Computers & Security 128 (2023) 103127

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

A systematic threat analysis and defense strategies for the metaverse and extended reality systems

Sara Qamar[a], Zahid Anwar[b,*], Mehreen Afzal[a]

[a] National University of Sciences and Technology, Pakistan
[b] Department of Computer Science and the Sheila and Robert Challey Institute for Global Innovation and Growth, North Dakota State University, USA

ARTICLE INFO

Article history:
Received 24 September 2022
Revised 20 December 2022
Accepted 27 January 2023
Available online 2 February 2023

Keywords:
Extended reality (XR)
Metaverse
Cyber defense
Privacy
Cyber threats
Cyberstalking
Physical safety
XR commerce
Virtual reality
Augmented reality
Mixed reality
Blockchain
Cybersickness
Currency scams

ABSTRACT

With the rapid development and evolution of immersive technologies there are growing concerns of security and privacy threats to the metaverse and extended reality (XR) systems. Immersive reality solutions are a combination of multiple vulnerable technologies allowing attackers to easily undermine security. Furthermore the deployment of appropriate security controls and defensive mechanisms for resource constrained proprietary XR products has been limited. In this paper, we provide a comprehensive overview of extended reality systems and the metaverse with emphasis on technology weaknesses, cyber security challenges and users' safety concerns. Five major taxonomies have been presented in this research with an aim of identifying privacy inference vectors and potential cyber threats; determining the impact on human health and the extent to which cyberstalking, and digital currency scam activities proliferate when using XR. This research also proposes strategies for primary lines of defense and provides recommendations on the adoption of safety measures.

1. Introduction

Extended reality (XR), also known as *cross reality* refers to all kinds of immersive technologies, their related human-machine interactions, environments such as the metaverse that rely on these and the use of spatial computing that enables and optimizes actions in these systems. XR technology merges the physical and digital world, and blends together concepts of *virtual reality (VR), augmented reality (AR), mixed reality (MR)* (Chuah, 2019) and the *metaverse* (Lee et al., 2021a). XR is considered as the next generation of computing (Chuah, 2019; Fast-Berglund et al., 2018) and experts claim that enabling immersive experiences is the next revolution in technology. XR devices are wearable computers that are mobile and are equipped with processors, storage media, and can transmit and receive data with collaborating entities. The emerging XR applications as discussed in Table 1 are nearly functional in every field of real life. XR applications require access to large volumes of streaming data to effectively perform their operations. The sensitivity of data acquired by XR applications includes*individual's physical appearance, biometric data including iris identification, pupil and gaze tracking*. The gathered data can reveal details of social activities, assets, lifestyle, home interior, and occupation of users. The significant growth of XR applications by a variety of technology firms and the sensitivity of information collected has given rise to new as well as aggravated existing types of cyber-attacks, privacy breaches, data exfiltration activities, account hijacking, and ethical risks. Moreover, XR raises concerns of physical safety, motion sickness, digital sovereignty, breach of individuals' virtual identities, and misuse of personal information and interlinked technology (Ko and Rogers, 2021; Schuemie et al., 2001).

1.1. Evolution

The development of immersive technology first started around the 1960s, when the first headset was created by a scientist named *'Ivan Sutherland'* (Marr, 2022). In 1975, *'Myron Krueger'* implemented a *Videoplace* which was a combination of video cameras

* Corresponding author.
E-mail addresses: 13msccssqamar@seecs.edu.pk (S. Qamar), zahid.anwar@ndsu.edu (Z. Anwar), mehreenafzal@mcs.edu.pk (M. Afzal).

https://doi.org/10.1016/j.cose.2023.103127
0167-4048/

Table 1
XR applications.

Health Care	XR devices are used to train health care specialists by providing an interactive 3D view of organs. The latest XR technology aids to perform surgery, treating phobias, helps doctors to monitor patient's health remotely(Hu et al., 2021; Lütkebohle, 2008). Specialists using HMD can render patients' infections, tumors, etc. in 3D to visualize medical conditions (Shinde et al., 2021). XR applications assist in hospitals e.g. to perform robot-assisted (Zhongming et al., 2021) operations(Paul et al., 2019a). XR technology also assists in stress-management therapies, to treat people with disability and is proved beneficial to provide treatment of mental well being (Matthews et al., 2021) (PwC, 2019a).
Disaster Management	XR is used for disaster management (Alizadehsalehi et al., 2020), XR creates a safe environment, to train users and employees for emergencies like firemen, etc., to rescue huge buildings by generating a simulated environment for firefighting team (Chen et al., 2021). *NIST* is designing virtual simulations for firefighters, military operations, law enforcement officers to operate and practice for emergencies (Bagchi, 2021; Orr, 2021; Ost, 2021; Public Safety Communications Research Division, 2021).
Defense	XR is used to train warriors and armed forces. The US army is acquiring XR devices to train their forces (Hu et al., 2021), They ordered *HoloLens* headsets and HMDs to coach military operations and pilots (Samsung Display Newsroom, 2021).
Prototyping	XR technology is the business need for rapid prototyping and design of complex expensive products including automotive vehicles, air crafts, drones, parachutes, military equipment, etc. Now the XR technology is used to train drones, UAVs, and to control air flights as well Sabet et al. (2021).
Malware Analysis	XR solutions are used to simulate cyber threats, attacks, and malware propagation (Chuah, 2019; Dall'acqua and Gironacci, 2019).
Handicap Learning	XR applications are designed by creating an environment for people with disability (Andrade and Bastos, 2019a; Paul et al., 2019a; 2019b) to ease their learning capabilities. The online education trend is expected to reach $10 trillion by 2030 (Top elearning trends 2022 New perspectives on proctoring technology, 2022) and the use of AR/VR technology is playing a major role.
Sports	XR sports simulators have been designed where an AI-based trainer, coaches movements (VR Motion Learning GmbH and Co KG, 2020)in a virtual environment. *Pregame Golf* (TrackMan, 2020) Simulator helps users to practice games in a designed virtual golf course. Oculus designed *VR tennis* trainers, coaches consumers in virtual tennis courts with players. Desk (2020)
Games	XR gaming industries of Asia-Pacific region are expected the fastest growth, according to the *CAGR 2020–2030*(PwC, 2019a). Futuresource Consulting VR report shows that the share of gaming industry is about *34%* and in 2021 the *95%* of *$9.4 billion* spent on VR content was on gaming sector (Mordor Intelligence, 2021; PwC, 2019a). Facebook Oculus also acquire *Sanzaru Games* to broaden its VR gaming portfolio (Global - extended reality market, 2020). An virtual kitten using virtual economy was sold for *$170,000*. In a game, named *Entropia*, a digital nightclub was sold for $635,000 (McFadden, 2020; Vr in gaming market size share and impact analysis, 2020)
Repair & Maintenance	XR technology plays a major contribution in the repair and maintenance of industrial products, for efficient identification and analysis of problems. XR solutions overlay technical details and highlight damages during repair and maintenance with the product details and relevant information (PwC, 2019a).
Retailers	XR technology also offer retailers and assist them extensively with virtual house tours and virtual fitting rooms. XR applications guide consumers about buildings architecture, furnished stores and consumers can virtually immerse themselves inside hotels, rental places, and buildings infrastructure. XR applications have created ease for real estate management by facilitating tenants to visit properties remotely (PwC, 2019a).
Business	The demand and growth of the online business is increasing as it reduces the distance barriers, real cost of infrastructure, equipment, machinery, transportation involved to conduct a business (Panagiotidis, 2021). Costumers can try, touch, and sense the quality of products using virtual haptic devices(Kumar, 2020).
TV & Films	Production companies and film studios using XR technologies could merge real and studio environments, render content and actors in an immersive environment with virtual projection mapping. The number of VR movies has been launched to watch using VR glasses in 2021 (Sensorium Corporation, 2021). Netflix is also planning for virtual content by integrating Oculus headsets by Facebook. Roblox signed a deal with Sony Music Entertainment to present live virtual concerts for its XR consumers (Robertson, 2021). 36 million people watched the live virtual concert of Lil Nas X using Roblox (Roblox Corporation, 2021).
Flight Simulator	Microsoft's Flight Simulator (MSFS2020) mirrors real-world surroundings and aerospace including the clouds, aviation system, airports, satellite information, air traffic controls with real-time weather systems for consumers to interact and travel in immersive environment (Microsoft Game Stack Team, 2021; Microsoft Xbox, 2021).
Sales	The XR applications overlay product information on real objects for its buyers. The study shows that *61%* of people use XR to visualize outfits before buying and the statistics show that the consumers of extended reality mostly use devices to try on clothes virtually, to take decisions before buying online, to travel virtually, and to learn new skills (Steele, 2021; The future of community media is extended reality, 2021d). VR technology also assists in salesperson training by creating problematic situations like dealing with harsh customers, robberies, etc (Nichols, 2022).
Tourism	XR applications allow consumers to explore museum and historical places in 3D and overlays digital information on real objects. Softengi's VR tour allows users to visit museums virtually from any physical location (The future of community media is extended reality, 2021d).
Agricultural	Softengi created an application for Zerno, a farming and agriculture magazine, which facilitates users by overlaying more digital information on magazine content and agricultural machinery (The future of community media is extended reality, 2021d). Many other immersive solutions for farming and agriculture are available like farmxr, Agriculture from EON-XR (Agriculture EON merged XR orchids experience, 2021c; Using spatial computing to combine the real world and the digital world, 2021j) which provides details regarding the latest farming techniques, hands-on training, crop details, stock management, and machinery usage.
Nuclear Plant	Power plants manufacturers and experts spend millions of dollars to create a simulating environment, especially for training. XR has provided a cost-effective solution by creating an immersive virtual nuclear power control room (Nichols, 2022).

and projectors to build a VR world. This research then witnessed rapid development and a variety of XR applications (Reiners et al., 2021a) started to became available for iOS, Android, Windows, and Mac operating systems. Subsequently, the term, XR, started to gain popularity and after 2010 various industries began to establish their XR product lines globally (Mordor Intelligence, 2021). A real impetus was witnessed in 2014 when companies such as Facebook, Sony, Samsung and Google started releasing their own VR head-mounted displays or headsets. Today this technology is mainly recognized through its use of these iconic headsets that are capable of providing a 360-degree view of virtual environments or immerse users in 3D video. In 2016 Microsoft implemented its *HoloLens* headset based on mixed reality (CHRP-INDIA, 2021) which gave rise to previously unseen experiences that combined physical and virtual objects to co-exist. Today, XR solutions are freehand involving see-through displays that render visuals and controls such as menu icons and feedback cues in mid air (Becker et al., 2019). A large number of sensors and displays are embedded in XR devices allowing them to analyze sensors' inputs and generate appropriate responses to the display as output for an immersive experience. XR devices are constructed so as to generate emotions, feelings and then capture those emotions through sensory systems attached to the human body giving the realization that the user is present in an immersive world. Vibro-haptic and thermo-haptic sensors designed into these devices work by generating vibrational and thermal sensations in the virtual world so that the human skin receives a feeling of physical touch (Ko and Rogers, 2021). Seamless interactions of consumers in the digital world with digital entities rely on XR's increasing sophisticated computer graphics (CG) and expanding bandwidth that allows for realistic object rendering. XR products are refining their usability, performance, efficiency, and productivity at a rapid pace (Gandhi and Patel, 2018a; 2018b; Group, 2021; Muñoz-Saavedra et al., 2020; Techliance, 2021; VirtualSpeech, 2021).

1.2. Security and privacy concerns

The widespread acceptance and rapid development of a plethora of XR applications creates physical, mental, social, and economic security concerns. The large number of elements contributing to this technology are riddled with a variety of vulnerabilities (Sillaber et al., 2016) which pose both existing as well as novel threats to security and privacy of users. Particularly threats involving XR data breaches can be quite stealthy, because they don't require users' input (de Melo Silva et al., 2016) making timely identification a major concern of hi-tech companies and government agencies (Abu et al., 2018). Availability and security of data at rest and in transit between XR devices and applications is a key requirement in order to be able to operate, maintain synchronization, and provide seamless interactions between consumers. XR technology's attack surface is therefore larger than that of traditional computers such as desktops and servers. As XR evolves, this attack surface will expand further and provide cyber criminals previously unseen opportunities to perfectly impersonate users, steal identities and undermine privacy. Before more and more XR technologies (Dick, 2021b) can meld together and multiply the impact of a single breach by effecting other integrated components it is necessary to build security into the design from the onset. It is necessary to devise defensive measures to promote responsible design, development, and safeguards to counter XR's potential vulnerabilities and threats.

1.3. Inherent challenges to securing XR systems

The major hurdles to addressing XR's security limitations using traditional security mechanisms are discussed in this section. XR gadgets are built using sophisticated hardware equipment resembling the Internet of Things (IoT) and are therefore constrained devices requiring high bandwidth network connectivity and access to cloud infrastructure for providing services. Due to memory and bandwidth constraints embedding complex security controls is challenging. XR systems employing multiple interlinked technologies allowing vulnerabilities of a single component to impact the entire XR ecosystem. Security and privacy measures are not taken into consideration with the rapid pace of development of various XR devices, applications and haptic controls due to a highly competitive market. Existing regulations don't cover XR technology and the lack of globally accepted standards further contribute to security and interoperability issues (Ko and Rogers, 2021; Schuemie et al., 2001). The current intrusion detection and prevention (IDS / IPS) techniques are not effective in protection of the latest immersive technologies (Happa et al., 2021a). Repositories for reporting security vulnerabilities are nonexistent and security measures are either not enforced or applicable due to the lack of regulations particular to XR. Limited policy guidelines are available for XR consumers, application developers, device manufacturers, and stakeholders to cater to emerging security threats.

The metaverse not only inherits and in many cases amplifies existing vulnerabilities and cyber attacks that have plagued the internet but also suffers from previously unseen attacks stemming from its use of immersive reality. The metaverse attack surface is huge due to interlinked technologies and provides attackers a variety of opportunities to exploit. The metaverse accessories including cameras, sensors, actuators, and many more, are attached to the human body which control real personal, mental, physical, and environmental data, and further the attacker can infer this knowledge to launch intrusive privacy attacks. The gathered users' personal information can then be used for profiling, and to generate revenues through customized advertisements. Real-life accidents can be planned by altering the input/output streams of XR devices used in sensitive domains like military, disaster management, health care, etc. The prolonged use of the metaverse negatively affects human health and psychology, causes cybersickness, addiction to the immersive world, and disassociates users from reality. The metaverse is used to trade physical and digital assets such as immersive property using crypto-currency, which leads to financial crimes, money laundering and currency scams. Even virtual sexual assault, abuse, and bullying is at a whole new level as compared to internet based cyber bullying because the metaverse allows for a fully immersive world and very close and life-like encounters. Cyber laws are lacking in their coverage of immersive crimes, misbehaviors, frauds and deep fakes. An in-depth analysis on potential threats is performed in Section 5.

1.4. Contributions

In this research, four major and trending immersive XR categories are considered namely VR, AR, MR, and the metaverse. A comprehensive analysis is performed pertaining to attack surface, cyber threats and potential attacks on XR applications. To identify security loopholes a thorough review is conducted of published articles, book chapters, conferences, interviews, web blogs, invited talks, expert opinions, and universities affiliated research. Existing surveys in this area are limited because of challenges in investigating such a new and emerging area, technologies being of proprietary nature and relatively closed to the public and research community and non-existent threat and vulnerability repository specific to XR. Related surveys that exist either only address a small subset of the entire XR space or focus mostly on issues not directly pertaining to cyber security and privacy. Other non-survey-based articles discuss XR security concerns related to very specific

XR applications. A detailed comparison of this research with existing works in this area is detailed in Section 4.

To the best of our knowledge, this paper presents the first systematic analysis of XR security and privacy concerns that highlights XR vulnerabilities, potential cyber threats, attacks, threats to human physical and psychological health, unethical and illegal issues in the immersive world, and currency scams. A panoramic view is provided of the challenges faced by the security community on addressing these concerns, along with opportunities for defining appropriate robust XR defensive mechanisms. Hence, we contend that our taxonomies will aid in visualizing the XR threat diversity in research, and in making informed decisions when devising new detection and defense mechanisms. To address these security concerns and to monitor XR threats in real-time, insights into the latest in XR defense mechanisms and safety measures along with recommendations are provided in the proposed research.

The rest of our work is organized as follows: The Section 2 discusses the emerging XR trends, the impact of the metaverse on economic growth, and the latest immersive projects. Section 3 introduces the base technologies of immersive reality, including augmented reality, virtual reality, mixed reality, and the metaverse. Section 4 provides a comprehensive review of the available research articles on related security concerns. Section 5 elaborates on a variety of cyber threats to the metaverse and XR community, including privacy inference, vulnerabilities, data breaches, unauthorized access, e-frauds, unavailability, integrity violations, and network attacks. The paper further presents the XR threats to human physical and mental health in Section 6. The unethical concerns are raised in Section 7, currency scams are highlighted in Section 8 and legal concerns are brief in brief in Section 9. Finally, our work concludes the research with possible defensive solutions and recommendations against emerging XR threats in Section 10.

2. XR Applications and market trends

Advancement in Extended Reality (XR) technology is transforming the way users interact, collaborate, conduct business, and play. Currently, 52% of businesses around the globe are working on extended reality (Kumar, 2020; PwC, 2019a). The demand for XR technology initially received considerable hype from the media and the gaming industries, but today it is widely accepted (Chuah, 2019). The need for social distancing during the COVID-19 pandemic further boosted XR demand owing to the wide range of apps supporting virtual meetings, conferences, immersive gatherings, and exhibitions across the globe. Industries are now launching their products virtually and encouraging online participation of their customers from remote locations (Kwok and Koh, 2021; Ong et al., 2021). The expansion of cellular network for supporting 5G and 6G will further contribute to the growth and access of XR applications. According to the PwC economist (PwC, 2022), the global XR market worth in 2019 was *$46.4 billion* and is estimated to reach *$206.5 billion* in 2022 and *$476.4 billion* by 2025; a compound annual growth rate (CAGR) of *62%* between 2020 to 2025 (PwC, 2019a; 2019b). XR technology is expected to contribute $1.5 trillion to the global economy by 2030 by transforming businesses and creating 23,360,639 new jobs (PwC, 2019a), as shown in Fig. 1.

