Master’s Degree in Computer Science

Security Issues in Virtual Reality: A Systematic Literature Review

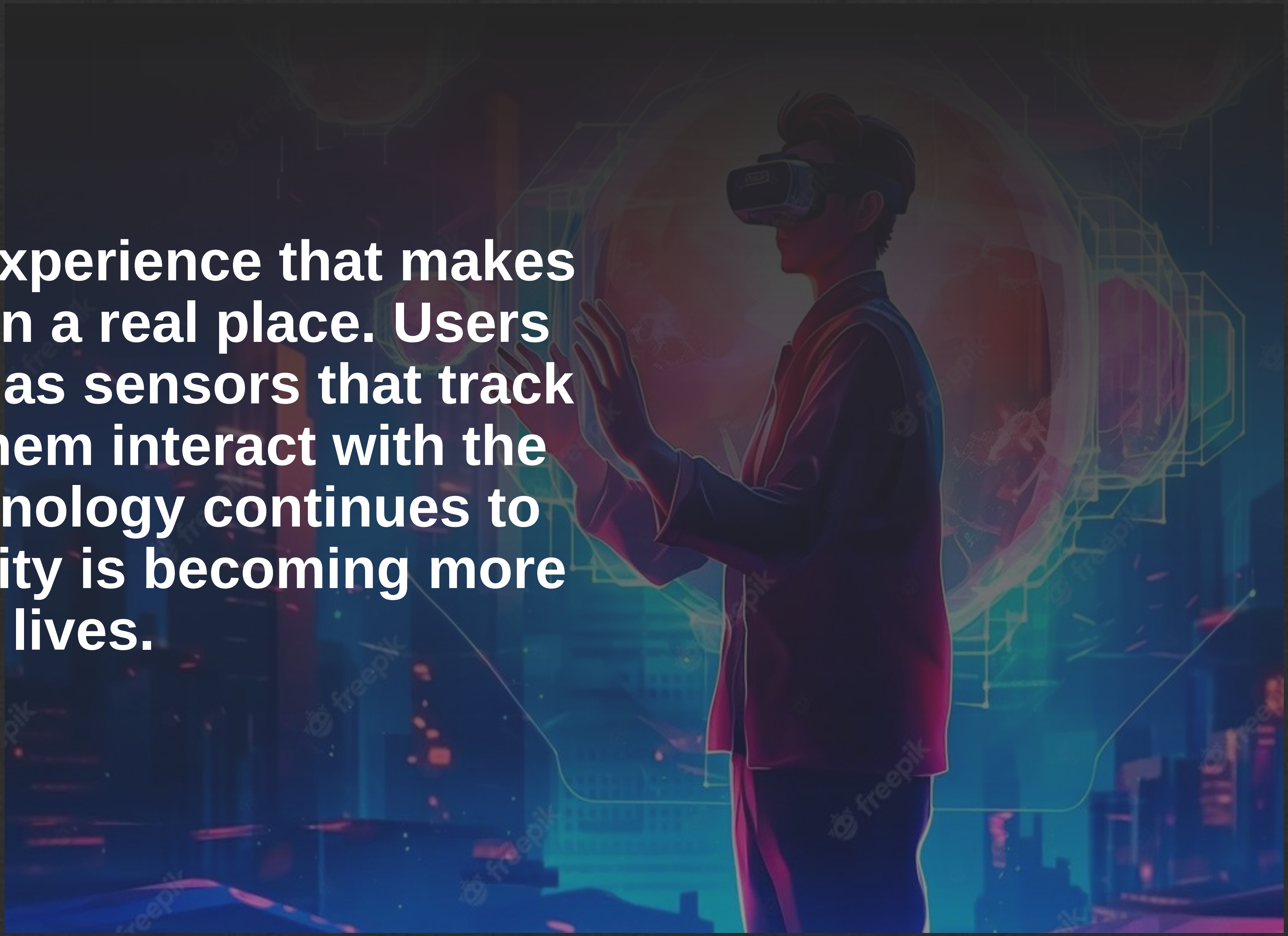
Prof. Fabio Palomba
Dott. Dario Di Dario

Muhammad Umair Manzoor
Mat.: 0522500904

✉ m.manzoor@studenti.unisa.it
https://github.com/Umairmanzoor5
www.linkedin.com/in/muhammad-umair7/

Introduction and Background

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. As technology continues to advance, Virtual Reality is becoming more prevalent in our daily lives.



Introduction and Background

Virtual Reality (VR) has seen significant advancements and widespread adoption in recent years, enabling immersive experiences in various domains such as gaming, education, healthcare, architecture, etc.

