UNIVERSITÀ DEGLI STUDI DI SALERNO

Computer Science Department

Master's Degree in Computer Science

Security Issues in Virtual Reality: A Systematic Literature Review

SUPERVISOR:
Prof. Fabio Palomba
Dott. Dario Di Dario
Università degli Studi di Salerno

CANDIDATE:
Muhammad Umair Manzoor
Matricola: 0522500904

Academic Year 2022/2023

This thesis was carried out in the

ABSTRACT

Virtual reality is an experience that makes you feel like you are in a real place. Users wear a headset that has sensors that track their moves and let them interact with the virtual world. In recent years, Virtual Reality (VR) has been the focus of a great deal of media attention due to its potential to disrupt multiple industries and create engaging new forms of experience, making a multimillionaire market year by year. Integrating into our everyday lives, VR is becoming a useful tool for transforming industries as diverse as gaming, education, healthcare, architecture and offering innovative experiences. In the early part of 2015, Mostly people were not familiar with Virtual Reality, and it was also quite expensive for the average user. But after the covid outbreak, the availability of VR gadgets have increased rapidly. The covid-19 pandemic has made virtual reality technology much more popular. Since a lot of people work from home and try to avoid public places. The increasing number of cutting-edge technologies have created plenty of new threats to the security, privacy, and morality of individuals. With the passage of time, a significant number of individuals are victimized by fraud due to insufficient education or inadequate training, resulting in the loss of their personal information, such as bank credentials, company usernames, various other sensitive data and financial loss. Virtual reality offers substantial assistance to individuals in avoiding such activities by utilizing biometric sign-in methods. The aim is to examine security challenges in VR systems and propose solutions. We conducted a literature review of 47 studies focusing on security and privacy issues in virtual reality. Our findings suggest that the metaverse and technologies like Blockchain can protect user data. We explore various techniques to secure user data, propose solutions, and highlight the need for research to ensure proper virtual reality protection.

Keywords: Security, User Data Privacy, Virtual Reality, Augmented Reality, Future Life, Metaverse

Contents

List of Figures

CHAPTER 1

Introduction

1.1 Context and Motivation

Virtual Reality (VR) is a computer-generated simulation of a three-dimensional environment that can be experienced through a specialized headset or other devices that simulate visual, auditory, and sometimes haptic sensations. It empowers you to sense, feel, and experience not only the present but also the past and the future [1, 2]. It is the mechanism by which we can construct our own unique reality. During the last decade, the word virtual became one of the most exposed words in the English language, especially after the covid-19 [3]. Now today we have virtual universities, virtual offices, pets, exhibitions, actors, studios, museums, and virtual doctors, and all because of virtual reality. Now we have gone on to the next session with virtual reality. Virtual reality is essential for achieving the realization of the Metaverse concept because it is one of the primary means of accessing this virtual world and interacting with its inhabitants. The advancement of VR technology has provided users with a more immersive and authentic way to experience the Metaverse. The word "Metaverse" is a mashup of verse, from the universe, and meta, which means transcendence. Science fiction has frequently used the idea of a shared virtual environment, sometimes known as a metaverse. Science fiction authors like

Neal Stephenson (Snow Crash) [4] and William Gibson (Neuromancer) [5] have made some early allusions to the concept of a metaverse. In the novel, avatars and VR glasses are also mentioned, as in the present day. The metaverse promises more experiences than just the time we spend on regular social networking platforms. There are promising initiatives known as pre-metaverse platforms. Sandbox provides blockchain-based gaming, virtual plots, and purchasing, for instance. Additionally, an Non-fungible token (NFT) world belongs to its own world. It allows the user to construct his or her own digital world. Metahero project comes to the forefront with its 3D scanning function that allows users to construct their avatar in 16K resolution and convert it to NFT [6]. It should be emphasised that in many games and virtual environments, anybody may have and own virtual objects, as well as exchange them, without necessarily employing blockchain technology, but rather through a licencing agreement [7]. The development of immersive technologies like virtual reality (VR), augmented reality (AR), and mixed reality (MR) has been credited with increasing interest in the metaverse [8]. As it is supported by the progress of information and communication technology, the concept of the metaverse is seen as the next engine for economic and social development. Metaverse assures a wealth of excellent commercial, economic, and lifestyle improvement options. And therefore, worries about metaverse security and privacy play a significant role in its dynamics. It seems sensible to think about the possibilities even though many firms are thinking about the metaverse's potential.

This review specifically addresses the potential emergent security and privacy vulnerabilities in Virtual Reality and emphasizes the importance of considering various security challenges during the implementation and management of a metaverse system. Additionally, our investigation into the security issues in VR may offer valuable insights into the potential security concerns associated with the broader concept of the Metaverse. VR and AR are both vital components of the Metaverse, Yet, These technologies are susceptible to a variety of security flaws, any of which may have important repercussions. First, consider data privacy and security. In a metaverse environment, users often create enormous amounts of personal data, such as their profiles, activities, and contacts with others, which might be subject to theft or unauthorised access. Second, Malware: Malware may infiltrate VR software, com-

promising the security of VR devices. Malware is the abbreviation for "Malicious Software" which refers to any sort of program designed to harm, damage, or exploit computer systems, networks, or devices without the user's knowledge or permission. Malware includes viruses, worms, trojans, spyware, adware, and ransomware, among others. Malware can be used to acquire sensitive data, such as user credentials, financial data, or personally identifiable information, or to gain unauthorized access to a computer or network. It can also be used to hijack the computing power of a computer for cryptocurrency mining or to conduct attacks against other computers. Typically, malware is distributed via email attachments, malicious websites, infected software downloads, or by exploiting operating system or application vulnerabilities. To protect against malware, it is essential to maintain up-to-date software and security patches, use strong passwords, exercise caution when opening email attachments or downloading software from the internet, and employ antivirus and anti-malware software from a respected vendor.

Network security: Since VR systems rely on network access, they are vulnerable to network-based assaults such as DDoS (Distributed Denial of Service) [9]. Eventually, due to cultural differences and other factors, there will be instances in the universe that make certain individuals feel inappropriate, not to mention destructive avatar acts such as harassment. To overcome these security issues, it is critical to adopt robust security measures like encryption, firewalls, and security software, as well as update VR software and equipment regularly. Therefore, VR users should exercise caution while sharing information in Virtual settings and take precautions to secure their personal information.

1.2 Structure of the thesis

In addition to discussing the extant systematic literature reviews on VR privacy and how our work differs from them, Chapter 2 provides Background on virtual reality. In Chapter 3, we describe the state of the art and related research terminology. In Chapter 4, we describe the search strategy and literature synthesis methodology. Chapter 5 Analyzes the findings and results, while Chapter 6 further discusses the implications of our findings, Chapter 7 discusses the validity threats and our strategies to address them, whereas Chapter 8 concludes the report by describing our future research objectives.

CHAPTER 2

Background

Virtual Reality has been around for decades, only in recent years has the technology improved sufficiently to make it more inexpensive and accessible to the general population [10]. Virtual reality is widely acknowledged to have originated during the 1950's [1] however, it garnered significant public recognition during the late 1980's and 1990's. Jaron Lanier contributed, an age-old pioneer in the field, popularized the term of Virtual Reality in the late 1980s [11]. In 1985, Lanier founded the company Virtual Programing Language (VPL) Research. In 1990, VPL research company faced the issue of bankruptcy, after 9 years it was purchased by the name company Sun Microsystem. Since then, the significance of virtual environment systems has grown substantially. VR may be the next entertainment medium. VR has the ability to revolutionize the entertainment industry and it might replace our televisions and theatres on over of our smart devices like mobile phones. Or virtually anything that utilizes a screen. Gamers may immerse themselves in a world and behave in ways never before possible. A number of methods exist in which virtual reality could improve our lives. Improvements in virtual reality technology hold great promise for a wide range of fields, from education and healthcare to social interactions and even entertainment.

2.1 Aspects and Working of VR

The hardware and software that makeup VR technologies collaborate to produce fully convincing simulations. VR relies on a number of different technologies[12], including:

- Head-mounted displays (HMDs):
  HMDs are the most popular piece of virtual reality equipment and are worn on the head to create a fully immersive sensory experience. For instance, the Oculus Rift and HTC Vive are two well-known HMDs that enable users to experience interactive and immersive gameplay.

- Motion tracking:
  In order to recognise and react to a user's motions in real-time, virtual reality systems employ motion-tracking technology. Users may interact with virtual items and settings naturally thanks to this technology. Users may walk about and interact with their virtual surroundings, for instance, using motion tracking in the PlayStation VR system.

- Haptic feedback:
  Haptic feedback simulates touch by delivering tangible sensations like pressure or vibrations. For instance, the Tesla Suit is a haptic suit that gives users full-body sensation, allowing them to experience virtual objects and settings. 3D audio technology generates spatial audio that reflects the user's activities and motions in the virtual world. The effect is enhanced immersion and a more genuine sense of realism. The Oculus Quest 2 is only one example of a virtual reality headset that employs spatial audio to enhance the user's experience.

- Artificial intelligence (AI):
  AI is being utilised in VR to develop more sophisticated and responsive virtual worlds. With the help of this technology, fictitious people and things may learn from their environment and react accordingly. For instance, chatbots powered by AI are being utilised in virtual reality to make discussions more dynamic and interesting.

Like any computer system or programme/application, VR may be attacked. Hackers might utilise VR system flaws to steal data, hijack accounts, or ruin the experience. Malware may steal data or impair security. In order to improve security, VR employs biometric authentication. Biometric authentication employs a person's unique biological traits, such as fingerprints, face recognition, or iris scans, to validate their identification. This system can ensure that only authorised persons have access to critical VR settings. Biometric authentication is one of the various security procedures that may be employed to defend against illegal access and assure the safety and security of VR users and settings.

