ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Technical Report

(12/2025)

XSTR.dpama

A landscape analysis for data protection of avatars in metaverse applications

Technical Report ITU-T XSTR.dpama

A landscape analysis for data protection of avatars in metaverse applications

Summary

Technical Report ITU-T XSTR.dpama provides an introduction and background on security threats and data protection in avatars and their spaces in metaverse applications and recommendations for standardization activities.

Avatars are digital representations of users within virtual environments or online platforms in metaverse applications. They can take various forms. Protection of the data of avatars which are digital and tied to users' information is a critical consideration in the metaverse applications. The data associated with avatars and their spaces include personally identifiable information (PII) and other sensitive information.

This Technical Report provides use cases for avatar interactions and activities and landscape analysis for the standards and the technologies related to avatars.

This Technical Report can be used in the design, development, evaluation and operation in order to protect the data related to avatars in the metaverse environments. It is also helpful in developing standards related to security and privacy in the metaverse.

Keywords

Avatars, interactions of avatars, metaverse, personally identifiable information (PII), protection measures, spaces, threats.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

Page

Technical Report ITU-T XSTR.dpama

A landscape analysis for data protection of avatars in metaverse applications

1 Scope

This Technical Report provides an introduction and background on security threats and data protection in avatars and their spaces in metaverse applications and recommendations for standardization activities.

This Technical Report also provides use cases for avatar interactions and activities, and landscapes for the standards and the technologies related to avatars.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 metaverse [b-ITU-T Y.4238]: A collective virtual environment where physical and virtual worlds converge, that enables users to interact with shared digital spaces, objects and services.

NOTE – A metaverse can be virtual, augmented, representative of or associated with the physical world.

3.1.2 personally identifiable information (PII) [b-ISO/IEC 29100]: Any information that (a) can be used to establish a link between the information and the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

3.2 Terms defined in this Technical Report

This Technical Report defines the following terms:

3.2.1 avatar: A digital representation or embodiment of a real-world user or entity in a virtual, augmented, mixed or extended reality environment, which may interact with other avatars or digital elements.

3.2.2 space: A virtual spatial environment in which avatars operate. The examples of space are virtual reality (VR), augmented reality (AR), mixed reality (MR) and extended reality (XR).

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

2D	2 Dimension
3D	3 Dimension
AR	Augmented Reality
GUI	Graphical User Interfaces
ID	Identification
IMT 2020	International Mobile Telecommunications 2020
MR	Mixed Reality

VR	Virtual Reality
XR	Extended Reality

5 Conventions

None.

6 Spaces

6.1 Overview

In this Technical Report, spaces refer to virtual spatial environments in which avatars operate, which can include virtual reality (VR) worlds, augmented reality (AR) spaces, mixed reality (MR) environments and extended reality (XR) environments. Extended reality (XR) is an umbrella term that encompasses all immersive technologies, including virtual reality (VR), augmented reality (AR), and mixed reality (MR).

Virtual reality (VR) is the computer-generated environment that replaces the real world and requires VR headsets. Users can explore and interact with the digital environment. Gaming, training simulations or virtual tourism are applicable in virtual reality (VR).

Augmented reality (AR) enhances the real world by overlaying digital content (e.g., text, images, 3 Dimension (3D) objects) and is viewed through smartphones, AR glasses, or tablets. Users can see and interact with digital objects in their physical environment.

Mixed reality (MR) combines elements of VR and AR, allowing digital objects to interact with the real world. MR devices track the user's surroundings and enable more advanced real-time interactions between physical and digital objects. MR is used in design, engineering, healthcare, and collaboration tools.

These technologies combine the real and digital worlds to create interactive and immersive experiences.

Table 1 illustrates the areas where avatars' spaces are applicable [b-Gujar].

Table 1 – Application of avatars' spaces

Application area	Description	Impact
Social media identity	Avatars serve as users' visual identity on social media platforms.	Enhances user engagement and personalization on social networks.
Virtual meetings	Avatars represent participants in virtual meetings, providing a more engaging and expressive way to interact.	Improves the virtual meeting experience, fostering a sense of presence and individuality.
E-commerce personalization	Avatars act as personalized shopping guides, helping users navigate e-commerce platforms based on their preferences. A virtual avatar which is specific for business domain assists businesses in providing a better virtual shopping experience to e-commerce and online shoppers. The avatar is an interactively personified image of the sales algorithm which assists in directing the potential client to their purchase.	Enhances user experience and increases user satisfaction in online shopping.

Table 1 – Application of avatars' spaces

Application area	Description	Impact
Virtual events and conferences	Attendees use avatars to represent themselves in virtual events, networking, and conferences.	Facilitates networking in a more immersive and enjoyable manner.
Gaming and entertainment	Avatars are central to gaming experiences, allowing players to immerse themselves in virtual worlds.	Elevates gaming experiences, creating a more visually appealing and personalized gaming environment.
Educational platforms	Avatars in online education represent students and educators, fostering a sense of community and engagement.	Enhances the learning environment, making it more interactive and personalized.
Health and fitness applications (apps)	Avatars guide users through virtual workout sessions, providing visual representations of exercises.	Encourages user participation and adherence to fitness routines.
Augmented reality (AR) navigation	Avatars guide users in AR navigation applications, offering a visually intuitive way to follow directions.	Simplifies navigation and enhances user experience in real-world spaces.
Customer service in virtual spaces	Avatars represent customer service agents in virtual spaces, providing a personalized and interactive support experience.	Improves the efficiency and user - friendliness of virtual customer support.
Avatar-based payments	Avatars act as digital wallets, allowing users to make secure and personalized transactions.	Offers a unique and visually appealing alternative to traditional payment methods.

Avatars' spaces will be advanced in International Mobile Telecommunications 2020 (IMT-2020), AI, and cloud computing in the future. Wearable devices (e.g., AR glasses, lightweight VR headsets) and digital twin technology have been enhancing in order to improve XR experiences.

6.2 Data related to spaces

Data related to XR (extended reality) environments where avatars operate includes various types of sensitive and personal information that require protection. The data related to personally identifiable information (PII) include the following in spaces:

a) User profiles, account details, and authentication data;

b) Biometric data (eye tracking, fingerprints, facial recognition); and

c) Voice and speech data.

The following behavioural and interaction data are included in spaces:

a) User movement patterns, gestures, and expressions;

b) Eye-tracking and gaze direction; and

c) Interaction history with other users and virtual objects.

The following environmental and spatial data are included in spaces:

a) 3D maps and scanned environments;

b) Room layout and object positioning; and

c) Real-time location tracking.

The following communication and social data are included in spaces:

a) Chat logs, voice conversations, and video recordings;

b) Friends lists and social interactions; and

c) User-generated content, such as avatars, virtual assets, and preferences.

The following device and system data are included in spaces:

a) Hardware and software configurations;

b) Sensor data from XR headsets, gloves, and wearables; and

c) Network and connectivity logs.

The data related to digital contents include the following in spaces:

a) Sensitive information; and

b) Intellectual property right (IPR) contents.

The data related to digital wallets include the following in spaces:

a) Credential information; and

b) Digital assets.

Figure 1 illustrates an example of digital contents that compose the space. The digital content is needed to have countermeasures against security threats such as forgery, tampering, theft, and leakage.

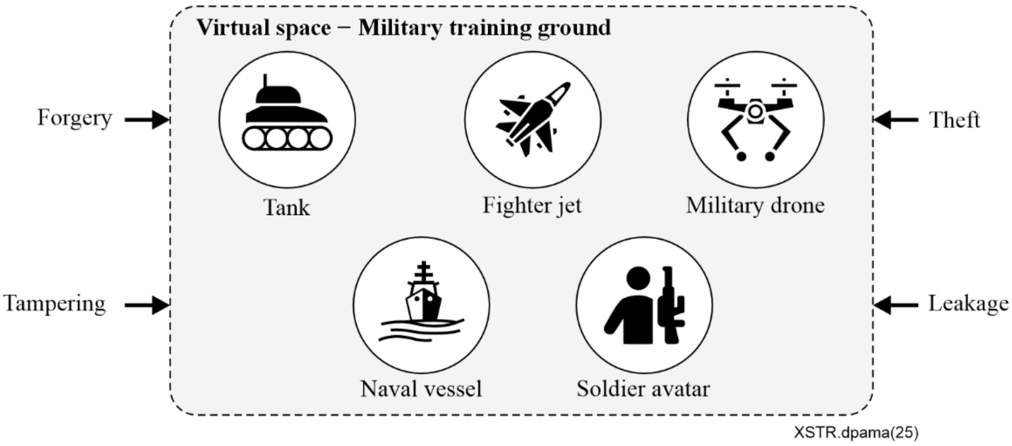

Figure 1 – Example of digital contents forming the space

7 Avatars

7.1 Overview

The term "avatar" originates from the Sanskrit word "avatāra," meaning "descent." In Hinduism, it refers to the descent of a deity to earth in a physical form. The background of avatars is deeply rooted in historical and cultural context. This concept of a higher being manifesting in a physical form has influenced the modern digital avatar. The development of graphical user interfaces (GUIs) allowed avatars to become visual representations of users.

Figure 2 illustrates examples of avatars which are customized [b-CHOSUN].

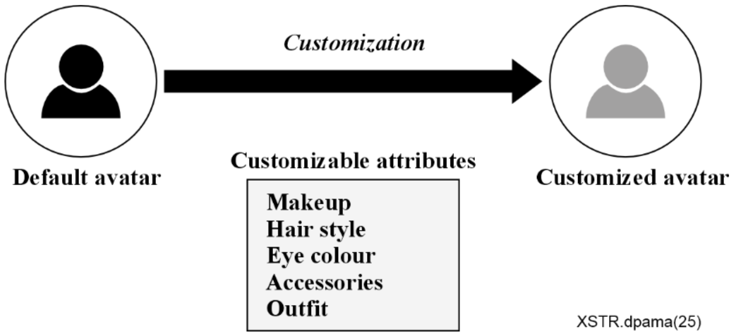

Figure 2 – Example of customized avatar

In the early days of computing, avatars were primarily text-based representations in systems where users interacted in a virtual space using text commands.