The XR sector has led to economic growth in several different types of industries as illustrated in Fig. 2. The expected GDP boost in the *disaster management* and *training* sector is expected to be *$294.2 billion (0.34%)* by 2030 (PwC, 2019a). In health care and prototyping the estimated economy growth is expected to be *$350.9 billion (0.41%)* and *$359.4 billion (0.42%)* respectively (PwC, 2019a). The XR gaming market is projected to be US$ 405.723 billion in 2030 with a CAGR of 31.4% (Vr in gaming market size share and impact analysis, 2020). The economy boost to tourism is expected

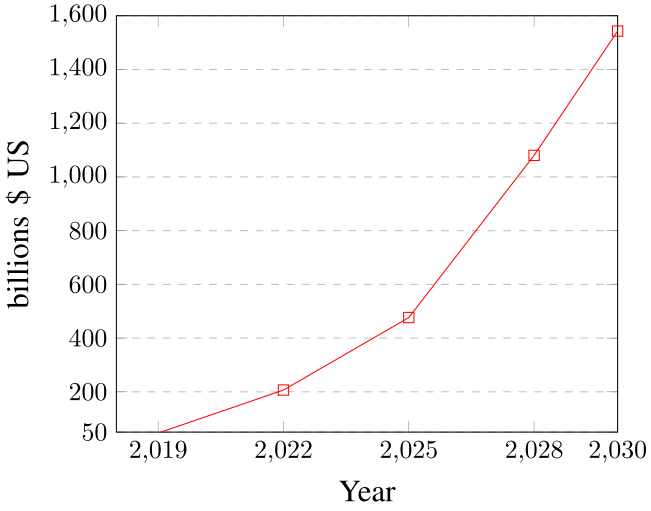

Fig. 1. Expansion of XR global market over time (Section 2) .

to be US$304.4 million by 2023, by a CAGR of *32.5%* (Global AR VR in travel and tourism market, 2020). Finally it is expected that online businesses would receive the most impetus with revenues being greater than $1,274.4 billion in 2030 (Kumar, 2020). Aside from the major industry sectors indicated above, XR technology is also becoming very popular in the fields of fluid dynamics, education, training, storytelling, virtual shopping, immersive social networking, virtual house tours, media content animation, digital studios, virtual travel, driving simulation, complex vehiclar design, virtual fitting rooms, telepresence, building and interior design, digital studio, tourism in a virtual setting, sports coaching, military defense, architecture, amusement, flight simulation, behavioral sciences, surgical procedures, and many more.

2.1. XR projects

Several innovative projects based on XR are worth mentioning here. Meta's *Reality Labs* and the EU's *VRTogether* are making efforts to render a photorealistic view of objects and avatars during an immersive session (Matthews et al., 2021). The Meta team is also working on *Codec Avatars* which is based on high-resolution image gathering techniques to generate a photorealistic view of consumers' avatars (Rubin, 2022). Meta has built *Sociopticon technology* which helps *Codec Avatars* replicate real

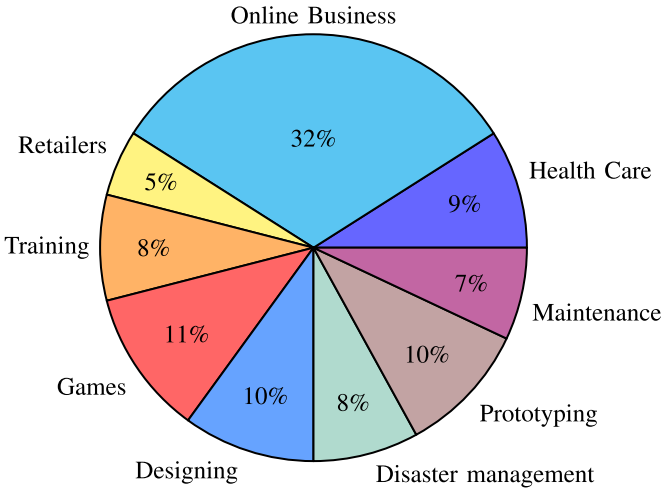

Fig. 2. The XR sector's estimated economic contribution by 2030 broken up by industry type (%) (Section 2).

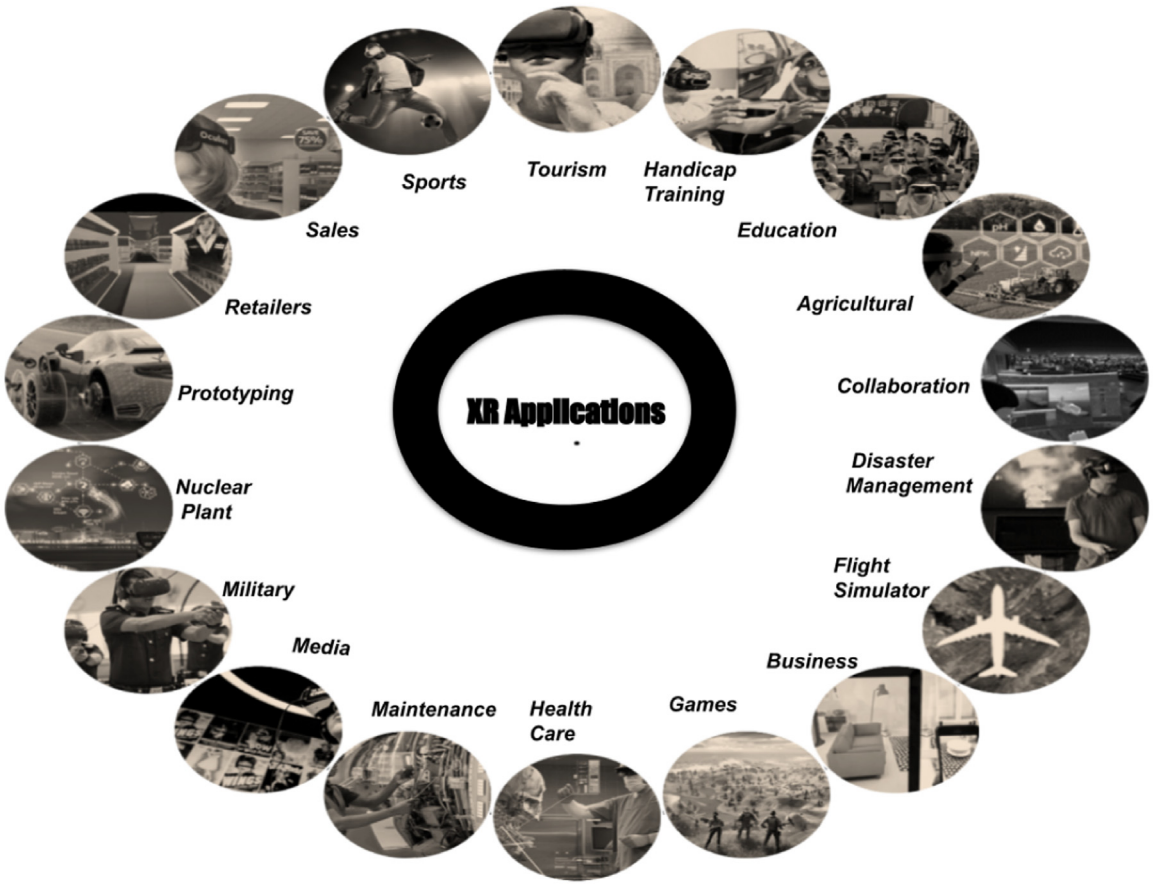

Fig. 3. XR applications (Section 2).

body movements and mirror clothing effects (Matthews et al., 2021) using 180 ◦ high-resolution and high-frame-rate cameras. Loom ai (2020) allows privileged users to create 3D avatars using their selfie. The *Spaces* project (Baker, 2020a; 2020b) allows hosting of virtual meetings to facilitate users with virtual whiteboards and individuals avatars that depict facial and body movements with audio cues. MeetinVr (2020) is a mixed reality application that merges real and virtual objects to provide a platform for users to attend 3D fully immersive remote sessions, build personalized avatars and integrate virtual 3D drawing applications. Using *AltspaceVR* (AltspaceVR, 2022a; 2022b) users can collaborate and co-present in small scale live virtual events. *Oxford Medical Simulation* is a 3D simulated environment designed to train medical specialists and facilitate users with either virtual reality HMD or with regular PCs (Helping you transform healthcare training, 2022). *Sketchbox* conducts online immersive training and assessments (Helping you transform healthcare training, 2022). Some popular XR applications available in market include but are not limited to Facebook 360 (Facebook, 2021b), Horizon Workrooms (Meta, 2021), Google's Expedition (Johnston et al., 2019), Google earth (Lisle, 2006), YouTube VR (Youtube VR, 2021e), Sense Glove (Perret and Vander Poorten, 2018), ROAR (Augmented reality campaign, in just few steps, 2021), Google Lens (Shapovalov et al., 2019), IKEA Place etc. A summary of important application areas of XR technology are discussed in Table 1 and are represented in Fig. 3.

3. Immersive technologies

For their proper functioning and to provide an immersive experience, XR hardware and software applications rely on a variety of technologies including but not limited to cloud-based remote rendering, multi-user collaborative environments, personal computers, smartphones, head-mounted displays, sensors such as sensory gloves, and other input devices (xrcollaboration, 2021). To collect useful environmental information, XR devices comprise multiple sensors such as cameras, motion trackers, and depth monitoring systems. Certain inward-facing sensors are used for gaze tracking, iris identification, collecting audio information from the attached microphone, tracking users' activities, interaction with others, time spent, and routine followed. As the technology upon which XR relies improves with time for example the miniaturization and enhanced connectivity of sensors it further enhances the realism of presence in the virtual world and interaction with virtual objects (Dick, 2021a; Ko and Rogers, 2021). This provides novel means of virtual sharing, collaboration, learning, spending, marketing, and living. Details of relevant immersive technologies are detailed in the following subsections.

3.1. Virtual reality

In virtual reality (Alraizzah et al., 2017; Anthes et al., 2016a), the end-users immerse themselves in an artificially created virtual world that shuts out the real physical surroundings. The level of environment immersion can be set to one of three settings namely: non-immersive, semi-immersive or fully-immersive. Immersive rooms are available to support virtual scenes, and *"avatars"* (Anand, 2017) may be used to represent real users in the virtual environment, and interaction with other users is typically enabled. The virtual sessions could be launched in a stationary environment where users remain seated or standing in a single posture and are also available in a room-scale environment where

users could move across the entire physical room during the virtual session. Multiple parties can collaborate in real-time and they all must receive identical information during an immersive VR session. The actions and responses of VR users must be synchronized and should be reflected in the digital world at low latency. *5G* networks or even more advanced communication technologies are recommended (Siriwardhana et al., 2021) for providing 3D rendering in the collaborative virtual environment with high bandwidth, high throughput, seamless interaction, and low jitter. Web-based virtual environments are also available.

VR devices create an environment which responds similarly to a realistic situation (Alqahtani et al., 2017; Anthes et al., 2016b; Schroeder, 1993) like for example *artificial wind* with high-quality, high-resolution impressions allow for the user's senses to preeive an outdoor setting. The basic VR device *'Window on World (WoW)'* is a desktop-based VR solution in which the user sees a virtual 3D world through the desktop and navigates within it using a mouse. On the other hand a *'Head Mounted Display (HMD)'* provides an immersive world for users with *stereoscopic* view of the user's sight with respect to its physical location. HMD's typically feature *spatial audio* and have *accelerometers* and *motion tracker* installed to track the position of users in the virtual world. *'Sensory data gloves'* based on fiber optics gauge finger movements to sense virtual objects during immersive interaction such as grabbing, drawing, throwing. ' *Controllers'* such as *joysticks, touch pads, data gloves, trackpads, bodysuits,* and *treadmills* are used as input devices. Numerous types of navigation devices such as *omnidirectional treadmills (ODTs), slide mills* are available for generating an illusion of movement in virtual space. *'Magnetic tracking'* technology is used for body tracking, posture tracking, gesture tracking of a person in a virtual environment. Output devices are used to generate an immersive feeling involving visual, auditory, and haptic displays.

In virtual reality, tracking features must be *low latency* and *accurate.Predictive algorithms* are used to synchronize users' physical and virtual movements. The concept of *three degrees of freedom 3DoF* or orientation tracking allows privileged users to perceive a 3D virtual environment without having to move physically in that environment. The users' physical movements are not tracked by 3DoF headsets, and they can only move in a 3D virtual environment by the means of *controllers* or *joysticks* like in the cases of watching a 3D movie or playing 3D video games. On the other hand *six degrees of freedom 6DoF* HMDs can map physical body movements to digital environments and can track users' position in real-time with the help of a *gyroscope* for tracking. The users using 6DoF HMDs can move in the virtual world in the same manner they would move in their real physical world. They may rotate, move forward, backward, up, down, left, and right in the virtual environment. 6DoF HMDs use sensors to track *"inside-out"* and *computer vision* technology to track these movements (Barnard, 2019; Baskette, 2022).

3.2. Augmented reality

In Augmented Reality (AR) (Azuma, 1997), the clients' physical environment is overloaded with virtual objects. While AR can't replace the actual environment, by embedding or rendering digital elements over the physical surroundings AR devices make both physical and virtual reality appear to a user's real sight. AR technology involves environmental understanding, motion tracking, and light estimation. In comparison to VR, AR devices (Behzadan et al., 2008) require less hardware. Typically a smartphone containing a processor, GPS, tracker, display, camera, microphone and touchpad are all the key elements needed for AR rendering. Commonly used AR devices include but are not limited to *smartphones, laptops, glasses, AR headsets, tabletops* (Roo et al., 2017) *and ceiling projectors* (Xie et al., 2016). Achieving a lightweight seamless interaction between physical and virtual objects is the key challenge of AR solutions. The latest AR headsets render 3D objects directly in front of the user's sight or on top of the user's head (LaViola et al., 2017; Lee and Hui, 2018), without occupying his hands and provide feedback cues just like in science fiction movies.

3.3. Mixed reality

Mixed Reality (Billinghurst and Kato, 1999; Milgram and Kishino, 1994; Speicher et al., 2019a) also known as *"hybrid reality"*, is an amalgamation of real and virtual worlds, where the user interacts with both. MR employs technologies related to *image processing, cloud-based rendering, 3D motions, vision tracking, spatial mapping, anchors for environmental judgment, eye tracking, hand movement recognition and speech input*. Mixed reality (Speicher et al., 2019b) merges 3D graphics with the real view, allowing users to interact with virtual objects in the real world. Thereby a user can walk in a virtual world that has real surroundings. In addition, MR causes users to experience *audio, spatial stimuli, haptics, noises, smells, physical stimuli, wind, temperature, geolocation, motion, and interactions* with other real and virtual members. In Mixed Reality, the virtual elements interact with and respond to the real physical environment. MR is also bound to use specific hardware such as the HoloLens (Microsoft hololens Mixed reality technology for business, 2021c) which superimposes virtual information over the real view. Among all immersive technologies MR technology and devices are in the most high demand and are the most marketable (Alizadehsalehi et al., 2020). MR shares goals and is considered as a first step towards the development of the metaverse as discussed in the next section.

3.4. Metaverse

The term "Metaverse" (meaning "beyond universe") is derived from two words, *"Meta"* and *"Universe"*. Metaverse technology is a blend of the digital and real-world, considered as a *"shared virtual space"*. Constructed on top of the pillars of XR (Ning et al., 2021) the Metaverse allows multiple virtual worlds to become interconnected. This technology leverages the concept of creating *"digital twins"* where digital copies of actual surroundings and digital *avatars* representing real users are created for virtual world experiences (Lee et al., 2021a). Multiple digital twins can be created for multiple virtual reality environments and users can easily teleport themselves from one virtual world to another (Goodfellow, 2021). Technology companies (Tech companies aim to take over physical world with metaverse, 2021) are planning to merge virtual and augmented reality to build the Metaverse, a deep immersive digital world for individual and business purposes. It can represent users as characters that move or interact with other community members like in the gaming world while employing real-time data from the physical world. The concept of the *AR Cloud* is also commonly used within the purview of the Metaverse where the replica or twin of the physical world will allow consumers to have shared experiences. The users of the AR cloud are not just limited to access of shared videos and messages but may virtually collaborate with others for designing, learning and playing, just like in the real world. The *Metaverse* technology & concept has many other titles such as *'3D AR CLOUD', 'Mirrorworld', 'The Real World Web' and 'The Spatial Web'* (Matthews et al., 2021). The concept of Metaverse (The metaverse: The evolution of a universal digital platform, 2021) involves multiple technologies and their interactions, portability, virtual currencies, and discoveries to come into existence where users can interact, work, do their business virtually

just like in their real physical world. During the pandemic, people realized the need for doing virtual business which spurred the shift towards Metaverse technology. The *Microsoft* team is preparing for the convergence of the digital and physical worlds. *Facebook* (Zuckerberg, 2021a; 2021b) is also aiming to shift from being just a social media company to building the Metaverse and announced the change of the company name to *"Meta"*. *Facebook* is planning to hire 10,000 developers to build the *metaverse* technology (LEE, 2021a) and investing billions to accomplish this (LEE, 2021b). *Roblox* (Powering imagination, 2021) is another entertainment platform transitioning towards the Metaverse where users can have a wide variety of immersive multi-user experiences. *"Second Life"* (Linden Lab Headquarters, 2021) is another noteworthy effort towards creating a virtual online environment using the 3D browser, where users can select an available avatar in their virtual environment and interact and communicate with other avatars and objects.

4. Related work

Our research benefits from surveys that consider XR applications, technological innovations and usage best practice guidelines. The metaverse technology is still evolving and in its infancy. The research community has started working on the consequences of fully immersive reality, and we have included in this study the limited research that is available. The reader will note that these works address a small subset of the entire XR space or scrutinize challenges that are not directly pertaining to the security and safety measures. Other non-survey-based articles discuss XR security concerns related to very specific XR applications. These works are summarized below.

A survey has been conducted regarding the role of artificial intelligence in extended reality applications. The authors performed a systematic review of existing works where a combination of both AI and XR technology is used. Various applications have been identified where the intersection of AI and XR plays a major contribution such as robotics, smart homes, health care, military, virtual gaming, entertainment, and training (Reiners et al., 2021b). Lik-Hang LEE et al. (Lee et al., 2021a) present a survey on the Metaverse ecosystem, and its enabler technologies, including XR, the internet-of-things (IoT), human-computer interaction (HCI), computer vision, edge computing, AI, and blockchain which drives the concept of Metaverse towards its existence. The authors discuss the opportunities, research challenges, and limitations towards the establishment of the entire Metaverse ecosystem and further conclude that the technology requires high bandwidth, extensive computation, and massive storage. In (Doolani et al., 2020), the researchers highlighted the importance of extended reality devices and applications used for manufacturing training. The aspects of manufacturing covered in the research article include installation, assembly, cleaning, etc. Extended reality adds a layer by simulating an environment to reduce training expenses, complexities while conducting training and to ensure workers' wellness and safety. A survey paper (Matthews et al., 2021) has defined various XR technologies and applications available in the market and explains how XR technology aided users during the Covid-19 circumstances. The authors detail social platforms designed to provide a 3D social experience and that the designers of these technologies must be extra cautious of the social damages these technologies may cause in the future. Lik-Hang Lee et al. (Lee et al., 2021b) perform a survey on computational artwork for metaverse environments like avatars, virtual scenes, and elaborate the concerning privacy and security issues such as ownership and recognition of digital contents. Integrating security features consume processing power and delays the output of XR solutions. Throughput is a major concern in the metaverse environment and researchers are already working on it to reduce this bottleneck and enhance throughput rates in an immersive environment.

