<2025 ITU-T Workshop>

Privacy Issues for Metaverse Frameworks

April 11th 2025

HoonJae LEE
Dongseo University, Busan, KR
hjlee@dongseo.ac.kr

Agenda

1. Introduction to some Metaverse Frameworks or Platforms

2. Privacy Issues for Metaverse Frameworks

3. Conclusive Remarks

[Appendix] ITU FG-MV(Focus Group on Metaverse)

Editor group

HoonJae Lee(KR): hjlee@dongseo.ac.kr

HeeBong Choi(KR): hhbchoi@gmail.com

Antonio Kung(FR): antonio.kung@trialog.com

Rusne Juozapaitiene(LT): rusne@duomenuapsauga.eu

Vishnu KANHERE(IN): vkanhere@gmail.com

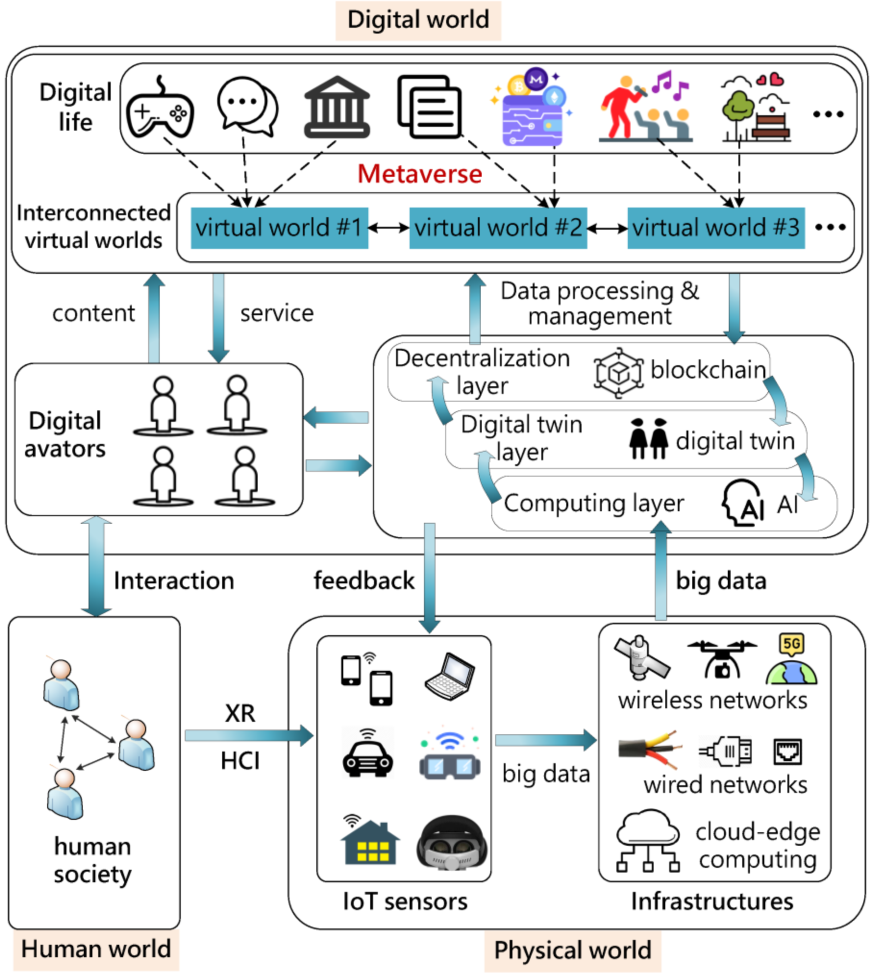
Dae-Ki Kang(KR): dkkang@dongseo.ac.kr

1. Introduction to some Metaverse Frameworks or Platforms

ISO/IEC 27573 “Privacy Protection of User Avatar and System Avatar Interactions in Metaverse “

Definition and Characteristics of Metaverse

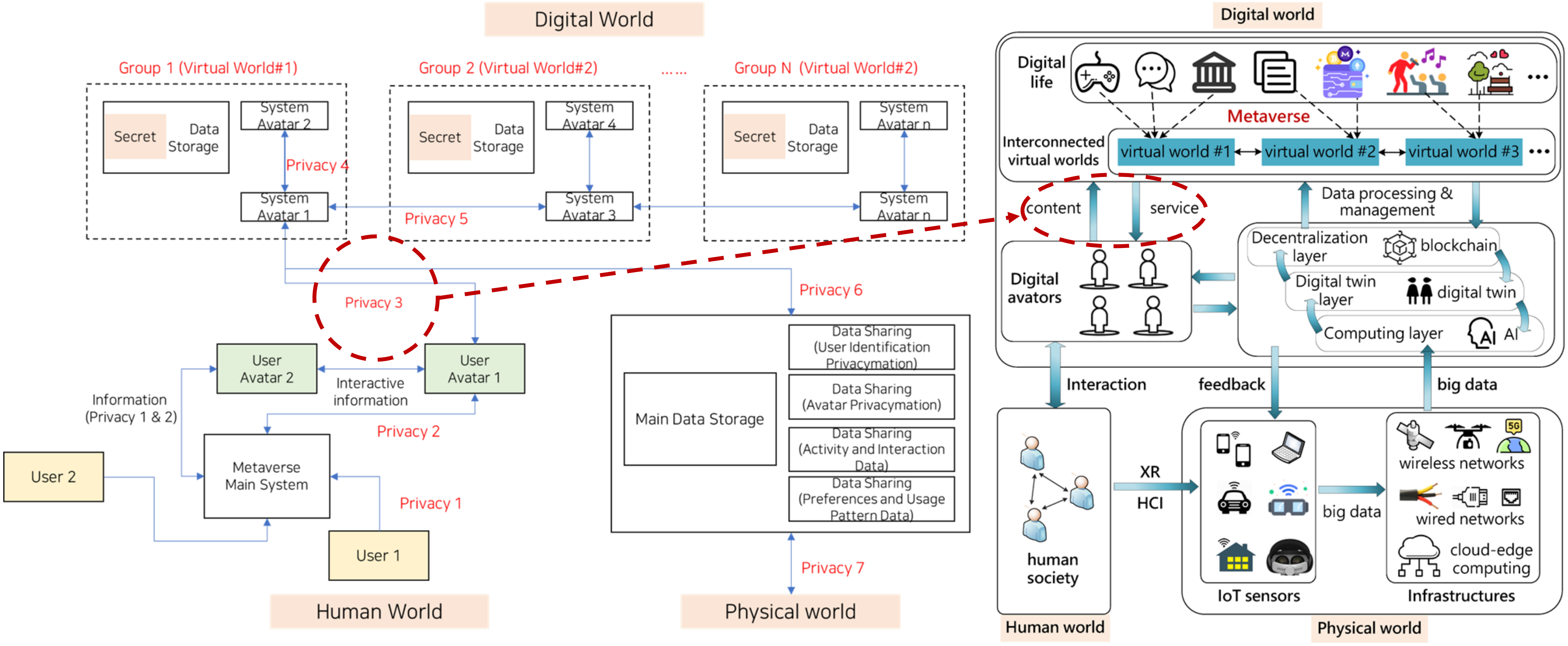
- According to Wang (2023), the Metaverse represents the paradigm of the next-generation Internet and an evolving reality. It aims to provide a shared space where individuals can play, work, and communicate through self-contained virtual environments that allow for complete immersion, functioning as an ultra-dimensional space.
- Based on the advancements in recent technologies like augmented reality, artificial intelligence, and blockchain, the Metaverse may not only embody but also exceed the imaginations depicted in science fiction, materializing into the realm of reality.
- : Wang Y., “A Survey on Metaverse: Fundamentals, Security, and Privacy”, IEEE Access, Volume: 11 , Issue: 3 , March 2023