2.2 Methodology in Metaverse using VR:

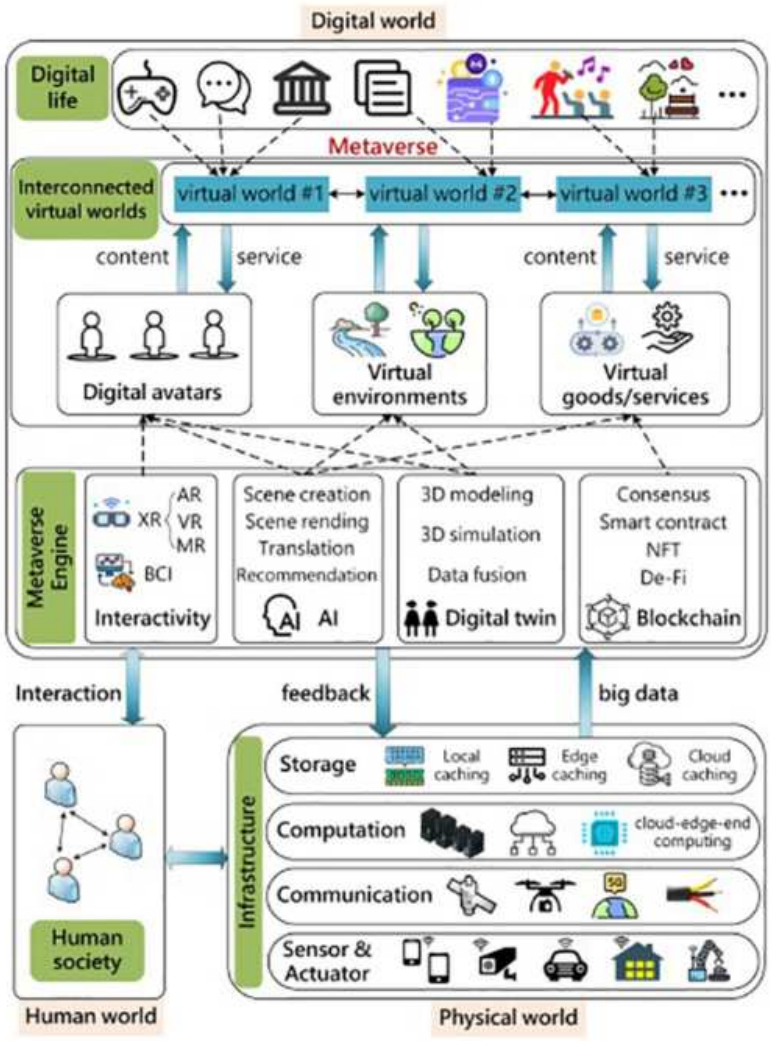

Figure 2.1: The metaverse architecture that integrates the digital, human, and physical worlds. Source: Jaber [7]

The physical, human, and computer worlds are combined to create the metaverse. The main architecture of the metaverse is shown in the above Figure with its underlying ternicity in mind[13]. Implicitly, the line between the metaverse and VR, AR, and MR looks thin. Thus, the metaverse might be summed up as a hyper virtual-reality ecosystem built on the Internet and comprised of multidisciplinary technology. In contrast, although being an essential component of the metaverse, VR/AR/MR is essentially a type of virtualized and digitised technology that does not require a whole ecosystem, laws, or the Internet[14]. The metaverse does not compete with the internet; rather, it expands on it. People "explore" the internet, but they may "live" in the metaverse to some extent. The expansion of the internet has created a wide range of products that are paving the way for the formation of the metaverse. There are two key reasons why the metaverse can be recreated lately, despite the fact that this notion has been proposed for many years. The COVID-19 outbreak has made individuals more comfortable with the virtual digital environment and has encouraged some socialising to transfer [3]from offline to online. The above-mentioned technologies recent tremendous advancement, akin to the Big Bang, makes it theoretically conceivable to construct a metaverse[3]. Think about the virtual world where people save time and money, connect to interworld for the trading, get an education, attend the meeting, and are connected the medical problem all over the world.

CHAPTER 3

State of the art

This chapter seeks to evaluate the present level of development, advancement, and innovation in a certain field or industry of VR/MR/AR security in order to determine the existence of various research approaches.VR/AR/MR consists of user identification and identity management systems, encryption and secure data transfer protocols, secure data storage and processing, and intrusion detection and prevention systems.
In addition, advancements in machine learning and artificial intelligence are being utilised to improve security measures and detect abnormal user activity in real-time.

3.1 What is the state of art in virtual reality security and what advances are expected in the near future?

The state of the art in virtual reality security at the moment comprises several methods and tools designed to improve the privacy, integrity, and confidentiality of sensitive data. One such method encrypts data and communications between virtual reality devices and servers using cryptography, guaranteeing that information is safe even if it is intercepted by unauthorized parties. The creation of access control

systems, which restrict access to sensitive information and virtual environments to only authorized individuals, is another significant advancement in virtual reality security. To make sure that only authorized users have access to sensitive information, these systems employ a variety of techniques including role-based access control, attribute-based access control, and multi-factor authentication.

***Role-based access control** (RBAC) is a security model that limits system access to authorised users according to their organisational responsibilities[15]. Users are assigned roles in RBAC based on their job responsibilities or organisational activities. Each position is provided a set of permissions that dictate what activities or resources the user can access within the system. In VR, RBAC can be used to control access to virtual spaces, objects, and information within a virtual environment. In a VR training simulation, for example, different levels of access can be allowed to various roles, such as trainers, trainees, and administrators. Trainers may have access to supplementary training resources, whilst trainees may only have access to the fundamental training modules. Administrators may have access to performance indicators and other data useful for training programme management. By implementing RBAC in virtual reality, organisations may ensure that users only have access to the resources and data pertinent to their jobs, hence lowering the risk of illegal access or data breaches. Moreover, RBAC can ease access management for VR administrators, since they can grant roles and permissions to users in a centralised manner, rather than controlling access on a per-user basis. RBAC can play a significant role in strengthening the security and efficacy of VR systems in a variety of applications, including training simulations and collaborative design environments.

***Attribute-based access control** (ABAC) is a methodology of access control that establishes resource access permissions based on attributes connected with the user, the resource, and the current environment. ABAC bases access decisions on policies that take into account a variety of variables, including a user's role, job function, clearance level, time of day, location, and access device. These parameters can be used to develop complicated access control policies that permit more granular resource access control[16]. ABAC is a sort of access control system in Virtual Reality (VR) that limits user access to VR resources based on attributes connected with the user, the resource, and the existing VR environment. For instance, Imagine a virtual

reality simulation of a hospital in which physicians, nurses, and administrators have varying degrees of access to patient records and medical equipment. In this Virtual environment, an ABAC system may use job title, department, and clearance level to decide which users have access to specific resources. A doctor may have access to patient information and be able to undertake specific medical treatments, whereas a nurse may only have access to certain areas of the patient's record and be able to perform less invasive procedures. An administrator may have access to administrative and financial records, but not patient records. In this scenario, the ABAC system would limit access to VR simulation resources based on user traits. This will improve security and privacy by ensuring that only authorised users may access sensitive information and conduct specific actions in the Virtual environment. Users would only be allowed to access information and conduct actions pertinent to their job function and level of competence, allowing for more efficient and successful training programmes.

***Multi-factor authentication** (MFA) is a security mechanism that requires users to supply two or more distinct authentication factors in order to access a system or application. Typically, these factors are something the user knows, something the user has, or something the user is.Users must submit several forms of authentication to gain access to a virtual environment or resource, for each VR security system. An example of an MFA in VR could be a virtual training session for high-security facility workers. Users would initially access the software by entering a username and password, which would function as the first level of authentication (something they know). As the second element of identification, individuals could be requested to produce a biometric identifier, such as a fingerprint scan or facial recognition (something they are). As a third point of authentication, the virtual training program may also require users to carry a real token, such as a smart card or RFID tag (something they have). A reader within the VR headset would detect the token, proving that the user is physically there and permitted to attend the training program.MFA in VR can provide an additional layer of security by demanding multiple means of authentication to prevent unwanted access and secure critical data and resources. It can be especially crucial in high-security organizations, where security breaches might have serious effects.

Future developments in virtual reality security are predicted to involve the creation of more complex biometric authentication systems, such as speech recognition and facial recognition technologies,Looking for a new authentication method for blockchain and passing all the necessary tests to ensure its privacy and security, which can offer a more convenient and secure method of user verification. Additionally, artificial intelligence and machine learning developments are anticipated to assist in real-time threat detection and prevention, offering a proactive approach to virtual reality security. AI systems, for instance, might examine user activity and spot abnormalities or potential security breaches, resulting in a warning or action to stop any harm.

As the use of virtual reality (VR) expands into new industries such as healthcare and finance, there will be an increasing demand for security solutions that are tailored to meet the specific challenges of these industries.Improving the scalability and efficiency of VR security protocols, developing new approaches to protect against advanced persistent threats (APTs)[17, 18], and utilizing emerging technologies such as blockchain to enhance security in virtual environments are among the key areas of focus for future advancements.

In general, virtual reality security is a sector that is always changing and will continue to make great strides as technology spreads and becomes more important for both businesses and consumers.

Based of the state of the art analysis, we can claim that our work presents the improve the privacy of sensitive data and provide the upcoming solution with the help of new emerging technology into the role of Security Issues in Virtual Reality.