A three-layer Metaverse architecture has been presented by Duan et al. (2021) in terms of its infrastructure, interaction, and ecosystem. A metaverse campus prototype has also been built for students physically present in a university, where they could join virtual library chat rooms. Ning et al. (2021), compared the Metaverse development attitude of different regions including the USA, UAE and China based on industrial and economic background and interests. Regional industries developing Metaverse products are also discussed such as *Amazon* in the USA is working on "VR shopping", *Alibaba* in China is planning to launch the *"Ali Metaverse"* and *"Taobao Metaverse"* etc.

A forensic investigation was performed (Yarramreddy et al., 2018) on social metaverse applications (like the Bigscreen app and Facebook spaces), systems (like the Htc Vive and Oculus Rift), and traffic flow to discover the victims' actions in immersive reality. The captured forensic artifacts were used to reconstruct the immersive event. An attacker could easily mimic and visualize the immersive environment of the victim by analyzing the memory dump of the metaverse system. The authors show that the vulnerabilities discovered in the metaverse systems can lead to integrity violations, content tampering, and the obstruction of users' views. Further these violations can also cause cybersickness among consumers. In addition, the researchers were able to modify metaverse sessions and corresponding inputs and outputs of the headsets to launch MITM (man-in-the-middle) attacks because the traffic and data flow in the metaverse system were unencrypted. Another study (Casey et al., 2019b) has been conducted on metaverse systems to extract the personal information of clients' environments. The researchers designed an open-source plugin called Vivedump to perform a *memory forensics of metaverse systems*, which was demonstrated on the HTC Vive headset. The results show that the users' immersive environment, including their location, body postures, and immersive room setup, could be easily reconstructed from filtered memory artifacts using Vivedump's memory forensics capabilities (Casey et al., 2019b). The authors conduct a forensics analysis of Unity API and social networking metaverse applications such as Bigscreen. The analysis identified vulnerabilities such as application input sanitization flaws that permit an attacker to inject malicious code in the system. The researchers exploited the vulnerability of unsanitized input fields and injected a malicious JavaScript script which executed on the browser, and downloaded malware from online servers. The malware affected all consumers of the immersive room. The JavaScript execution and other vulnerabilities in the authentication mechanism lead to several other attacks such as phishing, eavesdropping, illegitimate desktop sharing, man-in-the-room attack (MITR) and denial of services (Casey et al., 2019a; Critical vulnerabilities in bigscreen VR app, 2021d; Vondrek et al., 2022). It is shown that Casey et al. (2019a) in a social networking application can affect millions of connected users by propagating malware to target victims' machines. The MITR attack allows an attacker to eavesdrop on users' meetings, invisibly join any collaborative sessions, enter a private chat room, and modify the contents of an immersive environment, without the XR users' permission (Casey et al., 2019a).

Jassim Happa et al. discuss certification hurdles in XR technology, the need for policy formation and suggest that ethical concerns must be addressed in the context of privacy. However they observe that there is no specific standard or privacy compliance certificate available for these immersive applications (Happa et al., 2021a). Moreover, the researchers recommend that XR policies must be designed in a way that could be applied and updated on XR solutions conveniently and address the concerns of data sharing with the third party. A report (Dick, 2021a) by *Ellysse Dick*, highlights that AR/VR devices work by integrating a variety of technolo-

gies, and operate by collecting user's personal information which aggravates privacy risks. Government regulations such as *Health Information Portability and Accountability Act (HIPAA), Children's Online Privacy Protection Act (COPPA),* should be reviewed to include privacy policies, guidelines, and standards on the collection, usage, and storage of users personal data by AR/VR devices. A report (Jerome and Greenberg, 2021) by the *Future of Privacy Forum (FPF)*, provides guidelines and recommendations to deal with users' privacy and physical safety concerns regarding XR technology. The guidelines and policies must be designed for XR manufacturers, developers, consumers, and stakeholders elaborating their rights, obligations, and responsibilities to secure individuals' data at rest and in transit. XR designers and developers must consult all stakeholders including lawmakers, advocates and non-XR users before launching their products.

5. Cyber threat analysis of XR

With the rapid development of XR technology, various novel attacks have emerged that exploit *zero-day* vulnerabilities. Extended reality devices capture a variety of information to perform their functions including *body appearances, eye movements, domicile information, heart rate, household objects, nearby places, interiors of homes and offices, bystanders, location,* build *psychological profiles* and individuals' *emotional state* using inference (Happa et al., 2021a). Users can't disassemble headset devices or don't fully understand the data sharing and scope of XR services so the majority of XR users blindly trust these while processing and storing their personal information. Furthermore the latest iterations of XR applications continue to improve product quality mainly by gathering more and more public and personal information.

5.1. XR Privacy inference

XR solutions collect consumers' information to provide an immersive experience that involves identifying the users' actual location, preferences, likes and dislikes, physical movements, etc. However an excessive amount of collected users' personal information if improperly used may lead to serious harm, introduce novel security threats and increase privacy concerns. The taxonomy in Fig. 4, shows how privacy is inferred by XR applications by analyzing consumers' behavior and their biometric data in an immersive environment. The rest of this section will elaborate upon this taxonomy.

XR headsets utilize ***brain-computer interfaces (BCIs)*** also known as *neural-control interfaces (NCI), brain-machine interfaces (BMI), direct neural interfaces (DNI), or mind-machine interfaces (MMI).* The BCIs technology allows bidirectional information flow for opening up pathways for "writing back" to the brain and translating its activity into machines. BCIs in XR incorporate sensors such as *electroencephalogram (EEG)* that permit manufacturers to build personalized applications for the immersive world that respond to users' attitudes and emotions (Jerome and Greenberg, 2021). ***Holographic image*** technology is used in the Metaverse to reproduce real 3D images of objects which can be viewed by the naked eye without using any wearable devices. *Coherent light interfaces* allow this reproduction by obtaining object information such as shape, size and amplitude (Ning et al., 2021). The latest headset technology has **inward-facing sensors** that can track eye gaze and provide pupil measurements. XR applications collect users' biometric information using **health monitoring sensors** to authenticate virtual identity, measure *heart rate* to infer users' health and fitness level, *data watched, recorded, and shared* by consumers to identify personal hobbies, likes or dislikes, *physical surroundings, current location, and motion tracking* to precisely map physical boundaries in the digital world and perform inference on collected data to gather additional information (Ko and Rogers, 2021; Schuemie et al., 2001). XR technology is also capable of capturing ***biometrically-inferred data (BID)*** which is used for determining *users' behavior, identity, personality traits, mental fitness and workload, cultural background, physical conditions, race, color, origin, skill sets, interpersonal distances* etc. XR solutions can collect information related to ***non-verbal behavior*** such as *users' physical posture, iris, eye gaze, facial gestures,* etc. XR *eye-tracking sensors* identify *area of interests (AOI) and time spent (dwell time).* XR devices allow for ***gait tracking***, used in performing analysis on *humans' movements, track muscle motion, and observe the gaze and brain activity* of consumers. Further, *gait tracking* is useful for *identifying users, diagnosing diseases and physical illness and tracking users' movements* and to determine where they are looking. These XR technologies by nature are *intrusive* and will infringe upon a users' privacy and erode the users' ability to trust immersive systems (Pearlman et al., 2021).

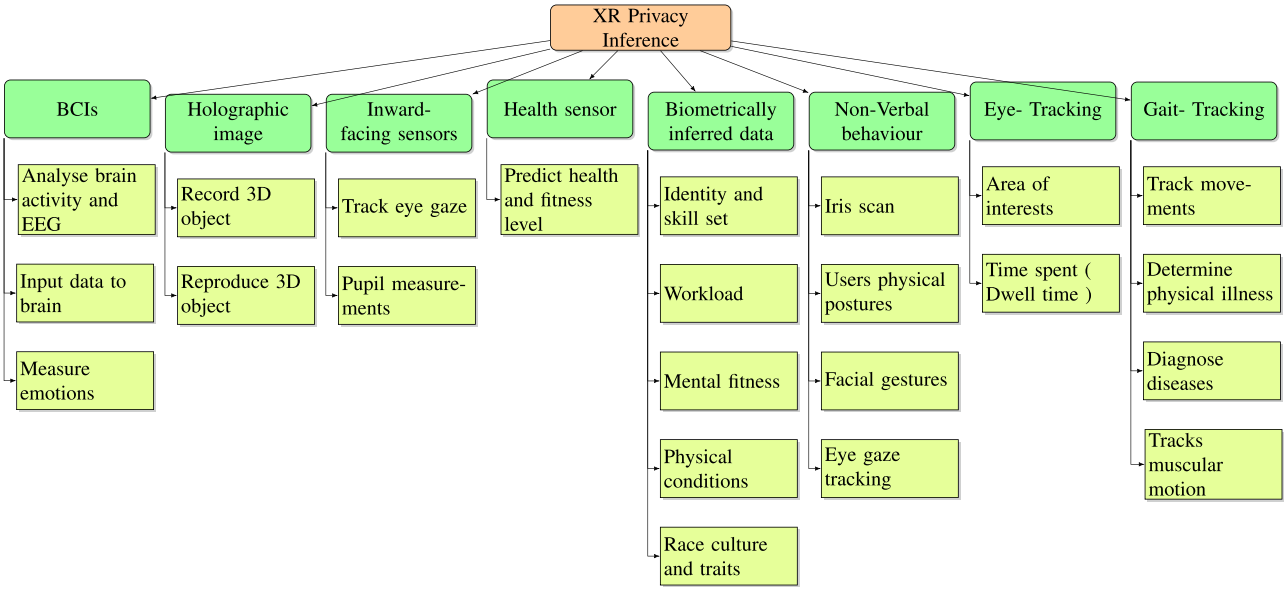

Fig. 4. Taxonomy of Privacy Inference using XR (Section 5.1) .

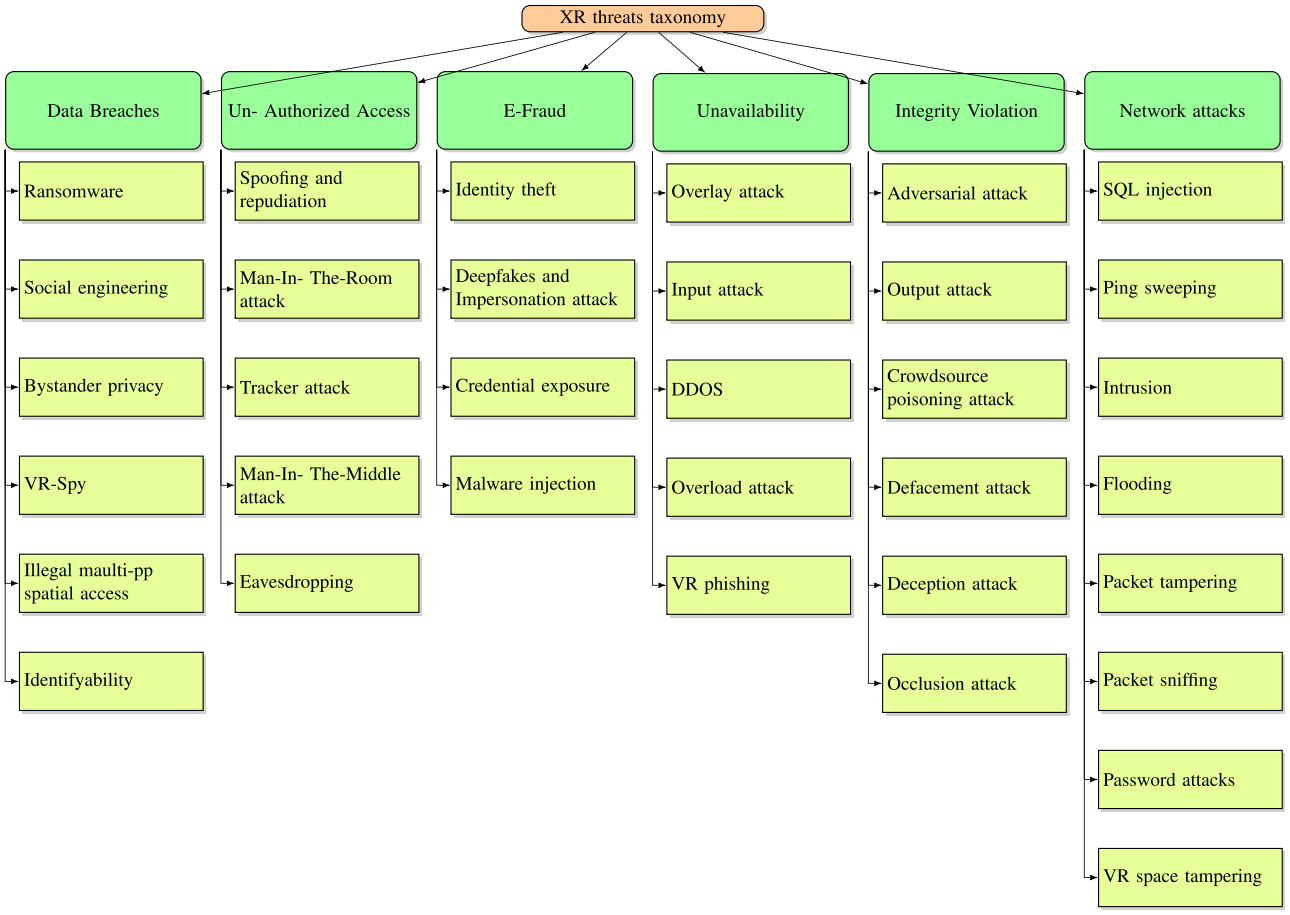

Fig. 5. Taxonomy of cyber threats/attacks on XR (Section 5.3).

5.2. Vulnerabilities in XR development platforms

While many XR development tools are available in the market only a few of them are open source. The dominant open-source platforms and frameworks used in XR application development are discussed in this section including *Unity3D, node.js, OpenXR / OpenMR / OpenVR,* and the *Unreal Engine* (Milgram et al., 1995; Reinhart and Patron, 2003). Technology enterprises such as Google, Amazon, Facebook, Microsoft, and Apple have extensive investments in developing XR solutions using these platforms. These development platforms have considerable usage for creating XR content and also have multiple reported security loopholes and vulnerabilities. Vulnerability identification and patch management for XR applications is much more challenging as compared to traditional desktop or cloud based software as several hardware, software, and operating systems contribute to providing a single XR experience. Patch updates in one software will affect all dependent modules and the management of portability and compatibility issues would be burdensome. Moreover, there currently exists no shared or centralized database for distribution of XR vulnerability information and patch updates. The few open-source available XR development platforms and recently identified security vulnerabilities are discussed in the remaining section.

The Unity Framework (Unity Power better collaboration and creativity, 2021f): Unity framework is popular for XR software development because of its extensive learning resources and support for multiple operating systems, including Android, Windows, Mac, Linux, PlayStation, Xbox, htc vive and Oculus Rift to build and test immersive interactive projects (Tyler, 2022). Unity was initially popular for 3D games development, but is presently operative in many other XR development industries like TV and Films, virtual architecture development, automotive designs and robotic simulations, etc (Goh, 2022). It is free for developers; only the professional edition requires a monthly licensing fee (Skidmore, 2020). Multiple vulnerabilities in the *Unity framework* have been reported (unity vulnerabilities and exploits, 2021) recently including *cross site scripting* (unity vulnerabilities and exploits, 2021) and *zero-day* (Zeroday disclosed in unity web player, 2021k) vulnerabilities in its web browser plugin. The latter allows hackers to gain access to locally stored files, services and websites using the victim's credentials and bypass cross-domain policies. *Out-of-bounds memory leaks* have been identified (Security update advisory, 2020) which can lead to *denial of service attacks* and input string validation exploits have been observed which could allow for *remote code execution* (Security update advisory, 2019). Other vulnerabilities in the *Unity Framework* have been discovered which if exploited could allow for *eavesdropping and man-in-the-room* attacks during virtual sessions.

Unreal Engine (Unreal build Automotive, 2021h; Unreal engine early access, 2021i) : Unreal engine is an open source XR development platform for high-end graphics with a marketplace to sell and purchase resources including free learning material, development libraries, and plugins (Epic Games, 2022a; 2022b; 2022c). Several security vulnerabilities (Cve details, 2021; VulDB : vulnerability databas, 2021f) has been reported for developers of the *Unreal Engine*, that allow for exploits such as *denial of service, overwriting of data by directory traversal, buffer overflow*, amongst others.

Node.js: *node.js*(Introduction to nodejs, 2021e) is used for creating applications based on *JavaScript*, and is popular for building 3d libraries and applications (best nodejs d libraries, 2021b). Several

extended reality libraries also integrate with *Node.js* (best nodejs virtual reality libraries, 2021a) to aid developers in the building of XR content. Recently various vulnerabilities have been exploited in this framework consisting of *remote code execution, manipulation of data, bypassing of security checks, XSS (cross site scripting) and memory exploitation* amongst several others (Cve details, 2021b; 2021c).

SNAP.N: Snapchat (Snap Inc) provides a platform for building virtual avatars and AR filters to overlay digital contents in the physical world (Snap Inc, 2021c; 2021d). Researchers have discovered a *server-side request forgery (SSRF) vulnerability* in Snapchat which draws information from Snapchat's hosts or devices. According to the authors, SnapchatDB.info discloses usernames and phone numbers of approximately 4.6 million U.S. users as well. Other security reports on Snapchat (Colao, 2020; Dimov, 2015; Hackerone snapchat vulnerabilities, 2015; Leyden, 2020) detail vulnerabilities such as *server-side remote code execution, significant authentication bypass, unrestricted file system access, XSS (cross-site scripting) and remote freezing of mobile phones*.

Roblox: The Roblox platform provides a means for developers to create virtual games and applications and aims to develop a virtual Robux currency to allow users to conduct virtual shopping and business activities using the platform (Ibanez, 2021; Roblox, 2021). Researchers claim that multiple vulnerabilities exist in the Roblox platform including but not limited to *cross site scripting, inappropriate hashing algorithms, hardcoded API keys, the Janus vulnerability, and data exposure using misconfiguration in Android manifest file*. According to the authors if a combination of these vulnerabilities is exploited it can reveal names, and email addresses of approximately a 100 million users. The platform fails to comply with average baseline CVSS security, achieving a low CVSS value of 6.4 and a 10/100 security score (blogrobloxcom cross site scripting vulnerability report, 2022; Hackerone roblox, 2021a; Khalili, 2021; Mikalauskas, 2021).

Google's Cardboard SDK: The open-source Google cardboard SDK provides a development environment for creating an immersive world for Android and iOS platforms (Google LLC, 2022). A vulnerability has been detected in the Google Cardboard SDK that pertains to the provision of virtual reality experiences on smartphones (Info CA, 2022). The vulnerability (CVE-2018-19111) (Hackerone snapchat vulnerabilities, 2022) sends users' personal and sensitive information as unencrypted plaintext to a third-party website used for collecting Unity 3D statistics.

5.3. Data breaches in XR

Privacy Exposure: This category of data breaches is subtle. XR privacy leakage doesn't interrupt the user and therefore users do not feel prompted to report that an attack has been launched against them or that their device has been compromised and is violating their privacy. Although privacy exposure attacks are low key they can capture consumers' personal information without their intent including e-mails, chats, and conversations happening onscreen (Anand, 2017). Most XR apps haven't implemented standard encryption for securing network connections and instant messaging from prying eyes. Constrained XR devices do not have the capability of providing complex (e.g. asymmetric) encryption.