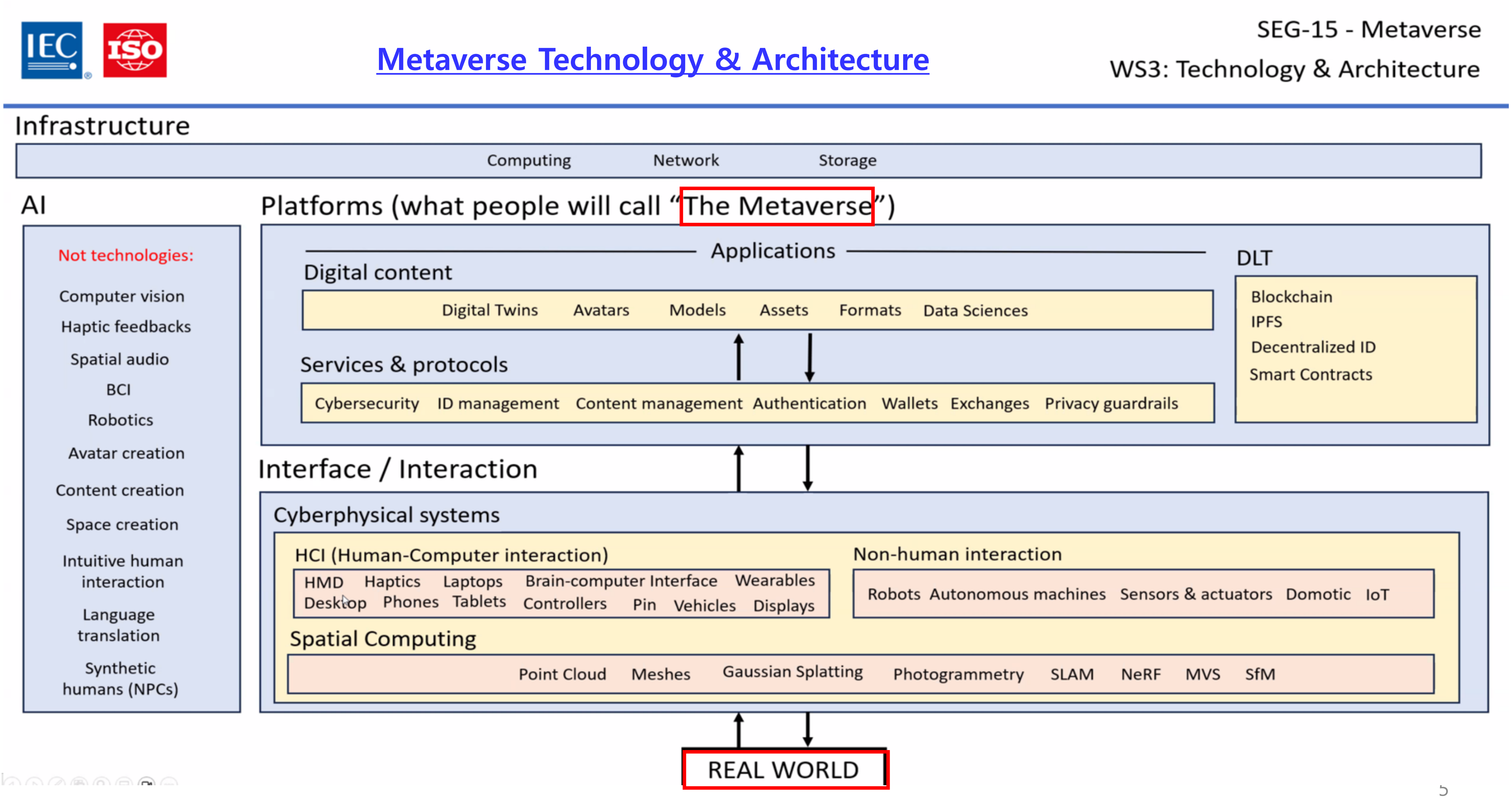
IEEE

ISO/IEC 27573 “Privacy Protection of User Avatar and System Avatar Interactions in Metaverse “

Scope of Application



IEC SEG15 WS3 Technology & Architecture – “Metaverse Platforms” (by Antonio Kung)



Metaverse Technology & Architecture

SEG-15 - Metaverse

WS3: Technology & Architecture

Infrastructure

Computing Network Storage

AI

Not technologies:

Computer vision
Haptic feedbacks
Spatial audio
BCI
Robotics
Avatar creation
Content creation
Space creation
Intuitive human interaction
Language translation
Synthetic humans (NPCs)

Platforms (what people will call “The Metaverse”)

Applications

Digital content

Digital Twins Avatars Models Assets Formats Data Sciences

Services & protocols

Cybersecurity ID management Content management Authentication Wallets Exchanges Privacy guardrails

DLT

Blockchain
IPFS
Decentralized ID
Smart Contracts

Interface / Interaction

Cyberphysical systems

HCI (Human-Computer interaction)

HMD Haptics Laptops Brain-computer Interface Wearables
Desktop Phones Tablets Controllers Pin Vehicles Displays