Launched in 2003, one of the use cases [b-Second Life] allowed users to create highly personalized avatars and interact in a complex virtual economy and social environment, further blurring the lines between the virtual and real worlds.

The advent of VR headsets and AR applications brought new dimensions to avatars, enabling more immersive and interactive experiences. Avatars in these environments can mimic users' movements and expressions in real-time.

The concept of the metaverse, a collective virtual shared space created by the convergence of virtually enhanced physical reality and physically persistent virtual space, relies heavily on avatars as the primary means of interaction and presence.

Social media platforms use avatars as profile pictures, which serve as the user's digital representation.

Tools have integrated avatars and virtual backgrounds to enhance remote communication, especially in professional settings.

Advances in artificial intelligence have led to the creation of more sophisticated avatars that can interact and respond to users in a human-like manner. Examples include virtual assistants and AI companions in gaming and customer service.

Technologies like deep learning enable more realistic and dynamic animations for avatars, enhancing their expressiveness and interaction capabilities.

7.2 Types of avatars

There are various types of avatars each designed for different purposes and levels of interaction in virtual environments.

2 Dimension (2D) avatars include static avatars which are simple images or icons representing the user, often used in online forums, chat rooms, and social media profiles and animated 2D avatars which are animated images or GIFs that add movement or expressions, used in messaging applications (apps) and some social media platforms.

3D avatars include basic 3D models which are simple three-dimensional characters that can move and interact within a virtual environment, used in many online games and virtual worlds and detailed 3D models which are detailed and customizable 3D avatars that can closely mimic real human appearances and movements, used in advanced gaming, virtual reality (VR) platforms, and simulation environment.

There are examples of types of avatars such as photorealistic avatars, VR/AR avatars, AI-powered avatars for chatbots and virtual assistants, social media avatars, game avatars for player characters and NPCs (non-player characters), corporate and professional avatars for virtual presenters and trainers, educational avatars for virtual students, teachers and interactive tutors, and health and therapy avatars for virtual therapists and health monitors.

User avatars represent users and system avatars are controlled by system logics or algorithms. Machine avatars represent machine or robotics. Animal avatar represents animals such as horses, dogs, and cats.

7.3 Interactions of avatars

The interaction of avatars refers to how avatars communicate, collaborate, or engage with each other and the metaverse environment.

The following types of interaction are included in interactions of avatars:

- Avatar-to-user interaction;
- Avatar-to-avatar interaction;
- Avatar-to-environment interaction;
- Avatar-to-application interaction;
- Avatar-to-device interaction.

Such interactions serve as key elements across various domains, including immersion, social connectivity, workplace collaboration, education, gaming, and commerce.

7.4 Data related to avatars

The avatar involves data related to the virtual representation and interactions. As the data of avatars which are tied to users' information are critical considerations in the metaverse applications, it is important to protect the data of avatars which is digital.

Generally, the data of avatars which are most personally identifiable information (PII) in metaverse applications may be defined as follows:

- Personal information: name, age, gender, position information, photo or image;
- Avatar attributes information: appearance traits, clothing and accessories, movements and behaviour patterns;
- Avatar behaviour data: activity history, interaction data, usage patterns;
- Social and network information: friend list, group and community participation information, messaging and communication history;
- Financial information: virtual currency and items, purchase history;
- Access information: device information, network information, connection records;
- Authentication information: login identification (IDs), passwords, two-factor authentication settings, keys; and
- Others: the other information depending on types of avatars or the virtual environment.

8 Introduction and background for security threats in avatars and their spaces

8.1 Overview

This clause provides an overview of the security threat landscape in avatars and their spaces in metaverse applications.

Security for avatars pose several challenges, largely due to the complexity of virtual environments and the integration of various technologies. Avatars can be tied to significant amounts of personal data, including real names, email addresses, and payment information. Protecting this data from unauthorized access is crucial. Avatars can generate vast amounts of data through interactions and activities within virtual environments, which can be used to profile users without their consent. Avatars can be impersonated, possessed or duplicated, leading to identity theft and fraud. Communications between avatars can be intercepted, leading to privacy breaches. Environments can be prone to harassment and abuse, impacting the privacy and security of users.

Virtual environments often operate across multiple jurisdictions, making it difficult to comply with various privacy laws and regulations. As the technology evolves, new threats and vulnerabilities continually emerge, requiring ongoing vigilance and adaptation.

Security threats in spaces impact the entire platform and its security architecture. Security threats related to avatars focus on individual users, their identity, and interactions.

8.2 Security threats for spaces

This clause provides the security threats for spaces where avatars operate, such as extended reality (XR) environments, include various security threats related to privacy, data security, identity protection, and system integrity.

These threats target the environment where avatars operate, including platforms, servers, and networks.

The security threats in identity and authentication include the following:

a) Avatar impersonation: Unauthorized users may hijack or mimic avatars, leading to identity theft or fraud;

b) Credential theft: Phishing, social engineering, or malware could be used to steal login credentials; and

c) Deepfake manipulation: AI-generated avatars or voice cloning can be used to deceive users.

The privacy and data security threats include the following:

a) Personal data exposure: XR spaces collect biometric data, location data, and behavioural analytics, which can be misused if not properly secured;

b) Unwanted tracking and surveillance: Persistent tracking of users' eye movements, gestures, and interactions may lead to invasive profiling; and

c) Unauthorized data collection: Apps or platforms may collect more data than disclosed, leading to privacy violations.

The security threats in system and infrastructure include the following:

a) Man-in-the-middle (MitM) attacks: Hackers can intercept communication between avatars or users, leading to eavesdropping or data manipulation;

b) Denial-of-service (DoS) attacks: Attackers may disrupt XR platforms, crashing servers or making spaces inaccessible; and

c) Exploits and malware: Vulnerabilities in XR software, AI systems, or hardware could be exploited for unauthorized access.

The content and interaction security threats include the following:

a) Malicious AI avatars: AI-driven avatars can be programmed for fraud, misinformation, or harmful interactions;

b) Virtual harassment and abuse: Cyberbullying, stalking, or deepfake-based deception can be major issues; and

c) Manipulated environments: Hackers may alter digital spaces to spread disinformation or psychological manipulation.

The economic and asset security threats include the following:

a) Virtual asset theft: Digital assets such as NFTs, cryptocurrency, or in-game items may be stolen through hacking.

b) Marketplace fraud: Fake transactions or scams within virtual economies can lead to financial losses.

8.3 Security threats for avatars

This clause provides the security threats for avatars that are identity theft, data breaches, fraud and manipulation. These threats affect individual users and their digital identities within virtual spaces.

The security threats related to avatars include the following:

a) Identity theft and impersonation: Stealing or cloning an avatar's identity;

b) Tracking and privacy violations: Collecting movement, speech, or biometric data without consent;

c) Social engineering and phishing: Tricking users into revealing personal data;

d) Avatar hijacking: Unauthorized takeover of an avatar's control; and

e) Harassment and cyberbullying: Exploiting avatars for psychological or social attacks.

9 Introduction and background for data protection of avatars and their spaces

9.1 Overview

This clause provides an overview of the data protections landscape in avatars interactions and activities in metaverse applications.

A metaverse application is a platform or service that provides an immersive, virtual environment where users can interact with each other and digital objects using avatars. These applications use technologies such as virtual reality (VR), augmented reality (AR), and blockchain to create a shared, persistent digital space that can support a variety of activities including socializing, gaming, working, and commerce.

Figure 3 illustrates example of metaverse applications [b-IEEE].

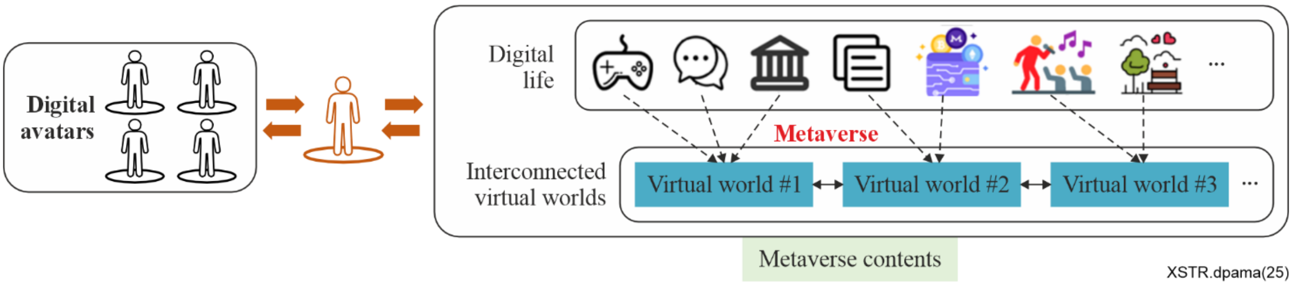

Figure 3 – Example of metaverse applications

Figure 4 illustrates sectors where avatar data is distributed or exchanged in metaverse applications.