✉ m.manzoor@studenti.unisa.it
https://github.com/Umairmanzoor5
www.linkedin.com/in/muhammad-umair7/

Introduction and Background

Virtual reality has been a topic of fascination for decades, Virtual reality is widely acknowledged to have originated during the 1950’s it met significant public recognition during the late 1980's and 1990's. Jaron Lanier contributed to this…

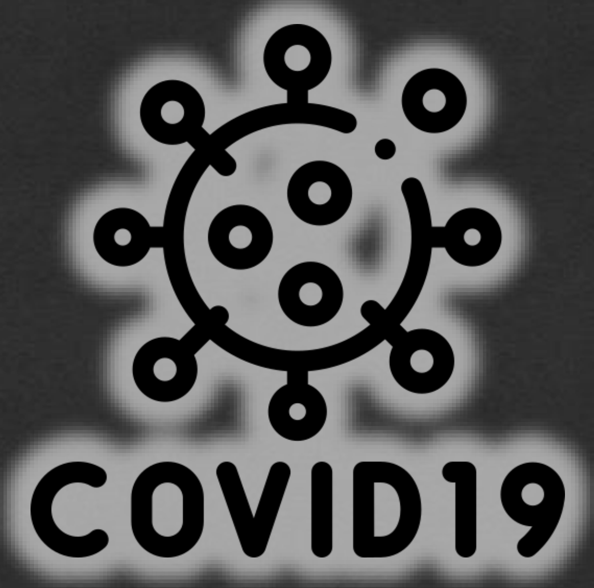
Introduction and Background

In 1985, Lanier founded the company Virtual Programing Language (VPL), the first company to sell VR products

Jaron Lanier: “There is nothing more gray, stultifying, or dreary than life lived inside the confines of a theory”

Introduction and Background

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. Virtual reality is no longer just a futuristic concept, but a rapidly growing technology that has the potential to revolutionize the way we experience the world around us.*



Introduction and Background

With this new Virtual Reality technology comes new challenges, bring new threats to user security and privacy. Many are victimized to fraud due to lack of education or training, losing personal information, bank credentials, usernames, and facing financial loss.

Method:

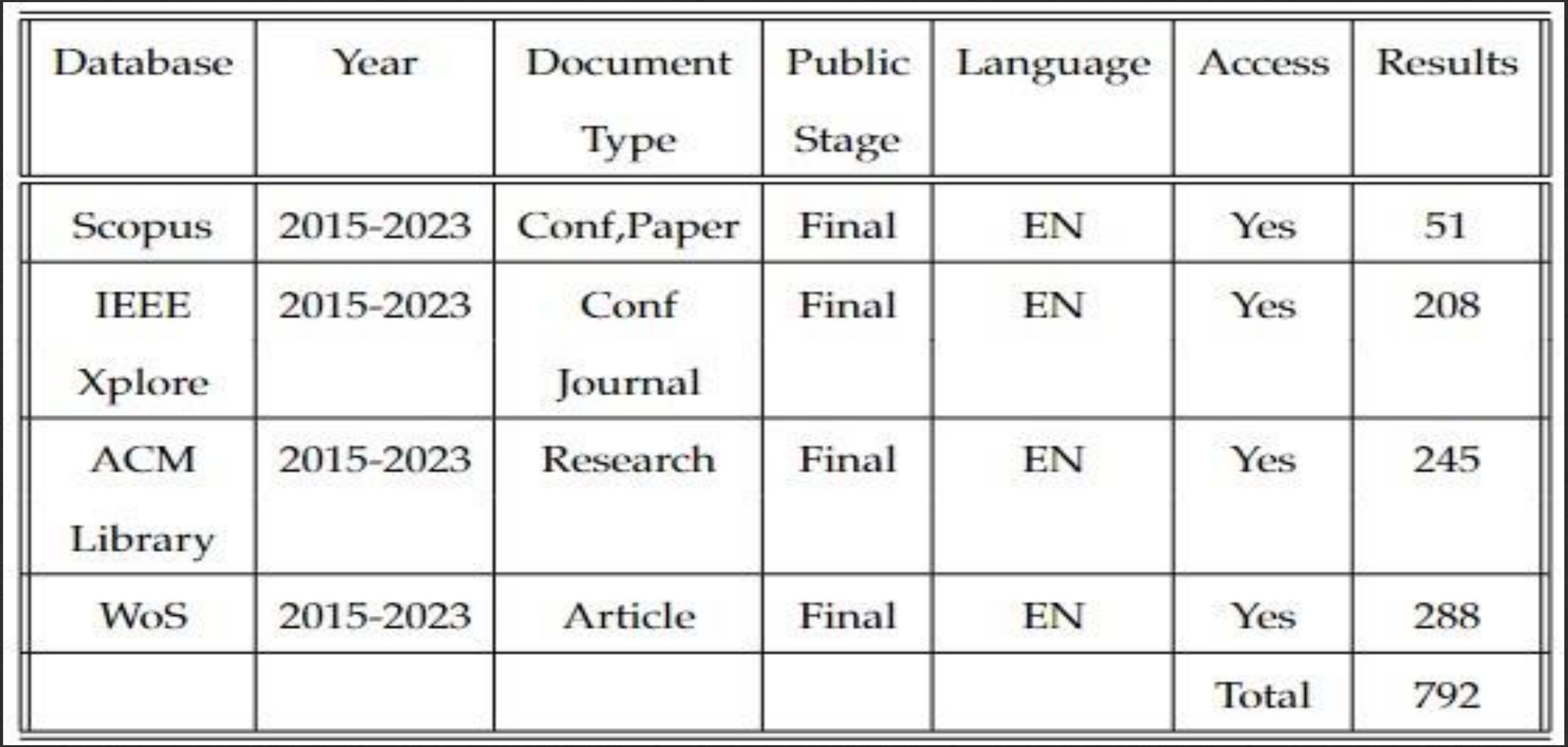
ACM DL DIGITAL LIBRARY
Scopus
NON SOLUS
IEEE Xplore® Digital Library
Clarivate Analytics
WEB OF SCIENCE™