3.2 Related Work

With the possibility of user data theft, fraud, and cyberattacks, security in VR metaverse environments is a crucial concern. Relevant works on this issue include academic studies, industry papers, and policy documents that investigate the many security concerns and potential solutions related with these contexts.
VR metaverse situations involve a number of security concerns, such as the necessity for comprehensive data protection and privacy safeguards to preserve user data, the possibility for fraud and cyberattacks, and the difficulties associated with managing

and securing user-generated content.

Alberto Giaretta's [19] is a comprehensive literature review on security and privacy methods in a VR environment. The popularity of VR has continuously increased over time, according to the poll, the number of US$ consumers. In 2020, 52.1 million people will use VR technology. From the US 7719.6 million in 2020, the worldwide VR market will reach US$ 26860 million by 2027.In this review, the author discusses about VR privacy issues, arranged by topology and cause. Cyber Security, and Physical Security Authentication Aspects in VR.An examination of vulnerabilities to VR security, including DoS and VR-specific attacks like dizziness (Motion sickness or Simulator sickness).

Patel and Trivedi [20], The authors provide a thorough examination of previous studies on data privacy, user authentication, data leaks, and permission difficulties. Depending on the device being used, AR authentication could be improved by using biometrics on mobile devices and face recognition on PCs.

Kurtunuoglu, Beste Akdik, and Enis Karaarslan [6] The authors identify different authentication systems for the Security of virtual reality authentication methods, including classic username/password combinations, biometric-based authentication, and multi-factor authentication, and assess their merits and shortcomings from the perspective of security. Places an emphasis on the significance of selecting suitable authentication methods according to the level of security necessary as well as the user experience.

Noah, Shearer, and Das [21] Conducted a security and privacy assessment of the VR/AR devices and their associated platforms, concentrating on-device authentication, user profiling, access control, database security, and webpage security.

-**Device Authentication:** Device authentication is an essential security component in VR as it ensures that only authorised users may access the VR environment. Conventional authentication methods like passwords aren't always sustainable in VR, thus biometric or token-based authentication may be needed. Biometric authentication involves using unique physical traits such as facial recognition or fingerprints to validate a user's identity, while token-based authentication employs a unique code or token to authenticate users.

-**User Profiling:** Profiling involves tracking user data to find target-related

information. User profiling in VR entails collecting and evaluating user data to generate a customised experience for the user. Yet, there are privacy issues because the data obtained could be used for discrimination or targeted advertising. To address these concerns, VR developers should be explicit about the types of data being gathered, give users with clear consent processes, and follow to ethical norms and data protection legislation.

-**Access Control:** Access control in VR entails restricting user access to specific VR settings, content, or features. This is often achieved by access control technologies such as role-based access control (RBAC) or attribute-based access control (ABAC). Although ABAC grants access based on user attributes like location, time of day, or device type, RBAC grants access to users based on their position or job function.

-**Database Security:** Database security in VR is crucial to avoid unwanted access or data breaches. This involves installing security mechanisms such as encryption, access control, and monitoring to secure sensitive data. Developers should also follow data protection rules and ethical norms to avoid misusing or sharing user data without their consent.

-**Website Security in VR:** Preventing malicious actors from exploiting vulnerabilities in the VR atmosphere is crucial. This includes serving VR content via HTTPS, CSRF protection, and input validation to prevent cross-site scripting (XSS) threats, and content security restrictions to stop unauthorised scripts from running.

- **Cross-Site Request Forgery** (CSRF) Protection is a security feature that prevents unauthorized actions from being carried out on a website or application on behalf of a user. It requires a token or verification to be sent with every user request to ensure that it is genuine and not manipulated by attackers. This feature helps to prevent attacks like session hijacking and data theft by verifying that the request is legitimate before it is processed.

-**Cross-Site Scripting** (XSS) is a security issue that occurs when an attacker inserts malicious code onto a web page that other users access. The attacker can inject malicious scripts using a variety of techniques, such as submitting a form containing the script or exploiting web application weaknesses. When a user accesses the website containing the malicious script, it executes on their browser and can capture sensitive information such as login credentials, session tokens, or other confidential data. The

attacker can also use the script to publish messages or make purchases on the user's behalf. To prevent XSS risks, it is necessary to validate user input, sanitise output, and establish strong security controls on web applications.
Relevant work on security in VR metaverse settings offers useful insights into the security concerns and potential solutions connected with these environments and may aid in the creation of effective security measures for these environments.

Both are treated differently due to the fact that they entail different types of attacks and have distinct outcomes.

CHAPTER 4

Research Method

4.1 Plan

Examining a variety of academic and industry sources in order to identify the key security issues that occur in virtual reality, as well as the planning and reduction strategies that have been proposed or implemented to address these issues, would be considered security issues in the VR in the direction of metaverse environment. Some of the potential security issues that could be identified in such a review include data privacy and security issues, such as the risks associated with collecting and storing user data in virtual reality for a metaverse environment, as well as identity and authentication issues, such as the risk of identity theft or fraudulent activity in a virtual environment. Other security issues that may be identified include content security issues, such as the risk of intellectual property theft or unauthorized distribution of copyrighted material, and physical security issues, such as the potential for cyberattacks or other types of malicious activity to compromise the safety and security of users in a VR environment. A systematic literature review (SLR) [22] may look at a variety of measures, such as using encryption and other security technology to secure user data and prevent illegal access, or using identity verification and authentication procedures to assure user validity and avoid fraud. Overall,

planning for security issues in VR/AR/MR approaching metaverse environments would be a valuable way to identify the key challenges and opportunities in this rapidly evolving field, as well as to investigate potential strategies and solutions for ensuring the safety and security of users in these environments.

4.2 Research Questions (RQs):

This article focuses on the fundamental systematic examination to evaluate the security and privacy risks associated with the nature of human engagement in virtual reality.

RQ_1. How can virtual reality systems be designed to enhance the security of sensitive information and data?

This research tries to identify and develop methods for overcoming the potential weaknesses of conventional security systems and methods. By recreating real-world scenarios in immersive, interactive environments, virtual reality technology has the potential to make accessing and sharing sensitive information safer. VR, for example, can be used to reproduce training scenarios for security experts or to establish virtual settings for conducting secure meetings and transmitting sensitive information. This research is to investigate the potential applications of VR technology for enhancing security measures and establishing a highly resilient and effective protection system. This may require examining the use of biometric authentication, encryption, and other security techniques inside VR systems, as well as identifying potential limitations and difficulties associated with this technology. The goal is to secure and design VR systems that provide a safer environment for accessing and sharing sensitive data and information.

Researchers, developers, and practitioners who are interested in building and implementing safe virtual reality systems can benefit from the knowledge provided in this question. Possible vulnerabilities and constraints of present security measures in VR systems can be identified, which can assist in the creation of more strong security solutions. Moreover, understanding the anticipated future advancements might inform the creation of new security tactics and technologies for VR systems. In particular,

advances in Artificial intelligence (AI) and Machine learning (ML) may enable more sophisticated security measures, whereas advances in hardware technology may increase the speed and dependability of encryption and other security methods.

$RQ_{2.}$ What are the best practices for securing virtual reality systems and environments from malicious actors?

As the technology powering VR gets more generally adopted, it is essential to make certain that the surroundings in which the technology is utilized, as well as the systems that comprise it, are sufficiently secured and safeguarded from potential security risks and vulnerabilities. It is essential to look into the most appropriate interventions for securing VR environments and systems in order to accomplish this goal. The implementation of secure authentication and access control protocols, the utilization of encryption to protect data and communication channels, and the monitoring of system activity for suspicious behaviour are some examples of the types of technical and procedural measures that are typically included in this category of best practices.

$RQ_{3.}$ How can virtual reality be used to improve physical security systems and processes in various industries?

Several industries, including healthcare, transportation, manufacturing, and retail, rely on physical security systems and processes, which can be complicated, costly, and difficult to implement efficiently. Thus, it is becoming increasingly important to examine how virtual reality might be used to enhance physical security systems and procedures. This aims to identify methods for enhancing safety while simultaneously reducing expenses and complexity. VR technology can be used to simulate insistence scenarios and instruct personnel on how to respond to a variety of threats. VR can be utilized to simulate physical security systems in order to evaluate their effectiveness and discover any faults. The objective is to identify innovative solutions and strategies that can be implemented to strengthen industry security protocols and reduce costs to a level that is highly accessible to all categories of users, in order to reduce the failure rate in health and defense systems.

RQ4. What role does virtual reality play in the development and deployment of advanced security technologies such as biometrics, AI, and blockchain??

The objective of our research on virtual reality to detect and prevent attacks and security issues is to develop new methods for enhancing security, such as using VR simulations to train personnel on how to respond to threats. Studying the role of security and privacy for virtual reality to deploying in modern security technologies such as biometrics, artificial intelligence, and blockchain aims to identify new opportunities for enhancing security measures. The primary purpose is to develop new approaches and technologies to strengthen security measures and protect against potential threats in a more interconnected world.

4.3 Search Term

The purpose of the study is to provide software engineering researchers with actionable items and insights that they can use to further investigate the topic and enhance the resources available to developers and managers to address privacy concerns. This is accomplished by conducting a systematic literature review pertaining to detecting privacy/security challenges and preserving privacy in Virtual reality systems. The viewpoint is that of researchers who are interested in examining existing approaches and ways to improve them.

4.4 Search Query

Definition of the Query String, Using the Boolean “OR" operator between related phrases and the “AND" operator between related keywords, a query string was constructed after a session of term generation. Hence, the resulting query string is:

(“Virtual Reality" OR “Augmented Reality" OR “Mixed Reality" OR “VR" OR “AR" OR “MR") AND (“Security" OR “Authentication" OR “Risks" OR “Privacy" OR “Identification")

The searches were made using the title, keywords, or abstract, depending on the

search engine and a total of 792 research outputs were obtained including papers published on various platforms. The results of these searches were filtered using the inclusion/exclusion criteria specified, and only those papers whose inclusion matched the searched-out paper will be considered.