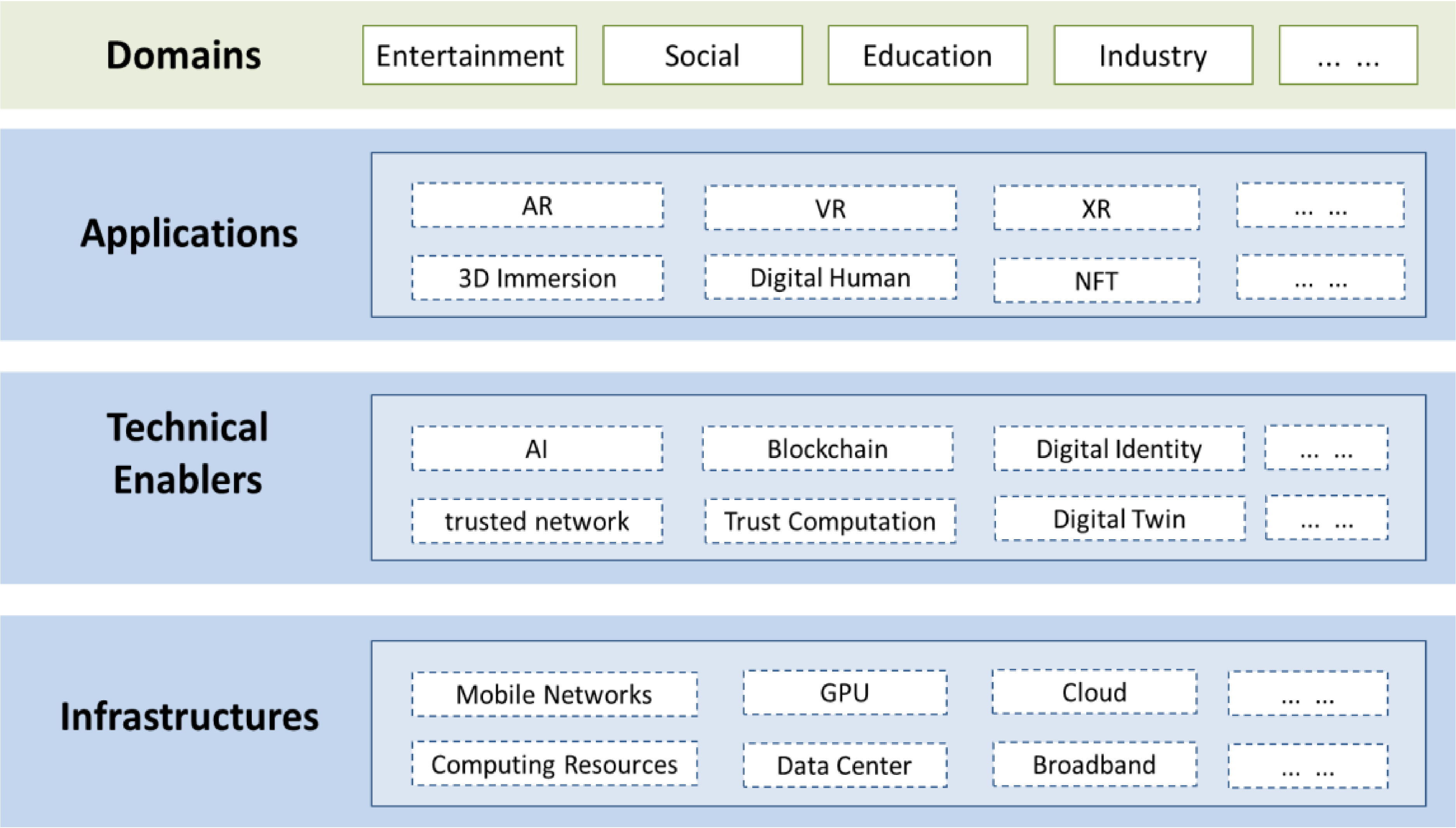
Non-human interaction

Robots Autonomous machines Sensors & actuators Domotic IoT

Spatial Computing

Point Cloud Meshes Gaussian Splatting Photogrammetry SLAM NeRF MVS SfM

REAL WORLD



Domains

Entertainment | Social | Education | Industry | … …

Applications

AR | VR | XR | … …

3D Immersion | Digital Human | NFT | … …

Technical Enablers

AI | Blockchain | Digital Identity | … …

trusted network | Trust Computation | Digital Twin | … …

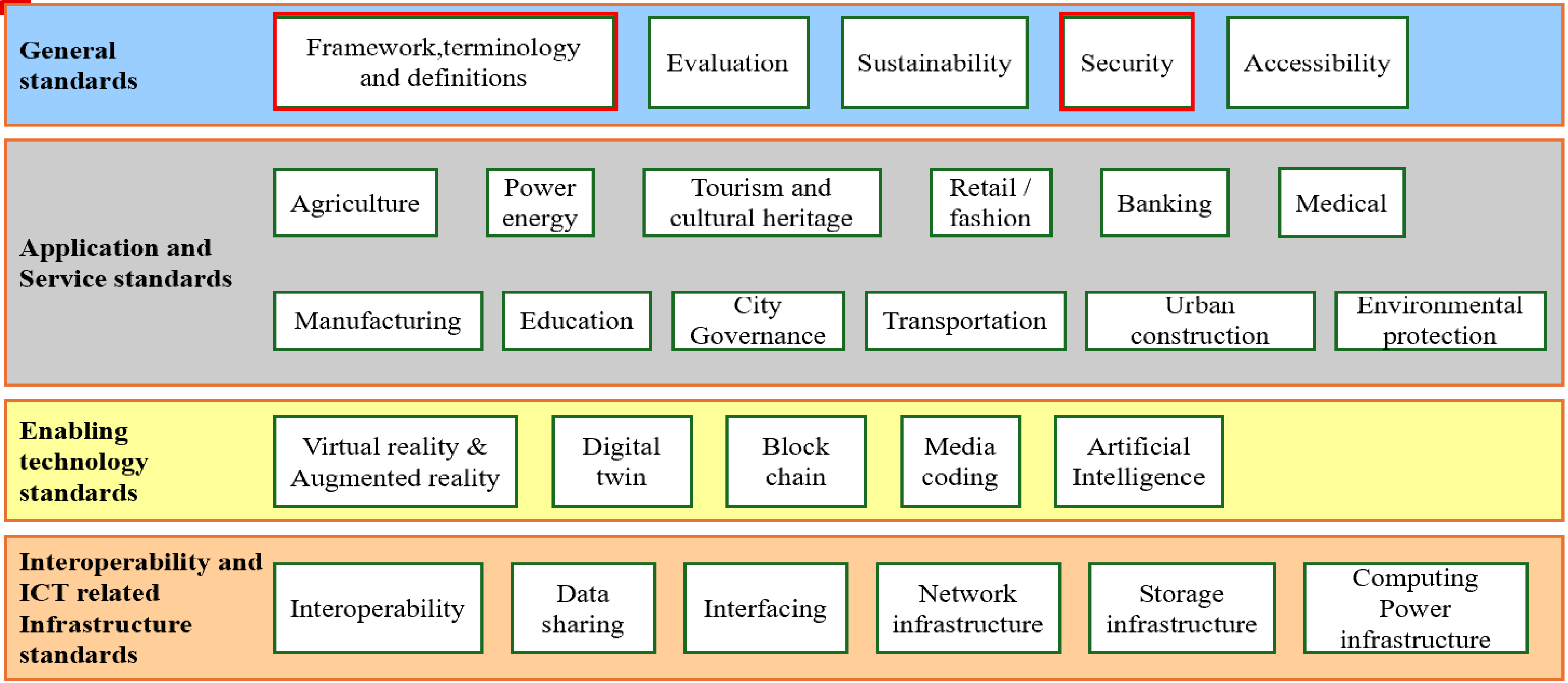
Infrastructures

Mobile Networks | GPU | Cloud | … …

Computing Resources | Data Center | Broadband | … …

A **reference model** for a trustworthy metaverse

[ITU-T] FG-MV(Focus Group on Metaverse) FGMV-51 “2024 - Standardization roadmap for metaverse”



General standards

Framework,terminology and definitions | Evaluation | Sustainability | Security | Accessibility

Application and Service standards

Agriculture | Power energy | Tourism and cultural heritage | Retail / fashion | Banking | Medical

Manufacturing | Education | City Governance | Transportation | Urban construction | Environmental protection

Enabling technology standards

Virtual reality & Augmented reality | Digital twin | Block chain | Media coding | Artificial Intelligence

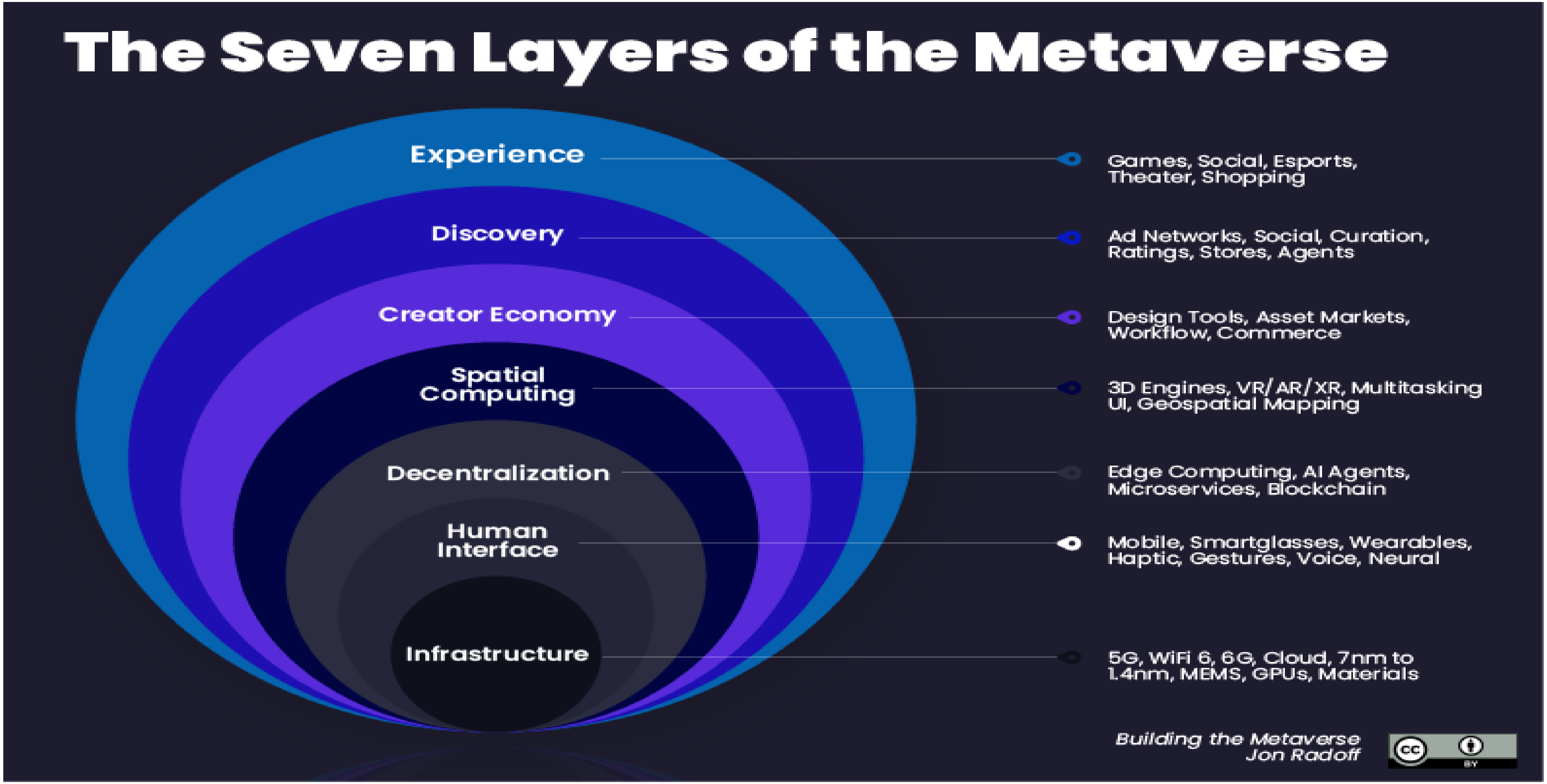
Interoperability and ICT related Infrastructure standards

Interoperability | Data sharing | Interfacing | Network infrastructure | Storage infrastructure | Computing Power infrastructure

<Standards for metaverse can be generally classified into four categories>

- General standards,
- Application and service standards,
- Enabling technology standards, and
- Interoperability and ICT related infrastructure standards.

Holonext https://holonext.com/metaverse-101-understanding-the-seven-layers/



The Seven Layers of the Metaverse

Experience — Games, Social, Esports, Theater, Shopping

Discovery — Ad Networks, Social, Curation, Ratings, Stores, Agents

Creator Economy — Design Tools, Asset Markets, Workflow, Commerce

Spatial Computing — 3D Engines, VR/AR/XR, Multitasking UI, Geospatial Mapping

Decentralization — Edge Computing, AI Agents, Microservices, Blockchain

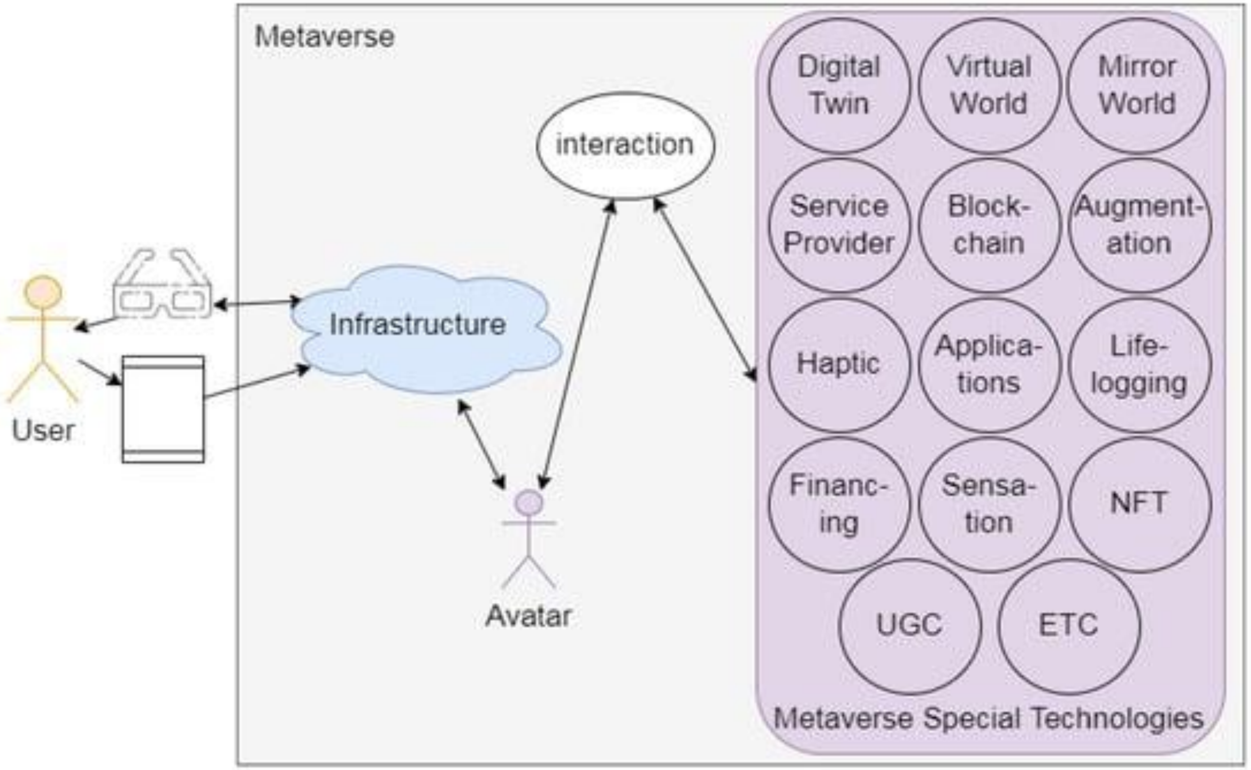
Human Interface — Mobile, Smartglasses, Wearables, Haptic, Gestures, Voice, Neural