m.manzoor@studenti.unisa.it

https://github.com/Umairmanzoor5

www.linkedin.com/in/muhammad-umair7/

Method:

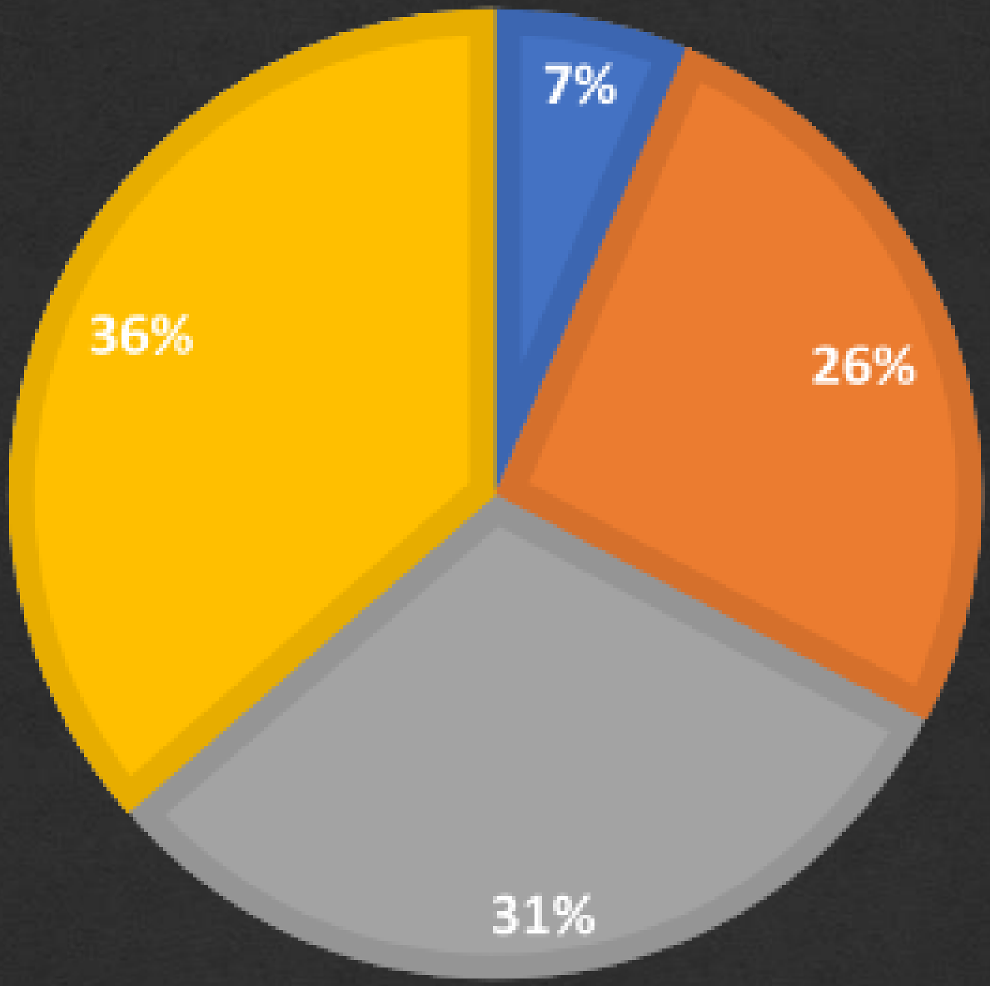


Database	Year	Document Type	Public Stage	Language	Access	Results
Scopus	2015-2023	Conf,Paper	Final	EN	Yes	51
IEEE Xplore	2015-2023	Conf Journal	Final	EN	Yes	208
ACM Library	2015-2023	Research	Final	EN	Yes	245
WoS	2015-2023	Article	Final	EN	Yes	288
					Total	792

Method:

The findings of the primary studies were provided to us after we had applied all of the criteria to the various databases.

- *ACM Library holds 31%*
- *Scopus holds 7%*
- *IEEE Xplore holds 26%*
- *WoS holds 36%*



m.manzoor@studenti.unisa.it
https://github.com/Umairmanzoor5
www.linkedin.com/in/muhammad-umair7/

Research Objective:

This review aims to identify and analyze security issues in virtual reality technology, proposing solutions to mitigate risks. The research seeks to raise awareness about addressing these concerns and ensuring a safe virtual reality environment for users.

- *Safety Measures:*

