usage and safety in relevant industries.

1. Innovations in AR/VR Security

Innovative strides in Augmented Reality (AR) and Virtual Reality (VR) security are crucial for addressing emerging challenges:

- Advanced Encryption: Preserving database confidentiality and integrity and protecting information in AR/VR environments using advanced encryptions.
- Biometric Authentication: Closing the gap by including advancements in biometrics for better and safer user recognition and access at the AR/VR systems [13].
- Behavioral Analytics: Integrating the analytics mechanism to identify the changes and reactions from the users of AR/VR applications.
- Blockchain Integration: Blockchain technology ensures enhanced security and transparency of the transactions in AR/VR business interactions.
- Secure Telecommunication: Creating a guideline to identify secure means of conducting telehealth and remote collaborations within an AR/VR context.

2. Research and Development Needs

Future progress in AR/VR security requires focused efforts on:

- Cybersecurity Education: Providing stakeholders with expertise in the field of cybersecurity to enhance the AR/VR environment.
- Interdisciplinary Collaboration: Cybersecurity contents, AR/VR development, and regulatory compliance: towards interdisciplinary cross-training.
- Regulatory Frameworks: Strengthen the regulations' adaptability to meet the data and ethical norms.
- Ethical Considerations: Specific risks and ethical issues of data privacy and proper data management in the case of AR/VR applications.
- Threat Monitoring: Improving the opportunities for time-critical threat identification and reaction in AR/VR solutions.
- Privacy Enhancements: Establish general guidelines for improving user privacy and overcoming the problems of gathering consent in AR/VR applications.

These efforts will further the security and dependability of augmented reality and virtual reality technologies and encourage the protection of augmented reality and virtual reality implementations throughout various industries with a decrease in improper effects and hazards.

VI. CONCLUSION

This study has explored the security landscape of Augmented Reality (AR) and Virtual Reality (VR), highlighting critical insights and contributions:

- Security Challenges: Explored potential risks inherent to surgical /training and gaming applications of AR & VR technologies in both industrial and healthcare fields.
- Effective Strategies: Explained the proper security frameworks, encryption, and regulations that need to be implemented to counter the threats.
- Case Study Insights: Highlighted specific real-world uses to demonstrate how security measures and approaches are applied in the field.

1. Recommendations

Based on the findings, the following recommendations are proposed to enhance the security of AR and VR deployments:

- Implement Comprehensive Security Frameworks: Design and implement adequate network security technologies, identity verification, and transmission security protocols that suit AR/VR contexts.
- Enhance User Awareness and Training: Inform the users and stakeholders of the proper practices and strategies for cybersecurity, as well as emphasize the significance of data security in implementing AR/VR.
- Adhere to Regulatory Standards: Implement policies regarding using personal information, depending on the field, such as healthcare or telecommunications, to protect user data and follow laws like HIPAA or GDPR.
- Invest in Research and Development: Promote new developments in encryption technologies, biometric identification, and threat identification in the Security of AR/VR.

These are some of the measures, and their implementation will help avoid risks, build users' trust, and promote the safe and productive use of AR and VR in various spheres.

REFERENCE

1. Pavlov, Igor Sosnovsky, V. Dimitrov, Vasilii Melentyev, and D. Korzun, "Case Study of Using Virtual and Augmented Reality in Industrial System Monitoring," DOAJ (DOAJ: Directory of Open Access Journals), Apr. 2020, doi: https://doi.org/10.23919/fruct48808.2020.9087410.
2. Asadzadeh, T. Samad-Soltani, and P. Rezaei-Hachesu, "Applications of virtual and augmented reality in infectious disease epidemics with a focus on the COVID-19 outbreak," Informatics in Medicine Unlocked, vol. 24, p. 100579, 2021, doi: https://doi.org/10.1016/j.imu.2021.100579.
3. R. M. Viglialoro, S. Condino, G. Turini, M. Carbone, V. Ferrari, and M. Gesi, "Augmented Reality, Mixed Reality, and Hybrid Approach in Healthcare Simulation: A Systematic Review," Applied Sciences, vol. 11, no. 5, p. 2338, Mar. 2021, doi: https://doi.org/10.3390/app11052338.
4. Syamimi, Y. Gong, and R. Liew, "VR industrial applications—A Singapore perspective," Virtual Reality & Intelligent Hardware, vol. 2, no. 5, pp. 409–420, Oct. 2020, doi: https://doi.org/10.1016/j.vrih.2020.06.001.
5. F. Bellalouna, "Digitization of industrial engineering processes using the augmented reality technology: industrial case studies," Procedia CIRP, vol. 100, pp. 554–559, 2021, doi: https://doi.org/10.1016/j.procir.2021.05.120.
6. S. Kumari and N. Polke, "Implementation Issues of Augmented Reality and Virtual Reality: A Survey," Springer Link, 2019. https://link.springer.com/chapter/10.1007%2F978-3-030-03146-6_97
7. X. Li, W. Yi, H.-L. Chi, X. Wang, and A. P. C. Chan, "A critical review of virtual and augmented reality (VR/AR) applications in construction safety," Automation in Construction, vol. 86, no. 0926-5805, pp. 150–162, Feb. 2018, doi: https://doi.org/10.1016/j.autcon.2017.11.00.
8. Sharma, D. Palrecha, and M. Parekh, "Security Awareness Game (Augmented Reality)," SSRN Electronic Journal, 2019, doi: https://doi.org/10.2139/ssrn.3353135.
9. Flavián, C. Orús, and S. Ibáñez-Sánchez, "The impact of virtual, augmented and mixed reality technologies on the customer experience," Journal of Business Research, vol. 100, no. 100, pp. 547–560, Nov. 2019, doi: https://doi.org/10.1016/j.jbusres.2018.10.050.
10. www.itcinfotech.com, 2020 https://www.itcinfotech.com/blogs/disrupting-digital-commerce-through-extended-reality/
11. F. Interactive, "VR and AR Technology: The Future Outlook," Forest Interactive, 2021, https://www.forest-interactive.com/insights/vr-and-ar-technology/
12. "AR VR in Healthcare Market Ecosystem Trend, Revenue and Growth Rate Analysis along with Decision Intelligence, 2020, AllTheResearch," www.alltheresearch.com. https://www.alltheresearch.com/report/335/ar-vr-in-healthcare-ecosystem.
13. N. M. Alzahrani and F. A. Alfouzan, "Augmented Reality (AR) and Cyber-Security for Smart Cities—A Systematic Literature Review," Sensors, vol. 22, no. 7, p. 2792, Apr. 2022, doi: https://doi.org/10.3390/s22072792.

14. Abrar Alismail, Esra Altulaihan, H. Rahman, and Abu Sufian, "A Systematic Literature Review on Cybersecurity Threats of Virtual Reality (VR) and Augmented Reality (AR)," pp. 761–774, Dec. 2022, doi: https://doi.org/10.1007/978-981-19-6004-8_57.
15. F. Roesner, T. Kohno, and P. Allen, "Security and Privacy for Augmented Reality: Our 10-Year Retrospective." Available: https://par.nsf.gov/servlets/purl/10312790
16. N. M. Alzahrani and F. A. Alfouzan, "Augmented Reality (AR) and Cyber-Security for Smart Cities—A Systematic Literature Review," Sensors, vol. 22, no. 7, p. 2792, Apr. 2022, doi: https://doi.org/10.3390/s22072792.

ACRONYMS

1. AR - Augmented Reality
2. VR - Virtual Reality
3. IT - Information Technology
4. GDPR - General Data Protection Regulation
5. HIPAA - Health Insurance Portability and Accountability Act
6. DoS - Denial of Service