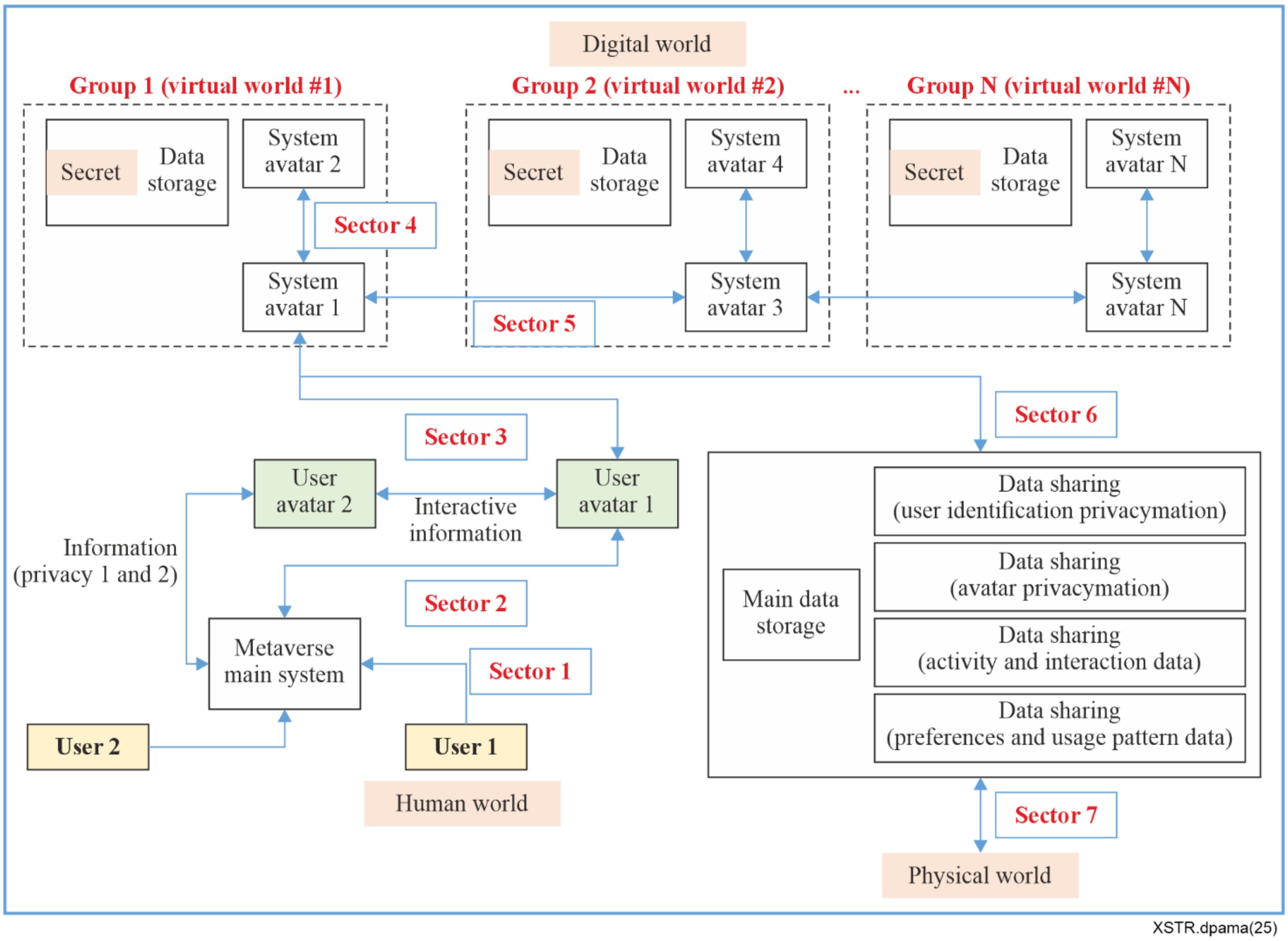

Figure 4 – Avatars' data sectors

Each sector is defined as follows:

- Sector 1: Communication space via interface between users and client metaverse main system;
- Sector 2: Communication space via interaction between user avatars and client metaverse main system;
- Sector 3: Communication space via interaction between user avatars and system avatars;
- Sector 4: Communication space via interaction between system avatars;
- Sector 5: Communication space via interaction between system avatars with different virtual world;
- Sector 6: Communication space via interaction between system avatars and main data storage; and
- Sector 7: Communication space via interface between server main data storage and physical world.

These sectors may be updated or modified by more research or study.

The personal data, digital assets and virtual identities related to avatars shall be protected against data breach, unauthorized access, theft, and misuse in each sector in Figure 4.

Generally, data protection for avatars may be defined as the following areas:

- Secure communication in metaverse network;
- End-to-end protection with security apps;
- Secure interaction between avatars and users, or between avatars and other avatars;
- Security settings and controls;
- Monitor and respond to suspicious activity of avatars;
- Authentication to users or avatars;
- Access control to resources of metaverse platform;
- Update for software and platform;
- Data encryption in storage;
- Audit;
- Backup; and
- Others.

Data protection methods may vary across different sectors. Clauses 9.2 to 9.4 aim to define the data related to avatars and provides a landscape analysis for the data protection of avatars in each sector.

9.2 Sector 1 and sector 2

9.2.1 Overview

Clauses 9.2.2 to 9.2.4 define the security environment which includes data of avatars, security threats, and measures for data protection. The data associated with avatars and their spaces include personally identifiable information (PII) and other sensitive information. User-to-avatar interaction and avatar-to-device interaction take place in sector 1 and sector 2.

User-to-avatar interaction includes the following:

- Users manipulate avatars via devices like keyboards, controllers, motion sensors, or VR gear (e.g., moving, speaking, or performing gestures);
- Users personalize their appearance, clothing, or traits to reflect identity or preferences;
- Avatars serve as a proxy for users in social interactions, using speech, text chat, or body;
- In immersive environments (like VR), users feel as if they have become the avatar, enhancing realism;
- The system responds to user inputs, creating a dynamic and interactive experience.

Avatar-to-device interaction includes the following:

- Integration with sensors, or haptic device;
- Real-world gestures mapped into virtual actions.

9.2.2 Data of avatars

In the user-to-avatar interaction, the data of avatars include the following:

- Identity data:
  - Avatar ID (username, unique identifier);
  - Visual appearance (e.g., 3D models, skin, clothes, accessories);
  - Assigned role or character traits (e.g., age, gender, occupation in a virtual world).
- Behavioural data:
  - Movement and gestures;
  - Facial expressions (e.g., via motion capture or present animations);

– Voice or text communication logs;
– Interaction logs (e.g., objects touched, places visited).

- Biometric or sensor data:
  – Voice patterns;
  – Facial tracking;
  – Eye movement or gaze tracking;
  – Body posture.
- Metadata:
  – Timestamps of interaction;
  – Location in virtual space.

In the avatar-to-device interaction, the data of avatars include the following:

- Control data:
  – Commands from the avatar to the device (e.g., move, activate, select);
  – Sensor feedback from the device to the avatar (e.g., haptic signals, visual confirmation).
- Identity data:
  – Avatar ID or credentials to authenticate access to the device;
  – Profile information or preferences used to personalize device behaviour.
- Status and context data:
  – Device status reported back to the avatar (e.g., battery level, error messages);
  – Environmental context (e.g., lighting, location) that the avatar users to adjust its interaction.
- Interaction logs:
  – History of avatar-device interaction (useful for diagnostics, personalization, or compliance).
- Biometric and sensory data if applicable:
  – Eye tracking, voice commands, gestures, or posture data captured by the device and interpreted by the avatar system.

9.2.3 Security threats

In the user-to-avatar interaction, the landscape of the security threats for the data of avatars includes the following:

- Authentication and impersonation:
  – Identity spoofing: attackers can impersonate a user to control their avatar;
  – Weak authentication: if login mechanisms are weak, unauthorized parties may hijack the avatar.
- Surveillance:
  – Behavioural tracking: Avatars may reveal sensitive behavioural patterns or preferences;
  – Biometric leakage: Gestures, voice, or eye movement data can be collected and misused.
- Data leakage:
  – Unencrypted communication: Chat, voice, and other interaction could be intercepted;
  – Contextual over-sharing: Avatars might inadvertently disclose location or identity-related metadata.

- Manipulation and social engineering:
  - Deceptive avatars: Malicious avatars might manipulate users via fake interactions;
  - Psychological profiling: Continuous avatar interaction can be used to profile users without their consent.
- Session hijacking:
  - Real-time session takeovers: If session is not protected, attackers could take over mid-interaction.
- Consent violations:
  - Non-consensual data use: Data gathered through avatars might be used beyond intended purposes;
  - Lack of transparency: Users may not be fully aware of what data is collected or shared.
- Cross-platform exploits:
  - Platform integration risks: An avatar used across multiple platforms can become a single point of failure if one platform is compromised.

In the avatar-to-device interaction, the landscape of the security threats for the data of avatars includes the following:

- Identity theft and impersonation:
  - An attacker may impersonate an avatar to gain unauthorized access to a device.
- Unauthorized access to devices:
  - If the link between the avatar and device is weakly authenticated, devices (e.g., IoT tools, smart glasses) may be controlled by malicious actors.
- Man-in-the-middle (MitM) attacks:
  - Communication between avatar and device can be intercepted or manipulated.
- Data leakage from avatar interactions:
  - Sensitive behavioural or biometric data collected during avatar-device interactions could be leaked or sold.
- Insecure device software or APIs:
  - The connected device software may include vulnerabilities.
- Malicious avatar scripts:
  - Avatars running unauthorized or malicious scripts that control devices.

9.2.4 Measures for data protection

Clause 9.2.4 describes measures to protect the data of avatars against security threats in user-to-avatar interaction and avatar-to-device interaction.

The following protection can be included in the measures:

- Secure interaction between avatars and users;
- Security settings and controls;
- Authentication to users or avatars;
- Access control to resources of metaverse platform;
- Update for software and platform;
- Data encryption in storage;
- Audit;
- Backup; and

- Others.

9.3 Sector 2, sector 3, sector 4 and sector 5

9.3.1 Overview

Clauses 9.3.2 to 9.3.4 define the security environment which includes data of avatars, security threats, and measures for data protection. The data associated with avatars and their spaces include personally identifiable information (PII) and other sensitive information. Avatar-to-avatar interaction takes place in sector 2, sector 3, sector 4 and sector 5. Avatar-to-avatar interaction includes the following:

- Text, voice, or gesture-based communication;
- Social behaviours (e.g., waving, dancing, emoting);
- Collaborative actions (e.g., building, gaming, working together).

9.3.2 Data of avatars

In the avatar-to-avatar interaction, the data of avatars include the following:

- Identity and authentication data:
  - Avatar ID and user ID;
  - Keys or authentication tokens;
  - Avatar attributes (e.g., name, appearance, affiliation).
- Communication data:
  - Text, voice, or gesture-based messages;
  - Emotional expression data (e.g., emojis, facial expressions)
  - Non-verbal cues (e.g., eye gaze, head movement).
- Positional and motion data:
  - Avatar location and orientation in 3D space;
  - Hand/arm/body movement data for gestures;
  - Motion trajectory and animations.
- Intent and interaction data:
  - Interaction triggers (e.g., handshake, object handover);
  - Engagement signals (e.g., following, approaching);
  - Shared object interaction logs.
- Security relevant data:
  - Access control data (who can interact with whom);
  - Consent or permissions;
  - Data logs for dispute resolution or auditing.
- Contextual and behavioural data:
  - Interaction history between avatars;
  - Behavioural patterns or AI-driven recommendations;
  - Presence data (e.g., online status, active/inactive).