In brief, discussed the current security measures implemented in VR systems to tackle identified issues, including encryption, two-factor authentication, and secure software engineering practices.

Issues in Virtual Reality:

Virtual reality technology has opened up a whole new world of possibilities, but with it comes a host of security concerns.

- *User Authentication and Identity Theft.*
- *Data Privacy and Personal Information.*
- *Malware and Cyberattacks.*
- *Physical Safety and VR-Induced Health Issues.*
- *Virtual Asset Theft and Fraud.*

Malware:

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 may infiltrate VR software, compromising the security of VR devices. 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.

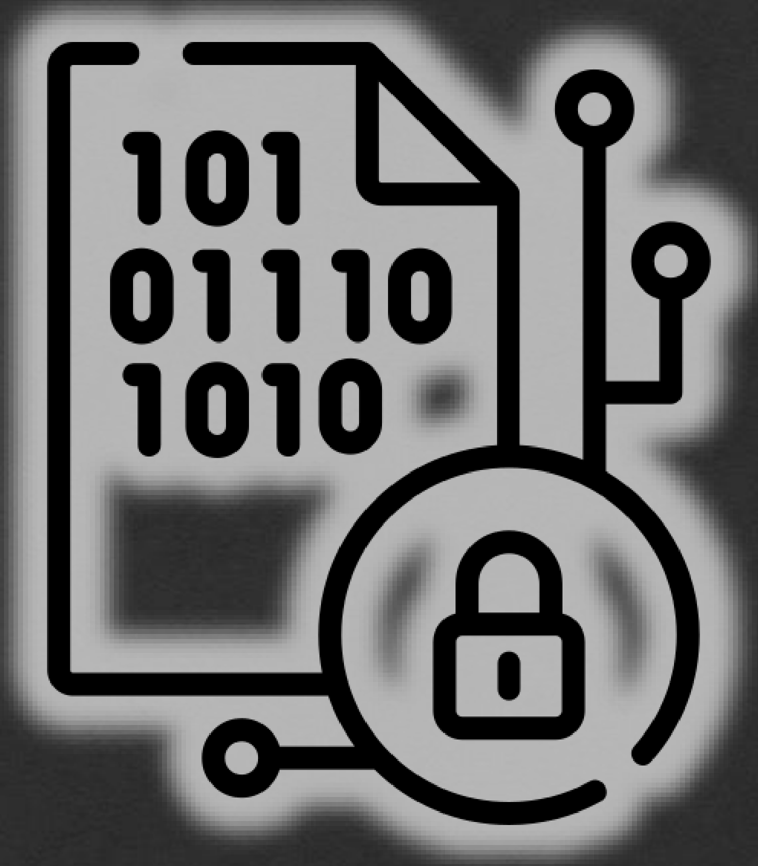
Malware:

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. Ensuring VR systems and environments are linked to secure networks, such as Virtual Private Networks (VPNs), can prevent unauthorized access and data breaches. 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.