4.5 Search Database

The original research criteria were to discover publications by using basic keywords like “Virtual reality”, “Augmented reality”, “Security”, “Authentication” and “Privacy”. To extract the relevant publications for our research, we attempted to search for papers using Query. This allowed us to display a variety of papers, some of which were pertinent and others of which were not the same keywords were used on many sources:

- Scopus
- IEEE Xplore
- ACM Digital Library
- Web of Science (WoS)

4.6 Inclusion/Exclusion Criteria

Exclusion and inclusion criteria enable the selection of materials that address the research questions of a systematic literature review [22]. We identified and implemented the following “Inclusion/Exclusion" criteria as part of our investigation.

The exclusion criteria for this SLR are:

- Papers not published in English language.
- Papers published before 2015.
- Momentary papers, namely those with fewer than six pages.

- Papers that do not discuss security issues in VR environments.
- Papers that do not propose potential solutions or best practices for addressing security challenges in VR environments.

The inclusion criteria for this SLR are:

- Papers published in English language.
- Papers published between 2015 and 2023.
- Keywords Searched.
- Papers that discuss security issues in VR/AR environments.
- Papers that propose potential solutions or best practices for addressing security challenges in VR/AR environments.

Selecting the 2015-2023 time range for our SLR ensures recent advancements, relevance to current issues, availability of solutions, alignment with research objectives, and manageable scope.

Using these filters, we may reject any preliminary research results, such as a workshop or short papers, and we will avoid reviewing the same document multiple times, such as with an archive journal paper that extends a conference publication or duplicates.

4.7 Quality Assessment

The parameters developed by Kitchenham and Charters[22] were utilised in the assessment of the primary research to determine its level of quality. Whenever we started the process of data extraction that was necessary to answer our research questions, we reviewed the quality and completeness of the resources that had been retrieved and eliminated those that did not provide adequate information for our investigation based on our findings. This was done before we started the process of data extraction that was necessary to answer our research questions.

Stage 1:

We can examine the relevant keyword in the “Title" of each and every result.

Stage 2:

Identify the relevant keyword in the “Abstract" of all the output results.

Stage 3:

Find the related keyword on the Keyword Column of all the output results.

Stage 4:

By finding a good title, The objectives of the investigation and its results need to be adequately contextualized. This will enable an accurate interpretation of the findings. Context of Security and Privacy to assist in answering Research Questions, the paper must describe security and privacy considerations.

Stage 5:

Q1: Do the authors clearly define the VR security issue?

Q2: Are the solution used to assess security issues in VR clearly defined, valid, and reliable?

Each stage could be responded to “Yes" or “No". After completing all of the inclusion/exclusion criteria checks in Stages 1-3, examine the paper’s quality in Stage 4[23]. Quality assessment criteria (QAC) were used to evaluate the papers that made the cut. To determine if single primary research is enough to meet our review’s aims, employed a quality assessment checklist (QAC). Each primary study’s quality was assessed by questions that were agreed upon by all authors. Each author asked a different set of questions to establish whether or not certain primary research were consistent with one another.

4.8 Data Extraction

Following the collection of the necessary data, this investigation will employ a number of inclusion and exclusion criteria to filter articles in an effort to reduce unnecessary attention to a broad range of topics. There were a total of 792 results obtained from the query that we ran. After obtaining the result of the initial filter, we examine the Title, Abstract, and Keyword for the purpose of locating high-quality primary studies on Privacy/Security applications in VR/MR/AR. A reference manager was used to document and store all of the papers and studies that were collected. Because of this, filtering elements based on results was made simpler. Excel was utilized to obtain a more comprehensive picture of the studies that were ultimately chosen, and the selection process itself was meticulously documented. Because of this, it was feasible to acquire quantitative data to use in answering the research questions.

Database	Year	Document Type	Public Stage	Language	Access	Results
Scopus	2015-2023	Conf,Paper	Final	EN	Yes	51
IEEE Xplore	2015-2023	Conf Journal	Final	EN	Yes	208
ACM Library	2015-2023	Research	Final	EN	Yes	245
WoS	2015-2023	Article	Final	EN	Yes	288
					Total	792

Table: The research queries included several filters to narrow the results.

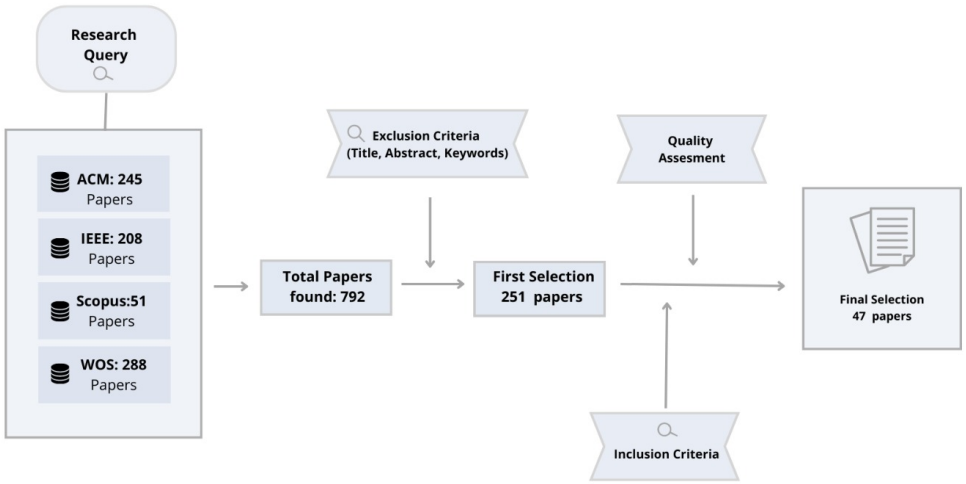

Figure 4.1: Paper selection overview.

4.9 Search Process Execution

After defining the fundamental components of our systematic literature review, we moved on to its execution. Figure provides a summary of the execution, illustrating the variation in the number of main studies examined while applying the various filters we established. The execution procedure was specifically as follows:

Query:

(Virtual Reality OR Augmented Reality OR Mixed reality OR VR OR AR OR MR) AND (security OR authentication OR Risks OR privacy OR identification)

Figure 4.2: Query

4.9.1 Keyword Search

The exclusion criteria were taken into reference. After applying exclusion criteria, each document entered the subsequent phase by selecting a different filter for each database's accessible possibilities. The author evaluated each paper's title, abstract, and keywords before deciding whether or not to discard it. If this was insufficient, the inspector read the paper's contents. In total, 541 papers were rejected, leading to the acceptance of 251.

As part of the selection process, the inclusion criteria were taken into account. In this instance, the first title of the paper acted as the inspector and began applying the established criteria to the 251 manuscripts. In contrast to the previous step, the inclusion was evaluated by looking on paper for security problems in VR/AR/MR settings. This method resulted in the elimination of more sources, bringing to a total of 47, the number of papers that were included in our systematic evaluation.

In the end, we gathered the data stored in each category in order to fulfil the objective of answering the research study's questions.

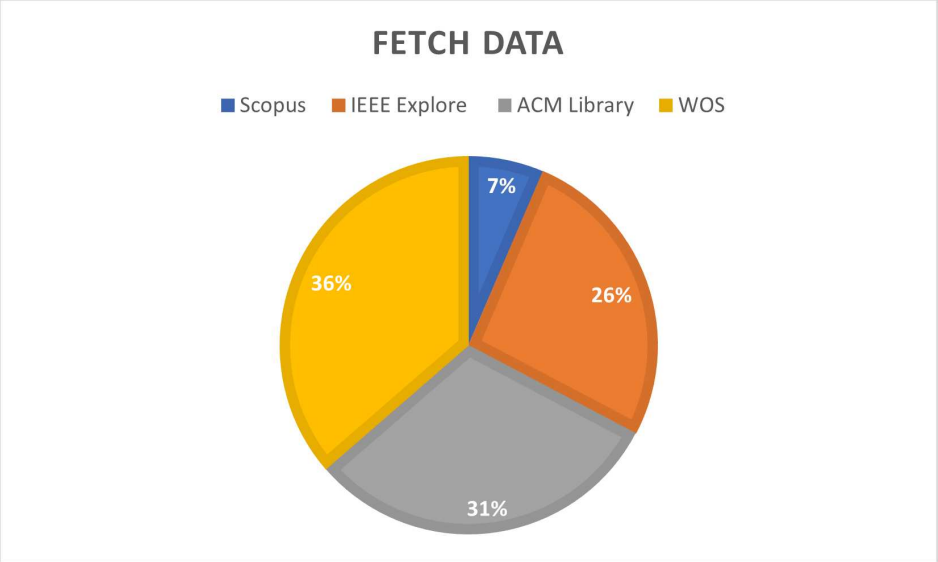

Figure 4.3: Selection Graph

The findings of the primary studies were provided to us after we had applied all of the criteria to the various databases. The ACM Library holds 31% of the material, while Scopus holds 6%, IEEE Xplore holds 26%, Web of Sciences (WoS) holds 37%,