Infrastructure — 5G, WiFi 6, 6G, Cloud, 7nm to 1.4nm, MEMS, GPUs, Materials

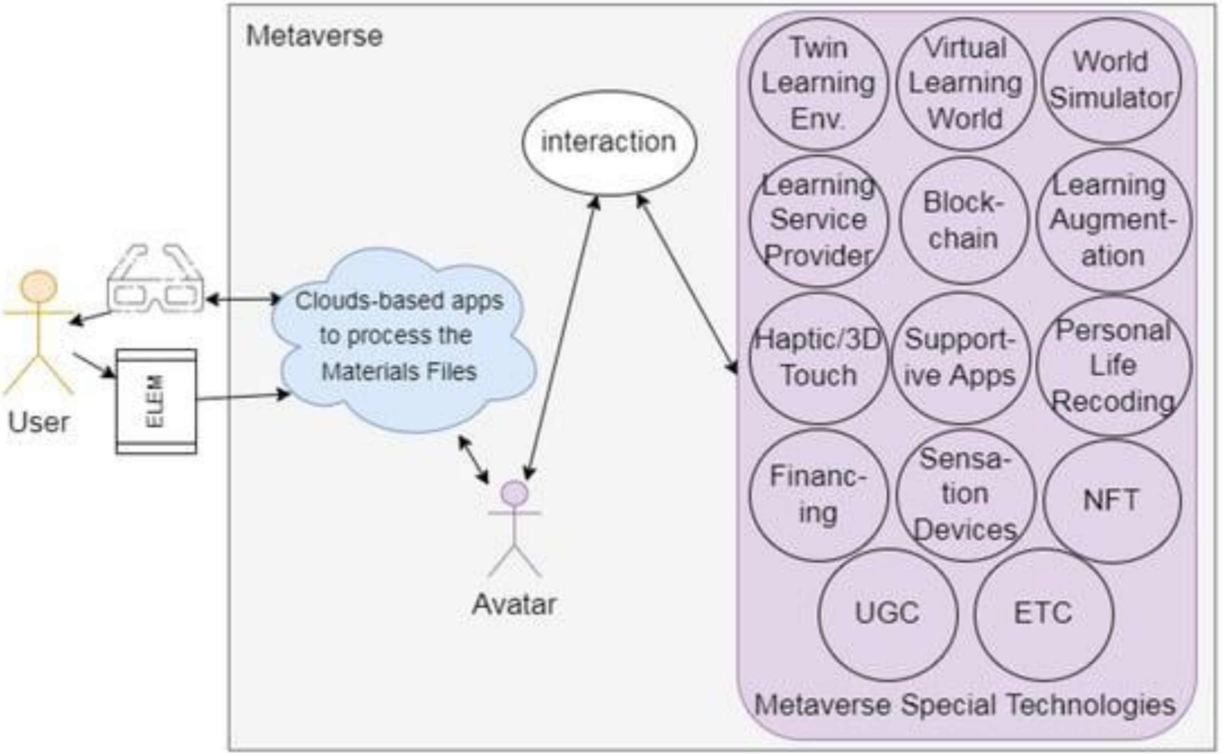
Building the Metaverse
Jon Radoff

2022 MDPI Electronics “Metaverse Framework: A Case Study on E-Learning Environment (ELEM)”

https://www.mdpi.com/2079-9292/11/10/1616

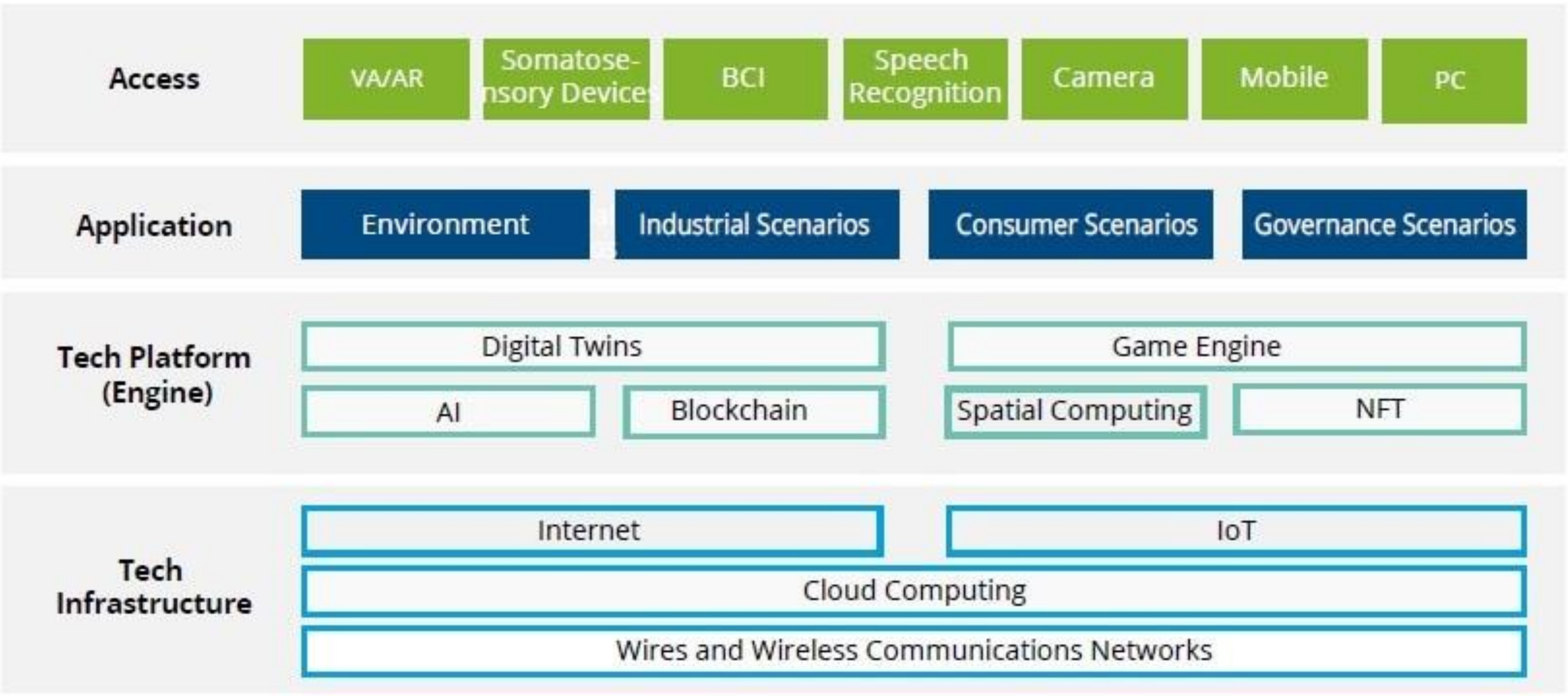


<Metaverse Framework>



<Metaverse ELEM Framework>

Deloitte analysis https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/metaverse-report.html