Identifiability / Likability / Detectability : XR technology gathers unprecedented levels of personal and biometric information of users including *eye scans, gaze tracks, heart rate, gestures, user movements, physical characteristics, body movements, financial transactions, credentials, locations and 3d motion* etc. (Kohnke, 2020). It can also keep track of user likes, behavior, friends, interactions, and collaborations in the virtual world. As compared to traditional devices such as smartphones, XR solutions have access to a lot more sensors and attached cameras that record the activity and provide a very large volume of information as long as the headset is powered on. This continuous collection, tracking, and gathering of personal, unintended, and unnecessary information during the immersive online sessions from wearable devices, cameras, and attached sensors lead to privacy threats of XR users' likability, detectability, and identifiability. The knowledge regarding users' identifiability, likability, and detectability gathered from personnel information targets users' anonymity in an immersive environment. The attackers can easily trace or infer knowledge from gathered personnel information to identify whether an operation is performed or likely to be committed by the victims' identity (Andreas et al., 2010). The user has no control over his information once it has been fetched by devices and stored in databases. XR applications detect and identify objects in a user's real surroundings and even after the user no longer intends to be detected and identified (De Guzman et al., 2019; Mahak and Singh, 2021; Syal and Mathew, 2020). To ensure users' privacy in a multiparty interactive immersive reality environment, personal information exposure needs to be minimized. Users' presence in an immersive virtual world should be unidentifiable, and their actions must be undetectable.

Bystander Privacy: HMD and XR glasses capture surroundings, bystander information, and can record personal information of collaborating users as well. XR consumers may be completely unaware that the gadgets they are using for entertainment are inadvertently collecting not only their personal real-life information but also that of their friends, family and co-workers. Furthermore, XR users can also share experiences of collaborative meetings, with other parties without the consent of their collaborative partners (kaspersky, 2021).

VR-Spy: The body movements of VR users can be subtly collected through side-channel attacks on VR devices. An example of this is recording of virtual key strokes where the user has to move his hands and wrist to enter key strokes virtually. Virtual keystrokes of VR headsets can be identified using channel state information (CSI) of wifi signals to capture unique hand gestures. VR-Spy is a side-channel attack, which captures unique gestures from the CSI waveform using signal processing techniques (Arafat et al., 2021).

Ransomware Attacks & Cyber Extortion: (kaspersky, 2021; Pearlman, 2020) In this category of data breaches the attacker records the behavior and interactions of XR users during immersive sessions and then later threatens to release these recordings publicly unless the user pays a ransom. An especially dangerous area that hackers can target is the healthcare industry whereby they gain access to XR health care devices, target patients and clinical staff and coerce them for money before giving the control back.

Multi-App Spatial Access: In multi-app future or spatial computing, metaverse users can place their virtual applications, devices, and cameras in someone else's virtual building without the owner's permission to watch, hear and observe victims' activity. Retailers from any area can analyze shopping trends by silently tracking customers' movements through virtual stores. Invisible avatars can experience virtual surgeries of patients without their knowledge. Metaverse avatars are allowed to interfere, invade and move freely in virtual worlds, including other users' workplaces, homes, and hospital rooms. All these loopholes facilitate adversaries in launching new attacks and can lead to severe privacy breaches (Happa et al., 2021b; Multi app The next evolution in spatial computing, 2021e; Ning et al., 2021).

Social Engineering Attacks: The digital footprints of XR users can be derived from their virtual world, by observing users' likes, preferences, social circles, business, and even financial details. In the metaverse, any avatar can follow others, and victims cannot restrict other virtual identities to abandon this behavior. By following the victim's avatar, attackers can record all his details, including his hobbies, personal likes/dislikes, lifestyle and travel history,

etc. The gathered users' information from virtual reality can also be used by adversaries in real life to perform social engineering attacks against them (Ning et al., 2021).

5.4. Unauthorized access

Tampering & Repudiation & Spoofing : XR vendors store users' personal information mostly in the cloud, where security profiles may not be enforced or remain hidden from users. XR devices lack strong access control mechanism which leads to security threats of data tampering, denial of service and unauthorized access to users' records (Dick, 2021a; Syal and Mathew, 2020). As XR security compliance policies, regulations, and standardization are limited if not completely unavailable (Dremliuga et al., 2020a), an intruder or adversary could repudiate, tamper or spoof actions during an interactive immersive XR session.

Tracker attack: An attacker can turn on the front facing camera of XR users and stream the video feed back to his desired location (Pearlman, 2020).

Man-In-The-Room Attack : The attacker can join any collaborative meetings without the XR users' permission and can modify the environment (Casey et al., 2019a).

Man-In-The-Middle Attack : (kaspersky, 2021) The attacker intercepts or monitors communications between the XR browser, XR provider, and third-party servers.

Eavesdropping : Unauthorized access during immersive XR sessions leads to privacy breaches and eavesdropping. In the past researchers have successfully launched eavesdropping attacks in both BigScreen (Critical vulnerabilities in bigscreen VR app, 2021d) and SocialVRLE (Valluripally et al., 2021) XR applications.

5.5. E-Fraud

Identity Theft : XR technology and its subdomains responsible for generating photo-realistic avatars, eye tracking and mirroring of body movements have further amplified the impact of identity theft and will affect human psychology (Matthews et al., 2021).

Impersonation Attack : (De Guzman et al., 2019) XR applications and devices monitor our gestures and voice commands and attackers can use these recordings to impersonate users.

Credential Exposure : (Josh, 2021; kaspersky, 2021) XR users can enter their credential information as input or may store it in the user's profiles maintained by XR solutions. This makes it convenient for attackers to monitor users' inputs or steal network credentials and mobile payment solutions to exploit users.

Deepfakes : If a hacker gains access to the monitored body movements of users from their XR headset, they can generate deepfakes or digital replicas (Bose and Aarabi, 2019; kaspersky, 2021) of users. Convincing deepfakes when displayed to other parties or to the public under the right context are a major risk to people's reputation, can allow for social engineering attacks, as well as cause political stability.

Malware Injection : (kaspersky, 2021) XR hackers can undermine security by redirecting users to their malicious website or malware-infected XR servers with illegal contents. Usually this is done by enticing users to click on advertisements in the VR environment.

5.6. Unavailability

Overlay Attack : (Casey et al., 2019a) The attacker can potentially overlay digital content on users' views to block their real view. The overlay attack tactfully inserts images, videos, and other digital content on top of a player's view thereby blocking the real view. Blocking of important data on an XR view during driving, tourism and military operations may be disastrous.

Input attack : (De Guzman et al., 2019; Syal and Mathew, 2020) The input attack prevents legitimate commands and inputs like touch, voice, gestures, vision navigation commands from being recognized. It also deceives detection algorithms.

DDOS : (Josh, 2021) In a DDoS attack on XR systems, the attacker can gain unapproved access to the XR resources, overwhelm XR applications with bogus data, manipulate content, or cut off the information stream so that users may feel exhausted, stressed, and ill. Network congestion and network faults may lead to DDoS (Valluripally et al., 2021). Particularly DDsS in IoT based XR solutions like robot-assisted-surgeries (Zhongming et al., 2021) may lead to dire results.

Feedback Overload Attack : (Roesner et al., 2014a) The overload attack overburdens the system and may cause a delay in the response time and feedback to be misaligned with the present real environment resulting in accidents.

VR Phishing : VR phishing attacks are used for gaining access to users' private and sensitive information such as credit card details, bank information and login credentials. The phishers attach a malicious script or malware via email attachment or any downloadable executable through a web URL (Naik, 2013). As a case study, researchers injected malware on users' systems for phishing virtual sessions and built a replicating worm which attached itself with the systems of all users participating in a virtual meeting (Critical vulnerabilities in bigscreen VR app, 2021d). Other phishing techniques involve blocking users' view, removing input content, distracting users and accessing the input and output data streams from other applications running within the device (Roesner, 2022).

5.7. Integrity violation

Hackers manipulate the input to the XR system, altering the system to behave in an undesirable manner (De Guzman et al., 2019).

Output Attack : XR applications after processing input commands, send output to XR devices. Malicious applications may alter outputs or display for users (De Guzman et al., 2019; Roesner et al., 2014b; Syal and Mathew, 2020). Research (Casey et al., 2019a) shows that the adversary can easily control the XR user's physical movements, without their knowledge during an immersive experience. The XR adversary can manipulate users' orientation, location, to misguide them in a virtual environment.

Crowdsource Poisoning Attack : Attackers insert crafted input to corrupt the stored aggregated information of XR applications (kaspersky, 2021).

Deception Attack & Defacement Attack : In a deception attack, the attacker changes the actual environment of the user such that he perceives false information. For example the attacker may post false street signs, incorrect directions and fake traffic signals (Roesner et al., 2014a).

Occlusion Attack : In the occlusion attack (Valluripally et al., 2021), the attacker obstructs the desired view during an immersive session or causes noise attenuation.

5.8. Network attacks

Most of the traditional cyber network attacks are applicable in an immersive environment. As a case study, numerous attacks have been launched against popular VRLE (Social Virtual Reality Learning Environment) systems. The triggered attacks include *Syn flood, SQL injection, Ping sweeping, Intrusion, Eavesdropping, Packet flooding, Packet tampering, Packet Sniffing, Password attacks, Unauthorized logins, Information disclosure, and user's data tampering.* These attacks adversely affect the user activity in an immersive environment and also contribute to cybersickness or motion sickness (Valluripally et al., 2020). During an immersive session, VR

sickness results in feeling of eye strain, nausea, dizziness, confusion, headache, and cold sweats. Another study (Mazloumi Gavgani et al., 2018), shows that the XR consumers experience severe motion sickness after a VR rollercoaster ride.

6. XR Threats to human health & lives

XR systems are facing serious health concerns as devices have the potential to harm consumers physically, psychologically, and emotionally. The damages from poorly configured or malformed XR systems range from simulator sickness to extremely dire permanent health conditions. Prolonged usage of XR applications causes nausea, fatigue, blurry vision, headache, and dizziness. This section describes health hazards of uncontrolled XR solutions including, simulator sickness, physical injuries, disorientation attacks, mental disorder, and psychological affects with reference to our proposed taxonomy in Fig. 6.

6.1. Cyber sickness, VR motion sickness & simulator sickness

XR users might feel anxiety, discomfort, fatigue, motion sickness and disorientation during or after an immersive session (Andrade and Bastos, 2019b). Network and synchronization delay between real and virtual movements, faulty gadgets and sensing devices such as the gyroscope contribute to distortion in virtual transmission, lead to cybersickness and simulator sickness which causes eye-strain, dizziness, vomiting, headache, nausea and faintness (Valluripally et al., 2021). Users of extended reality can be scared to death (Barack, 2018; Dremliuga et al., 2020b). The Daydream headset warns that usage of extended reality applications be discontinued if the user is already sick or suffering from headache, fever, upset stomach because the immersive experience can further worsen the situation (Google, 2016; 2017). Vulnerabilities of the social VRLE system have been previously exploited by attackers leading to cybersickness among consumers with XR DOS and data leakage contributing the most towards cyber sickness (Valluripally et al., 2021).

Zoom & Virtual Fatigue: (Matthews et al., 2021) Network delay, a faulty device, lag during the conversation, long periods of annoyances during an immersive session are all factors that will lead to*Zoom fatigue or Virtual fatigue*.

6.2. Physical injuries & physical collision attacks

The surroundings area should be cleared before using XR devices. The user should keep a safe distance from physical objects because serious injuries might occur. Due to malformed or buggy HMD, XR users may strike into walls, fall from stairs or rooftops, walk into ongoing traffic leading to several different types of accidents (Valluripally et al., 2021). The Oculus Go headset has warned its users to sit in a safe place before using the headset for an immersive experience otherwise they might get hurt by hitting appliances, fittings, and walls placed in their surroundings (Facebook Technologies, 2021; 2021). According to the HTC VIVE, the user must not blindly trust the system's virtual walls or chaperone systems (Sandee, 2021). In a alarming incident an episode of Pokémon caused seizures in approximately 700 Japanese children due to flashing strobe lights (Wudunn, 2021).

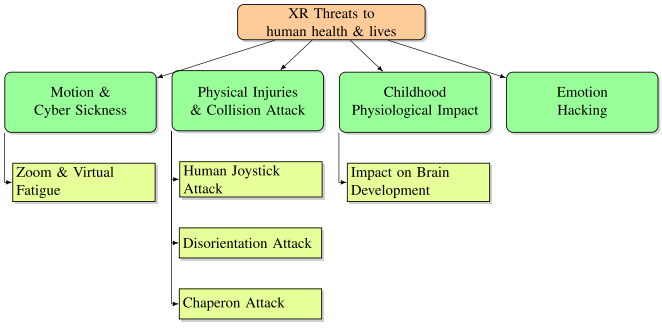

Fig. 6. A Taxonomy on XR Threats to human health & lives (Section 6).

Human Joystick Attack: (Casey et al., 2019a) In the human joystick attack, an immersed user is trapped. During the virtual session the user's physical movements are redirected to some other physical location of the attacker's choice without the user's knowledge by accessing the victim's front-facing camera and screen data.

Disorientation Attack: (Casey et al., 2019a; Pearlman, 2020) An adversary mounting a disorientation attack can alter the orientation, replacing the tracking mechanism of the HMD with the tracking mechanism that is in the hands or controller of the attacker, confusing an immersed session. XR users may hit physical objects and walls due to disorientation attacks.

Chaperon Attack: (Casey et al., 2019a; Pearlman, 2020) Chaperon attacks modify the boundaries and walls of the virtual environment, preventing users from identifying their physical boundaries during an immersive session.

6.3. Emotion hacking

Certain XR content can cause physiological problems. An emotion hacking virtual reality (EH-VR) (Gobbetti and Scateni, 1998; Ueoka et al., 2016) system hacks and accelerates the user's heartbeat, controlling it in such as manner so as to cause a scary VR experience (Ueoka and AlMutawa, 2019). Inappropriate content in XR can also cause health-related ailments by accelerating blood pressure, pulse rate, anxiety, and it might cause psychological issues (Daydream, 2021).

6.4. Childhood physiological impact

Current research shows that XR could cause physiological, emotional, and behavioral issues in children and the impact of upcoming latest XR technologies on childhood development and educational outcomes are unknown (Jerome and Greenberg, 2021). *Oculus Rift* prohibits the use of the product by under age of 13 Go and *PlayStation VR* (Sony Interactive Entertainment, 2022) declares that the device could be used by children above age 12. *HTC Vive* has issued a warning that their product is not built for children and adults should monitor if it is in use by elder children. According to *Gotsis* (Sandee, 2021), children must not use any uncontrolled media. Moreover virtual media has a much higher impact than traditional, and usage must be under the supervision of parents. Research shows that longer XR usage causes disorientation and cybersickness so educational activities using XR need to be limited to a maximum of 20 minutes (Rauschenberger and Barakat, 2020).

Impact on Brain Development: Researchers at the *University of California* identified that brain neurons act differently in an immersive environment as compared to in a real physical environment. According to their research, the neurons begin shutting down during the VR experience. According to *Marientina Gotsis, "VR could have an even bigger impact on the developing brains of children and prolonged exposure with improperly fitted devices could incur damage"* and *"Children also may not understand how to communicate eyestrain and may lack reflexes to remove the devices if they find them uncomfortable."* (Kaimara et al., 2021). *"Google Cardboard"* should not be used by children without parental supervision (LaMotte, 2022).

7. Ethical concerns in XR

7.1. Unauthorized amendments

Profile & Architectural Amendments: XR users are privileged to amend virtual representations of others in an immersive world, e.g., an XR participant can apply filters on other virtual identities to alter their appearances, audio stream, color, race, etc. These immersive illegal anonymous amendments elevate the ethical concerns of individuals in extended reality. The virtual representation of sacred places, monuments, and religious temples need to be preserved in their original form. In 2018, a team of developers modified the digital interactive representation of historical places including, *Jackson Pollock gallery* at the *New York Museum* of *Modern Art* and the *Isabella Stewart Gardner Museum in Boston* (Annear, 2022; Miranda Katz, 2022). Such illegal deliberate amendments using extended reality applications are hostile and must be discouraged (Jerome and Greenberg, 2021).

7.2. Abusive behaviour

The incidents and misbehavior of users in an immersive world are mostly not documented or reported because it occurs in real-time and all actions, conversations are difficult to track record, and witness (Sheera and Kellen, 2021). Researchers recorded and investigated the VRChat application and reported that 100 incidents happened over an 11-hour time slot where abusers' virtual avatars commit sexual and violent actions against minors (Sheera and Kellen, 2021).

Cyberstalking in XR: Cyberstalking is the attempt of virtual harassment by observing someone's activity unlawfully and forging their data. XR stalkers, harassment, cyberbullying, violence, and online abusive behaviors, are amplified because the harasser knows that their fake immersive identity is more challenging to catch (DUGGAN, 2021). This section describes cyberstalking concerns in XR and these are also listed in Fig. 7.

Sexual harassment: A survey (DUGGAN, 2021) has been conducted on virtual social harassment experienced by VR users (US residents) in 2019, and it reveals that nearly *92%* of users are witnessing harassment in social VR applications such as Altspace, VRChat, etc. Multiple studies (Blackwell et al., 2019; Outlaw and Duckles, 2017; 2018) show that women feel uncomfortable and experience abusive behavior during social XR experience, and it is more offensive than a 2D social experience. A community of XR hobbyists is developing avatars of real people and selling them to satisfy clients' sexual desires. No clear legal obligations are available to address these cybercrimes (Samantha and Emanuel, 2019). Such applications further raise concerns regarding control of users over their *digital identities* and *self avatars*. Multiple incidents of harassment have been reported in the metaverse (Basu, 2021); one of them is reported by a beta tester in *Horizon World* which is a social media platform, designed for a group of 20 avatars that can hang out together. She experienced a virtual groping incident by a male avatar.

Cyberbullying: Metaverse has further enhanced online bullying since cyberstalkers can now virtually insult or attack victim consumers publicly instead of just writing comments. A survey (Outlaw and Duckles, 2018) sharing the social experience of over 600 VR users found that *30%* males reported racist comments, *20%* of males experienced violent threats, and *49%* of females encountered incidents of sexual harassment.

Violence: Widespread bullying, taunting, racism, harassment and violence can be easily observed in XR games. Researchers at the *Center for Countering Digital Hate* (Center for Countering Digital Hate, 2021) analyse violent incidents in the popular game *VRChat* (VRChat Inc, 2021) and report that every seven minutes a violent incident occurs.

8. XR Currency scams

Consumers need digital money to avail opportunities in immersive reality. RFOX VALT (RFOX, 2021a) is a platform that serves as a distributed ledger, designed for a fully immersive experience with retail services for commercial enterprises. The RFOX VALT operates on technologies such as blockchains, NFTs, Ethereum, Binance Smart Chain, and WAX (RFOX, 2021b; 2021c). Similarly, DMarket is another immersive marketplace (Dmarket Inc, 2021a) which provides commerce and trade services for extended reality. DMarket also relies on Ethereum and BitCoin (Dmarket Inc, 2021b). NFTs is the most commonly used mechanism among XR platforms and the metaverse environment but the XR developers must realize that multiple threats and breaches have already been reported against digital currency and NFTs (Wang et al., 2021). The latest XR currency scams are shown in Fig. 8 and are elaborated in this section.