Encryption:

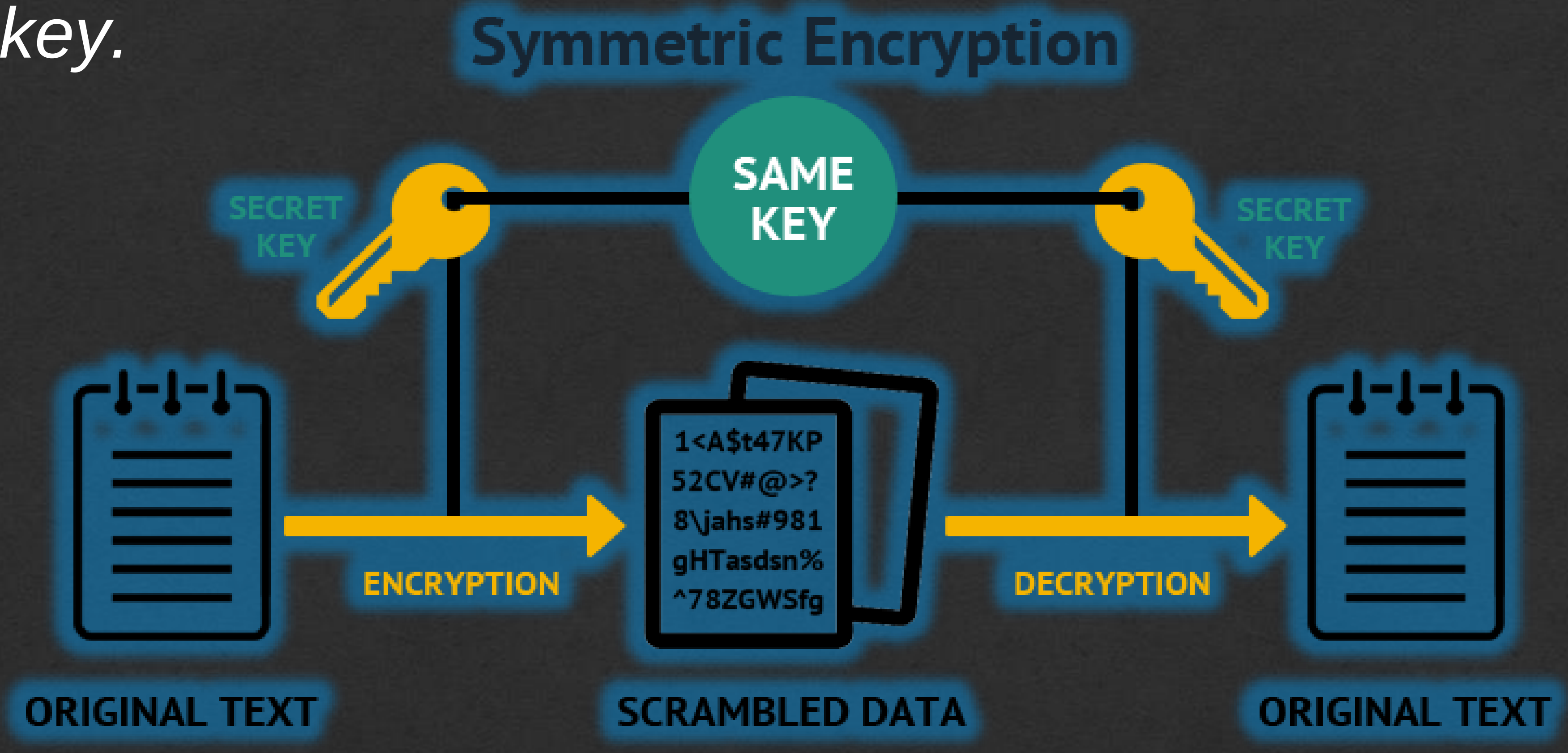
Through various encryption techniques, data communication between virtual reality devices and servers is secured, ensuring the safety of information, even if intercepted by unauthorized parties.

- *Symmetric Encryption*
- *Asymmetric Encryption*
- *RSA (Rivest-Shamir-Adleman)*
- *AES (Advanced Encryption Standard)*
- *DES (Data Encryption Standard), etc,*