9.3.3 Security threats

In the avatar-to-avatar interaction, the landscape of the security threats for the data of avatars includes the following:

- Impersonation and identity theft:
  - Attackers may forge or spoof an avatar to impersonate someone else.
- Harassment and abuse:
  - Verbal abuse, stalking, or inappropriate gestures between avatars;
  - Involving persistent bullying, hate speech, or sexual harassment.
- Phishing and social engineering:
  - One avatar may trick another into revealing personal or confidential information (e.g., passwords, wallet credentials).
- Malware transmission via virtual objects:
  - Sharing of malicious 3D objects or virtual items that exploit software vulnerabilities in XR systems.
- Behavioural manipulation:
  - Use of persuasive techniques to influence decisions, actions, or even emotions of other users through avatars (e.g., deepfake voices or realistic body language).
- Replay or recording attacks:
  - Recorded avatar interactions may be replayed to manipulate or frame someone, or to gather biometric behaviour data.
- Unwanted tracking:
  - Use of avatars to follow and monitor others' movement or activity across virtual spaces.

9.3.4 Measures for data protection

Clause 9.3.4 describes measures to protect the data of avatars against security threats in avatar-to-avatar interaction.

The following protection can be included in the measures:

- Secure communication in metaverse network;
- End-to-end protection with security apps;
- Secure interaction between avatars and other avatars;
- Security settings and controls;
- Monitor and respond to suspicious activity of avatars;
- Authentication to avatars;
- Access control to resources of metaverse platform;
- Update for software and platform;
- Audit;
- Backup; and
- Others.

9.4 Sector 3, sector 4, sector 5, sector 6 and sector 7

9.4.1 Overview

Clauses 9.4.2 to 9.4.4 define the security environment which includes data of avatars, security threats, and measures for data protection. The data associated with avatars and their spaces include personally identifiable information (PII) and other sensitive information. Avatar-to-environment interaction and avatar-to-application or system take place in sector 3, sector 4, sector 5, sector 6 and sector 7.

Avatar-to-environment interaction includes the following:

- Participating in simulations or games;
- Modifying virtual space (e.g., decorating rooms).

Avatar-to-application interaction includes the following:

- Using UI elements in virtual space (menus, dashboards);
- Accessing digital services (e.g., payment, identity verification);
- Triggering automated responses (AI assistants, NPCs).

9.4.2 Data of avatars

In the avatar-to-environment interaction, the data of avatars include the following:

- Identity and profile data:
  – Avatar ID (e.g., unique user handle).
  – Appearance attributes (e.g., clothing, face, body).
  – Personal settings or preferences.
- Locomotion and position data:
  – Avatar's position and movement (x, y, z coordinates).
  – Orientation and posture (head, hands, feet position).
  – Gaze direction and navigation path.
- Behavioural and interaction data:
  – Gestures, actions (e.g., waving, picking up objects).
  – Object manipulation (e.g., grabbing or pushing items).
  – Voice, chat, and text communication.
  – Interaction with other avatars or digital assets.
- Sensor and device data:
  – Inputs from motion sensors, haptics, or controllers.
  – Eye-tracking, facial expression capture, hand tracking.
  – Biometric signals if connected (e.g., heart rate in VR fitness).
- Environmental feedback data:
  – Response data from the environment (e.g., lighting change, object behaviour).
  – Triggered events or animations based on avatar actions.

In the avatar-to-application interaction, the data of avatars include the following:

- Identity data:
  – Avatar ID / user ID: Unique identifier for the avatar or its owner.
  – Profile information: Name, appearance attributes, personal settings, preferences.
- Positional and behavioural data:
  – Movement data: Position, orientation, gesture patterns, motion tracking.
  – Interaction logs: What objects or systems the avatar interacts with, and how.
  – Facial expressions / voice / emotion tracking (if supported).
- Application usage data:
  – Commands or queries: Inputs from the avatar to the system (e.g., requests, questions).
  – Activity history: Timestamped records of activities and sessions.

- Access permissions: What features or content the avatar can access.

- Security relevant data:
  - Authentication tokens: Credentials or tokens proving identity.
  - Access logs: Records of login attempts, session duration, etc.
- Derived or inferred data:
  - Behavioural patterns: Habits or preferences derived from usage.
  - AI-generated tags: System-inferred interests, emotional states, or intent.

9.4.3 Security threats

In the avatar-to-environment interaction, the landscape of the security threats for the data of avatars includes the following:

- Unauthorization:
  - Unauthorized data collection: The environment may capture behavioural, biometric, or location data without consent.
  - Overprofiling: Excessive tracking of avatar movements or interactions can lead to detailed profiling of the user.
- Surveillance and tracking:
  - Persistent tracking: Even when anonymized, avatar behaviour can be re-identified using movement or interaction patterns.
  - Location inference: Continuous tracking may reveal a user's real-world location or habits.
- Impersonation and identity theft:
  - Avatar cloning: A malicious actor may copy or replicate an avatar to deceive others.
  - Credential theft: If authentication methods are weak, attackers can take over an avatar's identity.
- Manipulation of interaction data:
  - Data tampering: Actions or logs may be altered to misrepresent user behaviour.
  - Replay attacks: Captured interaction data may be replayed to spoof real engagement.
- Data leakage:
  - Unintentional exposure: Avatar data (e.g., preferences, communications) may be leaked through weakly secured APIs or cloud storage.
  - Third-party sharing: Environment operators may share avatar interaction data with advertisers or unknown third parties.
- Behavioural manipulation:
  - Adaptive environments: AI-powered environments may tailor content based on avatar behaviour to manipulate user decisions or emotions.
- Biometric exploitation:
  - Facial expressions, gestures, or voice patterns collected during interactions can be used for biometric profiling or future spoofing.

In the avatar-to-application interaction, the landscape of the security threats for the data of avatars includes the following:

- Data interception during transmission:
  - Unencrypted communication between the avatar and application can be intercepted (e.g., man-in-the-middle attacks).

- Unauthorized data collection:
  - Applications may collect more data than needed from the avatar.
- Identity theft or impersonation:
  - Stolen avatar credentials or digital identifiers can be used to impersonate a user.
- Inference attacks:
  - Applications infer sensitive traits (e.g., emotional state, preferences, health) from seemingly harmless avatar data.
- Lack of user consent or transparency:
  - Avatar-to-application interfaces may not fully inform users of what data is being used or shared.
- Data modification or injection:
  - Malicious applications could alter avatar data or inject false inputs.
- Insecure storage in applications:
  - Applications store avatar-related data without proper encryption or access controls.

9.4.4 Measures for data protection

Clause 9.4.4 describes measures to protect the data of avatars against security threats in the avatar-to-environment interaction and the avatar-to-application interaction.

- The following protection can be included in the measures: Secure communication in metaverse network;
- End-to-end protection with security apps;
- Secure interaction between avatars and application or environment;
- Security settings and controls;
- Monitor and respond to suspicious activity of avatars;
- Authentication to avatars or application;
- Access control to resources of metaverse platform;
- Update for software and platform;
- Data encryption in storage;
- Audit;
- Backup; and
- Others.

10 Use cases for avatars interactions and activities

10.1 Overview

Clauses 10.2 to 10.6 provide use cases of avatars in metaverse applications and describes key features of metaverse. These use cases may include the methods to protect the data of avatars if applicable. These use cases show examples for the interaction of avatars refers to how avatars communicate, collaborate, or engage. The interaction examples include avatar-to-user interaction, avatar-to-avatar interaction, avatar-to-environment interaction, avatar-to-application interaction and avatar-to-device interaction.

10.2 Use case 1

Use case 1 [b-SK Ifland] is a metaverse platform which opened on 14 July 2021. It is designed to enable users to engage in various activities within a virtual space. It demonstrates the diverse possibilities of the metaverse, offering new ways of communication and experiences for both individuals and businesses. As of 16 August 2023, more than 500 000 users have made IfHome in it. On 31 March 2025, it closed its service.

Key features include the following:

a) Avatar customization: Users can create and customize their own avatars, providing a more personalized experience;

b) Virtual spaces: Various themed virtual spaces are available, allowing users to engage in activities in their preferred environments. For example, there are meeting rooms, concert halls, amusement parks, and more;

c) Social features: The platform includes real-time communication and collaboration features, enabling users to meet friends or network with new people;

d) Events and activities: it supports a variety of events and activities to keep users engaged. For instance, concerts, exhibitions, and workshops can be held within the virtual space; and

e) Business applications: Companies can also utilize it for virtual meetings, product launches, training sessions, and more. This enables global collaboration beyond physical limitations.

10.3 Use case 2

Use case 2 [b-IMVU] is a 3D avatar-based social networking platform launched in 2004, which can be seen as an early form of a metaverse system. It is an early form of a metaverse system, providing a platform where users can express themselves, interact with others, and experience a variety of activities in a virtual world. Through elements such as social networking, customization, economic systems, and user-generated content, it showcases the potential of the metaverse.

Key features include the following:

a) Avatar customization: It offers a wide range of options for users to create and customize their own avatars. Users can personalize their avatars with different hairstyles, outfits, accessories, and more. This serves as a significant way for users to express themselves in the virtual world;

b) Virtual spaces: It provides various themed virtual spaces where users can engage in activities. Each space has its unique design and features, allowing users to explore and meet friends in different environments;

c) Social interaction: One of the core functions is social interaction. Users can chat in real-time with other users through their avatars, make friends, and participate in group activities. It offers an experience similar to social networking in the real world;

d) Economic system: It has a virtual economy system. Users can purchase avatar items, virtual spaces, and services using virtual currency. Additionally, users can design and sell their own items to generate revenue;

e) User-generated content (UGC): It actively encourages user-generated content. Users can create and share their own items, virtual spaces, animations, and more with others. This is a crucial aspect that enhances creativity and diversity within the platform; and

f) Events and community activities: It hosts various events and community activities to keep users engaged. Virtual parties, contests, group activities, and more are regularly held.