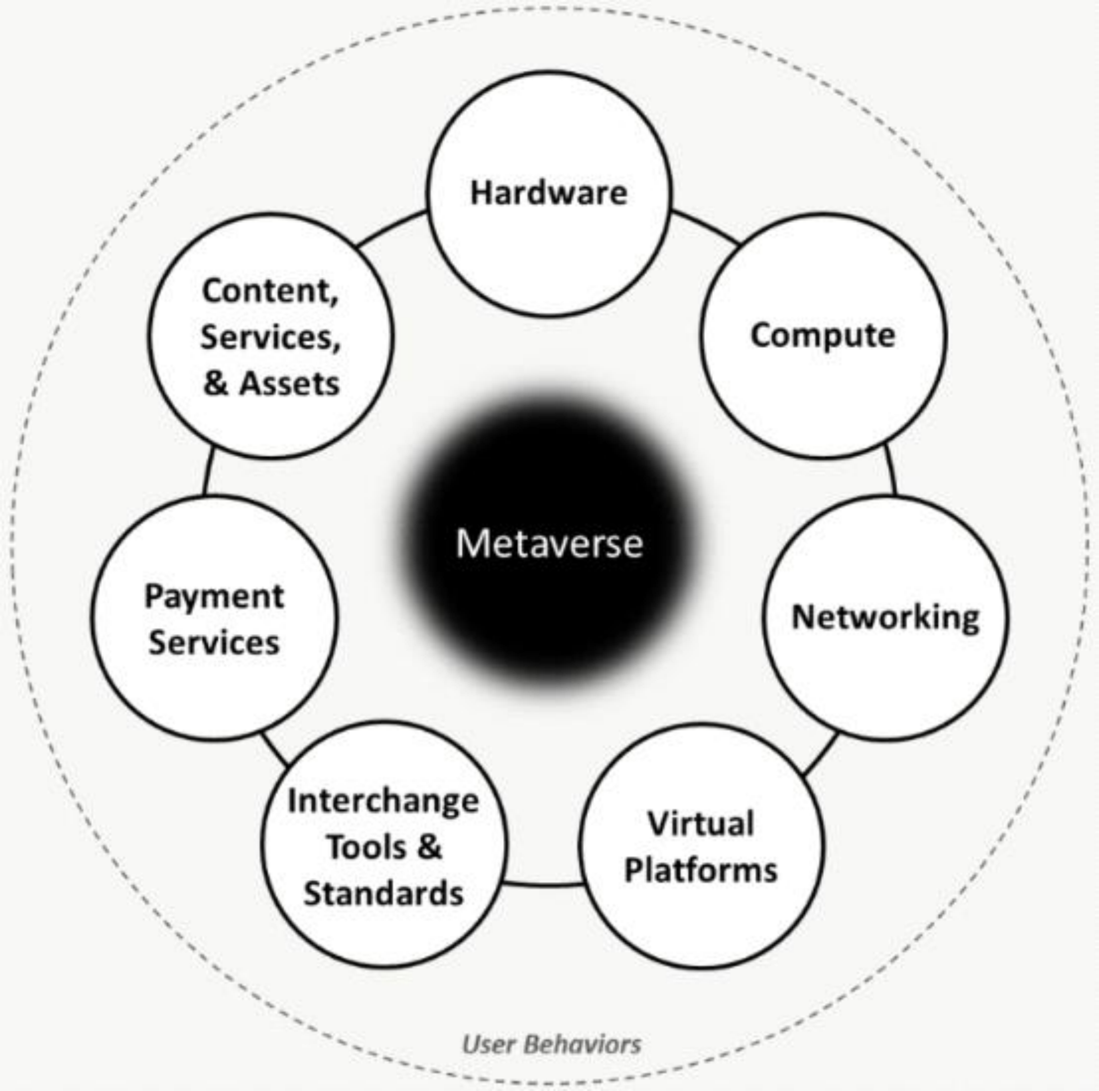


Access	VA/AR Somatose- nsory Devices BCI Speech Recognition Camera Mobile PC
Application	Environment Industrial Scenarios Consumer Scenarios Governance Scenarios
Tech Platform (Engine)	Digital Twins Game Engine AI Blockchain Spatial Computing NFT
Tech Infrastructure	Internet IoT Cloud Computing Wires and Wireless Communications Networks

Source: Deloitte analysis

<Industrial Framework: Four Layer>

MatthewBall. “A Framework for the Metaverse”,” https://www.matthewball.vc/the-metaverse

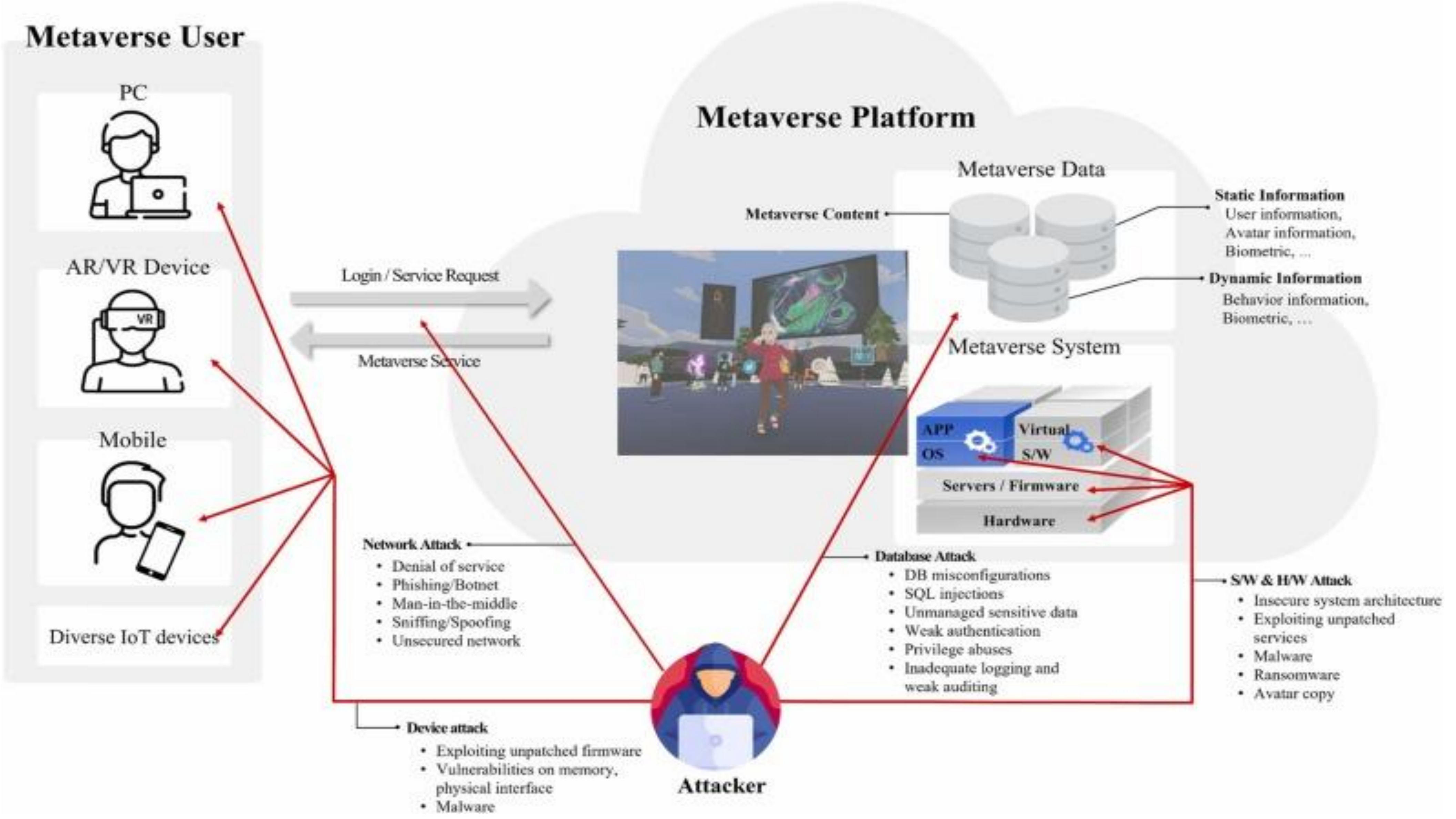


Framework for the Metaverse

2. Privacy issues in the metaverse frameworks

Elsevier: International Journal of Information Management, "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," 2022, https://doi.org/10.1016/j.ijinfomgt.2022.102542

Security and Privacy Threats in the Metaverse



Metaverse User

PC

AR/VR Device

Mobile

Diverse IoT devices

Login / Service Request

Metaverse Service

Metaverse Platform

Metaverse Data

Metaverse Content

Static Information
User information,
Avatar information,
Biometric, ...

Dynamic Information
Behavior information,
Biometric, ...

Metaverse System

APP
OS
Virtual S/W
Servers / Firmware
Hardware

Network Attack
- Denial of service
- Phishing/Botnet
- Man-in-the-middle
- Sniffing/Spoofing
- Unsecured network

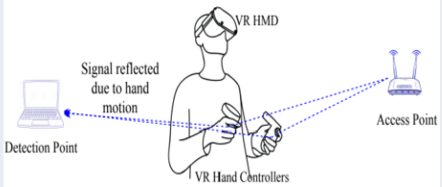
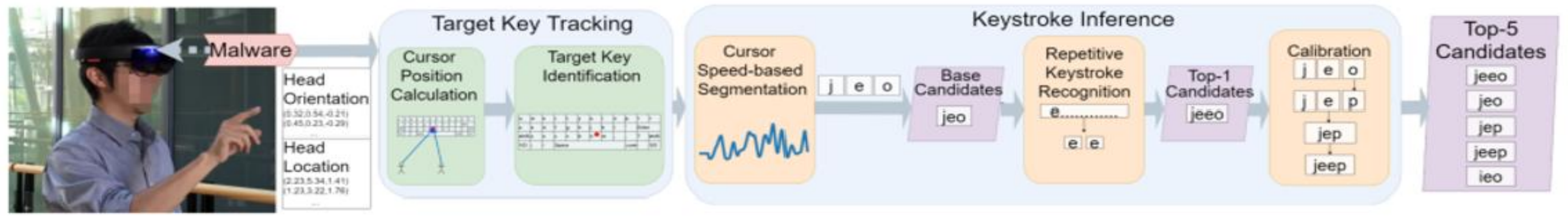
Database Attack
- DB misconfigurations
- SQL injections
- Unmanaged sensitive data
- Weak authentication
- Privilege abuses
- Inadequate logging and weak auditing

S/W & H/W Attack
- Insecure system architecture
- Exploiting unpatched services
- Malware
- Ransomware
- Avatar copy

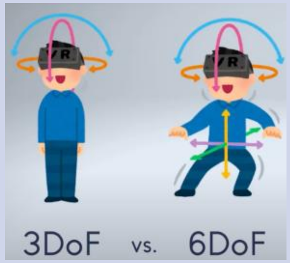
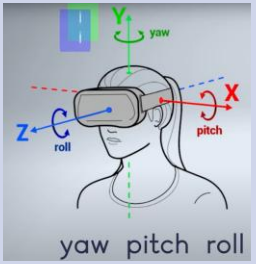
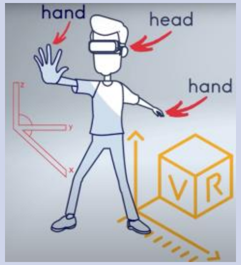
Device attack
- Exploiting unpatched firmware
- Vulnerabilities on memory, physical interface
- Malware