8.1. NFTs

NFTs (non-fungible tokens) are based on blockchain technology that ensure that sales or purchases are irreversible. NFTs differ from money or other classical cryptocurrencies as they are unique

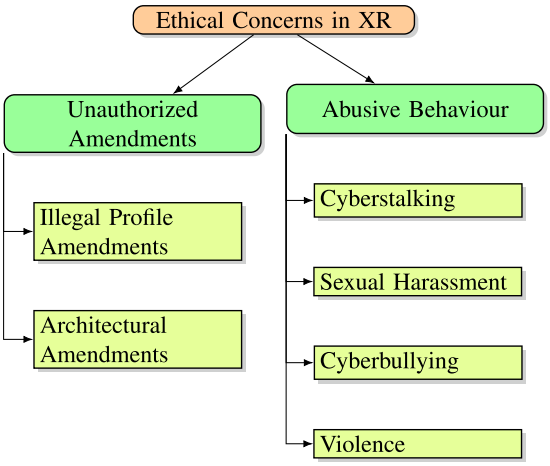

Fig. 7. A Taxonomy of Illegal Issues in XR (Section 7).

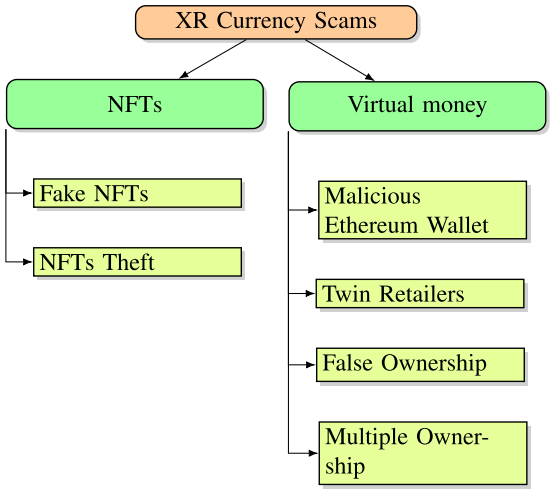

Fig. 8. A Taxonomy on XR Currency Scams (Section 8).

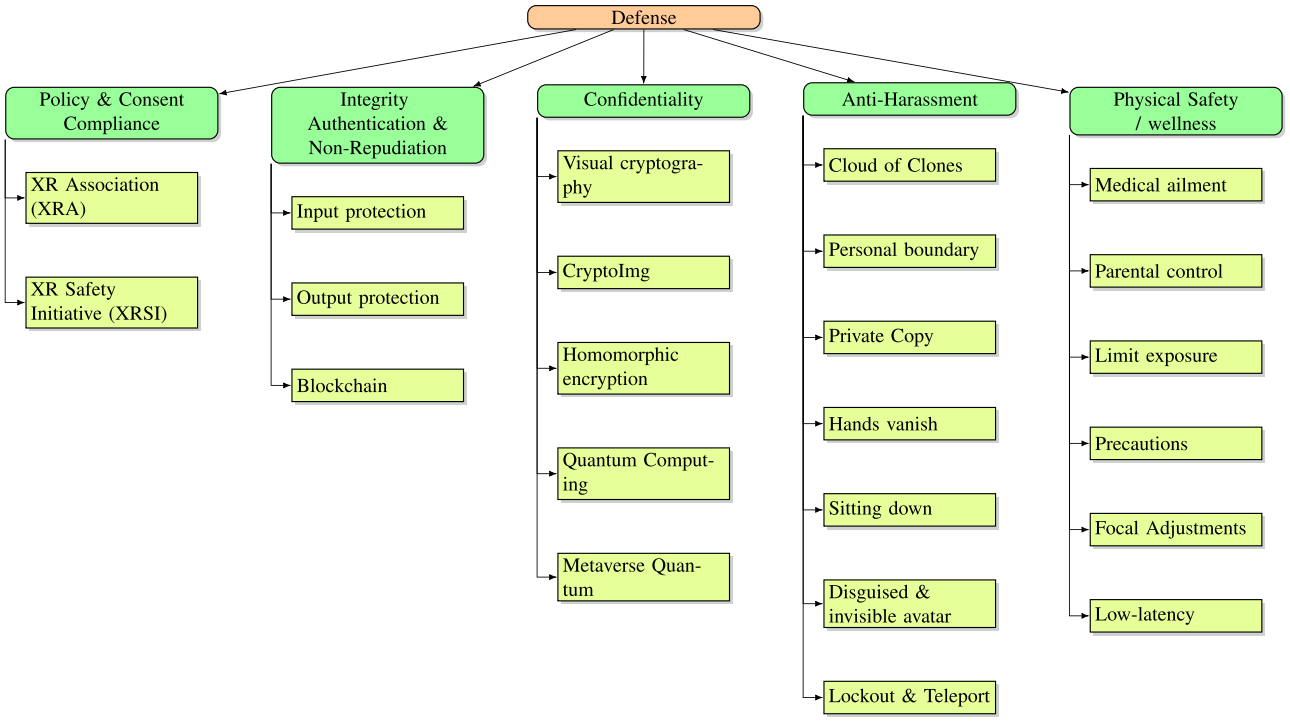

Fig. 9. A Taxonomy on Defense for XR (Section 10).

and noninterchangeable, just like an identity or certificate of asset ownership. As the extended reality community is relying on the NFTs, attackers are also making progress in exploiting and stealing NFTs. Extended reality researchers must be well aware of the technology vulnerabilities.

Fake NFTs: Bogus NFTs can be sold in extended reality and once they get linked with blockchain it is impossible to get the transaction reversed. Such transaction may negatively affect the reputation of a company (Staff, 2021).

NFTs Theft : Hackers can steal virtual assets from legitimate accounts and then sell the assets online because blockchain-based NFTs can only secure users' assets from forgery, not theft or account hijacking (Malwarebytes Labs, 2021).

8.2. Virtual money

Malicious Ethereum Wallet: Ethereum wallet is an online banking application for Ethereum accounts, and account holders can connect to any decentralized application using their wallets (Ethereumorg, 2022). Multiple cryptocurrency thefts, vulnerabilities in Ethereum transactions, malicious Ethereum Name Service (ENS) ".eth" domain names, and ownership scams have already been reported (Wang et al., 2021) against *Ethereum Wallet. Ethereum wallet* is required for most of the NFTs purchases in XR and it does not provide full anonymity to users. Users transactions are exposed to public.

Twin or Fake Retailers: In an immersive world, users have the ability to create digital twins of anything virtually. This allows for a number of attack scenarios. A virtual store for instance could replicate or claim to be any famous reputable company but no one would be able to identify the legitimacy of the brand to ensure that consumers are dealing with the authentic brand due to a lack of regulatory services (Truong, 2021).

Multiple Ownership: There could be multiple ownership created by hackers of the same virtual asset which will lead to various chains of ownership for the same asset.

False Ownership: In the absence of NFTs for virtual elements, initiating one does not authenticate a consumer to be the owner of a virtual asset and this will lead to false chains of ownership.

9. Legal concerns

Rules, policies, and regulations may be established or existing ones may be revised to encompass metaverse concerns. This is important for protecting the user's rights globally, create a sense of accountability, and to secure digital assets ownership in an immersive environment.

Antitrust: Metaverse consumers fear that some dominant digital marketers may monopolize the metaverse environment by influencing the policy-making process, and by defining regulations that favor their requirements and products. The metaverse community is facing antitrust challenges (Polona et al., 2022) such as data sharing agreements between multiple platforms and applications usage pricing between countries.

Metaverse economic policies: Governments and stakeholders have varied perspectives of the metaverse and are following different approaches (Dwivedi et al., 2022; Ning et al., 2021) to address the associated challenges based on their region, country norms, economics, and the metaverse development progress. Metaverse economics is dependent on blockchain, NFTs, and crypto wallets and each country has different policies for the token economy. There is a growing need for policymakers to define rules to regulate cross-border metaverse solutions, address economic barriers, and allow for data sharing between countries. The existing laws for IT industries may have to be modified for both public and private sector enterprises to promote partnerships.

Laws for Metaverse crimes: It is challenging for courts to apply real-life policies and laws in the metaverse, without modification as existing laws mainly apply to physical crimes. While this is an ongoing challenge with all cybercrime laws the metaverse has further exacerbated the issue. For instance if a hacker stole a piece of metaverse land then the punishment for real estate crimes in immersive reality would be different than if he has stolen ac-

tual physical land. Similarly, the policies of cybercrime must be redefined for an avatar who attempts to harass, spy, or steal other users' identities in the metaverse. The *European Parliament (EP)* calls to improve the *GDPR* to address the challenges of the metaverse, especially to enhance data protection laws (Polona et al., 2022).

Avatar Lawyers: Legal firms are opening their offices in the metaverse like Grungo Colarulo (a US law firm) as "Avatar Lawyers" to offer their services for virtual entrepreneurs and against metaverse crimes (Croft, 2022). What kind of training or certifications are required for an attorney to specialize in this area is as yet still undefined.

Metaverse Crypto Taxes: The terms and conditions for metaverse income taxes need to be revised. An artist in the physical world pays an income tax on selling his art. Similarly, a virtual artist selling their digital artwork should be obliged to pay taxes on his capital gains. Currently, consumers in the metaverse will perform their transactions according to multiple tax laws. The *Organization for Economic Cooperation and Development (OECD)* is currently working to design an international framework for crypto taxes (GBO-Global Business Outlook, 2022).

10. Defensive measures

Users blindly trust XR brand names, service providers, and device manufacturers. They assume that the security standards have already been in place while storing and sharing their data with third-party applications. The responsibility for addressing XR security risks lies on all contributors, however no security framework has been developed or documented yet, for XR systems (Dremliuga et al., 2020a; Happa et al., 2021a). In this section, we propose defensive measures and best practices that may be adapted to ensure users' security and safety by elaborating upon XR policies and consent compliance in section 10.1, the role of blockchains in XR for content integrity and authenticity 10.3, encryption techniques and quantum Computing for confidentiality and content availability in immersive reality 10.4.1, anti-harassment 10.5 and physical safety strategies 10.6. Furthermore, we provide security recommendations for mitigating critical XR security challenges.

10.1. Policy & consent compliance

Just a single XR experience involves a variety of technologies, and each associated technology, application, or device faces issues regarding privacy, information validity, repudiation, trust, and misinformation. A single policy or standard cannot possibly allow for compliance for all interlinked and collaborating XR technologies.

The XR Association (XRA) (Hurtado, 2021; Sweeney, 2021) is a combined effort for creating a safe, respectful and responsible XR environment. Some high-tech companies involved in XRA efforts include *Google, Facebook's Oculus, Sony Interactive Entertainment, Microsoft, HTC Vive and Samsung*. XRA releases guidelines, the current version of which at the time of writing is *XR Primer 2.0*, which list best practices for XR developers and manufacturers for considering safety measures in three-dimensional contexts. XRA is aiming to control cyberstalking by educating users in establishment of strong protection and reporting mechanisms in the XR environment. The designed guidelines encourage a positive attitude and penalize negative behavior and hate groups.

The **XR Safety Initiative (XRSI)**(XR Safety Initiative, 2021c) is a global effort to discover the XR and metaverse risks to individuals, organizations, manufacturers, and governments. The XRSI is currently proposing several frameworks such as *Medical XR* (XR Safety Initiative, 2021d), and *Child Safety XR* (XR Safety Initiative, 2021a) to address the privacy and safety concerns for healthcare applications and to protect children from risks associated with the metaverse. XRSI has launched several programs such as *Cyber-XR Coalition* (XR Safety Initiative, 2021b) to devise accessibility and inclusion standards, and *Ready HackerOne* (XR Safety Initiative, 2021e) to increase user awareness. In addition it has also released a set of shared vocabulary or taxonomy of XR and relevant domains such as *360 Degree Video, Brain-computer interface (BCI)* and *3D Spatial Audio* (XR Safety Initiative, 2021f).

The XRSI Privacy Framework (XR Safety Initiative and others, 2021a), is a community-driven, international, and freely attainable guide of security standards, policies, and best practices for the development of XR applications and devices. It promotes an iterative approach that focuses on access disclosure and privacy concerns for XR clients with a focus on biometric data inference. It combines security requirements drawn from the *General Data Protection Regulations (GDPR), National Institute of Standards and Technology (NIST) guidance, FERPA, COPPA,* and other evolving laws (Bao-Kun et al., 2018). XRSI Privacy Framework is adaptable in including other novel requirements as well.

For ensuring secure XR solutions, there is a need for a law enforcement authority, regulatory body, or a review committee to address functionality and ethical concerns before product launch. For instance *Medical XR privacy and safety framework* by XRSI prevents healthcare professionals from mishandling medical records and urges officials to create a procedure to incorporate safety measures in the metaverse system. The XRSI emphasizes that federal baseline legislation and policies must be defined to ensure users' trust and business reputation by establishing an industry review board for XR technologies.

The XR Industry review board must provide awareness and guidance to the industrial sector, and the defined policies must evolve with market trends. XRSI proposes that a regulatory framework is necessary to address the trust, security, and safety needs of XR applications, data, and hardware devices. The regulatory framework must address the risks that affect social values. There is no single mechanism or procedure to secure a metaverse environment. The government must regulate immersive technologies and provide awareness sessions for all stakeholders to practice and achieve a safe and secure XR ecosystem [235]. Beyond addressing safety and trust issues in the metaverse, XRSI discourages racial discrimination and the digital divide (Pearlman, 2021).

10.2. Meta-Crime investigation

Metaverse allows for novel attacks that need investigators and metaverse specialists specializing in digital forensics for properly investigating crime scenes. Forensic skills, tools, standards, and automated mechanisms that investigators have relied on thus far to gather evidence for prosecuting cybercrime need to be upgraded for immersive reality (Agarwaal, 2022; Umar, 2022). Metaverse artifacts captured through forensics analysis could be helpful in reconstructing metaverse events, identifying vulnerabilities and for investigating a metaverse crime scene (Yarramreddy et al., 2018). Digital camera images, video, and memory artifacts of immersive virtual reality could facilitate forensics experts during metaverse crime investigation (Li et al., 2021; Wang et al., 2022). The area of metaverse forensics is understudied and mataverse's decentralized nature, use of proprietary products, and deployment over cross border environments causes interoperability and trust challenges for effective forensic analysis in an immersive reality. On the converse in real life, virtual reality could assist crime investigators in visualizing past incidents in VR to discover witnesses and provide proof in criminal procedure (Dath et al., 2017), but it requires further research.

10.3. Defense using block-chains in XR

The various attacks discussed in Section 5 threaten the *authenticity and integrity* of XR services.

10.3.1. Authentication

Sensitive and confidential XR digital content raises the security concern of objects being stolen, hacked, disseminated, and copied (Top five effective use cases of blockchain in virtual reality, 2021d). The posted contents among heterogeneous XR applications and devices should be hack-proof. XR input/output interfaces must enable authentication, authorization, non-repudiation, and identification. *Blockchain* could provide the XR content available through blockchain-linked databases that allow XR members to access secure and interactive content by verifying their identities. Blockchain also helps to ensure the originality of content, being shared among multiple parties. It establishes a reliable and interoperable process of maintaining the copyrights of digital creations (Cannavò and Lamberti, 2021).

10.3.2. Integrity

Input protection mechanisms are required to protect the sensitive information gathered through XR attached sensors and wearable devices. The accuracy and availability of clients' data is compulsory for the successful execution of XR applications. Output protection is required to render information in the XR environment for the user himself and for collaborative parties. The permanent and immutable features of *blockchain* technology could ease the XR community in sharing content with uniformity and ensures the synchronization of data streams in virtual experience between multiple collaborating parties (Cannavò and Lamberti, 2021; Top five effective use cases of blockchain in virtual reality, 2021d).

10.4. Confidentiality

The XR system requires *confidentiality, pseudonymity, unobservability, undetectability, un-linkability, and anonymity* to secure the immersive collaborative sessions and financial transactions. Visual cryptography could play a key role to encrypt the XR streams. Using visual cryptography, a secret image is divided and encrypted into n shares and the embedded encrypted XR objects could be easily encrypted in the virtual and real-world without significant latency errors (Du et al., 2019). Another contribution to secure visual streams is the CryptoImg (Ziad et al., 2016) library, which uses homomorphic encryption and enables users to delegate their image processing operations to third-party sources. It's an efficient solution for performing operations over encrypted images.

10.4.1. Quantum computing & security

Appropriate resource optimization and throughput management is required in the metaverse and XR for compute-intensive immersive reality. The massive processing and computation required to develop a fully immersive world or the Metaverse will require *quantum computers*. Quantum computing eases Metaverse programming by facilitating the most powerful computing environment. Quantum security procedures can play a major role in securing the Metaverse. Quantum communication over a 5G or 6G network could provide communication security in the Metaverse architecture due to the superposition properties of qubits (Chowdhury et al., 2020). Quantum key technology like *quantum no-cloning theorem*, quantum security methods like *QRNG*, and *Metaverse Quantum (MTQ)* currency etc. enables privacy, security and stability of the metaverse (Allen, 2022; Huang, 2021; IQT News, 2022).

10.5. Anti-Harassment

XR developers must incorporate anti-harassment controls in XR devices. The standards, laws, and practices for the protection of consumers against cyberbullies and harassment must be revised for an extended reality environment (Sweeney, 2021). According to *Jesse Fox* (associate professor at *Ohio State University*, researcher of social implications of virtual reality, sexual harassment could be verbal and virtual, not necessarily be physical, and such virtual teasers must be banned. *Katherine Cross (University of Washington)*, researcher of online harassment, shares her opinion that the toxic attitude of users in extended reality is real, and the immersive world is developed in a manner that reflects users' physical environment, and every bodily action in the immersive world has an emotional and psychological effect on others.

Cloud of clones, is a designed privacy mechanism for the immersive world that generates identical avatars of users to create confusion for other observers in the metaverse, especially to avoid harassment. The observer loses track of the user's avatar (Falchuk et al., 2018). The concept of ***personal boundary*** in XR allows an avatar to create a personal space or enable a certain distance from others, to disallow unwanted interaction from avatars in the metaverse. The distance boundary is adjustable by XR clients (Holt, 2022; Sharma, 2022). To ensure privacy, users may request a ***Private Copy*** of virtual space from the metaverse provider to avoid surveillance and being observed in the metaverse (Falchuk et al., 2018). To avoid harassment in extended reality, an ***hands vanish*** scheme vanishes the avatar's hands, if they enter the personal boundary of another user (Holt, 2022; Sharma, 2022). If an avatar is feeling assaulted in the metaverse, he can select the option of ***sitting down***, and this action of an immersive environment will prevent the avatar from physical forces (Linden, 2022). The user could request one or more randomly generated ***disguised avatar*** appearances of his avatar to create confusion for observers attempting to identify the avatar's transformation (Falchuk et al., 2018). Metaverse users could become ***invisible avatars*** for other avatars and their activity and availability can not be monitored for a certain period (Falchuk et al., 2018). In the ***lockout*** feature of XR, a part of the immersive world is temporarily locked for other avatars from entering and will be available after the expiry of the lockout period (Falchuk et al., 2018). Using a ***teleport*** option in the XR environment, if a user is feeling harassed, he can transport his avatar to any other location of his choice in the digital world (Falchuk et al., 2018).