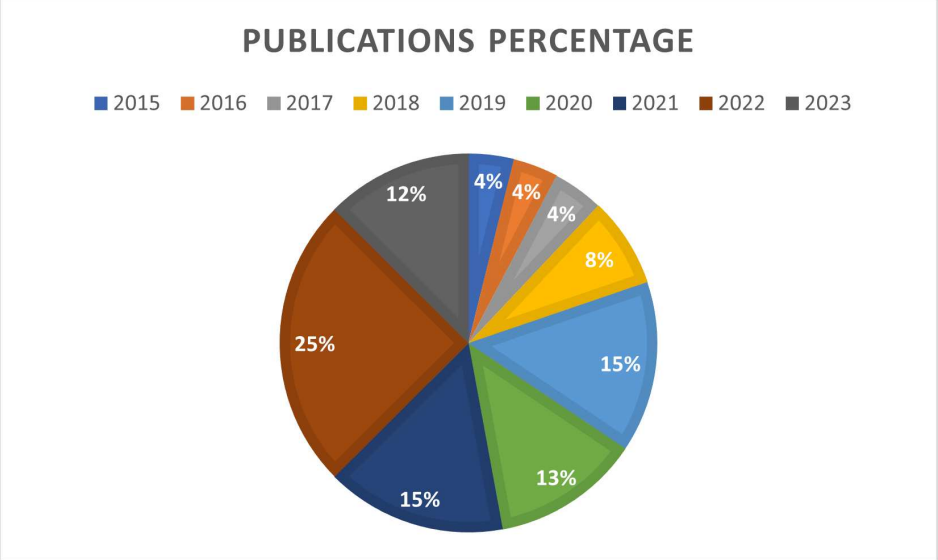

Figure 4.4: Annual Publication Percentage

CHAPTER 5

Analysis of the results

5.1 Analysis of the Results

Analysis of Results explains the results received from several databases (IEEE, ACM, Scopus, WoS) and identifies, organizes, and synthesizes the data gathered during the review process. The data is then organized and classified according to various criteria, including research objectives, study design, and outcomes. The findings are discussed in this section, together with the answers to the research questions. Regarding each RQ, the relevant research will be analysed, compared, and discussed. The graph in Figure 4.5 demonstrates the total number of publications published each year. The demand for virtual reality headsets has escalated in recent years as their necessity has increased.Several factors have contributed to this unanticipated popularity surge. Recent advancements in VR technology have made it possible to have more immersive experiences in a variety of situations. Moreover, data gathered thus far indicates an increase in public concern regarding the collection of personal information by VR systems. This trend is reflected in the growth study, which indicates that demand increased by 15% in 2015 and is projected to increase by 25% by 2022. As of 2023, virtual reality (VR) was experiencing an unprecedented demand increase, indicating a bright future for the industry.

This SLR was commissioned to carefully evaluate the risks associated with VR technology. Our objective is to learn as much as possible about the problems and dangers that VR technology.Paper's have been studied to overcome the issue. (Karim et al. [24] Seth et al. [25] Do and Ng [26] Fang et al. [27] Salimian et al. [28] Feng et al. [29] Wazir et al. [30] Lebeck, Kohno, and Roesner [31] Lele [32] Noah, Shearer, and Das [21] Alam et al. [33] Aslam et al. [34] Silva et al.[35] Berntsen, Palacios, and Herranz [36] Park and Kim [37] Lee et al. [38] Olade et al. [39] Pottle [40] Li et al. [41] Al-Ghaili et al. [42] Ryu et al. [43] Huang et al. [44] Salahdine and Kaabouch [45] David-John et al. [46] Serena, D'Angelo, and Ferretti [47] Alqahtani and Kavakli-Thorne [48] Siriwardhana et al. [49] Men and Zhao [50]Ryu et al. [43] Bhalla et al. [51] Olade, Fleming, and Liang [52] Zhu et al.[53] Casey, Baggili, and Yarramreddy [54] Olshannikova et al. [55] Luo, Hu, and Yan [56] El Merabet and Hajraoui [57] Liang, Zhou, and Gao [58] Pfeuffer et al. [59] Alneyadi, Sithirasenan, and Muthukkumarasamy [60] Mustafa et al. [61] Gaebel et al. [62] Li et al. [63])

RQ1. How can virtual reality systems be designed to enhance the security of sensitive information and data?

The security of sensitive information and data can be improved in virtual reality systems through a variety of techniques, including the use of encrypted communication protocols[25, 64, 24], restricting access to authorized personnel, anonymizing user data, monitoring user activity, and auditing system logs. The security of the virtual reality system may also be increased by including authentication procedures like biometric identification and multi-factor authentication.and lately, blockchains employed to secure such pieces of information.

Among the domains of VR security research, the topic of authentication merits its own section.We currently choose these studies whose primary objective is to characterize Authentication issues [6, 65, 66, 43, 30, 29, 43, 51, 53, 39, 62, 67]. In fact, the majority of VR security research concentrates on identifying and authenticating its users. In this section, we provide a comprehensive analysis of the literature and an overview of the works. There are a few different authentication techniques available, including the following: Users must provide a one-of-a-kind password in order to

access a computer system or an application when authentication is dependent on a password.Identification of individuals based on their distinct physical characteristics, such as fingerprints or facial identification, is an example of biometric authentication.Users are required to provide two or more distinct forms of identification, such as a password and a fingerprint, in order to meet the requirements of multi-factor authentication (MFA).Token-based identification is a method that verifies the identity of users by employing a tangible piece of hardware, like a smart card or a security token.Authentication based on certificates involves using the use of digital certificates in order to authenticate individuals and guarantee secure communication.Users are required to respond to one or more security questions in order to validate their identity when using a knowledge-based authentication system [65, 66]. The data that has been gathered in Metaverse can be simplified into three different categories: personal information, patterns of behaviour, and patterns of communication. It is possible to reveal other people's private lives by using information obtained through social networking sites, this practice is known as "doxing." One such framework is discussed in [6],proposed a method to secure the sensitive information by using MFA, but in our User prespective,Setting up and using MFA can be complicated, requiring multiple steps and factors for authentication. This can lead to confusion and frustration for users, potentially reducing adoption rates.

As was mentioned in [67], RubikAuth is a graphical password authentication method that generates a complex and unique password using a Rubik's Cube. Which provides an additional layer of security for sensitive data and systems by being difficult for attackers to predict or crack. Although the authors did not think about the Users who are unfamiliar with the Rubik's Cube may have difficulty generating or remembering their RubikAuth password. There is no direct connection between RubikAuth and motion sickness. However, some users may experience motion sickness or discomfort while manipulating the cube or viewing it in a virtual environment. Motion sickness is a typical occurrence that occurs when the brain receives contradictory information from the eyes and the inner ear.It is more likely to occur when there is a mismatch between visual cues and bodily movements, such as in virtual reality environments. It is important to consider the possibility of distress or adverse side effects when implementing any technology that involves physical or visual motion,

including RubikAuth. Motion sickness and other adverse effects can be mitigated by implementing user-friendly and accessible interfaces, providing clear instructions and support, and undertaking user testing and feedback.RubikAuth may not be accessible to all users, including those with visual or motor impairments who may struggle to manipulate the cube.

The use of eye-based biometric authentication in VR is an additional reliable authentication method in [21, 31].Biometric authentication systems are generally considered more secure than traditional password-based systems because biometric data is unique to each individual and difficult to replicate.Additionally, most biometric systems incorporate multiple layers of security to prevent hacking attempts, such as multi-factor authentication, continuous monitoring, and encryption.But the collection and storage of biological data raises concerns regarding the intended use and security of this information and Spoofing involves creating fake biometric data to fool the system, such as using a photo or a replica of a fingerprint to bypass the system. Replay attacks involve intercepting and replaying biometric data, which can fool the system into thinking the attacker is the authorized user.

In [43] Security of sensitive data and connection establishment between two VR sets was proposed using Mutual Authentication as well as Blockchain.Mutual authentication is a security procedure in which both parties to a communication verify each other's identity prior to the exchange of data. This procedure is used to prevent unauthorised access or data theft by validating the identities of both parties. In mutual authentication, the client and server verify each other's credentials prior to establishing a secure communication channel for data exchange, typically by exchanging digital certificates. Commonly used in secure communication protocols such as SSL/TLS and SSH to protect against attacks such as man-in-the-middle, this method is also employed in HTTPS.Mutual authentication provides an additional layer of security by requiring both parties to authenticate each other, as opposed to one-way authentication, in which only one party is authenticated. The proposed system model follows this process, To engage in VR environments, the user sends the certificate authority their pseudo-identity, public key, and personal information. Each platform server lets users construct avatars using their pseudo-identity, public key, and credential information. Then, the user authenticates to the platform server to enter the

virtual areas.After successful authentication, the platform server gives a session key to the user, who uses it to communicate securely with the server.Avatar-using users can interact with other avatars. User-authenticated avatar-to-avatar renewed are secure.Blockchain-based metaverse mutual authentication is secure. Avatar authentication also ensures secure avatar-to-avatar interactions in virtual spaces. Initialization, user setup, avatar generation, login and authentication, and avatar authentication make up the proposed approach.This is the only proposed system model that provides secure communication and protects your sensitive data.However, No practical work or demonstration was conducted to demonstrate its efficacy.Future efforts will be made to improve and secure the transition into the digital world.

As was discussed in [30] ,A doodle-base authentication is a form of graphical authentication that verifies a user's identity through the recognition of freehand drawings or sketches. In replacement of entering a password or using a fingerprint scanner, the user is required to draw a predetermined doodle or design. To authenticate the user, this doodle is then compared to a previously recorded doodle.Doodle-based authentication is considered more user-friendly and intuitive than traditional alphanumeric passwords because users can generate more personalized and memorable doodles. They anticipate the use of augmented reality in the authentication process, where the proposed technique is more useful, usable, and secure than extant authentication methods.In this review, they present a fantastic method to authenticate your VR/AR sets; nevertheless, in their experiment, they did not disclose the privacy of user personal information nor did they tell where they save the information about doodles.