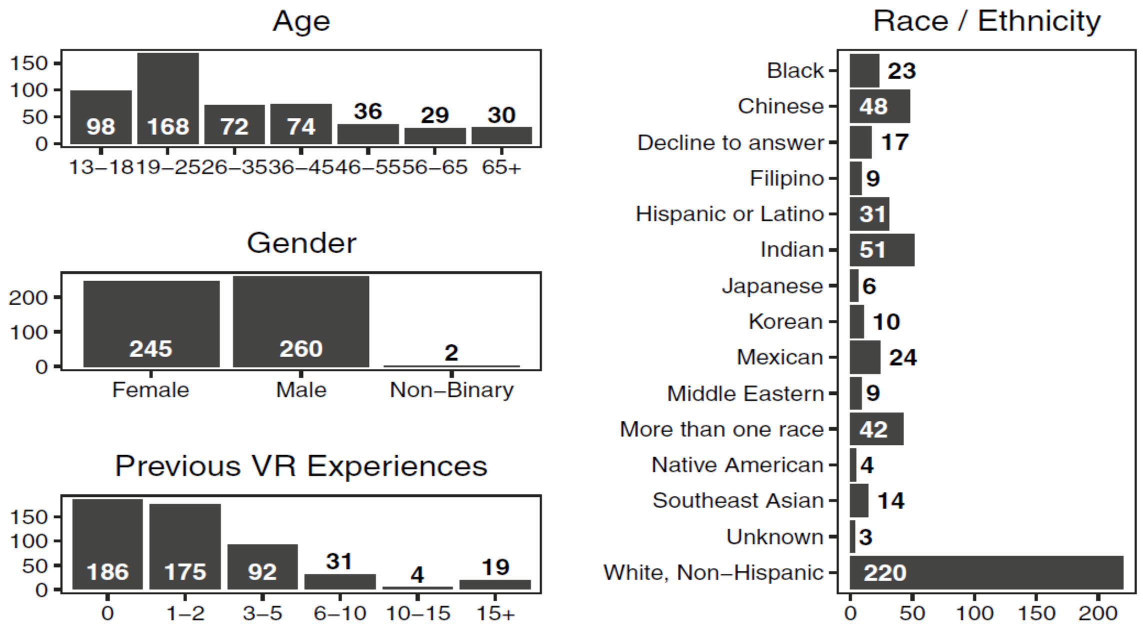
Attacker

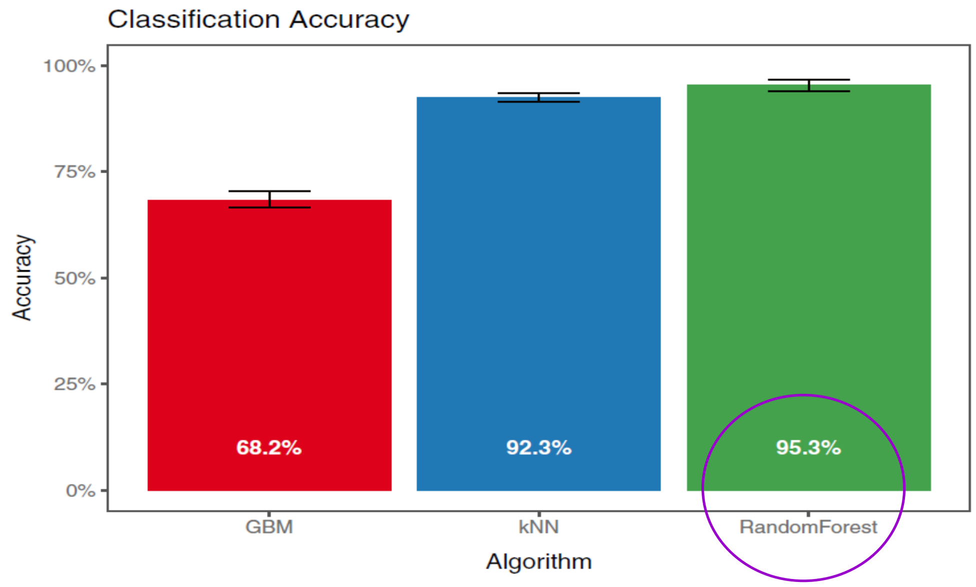
Recent VR/HMD device attacks

Attacks	Sources	Threats
Side-Channel Attacks to the VR User Authentication	**"Pivot: Panoramic-Image-Based VR User Authentication against Side-Channel Attacks," ACM Trans. Multimedia Comput. Commun. Appl., Vol. 21, No. 2, Article 52. Publication date: December 2024**	**with current password-based user authentication schemes in mainstream VR devices, studies demonstrate that side-channel attacks can pose a severe threat to VR user privacy**
VR-Spy: Side-Channel Attacks on Virtual Key-Logging in VR Headsets	**"VR-Spy: A Side-Channel Attack on Virtual Key-Logging in VR Headsets,"IEEE Virtual Reality and 3D User Interfaces (VR), 2021**  VR HMD Signal reflected due to hand motion Access Point Detection Point VR Hand Controllers	VR-Spy, a virtual keystrokes recognition method using channel state information (CSI) of WiFi signals. **VR -Spy is that the side-channel information of fine-granular hand movements associated with each virtual keystroke has a unique gesture pattern in the CSI waveforms**
HoloLogger: Side-Channel Attacks by Keystroke Inference on MR-HMD	**"HoloLogger: Keystroke Inference on Mixed Reality Head Mounted Displays,"IEEE Virtual Reality and 3D User Interfaces (VR), 2022.**  Malware Head Orientation Head Location Target Key Tracking Cursor Position Calculation Target Key Identification Keystroke Inference Cursor Speed-based Segmentation j e o Base Candidates jeo Repetitive Keystroke Recognition e.......... e e Top-1 Candidates jeeo Calibration j e o j e p jep jeep Top-5 Candidates jeeo jeo jep jeep ieo	**to monitor MR headset motion and infer the user input through a benign App.**

Recent VR/HMD device attacks

Attacks	Sources	Threats
Intelligent biometric personal information threats in metaverse environment	Mark Roman Miller et al.(Stanford U.),” Personal identifiability of user tracking data during observation of 360-degree VR video,” Nature, 2020.   	the identifiability of users under typical VR viewing circumstances, with no specially designed identifying task. Out of a pool of 511 participants, the system identifies 95% of users correctly when trained on less than 5 min of tracking data per person



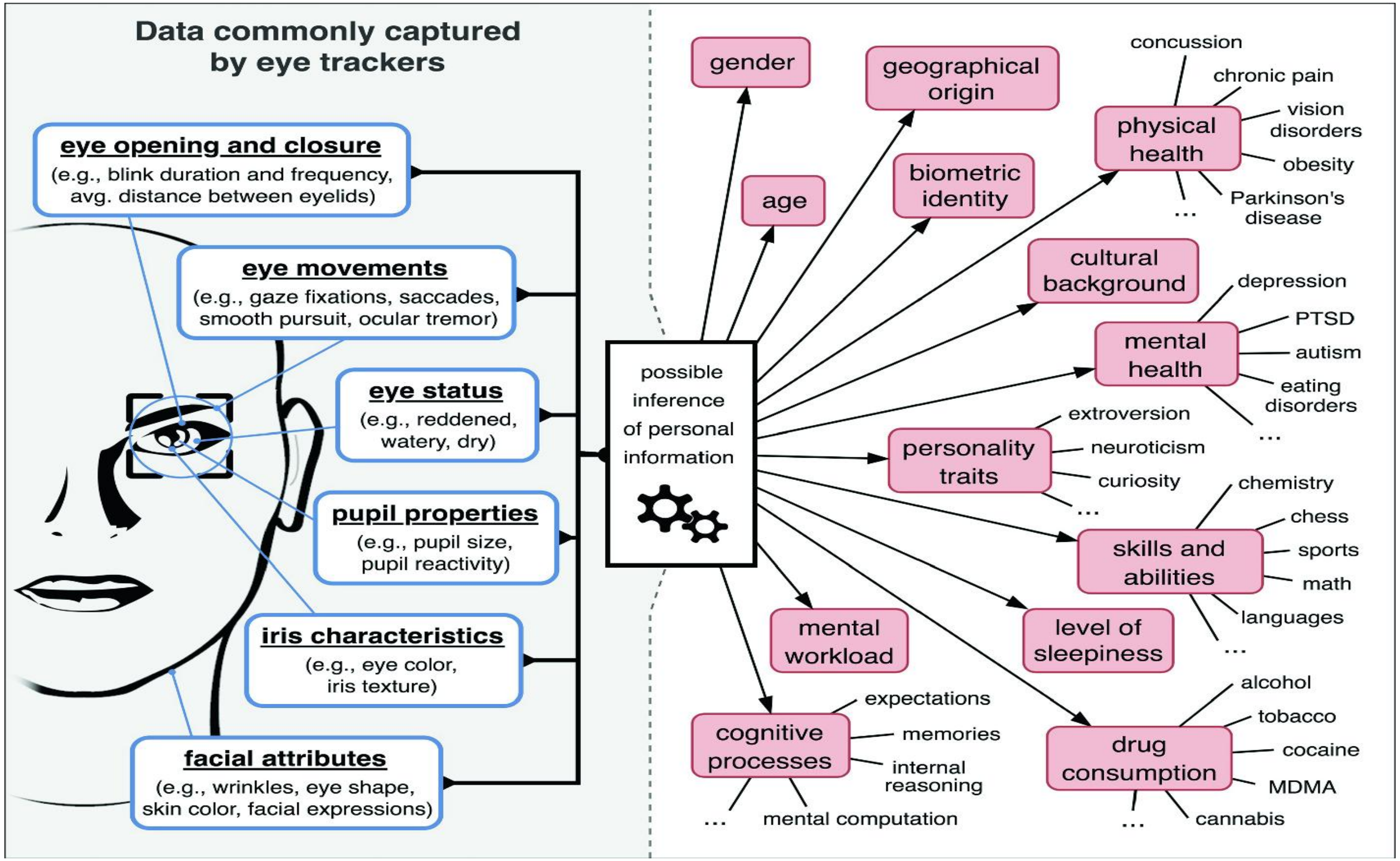


Intelligent biometric personal information threats in metaverse environment

* Jacob Leon Kröger," What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking," IFIP International Summer School on Privacy and Identity Management, Springer, 2020.