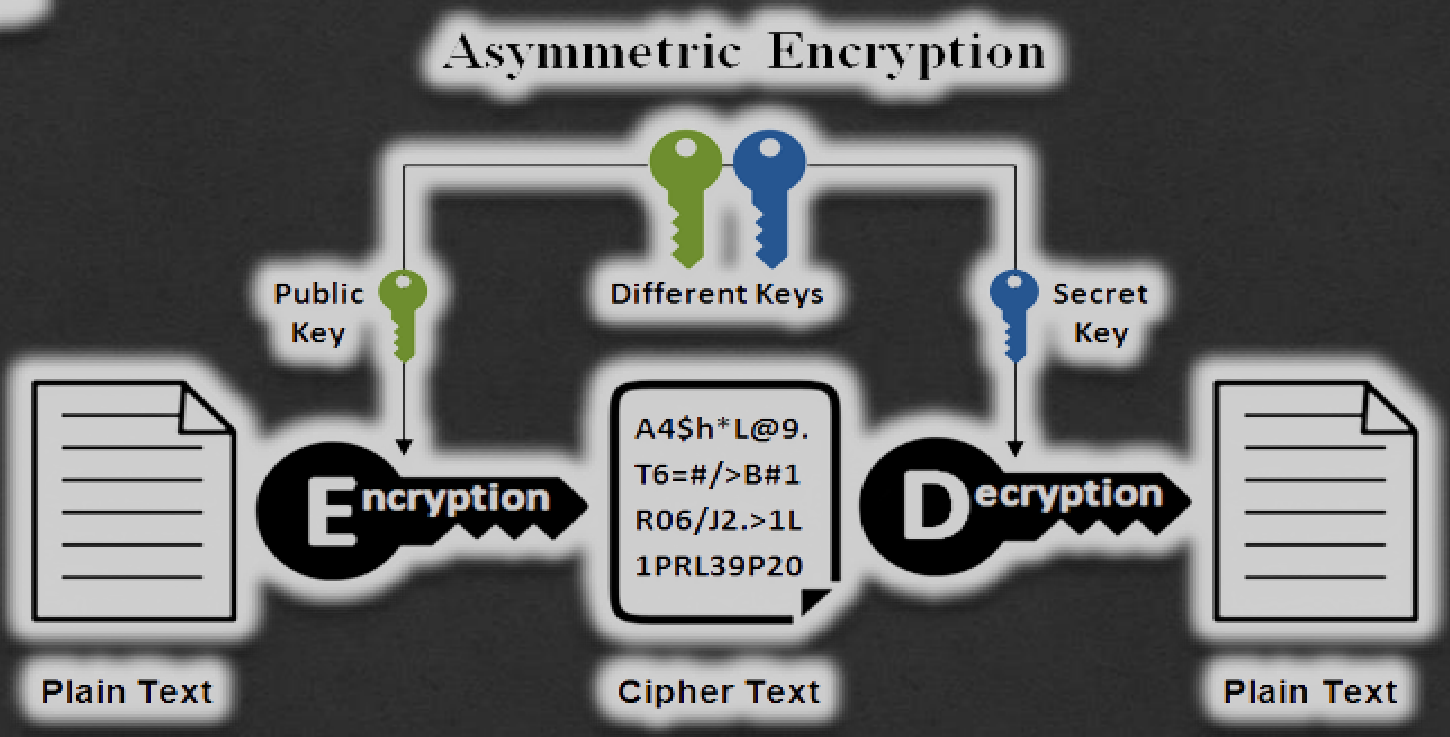
▪ Symmetric Encryption:

In this method, the same key is used for both encryption and decryption. The sender and receiver must share the secret key securely. While it's relatively fast, the challenge lies in securely exchanging the key.



Asymmetric Encryption :

This approach uses a pair of keys, a public key for encryption and a private key for decryption. Anyone can use the public key to encrypt a message, but only the owner of the private key can decrypt it. It's widely used for secure communication and digital signatures.