10.6. Physical safety

Before using XR devices or engaging in an immersive experience, clients must consult physicians, in case they are suffering from any medical abnormalities, vision impairment, psychopathy, blood pressure, or heart conditions (LaMotte, 2022). Users must clear their surroundings before using XR solutions to avoid getting hurt from nearby objects during immersive sessions. Oculus Go headset has also recommended that users must be at some ***safe environment*** before using the XR solution (Facebook Technologies, 2021; 2021). The clients should avoid using immersive applications, if suffering from any ***medical ailment*** including headache, fever, upset stomach. Daydream also warns against the use of extended reality applications, if a person is sick (Daydream, 2021; Google, 2016; 2017). Usage of immersive applications and devices should not be permitted for persons under the age of 13. Oculus Rift, PlayStation VR, HTC Vive, all prohibit the use of these products by persons under the age of 13 without ***parental control or supervision*** (Daydream, 2021; Facebook Technologies, 2021; 2021; LaMotte, 2022; Sandee, 2021). Longer usage of XR application causes cybersickness, and the usage must be limited, especially

for children to not more than 20 minutes (Rauschenberger and Barakat, 2020). ***Limited exposure*** to XR applications can save clients from motion-sickness or cyber-sickness. The XR consumers must take some ***precautionary measures*** after participating in the XR session. Users should not stand up immediately as they might feel nausea, dizziness, or cybersickness after an immersive experience (Stephan, 2021). Users should have a stable focus point or should do ***focal adjustments*** and must lower the brightness during the XR session to avoid eye strain, headache, and nausea (How to reduce virtual reality, 2022; What causes virtual reality, 2021b). Latency in XR is the time required for an in-app motion to get admitted by the human brain. ***low-latency*** is better for mental health, which causes less delay between synchronization of the mind's perception and the immersive reality experience (What causes virtual reality, 2021b).

10.7. Recommendations

Extended reality offers a universe of options. XR users can attend events, create a design, do immersive shopping, and play in virtual or even within their physical boundaries using mixed reality or metaverse technology. The immersive nature of XR experiences elevates some unaddressed concerns which affect human psychology and a healthy daily routine. Following are some recommendations to mitigate these risks.

1. XR Security awareness training must be conducted for stakeholders including developers, end-users, and parents, to limit the probability of being targeted by phishers and attackers. Security workshops can educate users about XR social engineering attacks, XR vulnerabilities, patches, zero-day exploits, and the respective policies to build a security culture.
2. XR privacy policies and security standards must be well defined for all stakeholders. The regulations and consent compliance must be documented and made accessible for various XR solutions. Legislators must enforce XR manufacturers to ensure users' protection in immersive settings and XR industries must be compliant with the devised legal policies and standards. The product vendors should legally abide by the contractual terms that the security procedures and protection mechanisms put in place to ensure users' protection. The chain of responsibility must be pre-defined for potential breaches and incidents between all manufacturers and vendors.
3. The existing network security applications like intrusion detection and prevention (IDS / IPS) techniques, and firewalls. etc. are not interoperable with the latest extended reality and metaverse solutions. No cyber security framework has been established and documented for XR applications, neither any threat repository is available to report and share XR incidents. Most of the reported XR threats and security concerns are observed on web blogs and are posted in traditional textual representation. No automated mechanism is proposed to share, classify, and analyse potential XR threats & attacks with suggested course of action. A cyber threat sharing and vulnerability repository with analysis mechanisms must be devised for immersive threats and vulnerabilities. This would allow data sharing and management of different levels of trust between each party. Regular security analysis, incident sharing, monitoring, audits, and applications such as anti-malware, ant-viruses, and bug bounty programs must be designed for XR tools and applications.
4. XR developers must ensure end-to-end encryption when dealing with data in transit. Multiple *lightweight* cryptographic algorithms have been proposed in the literature (Naser and Naif, 2022; Rana et al., 2022), with less computational complexity for supporting small devices such as IoT. Lightweight cryptographic primitives could play a major role in achieving confidentiality in resource-constrained XR devices.
5. XR applications should assign adequate privileges to users without any culture, or gender discrimination. The XR developers must grant access control to their consumers to digitally remove their immersive identity or virtual account and the associated information. The client must have access to hide their data and limit access to third-party applications. The consumers' consent must be taken before collection of personal traits and he must be informed about inferred knowledge. The amount of personal information gathered, recorded, and shared during the immersive session must be communicated to the owner of the data.
6. The performance and effectiveness of extended reality systems depend on gathered information such as consumers' biometric data, geolocation, nearby entities, clients' interests, infrastructure, business affairs, etc. To mitigate the associated risks of technology, the minimal information required by XR systems must be quantified.
7. After the complete transition of various industrial sectors towards the XR and metaverse, a single network failure or internet dis-connectivity will shut down the entire XR ecosystem, applications, businesses, transactions, medical aids, and each associated or dependent pursuit. The potential impact of XR attacks will be huge. Additional security and protective measures must be adopted while device manufacturing deals with patients, children, and senior individuals. XR systems must provide ease and assistance while dealing with children, the aged, and disabled people in immersive settings.
8. Using XR technology, the consumers might start living and enjoying their self-created fantasy virtual life, far from reality, and they might get addicted to it. This addiction and prolonged usage could badly affect the user's physical and psychological ability, including his strength to face real-life challenges, his performance in an uncontrolled environment, and his potential to bear stress. Moreover, it will lessen users' physical activity and interactions with each other, which is essential for healthy living.

   Consumers should use the technology wisely and purposely by adopting a mindful approach. XR potential harms must be less than the technology benefits. To avoid prolonged usage of immersive experience, consumers should set screen timers and alarms for their transition between virtual and physical life, for their digital well-being, and to avoid health hazards.

   Immersive solutions may also cause human physiological problems making it hard to differentiate between the actual and immersive relationships. XR users should create a boundary between physical lifestyle and relations with their immersive life and community including parents, families, cousins, colleagues, and course-mates. To give the mind a break from the immersive environment, consumers should schedule and cease their immersive activities for a few days and hours, and a suitable percentage of personal social interactions should be encouraged.
9. Basic device security principles should be available in XR gadgets like *hardening, tamper-proofing, and redundancy* before deployment, to avoid tampering and disclosure attacks in XR systems. *Hardening, diversity, and principle of least privilege* (Valluripally et al., 2020), also enhance the resilience and reduce privacy leakage, and loss of integrity attacks.

11. Conclusion

Extended reality (XR) and the metaverse are the next revolution in technology and their applications are employed in nearly every domain of life. XR applications are dependent on users' personal information to operate and the sensitivity of collected information

has opened new cyber challenges and associated risks. The availability and integrity of the content are crucial for an immersive experience. In this research, we offer a semantic analysis of the attack surface of XR and metaverse technologies by identifying their vulnerabilities, potential cyber threats, and attacks, threats to human physical and psychological health, and currency scams. Reflecting on the crucial cyber challenges, the presented taxonomies on XR cyber threats and defensive measures will assist researchers, developers, and policymakers in mitigating them.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

Abu, M., Rahayu, S., Ariffin DrAA, D.A., Robiah, Y., 2018. An enhancement of cyber threat intelligence framework. Journal of Advanced Research in Dynamical and Control Systems 10, 96–104.

Agarwaal G.. 2022Metaverse: Taking the whole IT industry by storm. Accessed: 2022-12-12, https://www.linkedin.com/pulse/metaverse-taking-whole-industry-storm-gaurav-agarwaal.

Agriculture – EON merged XR orchids experience. 2021c. Accessed: 2021-12-06, https://eonreality.com/agriculture-merged-xr-orchid-experience/.

Alizadehsalehi, S., Hadavi, A., Huang, J.C., 2020. From BIM to extended reality in AEC industry. Autom. Constr. 116, 103254. doi:10.1016/j.autcon.2020.103254.

Allen & Company of Florida. Metaverse – the future of the internet. 2022. Accessed: 20-02-2022, https://alleninvestments.com/therealvalue/metaverse-the-future-of-the-internet/.

Alqahtani, A.S., Daghestani, L.F., Ibrahim, L.F., 2017. Environments and system types of virtual reality technology in STEM: a survey. International Journal of Advanced Computer Science and Applications 8 (6). doi:10.14569/IJACSA.2017.080610.

Alraizzah, A., Lamya, F., Fattouh, L., 2017. Environments and system types of virtual reality technology in STEM: a survey. International Journal of Advanced Computer Science and Applications 8. doi:10.14569/IJACSA.2017.080610.

AltspaceVR. AltspaceVR be together, anywhere. 2022a. Accessed: 03-01-2022, https://altvr.com/.

AltspaceVR. AltspaceVR events. 2022b. Accessed: 03-01-2022, https://account.altvr.com/events/main.

Anand V.. Security approaches for virtual reality transactions. 2017. US Patent App. 15/184,759.

Andrade, T., Bastos, D., 2019a. Extended reality in IoT scenarios: Concepts, applications and future trends. In: 2019 5th Experiment International Conference (exp.at'19), pp. 107–112. doi:10.1109/EXPAT.2019.8876559.

Andrade, T., Bastos, D., 2019b. Extended reality in IoT scenarios: concepts, applications and future trends. In: 2019 5th Experiment International Conference (exp.at'19). IEEE, pp. 107–112.

Andreas P., Marit H., Hannes T.. Privacy by data minimization. 2010. Accessed: 28-07-2022, https://tools.ietf.org/id/draft-hansen-privacy-terminology-00.html.

Annear S.. This boston company uses augmented reality to view artwork stolen from gardner museum. 2022. Accessed: 28-07-2022, https://www.bostonglobe.com/metro/2018/03/21/this-boston-company-uses-virtual-reality-view-artwork-stolen-from-isabella-stewart-gardner-museum/.

Anthes, C., García-Hernández, R.J., Wiedemann, M., Kranzlmüller, D., 2016a. State of the art of virtual reality technology. In: 2016 IEEE Aerospace Conference. IEEE, pp. 1–19.

Anthes, C., García-Hernández, R.J., Wiedemann, M., Kranzlmüller, D., 2016b. State of the art of virtual reality technology. In: 2016 IEEE Aerospace Conference, pp. 1–19. doi:10.1109/AERO.2016.7500674.

Arafat, A.A., Guo, Z., Awad, A., 2021. Vr-spy: A side-channel attack on virtual keylogging in vr headsets. In: 2021 IEEE Virtual Reality and 3D User Interfaces (VR), pp. 564–572. doi:10.1109/VR50410.2021.00081.

Augmented reality campaign, in just few steps. 2021. Accessed: 2021-11-1, https://theroar.io/.

Azuma, R.T., 1997. A survey of augmented reality. Presence: teleoperators & virtual environments 6 (4), 355–385.

Bagchi S.. 2021Extended reality @ NIST?Accessed: 2021-10-03, https://www.nist.gov/information-technology/extended-reality.

Baker H.. How to attend zoom, skype, hangouts meetings in VR with SPACES. 2020a. Accessed: 03-01-2022, https://vrscout.com/news/spaces-app-vr-zoom-skype-hangouts/.

Baker H.. Spaces app enables folks to attend zoom meetings in VR. 2020b. Accessed: 01-01-2022, https://venturebeat.com/2020/03/29/spaces-app-enables-folks-to-attend-zoom-meetings-in-vr/.

Bao-Kun, Z., Lie-Huang, Z., Shen, M., Gao, F., Zhang, C., Yan-Dong, L., Yang, J., 2018. Scalable and privacy-preserving data sharing based on blockchain. J Comput Sci Technol 33 (3), 557–567.

Barack L.. Can you die in virtual reality?2018. Accessed: 15-01-2022, https://www.gearbrain.com/can-you-die-virtual-reality-2522553872.html.

Barnard D.. Degrees of freedom (DoF): 3-DoF 6-DoF for VR headset selection. 2019. Accessed: 28-05-2022, https://virtualspeech.com/blog/degrees-of-freedom-vr.

Baskette B.. 20223DoF vs. 6DoF - degrees of freedom in virtual reality. Accessed: 28-05-2022, https://roundtablelearning.com/3dof-vs-6dof-virtual-reality-which-is-better.

Basu T.. The metaverse has a groping problem already. 2021. Accessed: 15-01-2022, https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/.

Becker, V., Rauchenstein, F., Sörös, G., 2019. Connecting and controlling appliances through wearable augmented reality. Augmented Human Research.

Behzadan, A.H., Timm, B.W., Kamat, V.R., 2008. General-purpose modular hardware and software framework for mobile outdoor augmented reality applications in engineering. Adv. Eng. Inf. 22 (1), 90–105. doi:10.1016/j.aei.2007.08.005. Intelligent computing in engineering and architecture

5 best node.js virtual reality libraries. 2021a. Accessed: 2021-12-06, https://openbase.com/categories/js/best-nodejs-virtual-reality-libraries.

8 best node.js 3d libraries. 2021b. Accessed: 2021-12-06, https://openbase.com/categories/js/best-nodejs-3d-libraries.

Billinghurst, M., Kato, H., 1999. Collaborative mixed reality. In: Proceedings of the First International Symposium on Mixed Reality, pp. 261–284.

Blackwell, L., Ellison, N., Elliott-Deflo, N., Schwartz, R., 2019. Harassment in social virtual reality: challenges for platform governance. Proceedings of the ACM on Human-Computer Interaction 3 (CSCW), 1–25.

blog.roblox.com cross site scripting vulnerability report ID: OBB-318419. 2022Accessed: 12-03-2022, https://www.openbugbounty.org/reports/318419/.

Bose, A.J., Aarabi, P., 2019. Virtual fakes: Deepfakes for virtual reality. 2019 IEEE 21st International Workshop on Multimedia Signal Processing (MMSP). IEEE. 1–1

Cannavò, A., Lamberti, F., 2021. How blockchain, virtual reality, and augmented reality are converging, and why. IEEE Consum. Electron. Mag. 10 (5), 6–13. doi:10.1109/MCE.2020.3025753.

Casey, P., Baggili, I., Yarramreddy, A., 2019a. Immersive virtual reality attacks and the human joystick. IEEE Trans Dependable Secure Comput 18 (2), 550–562.

Casey, P., Lindsay-Decusati, R., Baggili, I., Breitinger, F., 2019b. Inception: virtual space in memory space in real space–memory forensics of immersive virtual reality with the HTC vive. Digital Invest. 29, S13–S21.

Chen, H., Hou, L., Zhang, G.K., Moon, S., 2021. Development of BIM, iot and AR/VR technologies for fire safety and upskilling. Autom. Constr. 125, 103631. doi:10.1016/j.autcon.2021.103631.

Chowdhury, M.Z., Shahjalal, M., Ahmed, S., Jang, Y.M., 2020. 6G wireless communication systems: applications, requirements, technologies, challenges, and research directions. IEEE Open Journal of the Communications Society 1, 957–975. doi:10.1109/OJCOMS.2020.3010270.

CHRP-INDIA. 2021Extended reality – the new age immersive technology star. Accessed: 12-11-2021, https://www.chrp-india.com/blog/extended-reality-the-new-age-immersive-technology-star/.

Chuah, S.H.W., 2019. Why and who will adopt extended reality technology? literature review, synthesis, and future research agenda. SSRN Electronic Journal (2018) doi:10.2139/ssrn.3300469.

Colao J.J.. The hackers who revealed snapchat's security flaws received one response from the company... four months later. 2020. Accessed: 12-03-2022, https://www.forbes.com/sites/jjcolao/2014/01/02/the-hackers-who-revealed-snapchats-security-flaws-received-one-response-from-the-company-four-months-later/?sh=3740acf5c2c7.

Center for Countering Digital Hate C.. Facebook's metaverse is unsafe. 2021. Accessed: 16-01-2022, https://www.counterhate.com/.

Croft J.. 2022Lawyers zoom in on the metaverse. Accessed: 2022-10-13, https://www.ft.com/content/3f17960c-fa99-4d17-8397-1bb71f28be70.

Critical vulnerabilities in bigscreen VR app, unity allow eavesdropping, 'man-in-the-room' attacks. 2021d. Accessed: 2021-12-06, https://www.scmagazine.com/news/-/critical-vulnerabilities-in-bigscreen-vr-app-unity-allow-eavesdropping-man-in-the-room-attacks.

Cve details. 2021a. Accessed: 2021-12-06, https://www.cvedetails.com/product/3236/Epic-Games-Unreal-Engine.html?vendor_id=1613.

Cve details. 2021b. Accessed: 2021-12-06, https://www.cvedetails.com/product/30764/Nodejs-Node.js.html?vendor_id=12113.

Cve details. 2021c. Accessed: 2021-12-06, https://www.cvedetails.com/vulnerability-list/vendor_id-12113/Nodejs.html.

Dall'acqua, L., Gironacci, I., 2019. Using extended reality to support cyber security. In: Political Decision-Making and Security Intelligence: Recent Techniques and Technological Developments. IGI-Global, pp. 146–166. doi:10.4018/978-1-7998-1562-4.

Dath, C., Dath, C., Laaksolahti, J., 2017. Crime scenes in virtual reality.

Daydream. 2021Daydream view health and safety information. Accessed: 2021-10-03, https://support.google.com/daydream/answer/7185037.

De Guzman, J.A., Thilakarathna, K., Seneviratne, A., 2019. Security and privacy approaches in mixed reality: aliterature survey. ACM Computing Surveys (CSUR) 52 (6), 1–37.

de Melo Silva, C.C., Ferreira, H.G.C., de Sousa Júnior, R.T., Buiati, F., García-Villalba, L.J., 2016. Design and evaluation of a services interface for the internet of things. Wireless Personal Communications 91, 1711–1748.