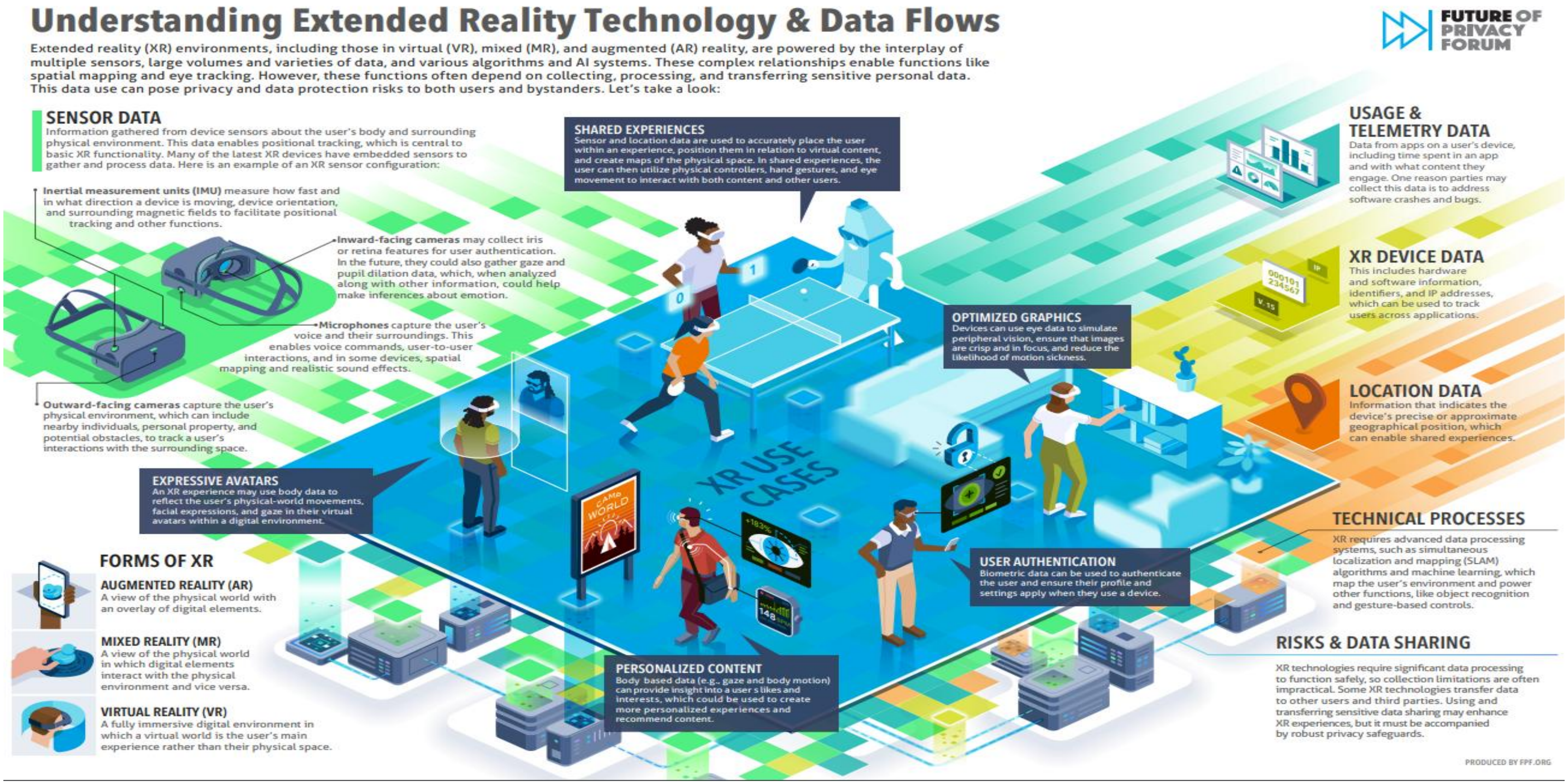
✓ [Eye-tracking: eye opening and closure, eye movements, eye status, pupil properties, Iris characteristic, facial attributes]

gender, age, geographical origin, biometric identity, physical health, cultural background, mental health, personal traits, skills and abilities, mental workload, level of sleepiness, cognitive processes, drug consumption



Intelligent biometric personal information threats in metaverse environment

* Future of Privacy Forum," https://fpf.org/wp-content/uploads/2022/10/XR-Infographic-Screen-reader-friendly-version.pdf ,2023.



Understanding Extended Reality Technology & Data Flows

Extended reality (XR) environments, including those in virtual (VR), mixed (MR), and augmented (AR) reality, are powered by the interplay of multiple sensors, large volumes and varieties of data, and various algorithms and AI systems. These complex relationships enable functions like spatial mapping and eye tracking. However, these functions often depend on collecting, processing, and transferring sensitive personal data. This data use can pose privacy and data protection risks to both users and bystanders. Let's take a look:

SENSOR DATA

Information gathered from device sensors about the user's body and surrounding physical environment. This data enables positional tracking, which is central to basic XR functionality. Many of the latest XR devices have embedded sensors to gather and process data. Here is an example of an XR sensor configuration:

Inertial measurement units (IMU) measure how fast and in what direction a device is moving, device orientation, and surrounding magnetic fields to facilitate positional tracking and other functions.

Inward-facing cameras may collect iris or retina features for user authentication. In the future, they could also gather gaze and pupil dilation data, which, when analyzed along with other information, could help make inferences about emotion.

Microphones capture the user's voice and their surroundings. This enables voice commands, user-to-user interactions, and in some devices, spatial mapping and realistic sound effects.

Outward-facing cameras capture the user's physical environment, which can include nearby individuals, personal property, and potential obstacles, to track a user's interactions with the surrounding space.

SHARED EXPERIENCES

Sensor and location data are used to accurately place the user within an experience, position them in relation to virtual content, and create maps of the physical space. In shared experiences, the user can then utilize physical controllers, hand gestures, and eye movement to interact with both content and other users.

OPTIMIZED GRAPHICS

Devices can use eye data to simulate peripheral vision, ensure that images are crisp and in focus, and reduce the likelihood of motion sickness.

EXPRESSIVE AVATARS

An XR experience may use body data to reflect the user's physical-world movements, facial expressions, and gaze in their virtual avatars within a digital environment.

USER AUTHENTICATION

Biometric data can be used to authenticate the user and ensure their profile and settings apply when they use a device.

PERSONALIZED CONTENT

Body based data (e.g., gaze and body motion) can provide insight into a user s likes and interests, which could be used to create more personalized experiences and recommend content.

FORMS OF XR

AUGMENTED REALITY (AR)
A view of the physical world with an overlay of digital elements.

MIXED REALITY (MR)
A view of the physical world in which digital elements interact with the physical environment and vice versa.

VIRTUAL REALITY (VR)
A fully immersive digital environment in which a virtual world is the user's main experience rather than their physical space.

USAGE & TELEMETRY DATA

Data from apps on a user's device, including time spent in an app and with what content they engage. One reason parties may collect this data is to address software crashes and bugs.

XR DEVICE DATA

This includes hardware and software information, identifiers, and IP addresses, which can be used to track users across applications.

LOCATION DATA

Information that indicates the device's precise or approximate geographical position, which can enable shared experiences.

TECHNICAL PROCESSES

XR requires advanced data processing systems, such as simultaneous localization and mapping (SLAM) algorithms and machine learning, which map the user's environment and power other functions, like object recognition and gesture-based controls.

RISKS & DATA SHARING

XR technologies require significant data processing to function safely, so collection limitations are often impractical. Some XR technologies transfer data to other users and third parties. Using and transferring sensitive data sharing may enhance XR experiences, but it must be accompanied by robust privacy safeguards.

PRODUCED BY FPF.ORG

Intelligent biometric personal information threats in metaverse environment

*** Future of Privacy Forum," https://fpf.org/wp-content/uploads/2022/10/XR-Infographic-Screen-reader-friendly-version.pdf ,2023.**

- ✓ **Sensor data** : user's body and surrounding physical environment
- ✓ **Expressive Avatars**: user's physical-world movements, facial expressions, and gaze in their virtual
- ✓ **PERSONALIZED CONTENT**: Body-based data (e.g., gaze and body motion) can provide insight into a user 's likes and interests
- ✓ **TELEMETRY DATA** : Data from apps on a user's device, including time spent in an app and with what content they engage. One reason parties may collect this data is to address software crashes and bugs.
- ✓ **XR DEVICE DATA**: This includes hardware and software information, identifiers, and IP addresses, which can be used to track users across applications.
- ✓ **LOCATION DATA**: Information that indicates the device's precise or approximate geographical position, which can enable shared experiences.
- ✓ **USER AUTHENTICATION**: Biometric data can be used to authenticate the user and ensure their profile and settings apply when they use a device.

Privacy issues in the metaverse frameworks

1. Personal Data Collection and Profiling

- **Types of Data Collected**

- Biometric Data: Eye movement, facial expressions, hand gestures, and physiological data from VR headsets or wearable sensors.

- Behavioral Data: User interactions, engagement patterns, preferences, and social behaviors in virtual environments.

- Location Data: Geolocation tracking for augmented reality (AR) applications.