In this article [29], the author discusses how using Mobile Crowd sourcing (MCS) with Anonymous Authentication on trust in Blockchain-Based can help solve the problem of maintaining data privacy and security.Mobile crowd sourcing is the process of outsourcing information collection or task completion to a large group of individuals using mobile devices. This method of crowd sourcing has grown in popularity due to the growth of smartphones and the availability of mobile applications that enable individuals to contribute to a variety of tasks.Mobile crowd sourcing can be utilized for numerous duties, including data collection.This approach to crowd sourcing can be more efficient and cost-effective than conventional methods because

it can reach a large number of people rapidly and participants can complete tasks from anywhere.Quality control is one of the most significant issues facing MCS.Due to the fact that anyone can participate in mobile crowd sourcing, there is a possibility that some individuals will provide inaccurate or low-quality data, resulting in inaccurate results.In actuality, however, centralized MCS presents severe security and privacy risks.To address this issue, we employ Intel software guard extension (SGX) and propose a method for anonymously authenticating trust in a blockchain-based MCS system with trustworthy trust evaluation.Anonymous authentication schemes either fail to preserve identity privacy in a decentralized manner or are incapable of supporting precise trust evaluation. Therefore, these works cannot be implemented directly to MCS systems based on the blockchain.Then, they suggested SGX-Based Key Management for MCS.SGX-Based Key Management is a method for securing MCS blockchain keys by leveraging the trusted execution environment supplied by Intel SGX.It provides server protection against attacks and robust key management.However, the SGX technology has some flaws or vulnerabilities, which could compromise the keys security.There is also the possibility that the keys could be lost if the SGX environment is compromised or if the system is not correctly backed up.

Cryptography is a method for protecting information and communications by transforming ordinary text into coded language or cypher text.Utilizing mathematical algorithms known as ciphers to encrypt and decrypt data [64].Using cryptographic techniques to secure data and ensure that only authorised people have access involves cryptographic authentication[68]. Using mathematical algorithms, cryptography encodes data so that only authorised persons with the correct key can decode it. Cryptography can be used in virtual reality to secure data transmission between virtual environments and verify user identity. It provides a high level of security for sensitive data, prevents data theft and unauthorised access, and contributes to the maintenance of privacy. Additionally, cryptography can provide non-repudiation, which means that a sender cannot deny sending a message, and authenticity, which means that the recipient can verify that the message is from the asserted sender.A high level of assurance that the data has not been tampered with or altered is provided by cryptographic authentication. This is due to the fact that any attempt to modify encrypted data requires the correct encryption key, which is extremely difficult to

obtain without authorization.

Encryption, digital signatures, and hash functions can be used to protect data from unauthorised access, modification, or interception, thereby enhancing the security of sensitive information and data in virtual reality[24]. Cryptography is a powerful instrument for preventing data breaches, cyberattacks, and other security threats in virtual reality, where sensitive information such as personally identifiable information, financial data, and health records can be stored or transmitted.Moreover, cryptography can facilitate the establishment of secure communication channels between diverse virtual reality devices or platforms, ensuring the confidentiality and integrity of the exchanged data.

RQ2.What are the best practices for securing virtual reality systems and environments from malicious actors?

In previous RQ we briefly defined the method of Authenication,Data encryption,and the most important user training for preventation to Malware. [54, 57, 56, 24, 68, 64, 30, 6] Proposes HoloLogger employs a key tracking method that is enabled by six degrees of freedom (6DoF) and is based on the head movements of the user.In the context of MR or VR systems, 6DoF is an abbreviation for "six degrees of freedom," which means a tracking system can detect the location and orientation of an object or user in all directions (forward, backward, up, down, left, and right). In this day and age, it is of the utmost importance for businesses to take steps to prevent malicious actors from gaining access to critical data or computer networks. There are various recommended practices to follow to safeguard sensitive data and information when protecting virtual reality systems and surroundings from bad actors. Implementing strong access control techniques to stop unwanted access to the system is one of the most crucial procedures. e.g., multi-factor or cryptography authentication and role-based access control can be used to make sure that only authorized workers can use the VR system. To prevent data theft and eavesdropping, it is also essential to encrypt all communication between the user's device and the virtual reality system. To prevent unauthorized access, virtual reality settings should also be separated from

the internet, and intrusion detection systems [69] should be put in place to watch the system for any unusual behaviour. Virtual reality may be utilized to identify and prevent cyberattacks from malicious actors and other security risks. Phishing assaults, malware infections, efforts at social engineering, and other security issues are examples of this. By sending fake emails to staff members, for instances a virtual reality training program might simulate a phishing attack. The software can monitor the number of employees who clicked on the phishing link and the information they provided on the phony website (The purpose of phony websites, often known as fake websites, is to trick people into stolen critical information, such as passwords or bank details). This can assist businesses in determining which staff members require further phishing attack detection and prevention training.Another illustration is the simulation of an intrusion detection system using virtual reality. A virtual reality environment may be used by security experts to test and improve intrusion detection systems and refine their abilities to recognize and respond to cyberattacks.It is also critical to frequently update the virtual reality system and its related software to fix any security flaws that may be used maliciously. Ensuring VR systems and environments are linked to secure networks, such as Virtual Private Networks (VPNs)[60], can prevent unauthorized access and data breaches.

Moreover, user training on safe techniques for utilizing the virtual reality system can assist users in staying secure from social engineering assaults and other cyber risks. Finally, it is important to frequently audit and keep an eye out for any suspicious behaviour or illegal access attempts on virtual reality systems. Using system logs and security information and event management solutions to monitor every user activity within the system can help you do this. Organizations may reduce the risk of cyberattacks and safeguard sensitive data from bad actors by putting these best practices into effect and keeping the virtual reality system current.

RQ3.How can virtual reality improve physical security systems and processes in various industries?

By offering [35, 41, 32, 5, 28, 40]immersive and realistic training experiences, boosting situational awareness, and assisting in the design and testing of security systems, virtual reality may enhance physical security systems and procedures in a variety of sectors. Virtual reality may be used to recreate realistic training scenarios that closely resemble real-life circumstances in the military and law enforcement businesses. This enables staff to practice handling security threats and crises in a secure setting without running the risk of endangering themselves or others.In the healthcare industry, for instance, virtual reality can be used to simulate emergency situations and instruct employees on how to respond to potential security threats.By facilitating reproducible and scalable clinical training, VR has the potential to enhance education in numerous professions. If it is incorporated into curricula and advances are made in the utilization of shared virtual experiences, the future of medical education is promising.Virtual reality can provide a secure and controlled environment for training security personnel to respond to security incidents and to become familiar with the security system.This may be helpful in identifying vulnerabilities and enhancing the facility's physical security system.Virtual reality can also be used to improve nuclear facility physical security [32]. Radiation poses significant hazards in nuclear facilities, making the training of security personnel and maintenance of security systems crucial. Before these technologies are ever implemented, engineers and security personnel may test their efficacy in VR simulations. In the retail sector, virtual reality may be used to teach staff members about loss prevention strategies and to recreate scenarios involving theft or fraudulent activities. Employees may be better able to recognize and address possible security issues as a result. Overall, by offering realistic training experiences, enhancing situational awareness, and assisting in the design and testing of security systems, virtual reality may improve physical security systems and procedures in a variety of sectors.

RQ4.What role does virtual reality play in the development and deployment of advanced security technologies such as biometrics, AI, and blockchain?

Advanced security technologies like biometrics [59], AI, and blockchain [70, 43, 29, 26, 47] may be developed and deployed with the help of virtual reality, which can be very important.Virtual Reality may be used to assess the effectiveness of new security systems and teach security personnel by generating immersive settings that replicate real-world circumstances.By simulating and testing various scenarios using virtual reality, security researchers and engineers can identify vulnerabilities and enhance the efficacy of security measures.VR can also benefit AI-powered security systems by providing a more intuitive method to visualise and comprehend complex data sets.By utilizing VR, security professionals can take advantage of the capability of the technology to generate realistic visualizations of massive and complex data sets[55, 71]. Blockchain may be used to protect and authenticate virtual transactions and decentralized networks, and biometric authentication can be used in virtual reality training exercises.The use of blockchain technology facilitates the exchange of data between parties. Due to its inherent properties, such as transparency, immutability, and decentralized (P2P) consensus, Blockchain technology is a reliable solution to the issue of preserving and validating digital transactions. Blockchain is a distributed ledger technology that employs cryptographic hash functions to ensure the authenticity and security of online transactions. This boosts operational efficiency and confidence in a decentralized setting. Blockchain has the potential to revolutionize numerous industries, making it a game-changer in the world of decentralized networks and digital transactions.In a supply chain scenario, VR visualisation could help identify any discrepancies or inconsistencies in the data recorded on the blockchain, enabling more efficient and accurate auditing. Biometrics, AI, and blockchain can all be incorporated into virtual reality settings to improve security measures. In general, innovative security solutions may be tested and improved in virtual reality before being used in the real world in a secure and controlled setting.

CHAPTER 6

Discussion

The findings of our study have generated a number of concerns that require further investigation and discussion. Researchers, developers, and professionals concerned with creating and deploying safe virtual reality systems would gain a great deal from this study's findings, as the implications of these findings are described in detail. Virtual reality has played significant importance in this era due to its potential to enhance user experiences, transform the entertainment industry, and facilitate remote work and communication.

Some worries have emerged over the privacy of users' personal information and potential vulnerabilities that could be exploited by malicious actors despite the rapid advancement of VR. Examining the existing systematic literature review on this topic enables us to gain insights into the current state of security and privacy in VR and to examine the implications of these issues for users and the broader technology landscape.