Desk W.. Extended reality gaming and the future of sports (infographic). 2020. Accessed: 2021-10-03, https://www.digitalinformationworld.com/2020/07/move-over-vr-xr-sports-are-the-future-infographic.html.
Dick, E., 2021a. Balancing User Privacy and Innovation in Augmented and Virtual Reality. Technical Report. Information Technology and Innovation Foundation.
Dick, E., 2021b. Principles and Policies to Unlock the Potential of AR/VR for Equity and Inclusion. Technical Report. Information Technology and Innovation Foundation.
Dimov D.. Top 5 snapchat security vulnerabilities. 2015. Accessed: 12-03-2022, https://resources.infosecinstitute.com/topic/top-5-snapchat-security-vulnerabilities-how-the-app-learned-its-lessons/.
Dmarket Inc. Dmarket logo NFT METAVERSE. 2021a. Accessed: 25-01-2022, https://dmarket.com/.
Dmarket Inc. Dmarket logo NFT METAVERSE. 2021b. Accessed: 25-01-2022, https://dmarket.com/.
Doolani, S., Wessels, C., Kanal, V., Sevastopoulos, C., Jaiswal, A., Nambiappan, H., Makedon, F., 2020. A review of extended reality (xr) technologies for manufacturing training. Technologies 8 (4), 77.
Dremliuga, R., Dremliuga, O., Iakovenko, A., 2020a. Virtual reality: general issues of legal regulation. J Pol & L 13, 75.
Dremliuga, R., Dremliuga, O., Iakovenko, A., 2020b. Virtual reality: general issues of legal regulation. J Politics Law 13, 75. doi:10.5539/jpl.v13n1p75.
Du, R., Lee, E., Varshney, A., 2019. Tracking-tolerant visual cryptography. In: 2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR). IEEE Computer Society, Los Alamitos, CA, USA, pp. 902–903. doi:10.1109/VR.2019.8797924.
Duan, H., Li, J., Fan, S., Lin, Z., Wu, X., Cai, W., 2021. Metaverse for social good: A university campus prototype. In: Proceedings of the 29th ACM International Conference on Multimedia, pp. 153–161.
DUGGAN M.. Online harassment. 2021Accessed: 12-11-2021, https://www.pewresearch.org/internet/2014/10/22/online-harassment/.
Dwivedi, Y.K., Hughes, L., Baabdullah, A.M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M.M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C.M.K., et al., 2022. Metaverse beyond the hype: multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. Int J Inf Manage 66, 102542.
ethereum.org. The key to your digital future. 2022. Accessed: 28-07-2022, https://ethereum.org/en/wallets/.
Epic Games. Best game engines for 2022 – which should you use?2022a. Accessed: 28-07-2022, https://gamedevacademy.org/best-game-engines/.
Epic Games. Unreal engine - learning library. 2022b. Accessed: 28-07-2022, https://dev.epicgames.com/community/learning?application=unreal_engine.
Epic Games. Unreal engine marketplace. 2022c. Accessed: 28-07-2022, https://www.unrealengine.com/marketplace/en-US/store.
Facebook 360. 2021. Accessed: 2021-10-17, https://facebook360.fb.com/.
Facebook Technologies L.. Oculus go health and safety. 2021. Accessed: 2021-10-03, https://www.oculus.com/safety-center/go/.
Facebook Technologies L.. Welcome to the oculus safety center. 2021. Accessed: 2021-10-03, https://www.oculus.com/safety-center/.
Falchuk, B., Loeb, S., Neff, R., 2018. The social metaverse: battle for privacy. IEEE Technol. Soc. Mag. 37 (2), 52–61. doi:10.1109/MTS.2018.2826060.
Fast-Berglund, Å., Gong, L., Li, D., 2018. Testing and validating extended reality (XR) technologies in manufacturing. Procedia Manuf. 25, 31–38. doi:10.1016/j.promfg.2018.06.054. Proceedings of the 8th Swedish Production Symposium (SPS 2018)
Gandhi, R.D., Patel, D.S., 2018a. Virtual reality–opportunities and challenges. Virtual Real 5 (01).
Gandhi, R.D., Patel, D.S., 2018b. Virtual reality–opportunities and challenges. Virtual Real 5 (01).
GBO-Global Business Outlook. 2022Tax on metaverse: How does it work?Accessed: 2022-10-13, https://www.globalbusinessoutlook.com/tax-on-metaverse-how-does-it-work.
Global AR VR in travel and tourism market ecosystem by raw material; by components, by products, parts and devices by services and solutions, by application (3d modelling, design, training, monitoring, maintenance, others), by region and forecast by 2023. 2020. Accessed: 05-02-2022, https://www.alltheresearch.com/report/389/AR-VR-in-Travel-and-Tourism.
Global - extended reality market. 2020. Accessed: 2021-10-03, https://www.psmarketresearch.com/market-analysis/extended-reality-xr-market-insights.
Go O.. Health and safety before using the headset.: 1–15.
Gobbetti, E., Scateni, R., 1998. Virtual reality: past, present and future. Stud Health Technol Inform 58, 3–20. doi:10.3233/978-1-60750-902-8-3.
Goh E.. 3 future programming languages you should learn between 2022 and 2030. 2022. Accessed: 28-07-2022, https://betterprogramming.pub/3-future-programming-languages-you-should-learn-between-2022-and-2030-8a618a15eca6.
Goodfellow J.. A peek into the metaverse: How to prevent a virtual world from becoming a dystopian nightmare. 2021. Accessed: 25-01-2022, https://www.campaignlive.com/article/peek-metaverse-prevent-virtual-world-becoming-dystopian-nightmare/1724998.
Google. Daydream view health and safety information. 2016. Accessed: 15-01-2022, https://support.google.com/daydream/answer/7185037?hl=en.
Google. Daydream standalone safety information. 2017. Accessed: 15-01-2022, https://support.google.com/daydream/answer/9009545?hl=en#:~:text=Daydream%20should%20not%20be%20used,discomfort%2C%20immediately%20discontinue%20using%20Daydream.
Google LLC. 2022Google cardboard - experience virtual reality in a simple, fun, and affordable way. Accessed: 15-01-2022, https://developers.google.com/cardboard/.
Group F.. 2021Exciting uses for virtual reality. Accessed: 2021-10-03, https://www.fdmgroup.com/5-exciting-uses-for-virtual-reality/.
Hackerone roblox. 2021a. Accessed: 12-03-2022, https://hackerone.com/roblox?type=team.
Hackerone snapchat vulnerabilities. 2015. Accessed: 12-03-2022, https://hackerone.com/snapchat?type=team.
Hackerone snapchat vulnerabilities. 2022Accessed: 12-03-2022, https://nvd.nist.gov/vuln/detail/CVE-2018-19111#vulnCurrentDescriptionTitle.
Happa, J., Steed, A., Glencross, M., 2021a. Privacy-certification standards for extended-reality devices and services. In: 2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), pp. 397–398. doi:10.1109/VRW52623.2021.00085.
Happa, J., Steed, A., Glencross, M., 2021b. Privacy-certification standards for extended-reality devices and services. In: 2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW). IEEE, pp. 397–398.
Helping you transform healthcare training. 2022. Accessed: 03-01-2022, https://oxfordmedicalsimulation.com/.
Holt K.. meta-adds-personal-boundaries-to-horizon-worlds-and-venues-to-fight-harassment. 2022. Accessed: 22-03-2022, https://techcrunch.com/2022/02/04/meta-adds-personal-boundaries-to-horizon-worlds-and-venues-to-fight-harassment/.
How to reduce virtual reality (VR) sickness. 2022. Accessed: 22-03-2022, https://filmora.wondershare.com/virtual-reality/how-to-reduce-virtual-reality-sickness.html.
Hu, M., Luo, X., Chen, J., Lee, Y.C., Zhou, Y., Wu, D., 2021. Virtual reality: a survey of enabling technologies and its applications in iot. Journal of Network and Computer Applications 178, 102970. doi:10.1016/j.jnca.2020.102970.
Huang P.H.. The quantum technology of the future. 2021. Accessed: 20-02-2022, https://trh.gase.most.ntnu.edu.tw/en/article/content/271#:~:text=In%20terms%20of%20quantum%20communication,equipment%20manufacturing%2C%20and%20other%20technologies.
Hurtado K.. 2021Online harassment targeted by xr association. Accessed: 13-11-2021, https://parentology.com/online-harassment-targeted-by-xr-association/.
Ibanez L.. Technology: Who is building the metaverse?2021. Accessed: 25-01-2022, https://lazaroibanez.com/technology-who-is-building-the-metaverse-part-1-17461638a761.
Info CA. 2022Google cardboard android & iOS applications - unencrypted third party analytics (CVE-2018-19111). Accessed: 12-03-2022, https://www.info-sec.ca/advisories/Google-Cardboard.html.
Introduction to node.js. 2021. Accessed: 2021-12-06, https://nodejs.dev/learn.
IQT News. Quantum technology's impact on the metaverse. 2022. Accessed: 20-02-2022, https://www.insidequantumtechnology.com/news-archive/quantum-technologys-impact-on-the-metaverse/.
Jerome, J., Greenberg, J., 2021. Augmented Reality + Virtual Reality Privacy and Autonomy Considerations in Emerging, Immersive Digital Worlds. Technical Report. Future of Privacy Forum.
Johnston J., Parks J., Delaney K.B., Thompson J., Salman M.. Earth and environmental science immersive learning experiences using a google expedition kit. 2019.
Josh N.. 2021Cybersecurity: Will ar & vr open new doors for security and privacy challenges?Accessed: 2021-10-17, https://www.bbntimes.com/technology/cybersecurity-will-ar-vr-open-new-doors-for-security-and-privacy-challenges.
Kaimara, P., Oikonomou, A., Deliyannis, I., 2021. Could virtual reality applications pose real risks to children and adolescents? a systematic review of ethical issues and concerns. Virtual Real 1–39.
kaspersky. 2021What are the security and privacy risks of VR and AR. Accessed: 2021-10-03, https://www.kaspersky.com/resource-center/threats/security-and-privacy-risks-of-ar-and-vr.
Khalili J.. Roblox accused of putting 100 million players at risk of data theft. 2021. Accessed: 12-03-2022, https://www.techradar.com/news/roblox-accused-of-putting-100-million-players-at-risk-of-data-theft.
Ko, S.H., Rogers, J., 2021. Functional materials and devices for XR (VR/AR/MR) applications. Adv Funct Mater 31. doi:10.1002/adfm.202106546.
Kohnke, A., 2020. The risk and rewards of enterprise use of augmented reality and virtual reality. DUBAI COMPLIANCE 116.
Kumar P.. Ar and vr market set to witness huge growth through 2030: P&s intelligence. 2020. Accessed: 05-02-2022, https://www.prnewswire.com/news-releases/ar-and-vr-market-set-to-witness-huge-growth-through-2030-ps-intelligence-301150811.html.
Kwok, A.O.J., Koh, S.G.M., 2021. Covid-19 and extended reality (xr). Current Issues in Tourism 24 (14), 1935–1940. doi:10.1080/13683500.2020.1798896.
LaMotte S., 2022, The very real health dangers of virtual reality. Accessed: 15-01-2022, https://edition.cnn.com/2017/12/13/health/virtual-reality-vr-dangers-safety/index.html.
LaViola, J.J., Kruijff, E., McMahan, R.P., Bowman, D.A., Poupyrev, I., 2017. 3D User interfaces: Theory and practice. Addison-Wesley. https://books.google.com.pk/books?id=ilUyjwEACAAJ
LEE K.. Facebook announces it's hiring 10,000 people in EU to build 'metaverse'. 2021a. Accessed: 25-01-2022, https://www.timesofisrael.com/facebook-announces-its-hiring-10000-people-in-eu-to-build-metaverse/.
LEE K.. Facebook announces it's hiring 10,000 people in EU to build 'metaverse'. 2021b. Accessed: 25-01-2022, https://www.timesofisrael.com/facebook-announces-its-hiring-10000-people-in-eu-to-build-metaverse/.

Lee, L.H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., Kumar, A., Bermejo, C., Hui, P., 2021a. All one needs to know about metaverse: a complete survey on technological singularity, virtual ecosystem, and research agenda. ArXiv abs/2110.05352. doi:10.13140/RG.2.2.11200.05124/8.
Lee, L.H., Hui, P., 2018. Interaction methods for smart glasses: a survey. IEEE Access 6, 28712–28732. doi:10.1109/ACCESS.2018.2831081.
Lee, L.H., Lin, Z., Hu, R., Gong, Z., Kumar, A., Li, T., Li, S., Hui, P., 2021b. When creators meet the metaverse: a survey on computational arts. arXiv preprint arXiv:211113486.
Leyden J.. Researchers nab $4,000 bug bounty after discovering SSRF vulnerability in snapchat's ad platform. 2020. Accessed: 12-03-2022, https://portswigger.net/daily-swig/researchers-nab-4-000-bug-bounty-after-discovering-ssrf-vulnerability-in-snapchats-ad-platform.
Li, M., Weng, J., Liu, J.N., Lin, X., Obimbo, C., 2021. Toward vehicular digital forensics from decentralized trust: an accountable, privacy-preserving, and secure realization. IEEE Internet Things J. 9 (9), 7009–7024.
Linden B.. How to deal with abuse and harassment. 2022. Accessed: 22-03-2022, https://community.secondlife.com/knowledgebase/english/how-to-deal-with-abuse-and-harassment-r610/.
Linden Lab Headquarters. 2021Second life. EXPLORE. DISCOVER. CREATE. a new world is waiting.Accessed: 27-11-2021, https://secondlife.com/.
Lisle, R.J., 2006. Google earth: a new geological resource. Geol. Today 22 (1), 29–32.
Loom ai. empowering virtual communication with avatars. 2020. Accessed: 03-01-2022, https://loomai.com/zh.
Lütkebohle I.. World robot control software. 2008. [Online; accessed 19-July-2008], http://aiweb.techfak.uni-bielefeld.de/content/bworld-robot-control-software/.
Mahak, M., Singh, Y., 2021. Threat modelling and risk assessment in internet of things: A review. In: Proceedings of Second International Conference on Computing, Communications, and Cyber-Security. Springer, pp. 293–305.
Malwarebytes Labs. Nfts explained: daylight robbery on the blockchain. 2021. Accessed: 25-01-2022, https://blog.malwarebytes.com/explained/2021/03/nfts-explained-daylight-robbery-on-the-blockchain/.
Marr B.. 2022The fascinating history and evolution of extended reality (XR) – covering AR, VR and MR. Accessed: 12-11-2021, https://www.forbes.com/sites/bernardmarr/2021/05/17/the-fascinating-history-and-evolution-of-extended-reality-xr--covering-ar-vr-and-mr/?sh=77df0b704bfd.
Matthews, B., See, Z.S., Day, J.J., 2021. Crisis and extended realities: remote presence in the time of COVID-19. Media International Australia 178, 198–209.
Mazloumi Gavgani, A., Walker, F.R., Hodgson, D.M., Nalivaiko, E., 2018. A comparative study of cybersickness during exposure to virtual reality and "classic" motion sickness: are they different? J Appl Physiol 125 (6), 1670–1680.
McFadden C.. You could become the next virtual economy millionaire. 2020. Accessed: 05-02-2022, https://interestingengineering.com/you-could-become-the-next-virtual-economy-millionaire.
MeetinVr. Business meetings better than in real life. 2020. Accessed: 03-01-2022, https://www.meetinvr.com/.
Meta. Introducing horizon workrooms: Remote collaboration reimagined. 2021. Accessed: 15-01-2022, https://about.fb.com/news/2021/08/introducing-horizon-workrooms-remote-collaboration-reimagined/.
Microsoft Game Stack Team. Microsoft flight simulator: The future of game development. 2021. [Online; accessed 04-Dec-2021], https://developer.microsoft.com/en-us/games/blog/microsoft-flight-simulator-the-future-of-game-development/.
Microsoft hololens: Mixed reality technology for business. 2021. Accessed: 2021-09-17, https://www.microsoft.com/en-us/hololens.
Microsoft Xbox. 2021Microsoft flight simulator: Standard edition xbox : Game studios simulation. [Online; accessed 04-Dec-2021], https://www.xbox.com/en-US/games/store/microsoft-flight-simulator-standard-edition/9NXN8GF8N9HT.
Mikalauskas E.. Is roblox secure? static analysis reveals subpar security practices on roblox android app. 2021. Accessed: 12-03-2022, https://cybernews.com/security/is-roblox-secure-static-analysis-reveals-subpar-security-practices-on-roblox-android-app/.
Milgram, P., Kishino, F., 1994. A taxonomy of mixed reality visual displays. IEICE Trans Inf Syst 77 (12), 1321–1329.
Milgram, P., Takemura, H., Utsumi, A., Kishino, F., 1995. Augmented reality: a class of displays on the reality-virtuality continuum. In: Das, H. (Ed.), Telemanipulator and Telepresence Technologies, International Society for Optics and Photonics, volume 2351. SPIE, pp. 282–292. doi:10.1117/12.197321.
Miranda Katz. Augmented reality is transforming museums. 2022. Accessed: 28-07-2022, https://www.wired.com/story/augmented-reality-art-museums/.
Mordor Intelligence. Extended reality (XR) market - growth, trends, covid-19 impact, and forecasts (2021 - 2026). 2021. [Online; accessed 19-July-2021], https://www.mordorintelligence.com/industry-reports/extended-reality-xr-market.
Multi-app: The next evolution in spatial computing. 2021e. Accessed: 2021-12-06, https://forestgibson.medium.com/multi-app-the-next-evolution-in-spatial-computing-364fa4494244.
Muñoz-Saavedra, L., Miró-Amarante, L., Domínguez-Morales, M., 2020. Augmented and virtual reality evolution and future tendency. Applied Sciences 10 (1). doi:10.3390/app10010322.
Naik B.. Security threats in virtual world. 2013. Accessed: 20-02-2022, https://resources.infosecinstitute.com/topic/security-threats-in-virtual-world/.
Naser, N.M., Naif, J.R., 2022. A systematic review of ultra-lightweight encryption algorithms. International Journal of Nonlinear Analysis and Applications 13 (1), 3825–3851.
Nichols G.. 2022Meltdown averted: How VR headsets are making nuclear power plants safer. Accessed: 15-01-2022, https://www.zdnet.com/article/meltdown-averted-how-virtual-worlds-are-making-nuclear-power-plants-safer/.
Ning, H., Wang, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., Ding, J., Daneshmand, M., 2021. A survey on metaverse: the state-of-the-art, technologies, applications, and challenges. arXiv preprint arXiv:211109673.
Ong, T., Wilczewski, H., Paige, S.R., Soni, H., Welch, B.M., Bunnell, B.E., 2021. Extended reality for enhanced telehealth during and beyond COVID-19: viewpoint. JMIR Serious Games 9 (3), e26520. doi:10.2196/26520.
Orr D.. 2021Developing virtual and augmented reality environments. Accessed: 2021-10-03, https://www.nist.gov/ctl/developing-virtual-and-augmented-reality-environments.
Ost L.. 2021This is not a game: NIST virtual reality aims to win for public safety. Accessed: 2021-10-03, https://www.nist.gov/news-events/news/2018/05/not-game-nist-virtual-reality-aims-win-public-safety.
Outlaw, J., Duckles, B., 2017. Why women don't like social virtual reality: a study of safety, usability, and self-expression in social VR. The Extended Mind.
Outlaw, J., Duckles, B., 2018. Virtual harassment: the social experience of 600+ regular virtual reality (VR) users. The Extended Mind Blog 4.
Panagiotidis, P., 2021. Virtual reality applications and language learning. International Journal for Cross-Disciplinary Subjects in Education 12, 4447–4454. doi:10.20533/ijcdse.2042.6364.2021.0543.
Paul, S., Hamad, S., Khalid, S., 2019a. The role of AR/ VR in an iot connected digital enterprise for smart education. In: 2019 Sixth HCT Information Technology Trends (ITT), pp. 305–308. doi:10.1109/ITT48889.2019.9075102.
Paul, S., Hamad, S., Khalid, S., 2019b. The role of ARVR in an IoT connected digital enterprise for smart education. In: 2019 Sixth HCT Information Technology Trends (ITT). IEEE, pp. 305–308.
Pearlman K.. 2021Building responsible, safe, and inclusive extended reality ecosystems. Accessed: 2021-10-30, https://xrsi.org/wp-content/uploads/2022/04/XRSI_Recommendations_Biden-Harris_11.pdf.
Pearlman K.. Virtual reality brings real risks: Are we ready?2020.
Pearlman K., Initiative X.R.S., Visner S., Magnano M., Cameron R. Securing the metaverse-virtual worlds need REAL governance. 2021. Accessed: 05-02-2022, https://www.sisostds.org/DesktopModules/Bring2mind/DMX/API/Entries/Download?Command=Core_Download&EntryId=52969&PortalId=0&TabId=105.
Perret, J., Vander Poorten, E., 2018. Touching virtual reality: a review of haptic gloves. In: ACTUATOR 2018; 16th International Conference on New Actuators. VDE, pp. 1–5.
Polona C., André M.T., Maria N.. Metaverse: Opportunities, risks and policy implications2022;.
Powering imagination. 2021Accessed: 28-10-2021, https://corp.roblox.com/.
Public Safety Communications Research Division. 2021Psiap augmented reality. Accessed: 2021-10-03, https://www.nist.gov/ctl/pscr/funding-opportunities/past-funding-opportunities/psiap-augmented-reality.
PwC. 2022How UK organisations are using XR. Accessed: 27-11-2022, https://www.pwc.co.uk/issues/emerging-technologies/metaverse-technologies/how-uk-organisations-use-vr-ar.html.
PwC. Seeing is believing. 2019a. Accessed: 27-11-2021, https://www.pwccn.com/en/tmt/economic-impact-of-vr-ar.pdf.
PwC. Seeing is believing report 2019. 2019b. Accessed: 27-11-2021, https://www.pwc.com/SeeingIsBelieving.
Rana, M., Mamun, Q., Islam, R., 2022. Lightweight cryptography in iot networks: a survey. Future Generation Computer Systems 129, 77–89.
Rauschenberger, R., Barakat, B., 2020. Health and safety of VR use by children in an educational use case. In: 2020 IEEE Conference on Virtual Reality and 3D User Interfaces (VR). IEEE, pp. 878–884.
Reiners, D., Davahli, M.R., Karwowski, W., Cruz-Neira, C., 2021a. The combination of artificial intelligence and extended reality: a systematic review. Frontiers in Virtual Reality 114.
Reiners, D., Davahli, M.R., Karwowski, W., Cruz-Neira, C., 2021b. The combination of artificial intelligence and extended reality: a systematic review. Frontiers in Virtual Reality 2. doi:10.3389/frvir.2021.721933.
Reinhart, G., Patron, C., 2003. Integrating augmented reality in the assembly domain - fundamentals, benefits and applications. CIRP Annals - Manufacturing Technology 52, 5–8. doi:10.1016/S0007-8506(07)60517-4.
RFOX. Building the metaverse for everyone. 2021a. Accessed: 25-01-2022, https://www.rfox.com.
RFOX. Rfox nfts. 2021b. Accessed: 25-01-2022, https://www.rfox.com/rfox-nfts.
RFOX. Rfox token: The multichain token for the metaverse. 2021c. Accessed: 25-01-2022, https://www.rfox.com/rfox-token.
Robertson A.. Roblox signs music partnership with sony. 2021. [Online; accessed 04-Dec-2021], https://www.theverge.com/2021/7/6/22564922/roblox-sony-music-partnership-lil-nas-x-collaboration-licensing.
Roblox. Learn roblox studio. 2021. Accessed: 25-01-2022, https://developer.roblox.com/en-us/onboarding.
Roesner F.. 2022Who is thinking about security and privacy for augmented reality?Accessed: 15-01-2022, https://www.technologyreview.com/2017/10/19/105305/who-is-thinking-about-security-and-privacy-for-augmented-reality/.
Roesner, F., Kohno, T., Molnar, D., 2014a. Security and privacy for augmented reality systems. Commun ACM 57 (4), 88–96.
Roesner, F., Kohno, T., Molnar, D., 2014b. Security and privacy for augmented reality systems. Commun ACM 57 (4), 88–96.
Roblox Corporation. Roblox partners with sony music entertainment to bring their artists into the metaverse. 2021. [Online; accessed 04-Dec-2021], https://corp.roblox.com/2021/07/roblox-partners-sony-music-entertainment-bring-artists-metaverse/.