10.4 Use case 3

Use case 3 [b-VRChat] is a virtual reality social platform where users can interact within a metaverse environment. It is a platform that implements several key elements of the metaverse, supporting creative and social experiences for users. This demonstrates that the metaverse goes beyond simple virtual reality and plays a crucial role in forming a new type of digital society.

Key features include the following:

a) User-generated content: One of the key features is that users can create and share their own content. Users can create their own 3D avatars and design various virtual spaces to share with others. This reflects the core element of the metaverse, which is a user-driven environment;

b) Diverse interactions: Users can communicate with each other through voice chat, text chat, and gestures. Additionally, users can cooperate or compete with each other in various mini-games or activities. These interactions provide a social experience similar to the real world;

c) Rich virtual spaces: It offers a wide variety of themed and styled virtual spaces. For example, users can engage in activities in fantasy worlds, futuristic cities, natural environments, and more. It allows users to freely explore and experience the environment they desire;

d) Community-centric: It is a community-centric platform where people with various interests and hobbies can form communities. For instance, discussion groups on specific topics, gaming clubs, and cultural events can be hosted. This makes the metaverse more than just a virtual space; it functions as an actual social network; and

e) Cross-platform compatibility: It is accessible on various VR headsets and desktop environments, making it highly accessible. It allows a diverse range of users to participate in the metaverse, forming a larger user base.

10.5 Use case 4

Use case 4 [b-Roblox] is a notable example of a metaverse system, allowing users to experience various activities in a virtual world. It is a platform that realizes the concept of the metaverse through diverse user experiences, social interactions, economic systems, and user-driven content creation. These elements provide an environment where users can transcend the boundaries between reality and virtuality, communicating, creating, and enjoying in new ways.

Key features include the following:

a) User-generated content: One of the main features is that users can create and share their own games and experiences. It is closely linked to the core element of the metaverse, which is user-driven content creation. Anyone can use the development tools to create their own virtual world and share it with users globally;

b) Avatars and customization: Each user can create and customize their own avatar. This allows users to express themselves and participate in various activities within the virtual world;

c) Social interaction: It provides a platform for users to make friends, play games together, and engage in various social activities. This strongly supports the important element of social interaction within the metaverse;

d) Virtual economy: It operates an economic system using its own virtual currency. Users can use it to purchase avatar items or trade in-game items created by other users. It enables economic activities within the metaverse;

e) Variety of experiences and events: It offers games and events of various genres, allowing users to continuously have new experiences. For example, concerts, movie screenings, educational programmes, and other events can be held in the virtual space; and

f) Cross-platform accessibility: It is accessible on various devices including PC, mobile, and consoles, allowing users to connect to the virtual world anytime and anywhere. This enhances the accessibility and connectivity of the metaverse.

10.6 Use case 5

Use case 5 [b-Second Life] is a virtual world developed in 2003 and is considered one of the early forms of the metaverse. In 2013 it had approximately one million regular users. By the end of 2017 the active user count had declined to "between 800 000 and 900 000".

Key features include the following:

a) User-generated content: Users can create buildings, items, clothing, and more, and then trade these creations. It allows users to express creativity and engage in economic activities within the metaverse.

b) Economic system: It features a virtual economy similar to real-world economies. Users use a virtual currency called "Linden dollars" to buy and sell goods, and this currency can be exchanged for real money.

c) Social interaction: It emphasizes interaction between users. Users can communicate with others through avatars, form groups, and participate in virtual events. This highlights the important characteristic of social connectivity in the metaverse.

d) Virtual space: It provides an extensive 3D virtual space where users can live and explore environments similar to the real world. This space consists of various locations that users can freely navigate and interact with.

e) Scalability: It is continuously updated and expanded to meet user demands and technological advancements. This demonstrates that the metaverse is a progressively developing and evolving digital ecosystem.

10.7 Use case 6

Use case 6 [b-Meta Horizon] is an online virtual reality game with an integrated game creation system developed and published by Meta Platforms. On this multi-player virtual platform, players move and interact with each other in various worlds that host events, games, and social activities.

10.8 Use case 7 [b-VIVERSE]

Use case 7 [b-VIVERSE] is an open platform for virtual worlds and environments and encompassing multiple devices and applications. Conceived as a metaverse, the platform is intended to create an interconnected series of virtual worlds and includes elements of augmented reality.

11 Recommendations for standardization activities

11.1 Overview

Clauses 11.2 to 11.4 provide trend of the avatar-related standards which have been developing, established or published in IEEE, IEC, ISO and ISO/IEC JTC 1. This clause suggests the need for additional standards for data protection of avatars based on the landscape of the avatar-related standards. Avatars may carry sensitive biometric and personal data, such as facial recognition details, voice patterns, and behavioural characteristics. With avatars being used across multiple virtual environments and platforms, there is a need for consistent data protection standards to ensure uniform security. Standardized protocols are required to securely share avatar data between different metaverse applications without compromising security.

11.2 IEEE

11.2.1 IEEE 3079 Working Group (human factors for immersive content WG)

The IEEE 3079 Working Group investigates human factors in virtual reality (VR), mixed reality (MR), and augmented reality (AR) environments, aiming to standardize the analysis of user behaviour and interactions in interactive and immersive content. The group's major standard documents address motion training systems, motion tracking and retargeting, quality evaluation of digital humans, and privacy in avatar interactions.

11.2.2 IEEE 3079.2 Mixed reality standard framework for motion training

This standard defines the basic framework within the overall architectural framework for motion training systems. This standard includes definitions for the functions and input/output interfaces of each component module, and the related data components and formats. To utilize this standard basic framework, various application-specific user interface/user experience (UI/UX) and service frameworks are specified. The meaning of "motion training" includes:

a) Human gestures and postures; and

b) Animated human gestures and postures.

The basic framework for VR/MR-based motion training systems includes the following:

a) Standardizes the architecture of motion training systems, the functionalities of individual modules, input/output interfaces, and data formats; and

b) Encompasses human motions (gesture & posture), animated movements, and representations of human animation in VR/MR environments.

Motion tracking includes the following:

a) Transitioning from traditional optical motion capture systems (e.g., Vicon, OptiTrack) to non-optical technologies. Advancements include the development of inertial sensors (IMU) and AI-based markerless motion capture methods;

b) Active research into camera-based markerless motion tracking using AI and deep learning – for example, tracking motions with a single camera; and

c) An increasing number of multiplatform tracking systems are being developed based on the OpenXR standard, supporting cross-compatibility among VR/MR devices.

Motion retargeting and evaluation include the following:

a) Advancements in motion retargeting algorithms using deep neural networks allow for mapping movements onto various avatars;

b) Ongoing research into personalized motion retargeting techniques in VR environments, incorporating adjustments that reflect users' physical characteristics; and

c) Development of frameworks to evaluate the accuracy of motion training systems, focusing on the consistency between motion capture data and actual movements.

Motion-training system includes the following:

a) Development of VR/MR-based real-time motion feedback learning systems that incorporate HMDs and haptic devices;

b) Increasing research on AI-based personalized motion guidance in medical and sports training; and

c) Commercialization of immersive training systems that integrate head mounted displays (HMD) with haptic devices.

11.2.3 IEEE 3079.3 Framework for evaluating the quality of digital human

The IEEE 3079.3 standard is an international standard that provides a framework for evaluating the quality of digital humans. It aims to establish objective and quantitative quality assessment criteria in line with the advancement of digital human technology. This standard includes a system for assessing key quality elements of digital humans, such as accuracy, realism, interactivity, and functionality.

This standard includes the following:

a) Digital human quality evaluation criteria which defines core quality factors of digital humans, such as realism, expressiveness, and naturalness;

b) Evaluation methodology which provides objective evaluation metrics alongside both quantitative and qualitative analysis techniques;

c) Evaluation models by application area which examines the applicability of evaluation models across various industries, including entertainment, education, healthcare, and the metaverse; and

d) Ethical and social considerations: Includes guidelines to address the ethical responsibilities and privacy protections associated with digital human technologies.

11.2.4 IEEE 3079.3.2 Framework for privacy protection through identifiability management arising from avatar interaction

IEEE 3079.3.2 is a standard for the protection and management of personally identifiable information (PII) generated during avatar interactions in metaverse environments. This standard defines the principles and management framework for the collection, storage, processing, sharing, deletion, and protection of PII, and it provides technical, administrative, and legal guidelines for safeguarding personal information on metaverse platforms.

This standard aims to address the following key issues:

a) Preventing identity tracking and privacy breaches through avatar interactions;

b) Developing techniques for protecting and anonymizing VR/AR-based user motion data;

c) Establishing a framework for data sharing and managing third-party access within the metaverse; and

d) Ensuring alignment with global personal data protection regulations (such as GDPR, CCPA, etc.).

Figure 5 illustrates general architecture.

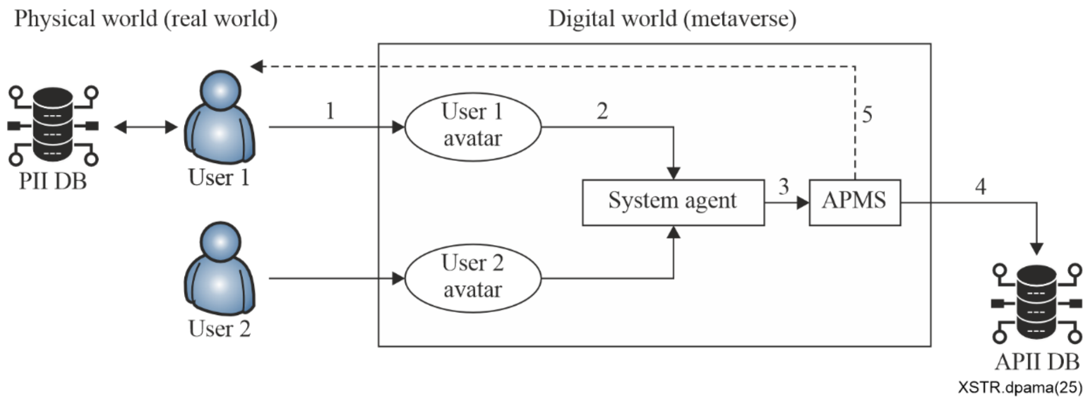

Figure 5 – General architecture

This framework standardizes the protection of personal information generated during avatar interactions in metaverse environments. It emphasizes a clear separation between physical world personal data (PII DB) and metaverse avatar data (APII DB) through a user-avatar authentication system. Key features include:

a) User authentication and avatar creation: Users authenticate with personal data to create their unique avatars with all information encrypted during transmission;

b) Real-time monitoring: System agents continuously monitor avatar interactions to detect privacy exposure risks; and

c) Risk-based alerts: The avatar privacy management system (APMS) analyses interaction data and provides staged alerts based on identified risk levels, empowering users to protect their personal information proactively.