We examine the need for biometric identification and multi-factor authentication for researchers and developers, as well as user-friendly initiatives and tools to assist users in defending their privacy. We examine, among other things, the significance of user education and awareness, the need for initiatives and user-friendly solutions, and the current use of blockchain to secure such data.Additionally, there should be

a focus on the effects of stringent security measures, privacy-by-design principles, and best practices on user data protection, as well as consumer confidence, market development, and the VR industry as a whole.

When navigating the virtual reality towards the metaverse, numerous factors must be considered. Prioritise the security of user information by implementing sophisticated encryption and authentication mechanisms. Second, you can give consumers control over information sharing by integrating privacy controls. To prevent fraud and impersonation, thirdly, dependable identity verification procedures must be implemented. The fourth phase entails instituting effective content control in order to remove any potentially harmful data. Protect people and infrastructure from attacks by making cybersecurity a top priority. Protect users by eliminating or reporting objectionable or abusive content as the sixth priority. Encourage interoperability and standards to improve the convenience and security of communications. The eighth step involves laying the legal and ethical foundation for metaverse management. Lastly, security measures should be updated frequently in response to newly discovered hazards and user feedback. To construct a secure metaverse, it is necessary to collaborate with others and establish a balance between the privacy and security requirements of users and their desire for interactive experiences.

The advancement of VR security depends on machine learning (ML) and artificial intelligence (AI).Using biometric techniques like facial recognition or voice recognition, machine learning algorithms can authenticate users. In this manner, only authorised users will be able to access private VR content and conduct mission-critical operations. For the purpose of identifying dubious activities, machine learning algorithms evaluate user behaviour and transactions data. Suspicious conduct includes odd spending or trading patterns. Content vetting security is another area where machine learning and artificial intelligence may be useful. This involves autonomously identifying and removing potentially harmful or incorrect content posted by users. In addition, these technologies assist in bolstering security defences, identifying and responding to security breaches, and protecting user data from unauthorised access or threats. The research and implementation of VR privacy and security solutions have significant repercussions. More security measures, privacy-protecting technologies, ethical standards, privacy education, collaboration, impact analysis, and user-centred

design are recommended. These acts aim to provide customised security measures, reduce privacy threats, address ethical concerns, educate users, establish standards, evaluate outcomes, and prioritise user needs. We can enhance VR security, protect user privacy, and encourage responsible VR use if we collaborate to address these issues.

CHAPTER 7

Threat to validity

The validity of the given findings may have been jeopardised due to the fact that our systematic literature study, just like every other one, has some limitations. In this part, both of these issues and the measures that have been used to overcome them will be discussed.

7.1 Literature Selection

Finding a suitable systematic literature review that provides a comprehensive account of the current state of the art is extremely challenging. In this way, we began by creating a search query with the aim of locating as many publications as possible pertaining to the use of virtual reality to address privacy and security issues, without imposing any time constraints. We chose this option despite the fact that it necessitated additional manual analysis labour because we prioritised accuracy over expediency. In addition, while developing the search query, we considered likely synonyms and alternative spellings of frequently used literary terms. In addition, we searched for possible additional phrases by determining whether the search terms were included in an existing systematic literature review on the topics of virtual reality security, privacy, authentication, and identification. Only articles that met

these inclusion and exclusion criteria were considered when drawing conclusions about the findings of our study. Our was completed so that our research would be as exhaustive as feasible. All phases preceding the selection of primary studies were always double-checked by at least one of the paper's authors, as this is one of the most crucial aspects of the research.During the weekly and monthly meetings between the first and second authors of this thesis, all of the questions that were intended to be answered during the course of our quality assessment were discussed, and a conclusion was mutually agreed upon.We are confident in the exhaustiveness of the literature selection as a consequence of combining these numerous operations. To ensure that our findings can be independently validated and replicated, we have nevertheless included an online appendix in our supplementary contribution that describes each stage of our experiments and their intermediate results.

7.2 Literature analysis and synthesis

After the selection process was completed, specific exclusion criteria were applied to eliminate papers that would not contribute to or would only marginally contribute to a synthesis of the state of the art in relation to the stated research questions. In addition, we did not restrict the selection of primary studies to those that met the inclusion criteria; rather, we conducted an additional quality assessment to determine if they were suitable for the purposes we had in mind. As a result of this form of manual evaluation, the possibility of including items that are unsuitable for our purposes has been further reduced. The overall literature synthesis relied on manual analyses, which are inherently defective as a result of human interaction. In this regard, two factors must be considered. First, as a result of the ongoing communication between the first and second authors, the likelihood of errors and/or instances of subjectivity has been greatly diminished. Second, the supervisor of the thesis was present throughout the entire process and offered assistance in completing the various phases of the systematic literature review at any point where it was needed.

CHAPTER 8

Conclusion

8.1 Conclusion

This systematic literature review is focused on the topic of emerging Virtual Reality techniques for privacy/security detection in the Virtual Environment. Virtual reality is becoming increasingly prevalent among local enterprises and families. Therefore, it is of the utmost importance to consider the problems that this innovative technology can cause. Authorization problems, data leaks, malicious actors, vulnerable software, and unauthorized access are identified as significant security issues in the technology itself by the research. To prevent assaults, VR security may be enhanced. VR settings may benefit from the implementation of blockchain technology as a result of blockchain research aimed at enhancing the security of sensitive user data. Thus concluding that AR and VR technologies have taken hold in the industry and offer a variety of applications, it remains vulnerable to numerous threats. To implement these technologies on a larger scale, we must conduct additional research and provide an analytical solution for implementing them in larger real-world initiatives.

8.1.1 Future Work

The thoughts and consequences of this comprehensive literature review are driving our agenda for the research we will conduct in the future. Investigate a variety of papers and look for a fresh authentication strategy that is able to protect critical user data, Investigate how the blockchain could be used in the future for conservative issues related to virtual reality, augmented reality, and mixed reality. Investigate how the blockchain could be utilized in the future for safeguarding issues associated with virtual reality, augmented reality, and mixed reality. Conduct research on a number of papers and look for a new authentication approach that is able to protect essential user data.

Bibliography

[1] Sharmistha Mandal. "Brief introduction of virtual reality & its challenges". In: *International Journal of Scientific & Engineering Research* 4.4 (2013), pp. 304–309.

[2] John Vince. *Introduction to virtual reality*. Springer Science & Business Media, 2004.

[3] Zhilong Chen et al. "Learning from home: A mixed-methods analysis of live streaming based remote education experience in chinese colleges during the covid-19 pandemic". In: *Proceedings of the 2021 CHI Conference on human factors in computing systems*. 2021, pp. 1–16.

[4] Neal Stephenson. *Snow crash: A novel*. Spectra, 2003.

[5] Huansheng Ning et al. "Cyberology: Cyber–Physical–Social-Thinking Spaces-Based Discipline and Interdiscipline Hierarchy for Metaverse (General Cyberspace)". In: *IEEE Internet of Things Journal* 10.5 (2022), pp. 4420–4430.

[6] Pınar Kürtünlüoğlu, Beste Akdik, and Enis Karaarslan. "Security of virtual reality authentication methods in metaverse: An overview". In: *arXiv preprint arXiv:2209.06447* (2022).

[7] Tanya Abdulsattar Jaber. "Security Risks of the Metaverse World." In: *International Journal of Interactive Mobile Technologies* 16.13 (2022).

[8] Amaizu Gabriel Chukwunonso et al. "Security in metaverse: a closer look". In: (2022), pp. 199–200.

[9] Tao Peng, Christopher Leckie, and Kotagiri Ramamohanarao. "Survey of network-based defense mechanisms countering the DoS and DDoS problems". In: *ACM Computing Surveys (CSUR)* 39.1 (2007), 3–es.

[10] Ayah Hamad and Bochen Jia. "How virtual reality technology has changed our lives: an overview of the current and potential applications and limitations". In: *International journal of environmental research and public health* 19.18 (2022), p. 11278.

[11] Jaron Lanier. *You are not a gadget: A manifesto*. Vintage, 2011.

[12] Georgios M Minopoulos et al. "A Medical Image Visualization Technique Assisted with AI-Based Haptic Feedback for Robotic Surgery and Healthcare". In: *Applied Sciences* 13.6 (2023), p. 3592.

[13] Yuntao Wang et al. "A survey on metaverse: Fundamentals, security, and privacy". In: *IEEE Communications Surveys & Tutorials* (2022).

[14] Ruoyu Zhao et al. "Metaverse: Security and privacy concerns". In: *arXiv preprint arXiv:2203.03854* (2022).

[15] Ravi Sandhu. "Rationale for the RBAC96 family of access control models". In: *Proceedings of the first ACM Workshop on Role-based access control*. 1996, 9–es.

[16] Bruhadeshwar Bezawada, Kyle Haefner, and Indrakshi Ray. "Securing home IoT environments with attribute-based access control". In: *Proceedings of the Third ACM Workshop on Attribute-Based Access Control*. 2018, pp. 43–53.

[17] Eric Baize. "Developing secure products in the age of advanced persistent threats". In: *IEEE Security & Privacy* 10.3 (2012), pp. 88–92.

[18] Ibrahim Ghafir et al. "Detection of advanced persistent threat using machine-learning correlation analysis". In: *Future Generation Computer Systems* 89 (2018), pp. 349–359.

[19] Alberto Giaretta. "Security and Privacy in Virtual Reality–A Literature Survey". In: *arXiv preprint arXiv:2205.00208* (2022).

[20] Parth Dipakkumar Patel and Prem Trivedi. "A systematic literature review on Virtual Reality and Augmented Reality in terms of privacy, authorization and data-leaks". In: *arXiv preprint arXiv:2212.04621* (2022).