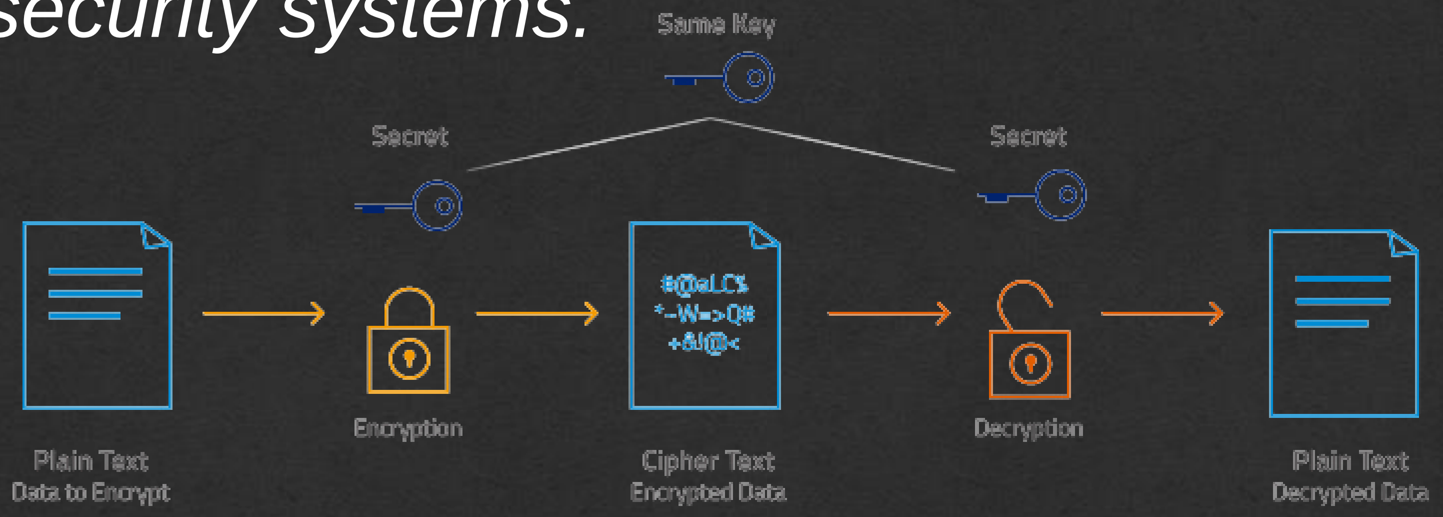


▪ RSA:

One of the most widely used asymmetric encryption algorithms in modern cryptography. As an asymmetric encryption algorithm, RSA uses a pair of keys, a public key and a private key. The public key is used for encryption, while the private key is used for decryption. The keys are mathematically related, but it is computationally infeasible to derive the private key from the public key.

▪ AES:

AES, a widely adopted symmetric encryption algorithm, is renowned for its robustness and efficiency in securing data transmission. Employed in modern cryptography, AES is designed to safeguard data confidentiality during transmission and storage. Its applications encompass securing sensitive data in communication protocols, VPNs, disk encryption, wireless networks, and other critical security systems.



m.manzoor@studenti.unisa.it
https://github.com/Umairmanzoor5
www.linkedin.com/in/muhammad-umair7/

DES:

In the past, DES served as a widely used symmetric encryption algorithm for securing sensitive data and communications. It utilized a 56-bit encryption key and operated on fixed-size data blocks of 64 bits. However, due to its susceptibility to brute force attacks, AES has largely replaced DES as a more secure alternative.

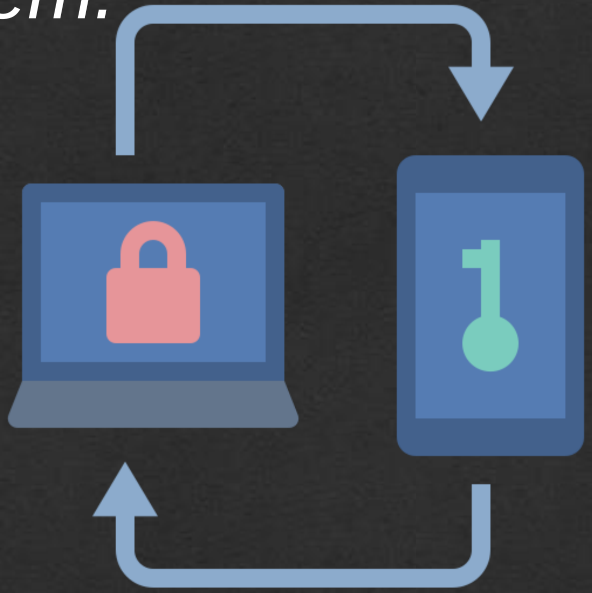
Authentication:

Authentication is a security step that requires a login code in addition to your username and password also known as Two-factor authentication. In the digital world, authentication is a crucial aspect of security, as it helps protect sensitive information, resources, and services from unauthorized access.

- Multi-Factor Authentication (MFA)
- Token-based Authentication
- Biometric Authentication
- Device Authentication

▪ MFA:

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.