Roo, J.S., Gervais, R., Frey, J., Hachet, M., 2017. Inner garden: Connecting inner states to a mixed reality sandbox for mindfulness. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 1459–1470. doi:10.1145/3025453.3025743.

Rubin P.. Facebook can make VR avatars look–and move–exactly like you. 2022. Accessed: 21-11-2021, https://www.wired.com/story/facebook-oculus-codec-avatars-vr/.

Sabet M., Orand M., David W.M.. Designing Telepresence Drones to Support Synchronous, Mid-Air Remote Collaboration: An Exploratory Study; New York, NY, USA: Association for Computing Machinery, https://doi.org/10.1145/3411764.3445041.

Samantha C., Emanuel M.. They can't stop us: People are having sex with 3d avatars of their exes and celebrities. 2019. Accessed: 15-01-2022, https://www.vice.com/en_us/article/j5yzpk/they-cant-stopus-people-are-having-sex-with-3d-avatars-of-their-exes-and-celebrities.

Samsung Display Newsroom. Extended reality (XR) | technology behind metaverse. 2021. Accessed: 21-11-2021, http://global.samsungdisplay.com/27589/.

Sandee L.. 2021CNN - the very real health dangers of virtual reality. Accessed: 2021-10-03, https://edition.cnn.com/2017/12/13/health/virtual-reality-vr-dangers-safety/index.html.

Schroeder, R., 1993. Virtual reality in the real world: history, applications and projections. Futures 25 (9), 963–973. doi:10.1016/0016-3287(93)90062-X.

Schuemie, M.J., Van Der Straaten, P., Krijn, M., Van Der Mast, C.A., 2001. Research on presence in virtual reality: a survey. CyberPsychology & Behavior 4 (2), 183–201.

March 2019 security update advisory (CVE-2019-9197). 2019. Accessed: 2021-12-06, https://unity.com/security/unity-sec-1291.

May 2020 security update advisory (CVE-2020-12630, CVE-2020-12631). 2020. Accessed: 2021-12-06, https://unity.com/security/unity-sec-2143#vulnerability-details--2.

Sensorium Corporation. Best virtual reality movies to watch in 2021. 2021. [Online; accessed 04-Dec-2021], https://sensoriumxr.com/articles/best-virtual-reality-movies.

Shapovalov, V.B., Shapovalov, Y.B., Bilyk, Z.I., Megalinska, A.P., Muzyka, I.O., 2019. The google lens analyzing quality: an analysis of the possibility to use in the educational process. Educational Dimension 53 (1), 219–234. doi:10.31812/educdim.v53i1.3844.

Sharma V.. Introducing a personal boundary for horizon worlds and venues. 2022. Accessed: 22-03-2022, https://about.fb.com/news/2022/02/personal-boundary-horizon/.

Sheera F., Kellen B.. The metaverse's dark side: Here come harassment and assaults. 2021. Accessed: 15-01-2022, https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html.

Shinde, G.R., Dhotre, P.S., Mahalle, P.N., Dey, N., 2021. Internet of Things Integrated Augmented Reality. Springer.

Sillaber, C., Sauerwein, C., Mussmann, A., Breu, R., 2016. Data quality challenges and future research directions in threat intelligence sharing practice. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, pp. 65–70. doi:10.1145/2994539.2994546.

Siriwardhana, Y., Porambage, P., Liyanage, M., Ylianttila, M., 2021. A survey on mobile augmented reality with 5g mobile edge computing: architectures, applications, and technical aspects. IEEE Communications Surveys Tutorials 23 (2), 1160–1192. doi:10.1109/COMST.2021.3061981.

Skidmore P.. Why unity is so popular with 3D rendering companies and CAD firms. 2020. Accessed: 28-07-2022, https://www.cadcrowd.com/blog/why-unity-is-so-popular-with-3d-rendering-companies/.

Snap Inc. Develop with snap. 2021c. Accessed: 25-01-2022, https://developers.snap.com/.

Snap Inc. Dream it. build it. snap augmented reality. 2021d. Accessed: 25-01-2022, https://ar.snap.com/.

Sony Interactive Entertainment. 2022Playstation.VR instruction manual- includes important health and safety measures. Accessed: 15-01-2022, https://xra.org/wp-content/uploads/2020/07/health-safety-vr-use-children-educational-use-case-01.pdf.

Speicher, M., Hall, B.D., Nebeling, M., 2019a. What is mixed reality? In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–15.

Speicher M., Hall B.D., Nebeling M.. What is Mixed Reality?; New York, NY, USA: Association for Computing Machinery. p. 1–15. 10.1145/3290605.3300767.

Staff. Cybercriminals exploit the lack of regulation in the metaverse. 2021. Accessed: 25-01-2022, https://www.aluriasoftware.com/cybercriminals-exploit-the-lack-of-regulation-in-the-metaverse/.

Steele C.. 2021Consumers see themselves living in mixed reality. Accessed: 2021-12-06, https://www.pcmag.com/news/consumers-see-themselves-living-in-mixed-reality.

Stephan A.. Vr motion sickness: How to design virtual reality training for mitigation and prevention. 2021. Accessed: 22-03-2022, https://trainingindustry.com/articles/learning-technologies/vr-motion-sickness-how-to-design-virtual-reality-training-for-mitigation-and-prevention/.

Sweeney M.S.. 2021What the law can (and can't) do about online harassment. Accessed: 12-11-2021, https://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/.

Syal, S., Mathew, R., 2020. Threats faced by mixed reality and countermeasures. Procedia Comput Sci 171, 2720–2728.

Tech companies aim to take over physical world with metaverse. 2021Accessed: 28-10-2021, https://www.aa.com.tr/en/science-technology/tech-companies-aim-to-take-over-physical-world-with-metaverse/2406920.

Techliance. 2021Demand of augmented reality and virtual reality apps on the rise. Accessed: 2021-10-03, https://blog.techliance.com/augmented-reality-virtual-reality-apps-demand-increasing/.

Top 5 effective use cases of blockchain in virtual reality. 2021. Accessed: 2021-10-30, https://www.blockchain-council.org/blockchain/top-5-effective-use-cases-of-blockchain-in-virtual-reality/'.

Top elearning trends 2022: New perspectives on proctoring technology. 2022. Accessed: 05-02-2022, https://examus.com/trends-2030.

The future of community media is extended reality. 2021. Accessed: 2021-12-06, https://softengi.com/blog/the-future-of-community-media-is-extended-reality/.

The metaverse: The evolution of a universal digital platform. 2021Accessed: 28-10-2021, https://www.nortonrosefulbright.com/en-pk/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform#section1.

TrackMan. The game. any day. every day. 2020. Accessed: 2021-10-03, https://www.trackman.com/golf/simulator.

Truong J.. Is the metaverse ready for cyberattacks?2021. Accessed: 25-01-2022, https://hackernoon.com/is-the-metaverse-ready-for-cyberattacks-wj1q3725.

Tyler D.. How to choose the best video game engine. 2022. Accessed: 28-07-2022, https://www.gamedesigning.org/career/video-game-engines/.

Ueoka, R., AlMutawa, A., 2019. Emotion hacking VR: amplifying the VR fear experience using false vibrotactile heartbeat feedback. Transactions of the Virtual Reality Society of Japan 24 (3), 231–240. doi:10.18974/tvrsj.24.3_231.

Ueoka, R., AlMutawa, A., Katsuki, H., 2016. Emotion hacking VR (EH-VR): amplifying scary VR experience by accelerating real heart rate using false vibrotactile biofeedback. SIGGRAPH ASIA 2016 Emerging Technologies.

Umar A.. Metaverse for UN SDGs–an exploratory study. 2022. https://sdgs.un.org/sites/default/files/2022-05/2.1.4-27-Umar-Metaverse4SDG.pdf.

Unity : Power better collaboration and creativity. 2021f. Accessed: 2021-12-06, https://unity.com/.

unity vulnerabilities and exploits. 2021g. Accessed: 2021-12-06, https://vulmon.com/searchpage?q=unity&sortby=bydate.

Unreal build: Automotive 2021. 2021h. Accessed: 2021-12-06, https://www.unrealengine.com/en-US/events/unreal-build-automotive-2021.

Unreal engine 5 early access. 2021i. Accessed: 2021-12-06, https://www.unrealengine.com/en-US/unreal-engine-5.

Using spatial computing to combine the real world and the digital world. 2021j. Accessed: 2021-12-06, https://farmxr.com/.

VRChat Inc. Vrchat-over 25,000 community created worlds and growing. 2021. Accessed: 16-01-2022, https://hello.vrchat.com/.

VR Motion Learning GmbH and Co KG. Vr motion learning. 2020. Accessed: 2021-10-03, https://www.vr-motion-learning.com/vision.

Valluripally, S., Gulhane, A., Hoque, K.A., Calyam, P., 2021. Modeling and defense of social virtual reality attacks inducing cybersickness. IEEE Trans Dependable Secure Comput doi:10.1109/TDSC.2021.3121216. 1–1

Valluripally, S., Gulhane, A., Mitra, R., Hoque, K.A., Calyam, P., 2020. Attack trees for security and privacy in social virtual reality learning environments. In: 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC). IEEE Press, pp. 1–9. doi:10.1109/CCNC46108.2020.9045724.

VirtualSpeech. 2021Vr applications: 21 industries already using virtual reality. Accessed: 2021-10-03, https://virtualspeech.com/blog/vr-applications.

Vondrek, M., Baggili, I., Casey, P., Mekni, M., 2022. Rise of the metaverse's immersive virtual reality malware and the man-in-the-room attack & defenses. Computers & Security 102923.

Vr in gaming market size, share and impact analysis. 2020. Accessed: 05-02-2022, https://www.fortunebusinessinsights.com/industry-reports/virtual-reality-gaming-market-100271.

VulDB : vulnerability databas'. 2021. Accessed: 2021-12-06, https://vuldb.com/?product.epic:unreal_engine.

Wang, Q., Li, R., Wang, Q., Chen, S., 2021. Non-fungible token (NFT): overview, evaluation, opportunities and challenges. ArXiv abs/2105.07447.

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T.H., Shen, X., 2022. A survey on metaverse: fundamentals, security, and privacy. IEEE Communications Surveys & Tutorials.

What causes virtual reality (VR) motion sickness? 2021b. Accessed: 22-03-2022, https://www.healthline.com/health/vr-motion-sickness#prevention.

Wudunn S.. 2021Tv cartoon's flashes send 700 japanese into seizures. Accessed: 2021-10-03, https://www.nytimes.com/1997/12/18/world/tv-cartoon-s-flashes-send-700-japanese-into-seizures.html.

Xie, C., Kameda, Y., Suzuki, K., Kitahara, I., 2016. Large scale interactive AR display based on a projector-camera system. In: Proceedings of the 2016 Symposium on Spatial User Interaction. Association for Computing Machinery, New York, NY, USA, p. 179. doi:10.1145/2983310.2989183.

xrcollaboration. 2021The future is collaborative. Accessed: 2021-10-03, https://xrcollaboration.com/.

XR Safety Initiative and others. The XRSI privacy framework version 1.0, september 2020. 2021a. Accessed: 2021-10-30, https://xrsi.org/publication/the-xrsi-privacy-framework.

XR Safety Initiative. The child safety initiative. 2021a. Accessed: 2021-10-30, https://xrsi.org/programs/child-safety.

XR Safety Initiative. Help build safe and inclusive digital experiences. 2021b. Accessed: 2021-10-30, https://cyberxr.org/.

XR Safety Initiative. Helping build safe immersive environments. 2021c. Accessed: 2021-10-30, https://xrsi.org/.

XR Safety Initiative. Medical xr privacy and safety framework by xrsi. 2021d. Accessed: 2021-10-30, https://medical.xrsi.org/.

XR Safety Initiative. Ready hacker one : The XR news you can trust. 2021e. Accessed: 2021-10-30, https://readyhackerone.com/.
XR Safety Initiative. The XRSI taxonomy of XR. 2021f. Accessed: 2021-10-30, https://xrsi.org/definitions.
Yarramreddy, A., Gromkowski, P., Baggili, I., 2018. Forensic analysis of immersive virtual reality social applications: a primary account. In: 2018 IEEE Security and Privacy Workshops (SPW). IEEE, pp. 186–196.
Youtube VR. 2021. Accessed: 2021-11-1, https://vr.youtube.com/.
Zero-day disclosed in unity web player. 2021k. Accessed: 2021-12-06, https://threatpost.com/zero-day-disclosed-in-unity-web-player/113124/.
Zhongming Z., Linong L., Wangqiang Z., Wei L., et al. Robot-assisted surgery: Putting the reality in virtual reality. 2021.
Ziad, M.T.I., Alanwar, A., Alzantot, M., Srivastava, M., 2016. Cryptoimg: privacy preserving processing over encrypted images. In: 2016 IEEE Conference on Communications and Network Security (CNS), pp. 570–575. doi:10.1109/CNS.2016.7860550.
Zuckerberg M.. Connect 2021: Our vision for the metaverse. 2021a. Accessed: 28-10-2021, https://tech.fb.com/connect-2021-our-vision-for-the-metaverse/.
Zuckerberg M.. Meta - founder's letter, 2021b. Accessed: 28-10-2021, https://about.fb.com/news/2021/10/founders-letter/.

Sara Qamar is a Ph.D. candidate of Information Security from the National University of Sciences and Technology (NUST), Pakistan. She is conducting her research under the supervision of Dr. Mehreen Afzal and Dr. Zahid Anwar. Her research interests include secure software development, cyber defense, and threat analytics.

Zahid Anwar serves as Associate Professor of Cybersecurity in the Department of Computer Science and a scholar at the Sheila and Robert Challey Institute for Global Innovation and Growth at NDSU. He earned an MS and PhD in Computer Science at the University of Illinois at Urbana-Champaign, and conducted postgraduate research at Concordia University. Previously, Anwar served on the faculties of the National University of Sciences and Technology in Pakistan, the University of North Carolina at Charlotte and Fontbonne University. He has also worked as a software engineer at IBM, Intel, Motorola, the National Center for Supercomputing Applications, xFlow Research and at CERN on various projects related to information security and data analytics. Anwar's research focuses on cybersecurity policy and innovative cyber defense. He is a CompTIA certified penetration tester, security+ professional and an AWS certified cloud solutions architect.

Mehreen Afzal graduated in mathematics and received the Ph.D. degree in information security from the National University of Sciences and Technology (NUST), Pakistan, in 2010. She is currently associated with the NUST, Pakistan. Her research interests include information security and cryptology. Her contributions include research articles on cryptanalysis and design of cryptographic algorithms and protocols.