Figure 6 illustrates avatar personal information protection architecture based on system agent.

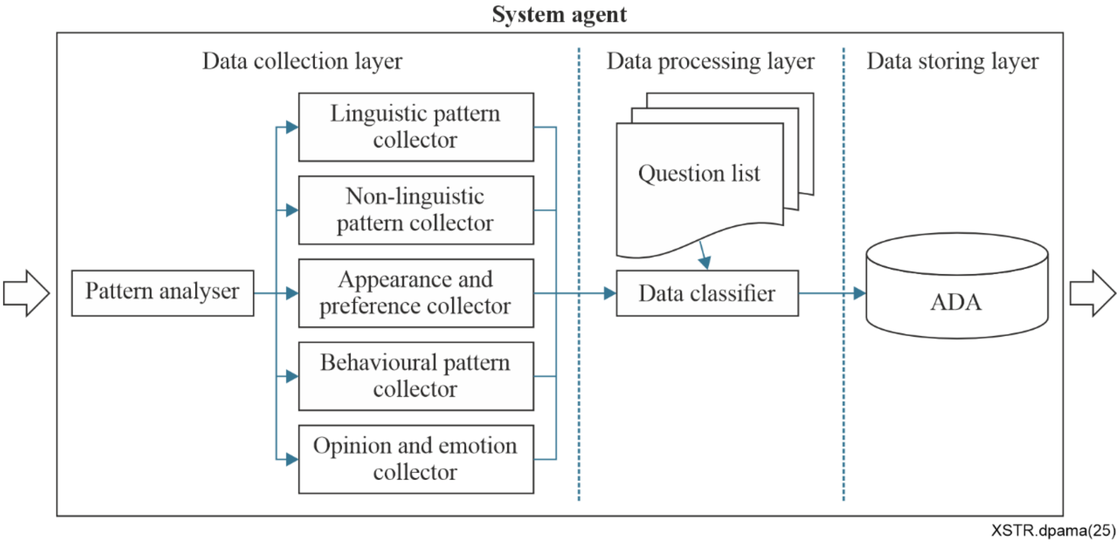

Figure 6 – Avatar personal information protection architecture based on system agent

This architecture outlines a three-layered backend service designed to manage and safeguard avatar interactions on a metaverse platform. The system is organized as follows:

a) Data collection layer: A pattern analyser directs data to five specialized collectors covering linguistic, non-linguistic, appearance, behavioural, and emotional cues;

b) Data processing layer: A question list establishes security criteria, while a data classifier organizes and prepares the collected data for secure storage;

c) Data storing layer: The avatar data archive (ADA) serves as a central repository, ensuring data is securely stored and easily retrievable; and

d) This structured approach ensures consistent data management and security for complex metaverse interactions.

Avatar privacy management system (APMS) architecture is critical for processing and managing data from the avatar data archive to ensure comprehensive privacy protection in the metaverse. Its core components include:

a) Pattern frequency analysis: Evaluates interaction data to identify recurring patterns and potential privacy implications;

b) Privacy level classifier: Categorizes data based on sensitivity and determines additional security measures, with highly sensitive data transferred to a secure APII DB;

c) Risk alert generator: Monitors classified data in real-time and issues timely alerts to users, enabling proactive privacy protection; and

d) Overall, APMS integrates these processes to provide robust risk management and maintain a secure, trustworthy metaverse experience.

Figure 7 illustrates framework for avatar privacy management system.

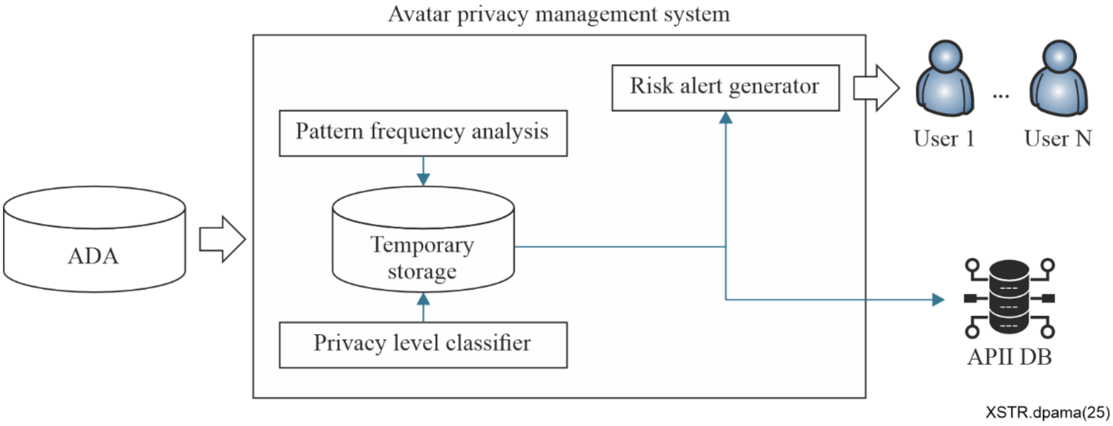

Figure 7 – Framework for avatar privacy management system

11.3 IEC, ISO and ISO/IEC JTC 1

11.3.1 ISO/IEC JTC 1 SC 24 Visual security in the metaverse

This document provides standard data model for mapping 2D images to 3D avatar faces using deepfake technology, enabling secure storage and exchange.

This work item is currently under development in SC 24/WG 10. Ad Hoc Groups will then be created in SC 24 to progress this work.

11.3.2 ISO/IEC JTC 1 SC 27 ISO/IEC 27001 Information security management systems-Requirements

This document is the world's best-known standard for information security management systems (ISMS). It defines requirements an ISMS must meet.

The [b-ISO/IEC 27001] standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this international standard.

With cyber-crime on the rise and new threats constantly emerging in the metaverse, it can seem difficult or even impossible to manage cyber-risks. ISO/IEC 27001 may help information security management in Metaverse be developed.

11.3.3 ISO/IEC JTC 1 SC 27 ISO/IEC 15408 series Evaluation criteria for IT security

Part 1 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT security products.

Part 2 includes a catalogue of functional components that meets the common security functionality requirements of many IT security products.

Part 3 includes the individual assurance components from which the evaluation assurance levels and other packages contained in [b-ISO/IEC 15408-5] are composed, and the criteria for evaluation are protection profiles (PPs), PP-configurations, PP-modules, and security targets (STs).

Part 4 provides a standardized framework for specifying objective, repeatable and reproducible evaluation methods and evaluation activities.

Part 5 provides packages of security assurance and security functional requirements that have been identified as useful in support of common usage by stakeholders.

ISO/IEC 15408 series may help security requirements for IT security products which are defined and evaluated in the metaverse.

11.3.4 ISO/IEC JTC 1 SC 27 ISO/IEC 19790 Security requirements for cryptographic modules

This document specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in information and communication technologies (ICT). It defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity and a diversity of application environments. This document specifies up to four security levels for each of the 11 requirement areas with each security level increasing security over the preceding level.

[b-ISO/IEC 19790] may help security requirements for cryptographic modules which provide security services in the metaverse.

11.3.5 ISO/IEC JTC 1 SC 27 ISO/IEC 24759 Test requirements for cryptographic modules

This document specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2025. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories.

This document also specifies the information that vendors are required to provide testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformity to the requirements specified in ISO/IEC 19790:2025.

Vendors can also use this document to verify whether their cryptographic modules satisfy the requirements specified in ISO/IEC 19790:2025 before applying to a testing laboratory for testing.

ISO/IEC 24759 may help test methods for cryptographic modules which are defined and tested in the metaverse.

11.3.6 ISO/IEC JTC 1 SC 27 ISO/IEC TS 20540 Test requirements for cryptographic modules

This document provides recommendations and checklists which can be used to support the specification and operational testing of cryptographic modules in their operational environment within an organization's security system.

The cryptographic modules have four security levels which ISO/IEC 19790 defines to provide for a wide spectrum of data sensitivity (e.g., low-value administrative data, million-dollar funds transfers, life-protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g., a guarded facility, an office, removable media, and a completely unprotected location).

This document includes:

a) Recommendations to perform secure assessing for cryptographic module installation, configuration and operation;

b) Recommendations to inspecting the key management system, protection of authentication credentials, and public and critical security parameters in the operational environment;

c) Recommendations for identifying cryptographic module vulnerabilities;

d) Checklists for the cryptographic algorithm policy, security guidance and regulation, security manage requirements, security level for each of the 11 requirement areas, the strength of the security function, etc.; and

e) Recommendations to determine that the cryptographic module's deployment satisfies the security requirements of the organization.

[b-ISO/IEC TS 20540] may help the guidelines how to use cryptographic modules which provide security services in their application environment such as the metaverse.

11.3.7 ISO/IEC JTC 1 SC 27 ISO/IEC TS 27115 Cybersecurity evaluation of complex systems

This document provides the foundations and concepts for the cybersecurity evaluation of complex systems. Two frameworks are defined:

a) The first is used to specify the cybersecurity of a complex system, including system of systems; and

b) The second is used to evaluate the corresponding cybersecurity solutions.