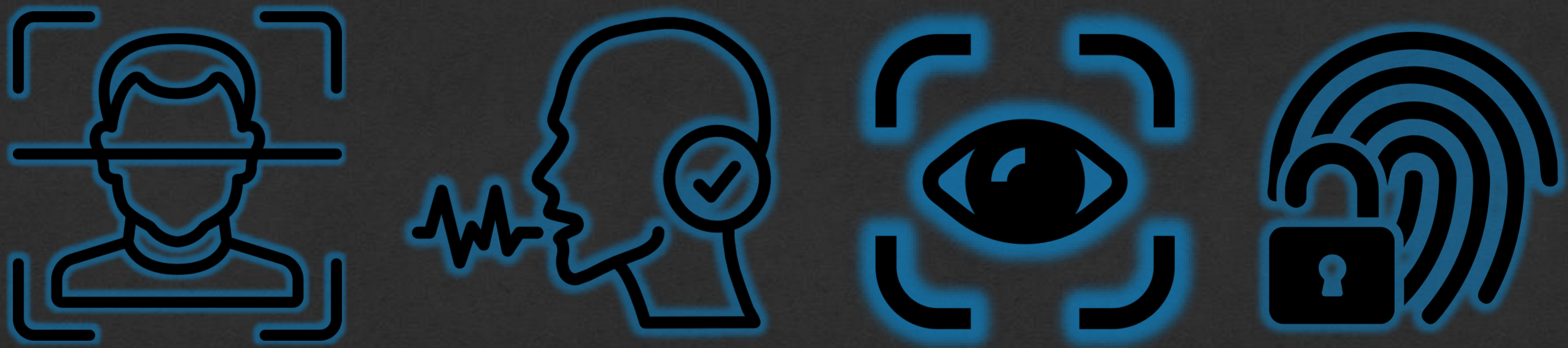


▪ Token-based Authentication

Tokens are used as temporary authentication credentials. These tokens are often generated by an authentication server and are provided to users for a limited time. They can be used to access certain resources or services without requiring the user to enter their credentials repeatedly.

Biometric Authentication

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. Biometric authentication uses unique physical or behavioral characteristics of an individual to verify their identity. Common biometric methods include fingerprint scanning, iris or retina scanning, facial recognition, and voice recognition.



✉ m.manzoor@studenti.unisa.it
https://github.com/Umairmanzoor5
www.linkedin.com/in/muhammad-umair7/

Result:

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.

▪ Doodle Based Authentication

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.

✉ m.manzoor@studenti.unisa.it

https://github.com/Umairmanzoor5

www.linkedin.com/in/muhammad-umair7/

Result:

Doodle-based authentication was not a widely recognized or established authentication method. It use of augmented reality in the authentication process, where the proposed technique is more useful, usable, and secure than extant authentication methods. The system records the user's doodle strokes, speed, and possibly other behavioral traits during the drawing process. The system employs machine learning algorithms or pattern recognition techniques to assess the similarity between the drawn doodle and the stored template.

Result:

Doodle passwords are difficult to decrypt due to the huge variety of possible doodle shapes, and augmented reality, a technological breakthrough, can serve as both a humorous and effective authentication tool. However, in the experimental results, we observed a prevalence of negative outcomes rather than positive ones when utilizing doodle-based authentication.

Mutual Authentication

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. In traditional one-way authentication, only the server is verified by the client, whereas mutual authentication ensures that both the client and the server authenticate each other, creating a two-way trust relationship, typically by exchanging digital certificates.

✉ m.manzoor@studenti.unisa.it
https://github.com/Umairmanzoor5
in www.linkedin.com/in/muhammad-umair7/

▪ Mutual Authentication

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. To engage in VR environments, the user sends the certificate authority their pseudo-identity, public key, and personal 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.

Mutual Authentication

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. Blockchain-based mutual authentication is secure. Mutual authentication finds practical application in various online activities such as online banking, digital currency trading, and NFT transactions.

Recommendations:

- *Offer recommendations for VR developers and users to enhance security:*
- *Regular security audits and updates of VR software.*
- *Educating users about potential security risks and best practices.*
- *Collaboration with security experts to address vulnerabilities.*

Conclusion

Virtual Reality technology has rapidly gained popularity, but it also poses serious security risks. Our systematic literature review identified several security issues including data privacy, hacking, and malware. It is acute that we address these issues to ensure safe and secure use of virtual reality. 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. By taking these steps, we can enjoy the benefits of virtual reality while minimizing the associated risks. 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.

✉ **m.manzoor@studenti.unisa.it**
🌐 **https://github.com/Umairmanzoor5**
in **www.linkedin.com/in/muhammad-umair7/**

Future Development:

In the future, highlight potential research areas for improving security in VR, including advancements in biometric authentication, AI-based threat detection, and secure data storage. Conduct research on a number of papers and look for a new authentication approach that is able to protect essential user data.

THANK YOU FOR YOUR ATTENTION!

Security Issues in VR: A Systematic Literature Review

MUHAMMAD UMAIR MANZOOR

m.manzoor@studenti.unisa.it ✉
https://github.com/Umairmanzoor5 🌐
linkedin.com/in/muhammad-umair7/ in