[21] Naheem Noah, Sommer Shearer, and Sanchari Das. "Security and privacy evaluation of popular augmented and virtual reality technologies". In: *Proceedings of the 2022 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence, and Neural Engineering (IEEE MetroXRAINE 2022)*. 2022.

[22] Barbara Kitchenham et al. "Systematic literature reviews in software engineering–a systematic literature review". In: *Information and software technology* 51.1 (2009), pp. 7–15.

[23] Pablo Vicente Torres-Carrión et al. "Methodology for systematic literature review applied to engineering and education". In: *2018 IEEE Global engineering education conference (EDUCON)*. IEEE. 2018, pp. 1364–1373.

[24] Rafat Karim et al. "Digital signature authentication for a bank using asymmetric key cryptography algorithm and token based encryption". In: *Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020*. Springer. 2021, pp. 853–859.

[25] Bijeta Seth et al. "Integrating encryption techniques for secure data storage in the cloud". In: *Transactions on Emerging Telecommunications Technologies* 33.4 (2022), e4108.

[26] Hoang Giang Do and Wee Keong Ng. "Blockchain-based system for secure data storage with private keyword search". In: *2017 IEEE World Congress on Services (SERVICES)*. IEEE. 2017, pp. 90–93.

[27] Weidong Fang et al. "Digital signature scheme for information non-repudiation in blockchain: a state of the art review". In: *EURASIP Journal on Wireless Communications and Networking* 2020.1 (2020), pp. 1–15.

[28] Mohamad H Salimian et al. "Physical-digital privacy interfaces for mixed reality collaboration: an exploratory study". In: *Proceedings of the 2016 ACM International Conference on Interactive Surfaces and Spaces*. 2016, pp. 261–270.

[29] Wei Feng et al. "Anonymous authentication on trust in blockchain-based mobile crowdsourcing". In: *IEEE Internet of Things Journal* 9.16 (2020), pp. 14185–14202.

[30] Waqas Wazir et al. "Doodle-based authentication technique using augmented reality". In: *IEEE Access* 8 (2020), pp. 4022–4034.

[31] Kiron Lebeck, Tadayoshi Kohno, and Franziska Roesner. "How to safely augment reality: Challenges and directions". In: *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*. 2016, pp. 45–50.

[32] Ajey Lele. "Virtual reality and its military utility". In: *Journal of Ambient Intelligence and Humanized Computing* 4 (2013), pp. 17–26.

[33] Md Fasiul Alam et al. "Augmented and virtual reality based monitoring and safety system: A prototype IoT platform". In: *Journal of Network and Computer Applications* 89 (2017), pp. 109–119.

[34] Anjum Mohd Aslam et al. "Metaverse for 6G and Beyond: the next revolution and deployMent ChallenGes". In: *IEEE Internet of Things Magazine* 6.1 (2023), pp. 32–39.

[35] Márcio Henrique da Silva et al. "Using virtual reality to support the physical security of nuclear facilities". In: *Progress in Nuclear Energy* 78 (2015), pp. 19–24.

[36] Kristina Berntsen, Ricardo Colomo Palacios, and Eduardo Herranz. "Virtual reality and its uses: a systematic literature review". In: *Proceedings of the Fourth International Conference on Technological Ecosystems for Enhancing Multiculturality*. 2016, pp. 435–439.

[37] Sang-Min Park and Young-Gab Kim. "A metaverse: Taxonomy, components, applications, and open challenges". In: *IEEE access* 10 (2022), pp. 4209–4251.

[38] Sungjin Lee et al. "Effect Analysis of Virtual-reality Vestibular Rehabilitation based on Eye-tracking." In: *KSII Transactions on Internet & Information Systems* 14.2 (2020).

[39] Ilesanmi Olade et al. "Exploring the vulnerabilities and advantages of swipe or pattern authentication in virtual reality (vr)". In: *Proceedings of the 2020 4th International Conference on Virtual and Augmented Reality Simulations*. 2020, pp. 45–52.

[40] Jack Pottle. "Virtual reality and the transformation of medical education". In: *Future healthcare journal* 6.3 (2019), p. 181.

[41] Lan Li et al. "Application of virtual reality technology in clinical medicine". In: *American journal of translational research* 9.9 (2017), p. 3867.

[42] Abbas M Al-Ghaili et al. "A review of metaverse's definitions, architecture, applications, challenges, issues, solutions, and future trends". In: *IEEE Access* (2022).

[43] Jongseok Ryu et al. "Design of secure mutual authentication scheme for metaverse environments using blockchain". In: *Ieee Access* 10 (2022), pp. 98944–98958.

[44] Huakun Huang et al. "Fusion of building information modeling and blockchain for metaverse: a survey". In: *IEEE Open Journal of the Computer Society* 3 (2022), pp. 195–207.

[45] Fatima Salahdine and Naima Kaabouch. "Social engineering attacks: A survey". In: *Future internet* 11.4 (2019), p. 89.

[46] Brendan David-John et al. "A privacy-preserving approach to streaming eye-tracking data". In: *IEEE Transactions on Visualization and Computer Graphics* 27.5 (2021), pp. 2555–2565.

[47] Luca Serena, Gabriele D'Angelo, and Stefano Ferretti. "Security analysis of distributed ledgers and blockchains through agent-based simulation". In: *Simulation Modelling Practice and Theory* 114 (2022), p. 102413.

[48] Hamed Alqahtani and Manolya Kavakli-Thorne. "Factors affecting acceptance of a mobile augmented reality application for cybersecurity awareness". In: *Proceedings of the 2020 4th International Conference on Virtual and Augmented Reality Simulations*. 2020, pp. 18–26.

[49] Yushan Siriwardhana et al. "A survey on mobile augmented reality with 5G mobile edge computing: Architectures, applications, and technical aspects". In: *IEEE Communications Surveys & Tutorials* 23.2 (2021), pp. 1160–1192.

[50] Liang Men and Danqi Zhao. "Designing privacy for collaborative music making in virtual reality". In: *Proceedings of the 16th International Audio Mostly Conference*. 2021, pp. 93–100.

[51] Arman Bhalla et al. "MoveAR: Continuous biometric authentication for augmented reality headsets". In: *Proceedings of the 7th ACM on Cyber-Physical System Security Workshop*. 2021, pp. 41–52.

[52] Ilesanmi Olade, Charles Fleming, and Hai-Ning Liang. "Biomove: Biometric user identification from human kinesiological movements for virtual reality systems". In: *Sensors* 20.10 (2020), p. 2944.

[53] Huadi Zhu et al. "Blinkey: A two-factor user authentication method for virtual reality devices". In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4.4 (2020), pp. 1–29.

[54] Peter Casey, Ibrahim Baggili, and Ananya Yarramreddy. "Immersive virtual reality attacks and the human joystick". In: *IEEE Transactions on Dependable and Secure Computing* 18.2 (2019), pp. 550–562.

[55] Ekaterina Olshannikova et al. "Visualizing Big Data with augmented and virtual reality: challenges and research agenda". In: *Journal of Big Data* 2.1 (2015), pp. 1–27.

[56] Shiqing Luo, Xinyu Hu, and Zhisheng Yan. "Holologger: Keystroke inference on mixed reality head mounted displays". In: *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. IEEE. 2022, pp. 445–454.

[57] Hoda El Merabet and Abderrahmane Hajraoui. "A survey of malware detection techniques based on machine learning". In: *International Journal of Advanced Computer Science and Applications* 10.1 (2019).

[58] Zhipeng Liang, Keping Zhou, and Kaixin Gao. "Development of virtual reality serious game for underground rock-related hazards safety training". In: *IEEE access* 7 (2019), pp. 118639–118649.

[59] Ken Pfeuffer et al. "Behavioural biometrics in VR: Identifying people from body motion and relations in virtual reality". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 2019, pp. 1–12.

[60] Sultan Alneyadi, Elankayer Sithirasenan, and Vallipuram Muthukkumarasamy. "A survey on data leakage prevention systems". In: *Journal of Network and Computer Applications* 62 (2016), pp. 137–152.

[61] Tahrima Mustafa et al. "Unsure how to authenticate on your vr headset? come on, use your head!" In: *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics*. 2018, pp. 23–30.

[62] Ethan Gaebel et al. "Looks good to me: Authentication for augmented reality". In: *Proceedings of the 6th international workshop on trustworthy embedded devices*. 2016, pp. 57–67.

[63] Kai Li et al. "When internet of things meets metaverse: Convergence of physical and cyber worlds". In: *IEEE Internet of Things Journal* 10.5 (2022), pp. 4148–4173.

[64] Tzong-Mou Wu. "One-to-one mapping matrix". In: *Applied mathematics and computation* 169.2 (2005), pp. 963–970.

[65] Dwiti Pandya et al. "An overview of various authentication methods and protocols". In: *International Journal of Computer Applications* 131.9 (2015), pp. 25–27.

[66] Syed Zulkarnain Syed Idrus et al. "A review on authentication methods". In: *Australian Journal of Basic and Applied Sciences* 7.5 (2013), pp. 95–107.

[67] Karthik Viswanathan and Abbas Yazdinejad. "Security considerations for virtual reality systems". In: *arXiv preprint arXiv:2201.02563* (2022).

[68] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. "Survey on VANET security challenges and possible cryptographic solutions". In: *Vehicular Communications* 1.2 (2014), pp. 53–66.

[69] Rebecca Gurley Bace, Peter Mell, et al. "Intrusion detection systems". In: (2001).

[70] Qinglin Yang et al. "Fusing blockchain and AI with metaverse: A survey". In: *IEEE Open Journal of the Computer Society* 3 (2022), pp. 122–136.

[71] Mohamed El Beheiry et al. "Virtual reality: beyond visualization". In: *Journal of molecular biology* 431.7 (2019), pp. 1315–1321.