The frameworks use basic architecture concepts:

a) to enable description of reference or solution cybersecurity architectures;

b) to support model-based, comprehensive and scalable security solutions and their evaluation; and

c) to allow for the definition of architecture-based cybersecurity profiles (ACP) and hierarchies of profiles.

[b-ISO/IEC CD TS 27115] may help the cybersecurity evaluation of complex systems which are applicable in the metaverse.

11.3.8 ISO/IEC WD 27504.2 Privacy protection of user avatar and system avatars interactions in the metaverse

This document provides requirements for protecting privacy information during interactions between user avatars and system avatars in the metaverse.

This document identifies and classifies the privacy information generated and used by user avatars and system avatars and addresses privacy threats in the spaces where the avatar operates during the interactions between the user avatar and the system avatar.

11.3.9 ISO/IEC JTC 1 SC 27 PWI 27575 Privacy for metaverse frameworks

This PWI aims to analysis a landscape of elements, personal identifiable information (PII), privacy threats, and privacy protection measures in the metaverse framework.

It provides a landscape of regulations, industry approaches and standards development in order to protect PII in the metaverse frameworks.

It will suggest a standard that provides a structured set of principles, guidelines, and technical and policy mechanisms designed to protect PII within general metaverse environments. [b-ISO/IEC PWI 27575]

11.4 Recommendation of additional new standards

This subclause suggests additional necessary standards based on the findings of this Technical Report.

To protect avatars' data in the metaverse, the following recommendation for new international standards can be included:

- **Suggested standard 1: Privacy framework for avatar-related data**:
  - Defining categories of PII associated with avatars (e.g., biometric gestures, behaviour patterns, inferred preferences);
  - Requiring explicit consent, data minimization, and purpose limitation;
  - Including privacy-preserving mechanisms (e.g., anonymization, differential privacy) in avatar data.

- **Suggested standard 2: Identity and authentication framework for avatars**:
  - Establishing standardized digital identity models for avatars with support for pseudonymity and revocable credentials;
  - Defining multi-factor and biometric authentication for controlling avatar access;
  - Ensure secure linkage between real-world users and virtual avatars.
- **Suggested standard 3: Security control for avatar interactions environments**:
  - Defining secure communication protocols between avatars and metaverse platform;
  - Protecting against impersonation, avatar cloning, and session hijacking.
- **Suggested standard 4: Risk management and threat modelling for avatars**:
  - Developing a threat model specific to avatars (e.g., identity theft, deepfake attacks, behavioural tracking);
  - Suggesting continuous risk assessment frameworks for avatar spaces.
- **Suggested standard 5: Interoperability and portability framework for avatars**:
  - Ensuring avatars and their data can be securely transferred across different metaverse platforms;
  - Suggesting standardized formats and schemas for avatar profiles and attributes.
- **Suggested standard 6: Secure spatial data exchange in the metaverse environment**:
  - Defining protocols and encryption requirements for real-time transmission of spatial, behavioural and environmental data;
  - Protecting against interception, spoofing or tampering of spatial data exchanged between devices and cloud/XR services.
- **Suggested standard 7: Interoperable data labelling and usage control for the assets in the metaverse environment**:
  - Setting metadata and usage policy labelling rules for 3D models and user-generated content;
  - Ensuring secure, lawful reuse or transfer of data between virtual worlds.
- **Suggested standard 8: Requirements for avatars signature and integrity**:
  - Signing digitally each avatar's actions (e.g., chat, movements, transactions);
  - Ensuring that the avatar has not been altered maliciously and that it originates from a legitimate source.

12 Research trend of avatars and their spaces

12.1 Overview

This clause provides the research trend for security and privacy issues on avatars and their spaces in academia and industry. This clause provides the technology trend which has been developing in the area of creating and using digital human and its legal or ethical issues.

12.2 Advances in AI-based digital human creation technologies

Recent developments in generative AI and deep learning have drastically enhanced the quality of digital humans. The integration of high-resolution 3D modelling, real-time animation, natural language processing (NLP), and emotion recognition AI has led to the creation of digital humans that are nearly indistinguishable from real people.

Digital human generation using generative AI includes the following:

a) AI models (e.g., GANs, NeRF, StyleGAN) have been developed to automatically generate digital humans from text or image inputs;

b) The combination of AI-driven facial synthesis (Deepfake technology) with 3D scanning techniques enables the real-time generation of customized digital humans; and

c) Leading research institutions and companies are actively developing high-quality AI avatar generation models.

Deep learning-based real-time animation and motion generation includes the following:

a) Moving beyond traditional motion capture methods, AI now learns from user facial expressions and body movements to generate natural, real-time animations;

b) Companies are researching deep learning-based motion capture technologies to enhance digital human movements; and

c) The integration of AI-based voice synthesis and emotion expression technologies is enabling more natural conversational digital humans.

Photorealistic virtual characters is developing as the following:

a) Real-time rendering technologies based on AI (e.g., Unreal Engine 5, Unity HDRP) are improving the texture quality of digital humans and enhancing immersion;

b) AI precisely renders skin, hair, and muscle movements, providing tactile realism similar to actual human sensations; and

c) High-quality digital human implementations have been showcased at major technology conferences such as CES 2023 and SIGGRAPH.

12.3 Expanded use of digital humans in the metaverse and virtual environments

As digital humans become increasingly integral in the metaverse, VR/AR platforms, gaming, and virtual meetings, the need for quality evaluation criteria is becoming even more critical.

Increased utilization in the metaverse includes the following:

a) Companies are building AI-driven metaverse environments where digital humans are actively utilized;

b) Digital humans are being adopted for user interaction in virtual conferences, education, remote work, and entertainment; and

c) Advances in AI-based avatar generation and customizable features have led to the rise of personalized digital humans.

Virtual humans and AI influencers rise as follows:

a) AI influencers are increasingly active in social media, advertising, and the entertainment industry;

b) Companies are employing digital humans for brand promotion and customer service, strengthening marketing strategies via AI characters; and

c) There is a growing need for evaluation criteria addressing the identity and personalization of AI-generated digital humans.

Expanded roles in virtual education and healthcare includes the following:

a) AI-driven digital humans are being used in remote medical consultations and psychological counselling;

b) Digital human models, such as virtual patients and medical training avatars, are increasingly employed in medical education and practical training, intensifying the need for quality evaluation standards; and

c) Virtual teachers (AI tutors) and virtual trainers in sports training require evaluation criteria that assess interactivity and reliability.

12.4 Emerging legal and ethical issues of digital humans

As digital humans proliferate in society, establishing guidelines for legal regulation and ethical issues has become essential.

Reliability and transparency of digital humans include the following:

a) When AI-based digital humans closely mimic real individuals in appearance and voice, risks such as misuse (Deepfake), fraud, and the spread of fake news can arise; and

b) International standard bodies like IEEE, ISO, IEC, ISO/IEC JTC 1, ITU-T and NIST are developing technical and legal guidelines to ensure the reliability of digital humans.

Data privacy and personal information protection includes the following:

a) The process of AI-based digital human learning can lead to risks of personal data breaches and misuse; and

b) Compliance with data protection laws such as the EU's GDPR (General Data Protection Regulation) and the U.S. CCPA (California Consumer Privacy Act) necessitates establishing standards for handling the data collected by digital humans.

Intellectual property and copyright issues include the following:

a) Ongoing discussions about whether AI-generated digital humans can hold independent copyrights and how the ownership rights of creators should be determined; and

b) Resolving copyright and ownership issues for AI avatars and virtual influencers requires clear legal definitions and the establishment of international standards.

Ethical guidelines for digital human use have been establishing as the following:

a) The potential of digital humans to replace human labour has raised ethical debates on the impact of AI-driven automation on the job market;

b) Discussions are underway in some countries and academic circles on whether AI digital humans should be granted the same legal and social rights as humans; and

c) Guidelines for corporate social responsibility (CSR) in the development and operation of AI-based digital humans are needed, considering their potential emotional and psychological impact on people.

12.5 Unique identifiability of VR/AR motion data and privacy risks

Recent studies indicate that motion data collected from VR headsets and controllers could serve as powerful biometric information uniquely identifying individual users.

UC Berkeley research findings (2023) include the following:

a) Analysis of data from over 50 000 users playing the VR game beat saber, using machine learning techniques, demonstrated that just 100 seconds of head and hand movement data can identify a specific user with 94% accuracy; and

b) This is the first case showing that motion itself in VR/AR environments can serve as key identifying data, distinct from conventional biometrics like facial recognition or fingerprints.

The following risks of motion data-based user identification (ID) are included:

a) VR/AR devices continuously track user movements in real time, and such data is inherently accessible to platform operators;

b) In metaverse environments, multiple companies and service providers might share or exploit this data, posing new threats to personal privacy; and

c) Unlike traditional Internet services where users can control the disclosure of personal information, in VR/AR environments, motion data can inadvertently function as a unique identifier even without explicit consent.

The following further research and mitigation strategies are needed:

a) In June 2023, UC Berkeley researchers analysed behaviour patterns and identity inference using movement data from over 1 000 users, achieving a confidence level exceeding 40%; and

b) This study suggests that beyond identification, motion data could potentially reveal insights into a user's background, behavioural patterns, and even health information, highlighting the urgent need for a robust personal data protection framework.

Consequently, multi-user VR applications and metaverse platforms need to implement both technical and administrative safeguards to protect privacy. The IEEE 3079.3 standard should also be updated to address these emerging privacy risks.

12.6 Privacy protection techniques in the literature

In response to privacy concerns regarding avatars in the metaverse, researchers have begun exploring various solutions aimed at mitigating risks associated with the disclosure of private information. This clause discusses the proposed solutions that aim to create a secure metaverse environment.

Figure 8 illustrates the diagram of privacy protection techniques.

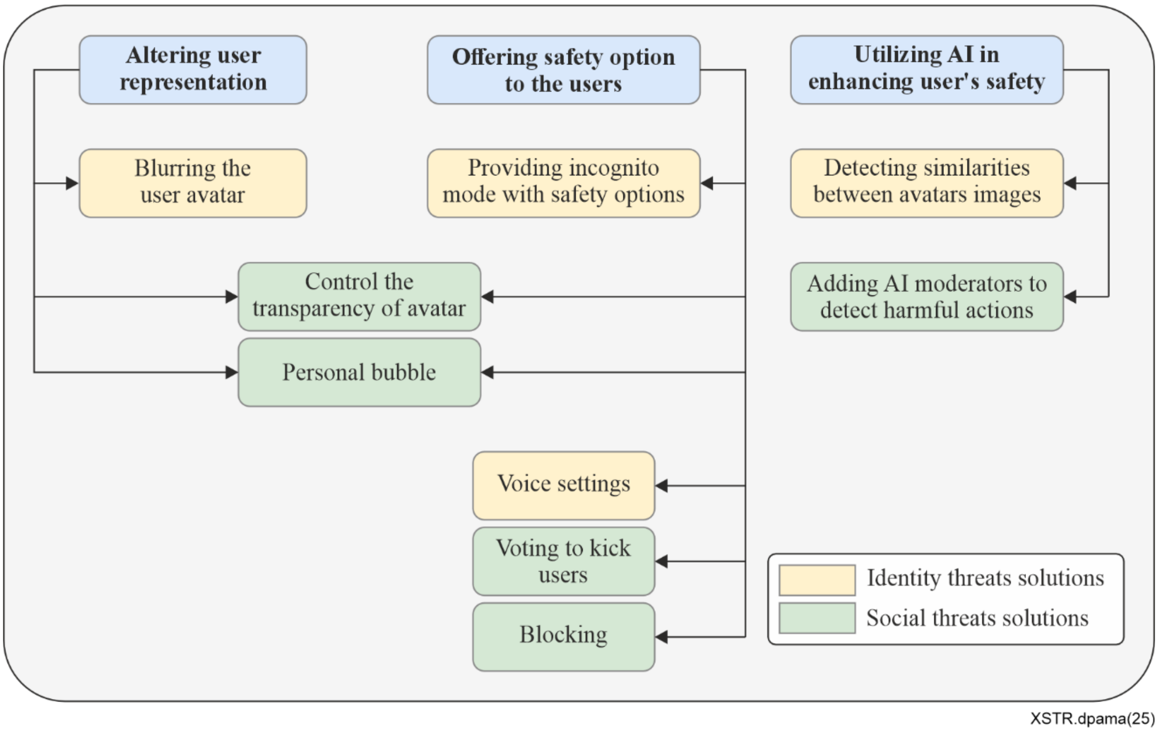

Figure 8 – Diagram of privacy protection techniques

Several researchers have identified threats related to user identities, including personal information and emotional disclosure, avatar cloning, and real user identification. To address these issues, various strategies have been proposed to enhance user identity privacy. One notable solution is presented by Wang et al. [b-Wang], who introduced a method called BlurReality. This approach involves blurring the user's avatar when reconstructing it from reality to the virtual environment using a Gaussian blur. The BlurReality technique allows users to maintain privacy regarding their emotions and surroundings, making it more challenging to identify them through the blurred avatar. A user study indicated that 80% of participants preferred using their blurred avatar when interacting with unfamiliar individuals, as it provided greater privacy and reduced feelings of embarrassment. Users reported that BlurReality gave them confidence that their sensitive information would not be disclosed by others. However, the study also noted that the blurred representation diminished the sense of presence and realism, leading to reduced user satisfaction.

Similar approaches aimed at reducing the accuracy of user data have been proposed by Nair et al. [b-Nair] and Yao et al. [b-Yao]. [b-Nair] introduced MetaGuard, an open-source plugin for the unity engine designed to help developers enhance privacy in their metaverse applications. MetaGuard aims to lower the accuracy of user data to prevent attackers from obtaining useful information. The defence mechanisms include protecting the user's voice, height, room size, and more. For instance, the voice pitch can be altered to obscure gender and ethnicity detection, while noise can be added to the edges of the user's room to prevent others from inferring room size based on avatar movement. MetaGuard also offers users three types of settings: the ability to toggle incognito mode, select specific defences, and control privacy levels to balance accuracy and privacy based on current usage. The proposed defences have shown effectiveness in reducing attacks, significantly lowering the ability of machine learning models to detect users' gender, ethnicity, age, and income, even at the lowest privacy settings.

[b-Yao] provided additional defence options that can be visualized on a voodoo doll, including adjustments to eye tracking and pupil reflection. However, this study did not include evaluation details, leaving the effectiveness of the proposed system unproven.

In addition to techniques for minimizing user identification, a solution addressing the issue of avatar cloning has been proposed by Zelenyanszki et al. [b-Zelenyanszki]. Their approach utilizes machine learning to detect cloning activities. When a user enters the virtual world, a unique NFT avatar is created based on an uploaded image representing the user's physical appearance. The system compares similarities in appearance and behaviour between avatars to detect cloning attempts and notify the affected user. The implementation involves comparing the uploaded image's similarities, using string comparison for token URIs and an image processing library to assess pixel differences. Similar images may receive a similarity score of around 63%, while nearly identical images can score over 95%. However, since cloning can occur from the same user, additional criteria need to be considered to enhance the system, including behavioural data comparisons.

Overall, researchers have proposed various solutions to protect users' identities in the metaverse from being leaked or cloned. While these solutions show promising results in maintaining user privacy, they also present several limitations and trade-offs, such as impacts on user experience, missing features, and system constraints. Addressing these challenges will be crucial for the successful implementation of privacy-enhancing measures in the metaverse.

Bibliography

[b-ITU-T Y.4238] Recommendation ITU-T Y.4238 (2025), *Requirements for integrating virtual and physical worlds through digital twins in the metaverse*.

[b-ISO/IEC 15408-5] ISO/IEC 15408-5:2026, *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security. Part 5: Pre-defined packages of security requirements*. <https://www.iso.org/standard/15408-5>

[b-ISO/IEC 19790] ISO/IEC 19790:2025, *Information security, cybersecurity and privacy protection – Security requirements for cryptographic modules*. <https://www.iso.org/obp/ui/es/#iso:std:iso-iec:19790:ed-3:v1:en>

[b-ISO/IEC 24759] ISO/IEC 24759:2025, *Information security, cybersecurity and privacy protection – Test requirements for cryptographic modules*. <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:24759:ed-4:v1:en>

[b-ISO/IEC 27001] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. <https://www.iso.org/standard/27001>

[b-ISO/IEC 29100] ISO/IEC 29100:2024, *Information technology – Security techniques –Privacy framework.* <https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-2:v1:en>

[b-ISO/IEC TS 20540] ISO/IEC TS 20540:2025, *Information security, cybersecurity and privacy protection – Testing cryptographic modules in their field*. <https://www.iso.org/standard/84247.html>

[b-ISO/IEC CD TS 27115] ISO/IEC WD TS 27115 (n.d.), *Cybersecurity evaluation of complex systems*. <https://www.iso.org/standard/81627.html>

[b-ISO/IEC WD 27504.2] ISO/IEC WD 27504.2 (2026), *Privacy protection of user avatar and system avatar interactions in the metaverse*. <https://www.iso.org/standard/89525.html>

[b-ISO/IEC PWI 27575] ISO/IEC PWI 27575:2025, *Privacy framework in the metaverse including support on AI agent orchestration.* <https://ipen.trialog.com/wiki/ISO#PWI_27575_Privacy_framework_in_the_metaverse_including_support_on_AI_agent_orchestration_(Started_in_March_2025)>

[b-IEEE] Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T.H., and Shen, X. (2022), *A Survey on Metaverse: Fundamentals, Security, and Privacy*. <https://arxiv.org/abs/2203.02662>

[b-CHOSUN] The CHOSUN Daily. <https://www.chosun.com/national/national_general/2018/2HXMXPC7WZHNXH2BNFX6LILS7Q/>

[b-Gujar] Gujar, V. (2024), *Avatars as Digital Identity: A Case Study of Avatar in Facial Recognition Technology & eKYC* by IndoAI. Saudi Journal of Engineering and Technology. <https://saudijournals.com/media/articles/SJEAT_93_165-172.pdf>

[b-IMVU] Together Labs. "*IMVU – 3D avatar-based social metaverse*". IMVU. <https://www.imvu.com>

[b-Meta Horizon] Meta Platforms, Inc. *Meta Horizon Worlds – Explore, play, and create in VR*. <https://www.meta.com/horizon-worlds/>

[b-Nair] Nair, V., Garrido, G.M., Song, D. (2022), *Going incognito in the metaverse*: Achieving theoretically optimal privacy-Usability tradeoffs in VR. <http://arxiv.org/abs/2208.05604>

[b-Roblox] Roblox Corporation. *Roblox – Reimagining the way people come together*. <https://www.roblox.com>

[b-Second Life] Linden Lab. "*Second Life – The virtual world created by its residents*". <https://secondlife.com>

[b-SK Ifland] SK Telecom, "*ifland – SK Telecom's metaverse platform*". <https://pestle-analysis.com/products/sktelecom-swot-analysis>

[b-VIVERSE] HTC Corporation. (2025). "*VIVERSE – Open, secure, and immersive metaverse ecosystem*". <https://www.viverse.com>

[b-VRChat] VRChat Inc. "*VRChat – The immersive social VR platform*". VRChat. <https://hello.vrchat.com>

[b-Wang] Wang, C.Y., Sriram, S., & Won, A.S. (2021), *Shared Realities: Avatar Identification and Privacy Concerns in Reconstructed Experiences*. Proceedings of the ACM on Human-Computer Interaction, Volume 5. <https://doi.org/10.1145/3476078>

[b-Yao] Yao, P., Lympouridis, V., & Zyda, M. (2021), *Virtual equipment system: Face mask and voodoo doll for user privacy and self-expression options in virtual reality*. IEEE. <https://doi.org/10.1109/VRW52623.2021.00256>

[b-Zelenyanszki] Zelenyanszki, D., Hóu, Z., Biswas, K., & Muthukkumarasamy, V. (2023), *A privacy awareness framework for NFT avatars in the metaverse*. <https://doi.org/10.1109/ICNC57223.2023.10074107>