- Financial Data: Transactions conducted within Metaverse platforms.

- **Privacy Risks**

- Detailed behavioral profiles can be created without explicit user consent.
- Risks of identity theft due to the storage of sensitive biometric data.

2. Lack of Robust Data Governance

- **Data Ownership and Control**

- Ambiguity over who owns user-generated content and data.
- Limited transparency in how user data is shared with third parties.

- **Implications**

- Potential misuse of data for targeted advertising, profiling, or even discrimination.
- Difficulty for users to track where their data is stored and how it is processed.

Privacy issues in the metaverse frameworks

3. Identity and Anonymity Concerns

- **Digital Identity**

- Persistent virtual avatars increase the exposure of personal and behavioral data.
- Risk of identity theft as users may bind personal information to their digital identities.

- **Anonymity and Privacy**

- Inability to remain anonymous in certain Metaverse environments.
- Challenges in separating personal and professional identities.

4. Enhanced Tracking and Surveillance

- **Tracking Mechanisms**

- Real-time tracking of user movements, body language, and interactions.
- Persistent cookies and analytics tools for monitoring user activity.

- **Privacy Implications**

- Users face increased exposure to constant surveillance, leading to a loss of privacy.
- Risk of covert government or corporate surveillance.

Privacy issues in the metaverse frameworks

5. Data Security and Breaches

- **Threats**

- Potential for large-scale data breaches involving biometric and sensitive personal data.
- Vulnerabilities in decentralized systems for authentication and data storage.

- **Consequences**

- Exploitation of user data for cybercrime activities.
- Increased risk of fraud and exploitation.

6. Cross-border Data Transfers and Jurisdictional Challenges

- **Jurisdiction Issues**

- Variability in data protection laws across different regions.
- Metaverse platforms often operate across multiple jurisdictions, complicating legal enforcement.

- **Privacy Concerns**

- Inconsistent levels of privacy protection.
- Difficulty in enforcing user rights across international borders.

Privacy issues in the metaverse frameworks

7. Consent and Transparency Issues

- **Consent Mechanisms**

- Complex and lengthy user agreements.
- Lack of informed consent regarding data collection and sharing.

- **User Rights**

- Users may be unaware of how their data is collected and used.
- Limited options to opt out of data collection practices.

8. Augmented Reality (AR) Privacy Challenges

- **Data Overlap**

- Integration of real-world and digital information raises concerns about unauthorized data collection.
- AR applications may inadvertently capture data from bystanders who have not consented.

- **Privacy Risks**

- Bystanders’ images and locations can be stored and analyzed without their knowledge.
- Difficulty in distinguishing between private and public spaces.

Privacy issues in the metaverse frameworks

9. Interpersonal Privacy and Harassment

- **Social Interactions**

- Risks of harassment, cyberbullying, and stalking within virtual environments.
- Lack of mechanisms to ensure user safety and privacy during interactions.

- **Privacy Implications**

- Psychological distress and harm to users.
- Loss of personal boundaries in virtual spaces.

10. Children and Vulnerable Populations

- **Data Privacy Risks**

- Collection and exploitation of data from minors without proper safeguards.
- Vulnerable users may be more susceptible to privacy invasions.

- **Ethical Concerns**

- Inadequate age verification mechanisms.
- Lack of child-specific privacy protections.

3. Conclusive Remarks

ISO/IEC 27573 & 27575 “Privacy for the metaverse frameworks”

❖ **Mitigating Privacy Issues in the Metaverse**

- **Strong Data Encryption:** Ensure data is securely transmitted and stored.
- **User Consent and Transparency:** Simplify privacy agreements and ensure informed consent.
- **Robust Identity Management:** Implement decentralized identity solutions and multi-factor authentication.
- **Regulatory Compliance:** Adhere to global data protection laws such as GDPR and CCPA.
- **Privacy by Design:** Integrate privacy considerations into the development of Metaverse platforms.
- **User Awareness:** Educate users on privacy risks and best practices for protecting personal information.

3. Conclusive Remarks

ISO/IEC 27573 “Privacy Protection of User Avatar and System Avatar Interactions in Metaverse “

Privacy Protection during Interaction with System Avatars

The potential for personal information leakage in Privacy3 (User Avatar - System Avatar) is outlined in the table below

Type of Data Breach	Description	Potential Risks
Personal Data Leakage	Conversations between user and system a vatars may contain names, addresses, ph one numbers, and credit card information.	Spam, voice phishing, credit card theft
Behavior Pattern Leakage	Behavior patterns of user avatars can infer users’ interests, preferences, and lifestyles .	Privacy infringement, misuse for marketing /promotion
Voice/Facial Expression Data Leak	Data related to voice or facial expressions encapsulates information about users' em otions and personality.	Invasion of privacy, discrimination, criminal activity
Data Transmission Leakage	Improperly encrypted data during transmis sion between avatars is susceptible to inte rception.	Leakage of personal, financial, or business information

Preventing Personal Information Leakage during Interactions

Technical Areas

- **Encryption:** Protect data by using encryption techniques when it is stored or transmitted. T**his makes it difficult to decipher the contents even if the data is exposed.**
- **Access Control and Authorization Management**: Access to data should be controlled, and the minimum necessary permissions should be granted based on the user's role and needs. May implement access control lists (ACLs) or role-based access control (RBAC) to prevent unnecessary data access.
- **Regular Security Audits and Vulnerability Analysis**: Monitor and review the security status of the system, identify security vulnerabilities, and apply improvement measures. This allows for the early detection and response to potential risks.
- **Data Breach Detection and Response Systems**: Establish a system that can detect data breaches in real time and prepare protocols for immediate response when a breach is detected. **This minimizes the impact of breaches and allows for swift response.**

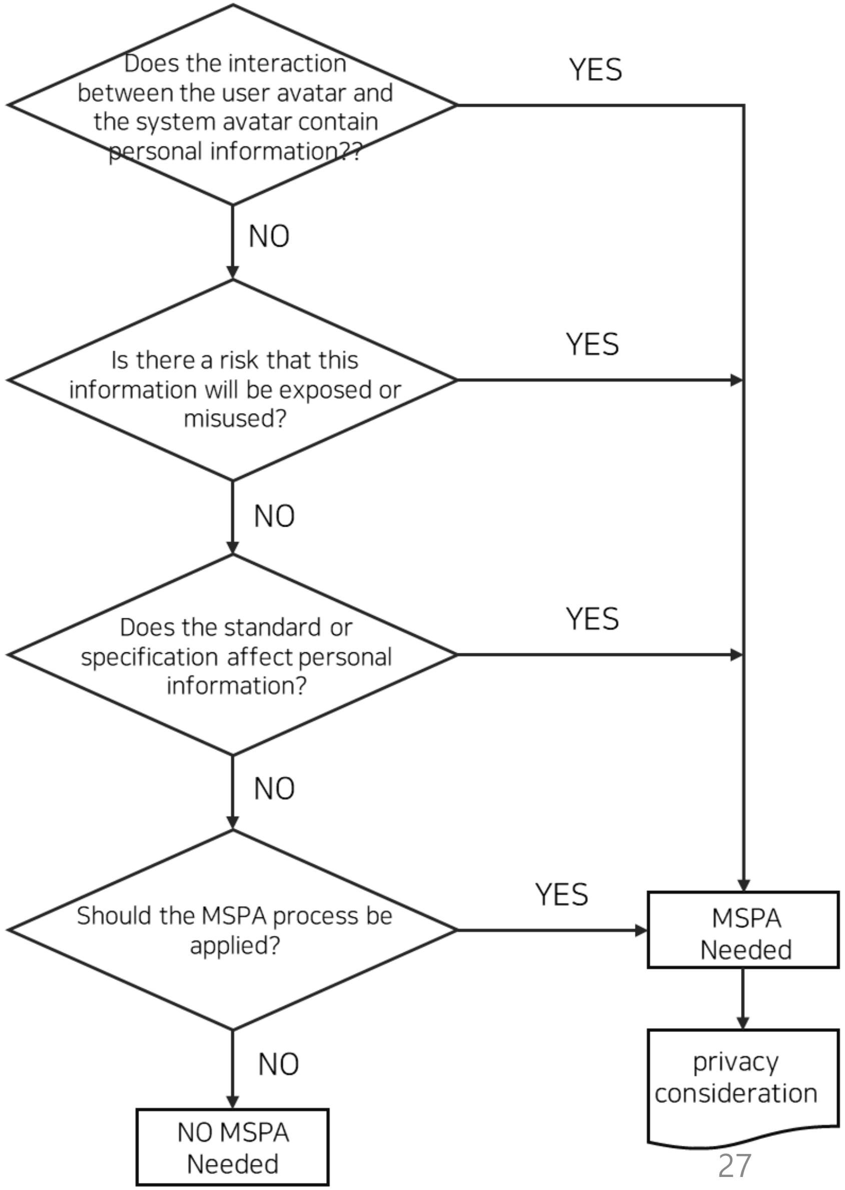
3. Conclusive Remarks

ISO/IEC 27573 “Privacy Protection of User Avatar and System Avatar Interactions in Metaverse “

MSPA Processor

Questions for Determining MSPA Process Application in Standard or Specification Under Review (SUR):

1. **PII Handling**: Review if the SUR includes technologies that process Personally Identifiable Information (PII) or are capable of identifying individuals.
2. **Sensitivity and Protection Need**: Evaluate the sensitivity of the information and the need for protection in case of exposure or improper use.
3. **PII Generation**: Confirm whether the SUR directly generates PII.
4. **MSPA Execution Review**: Reassess the above three questions collectively and decide on the execution of the MSPA process.

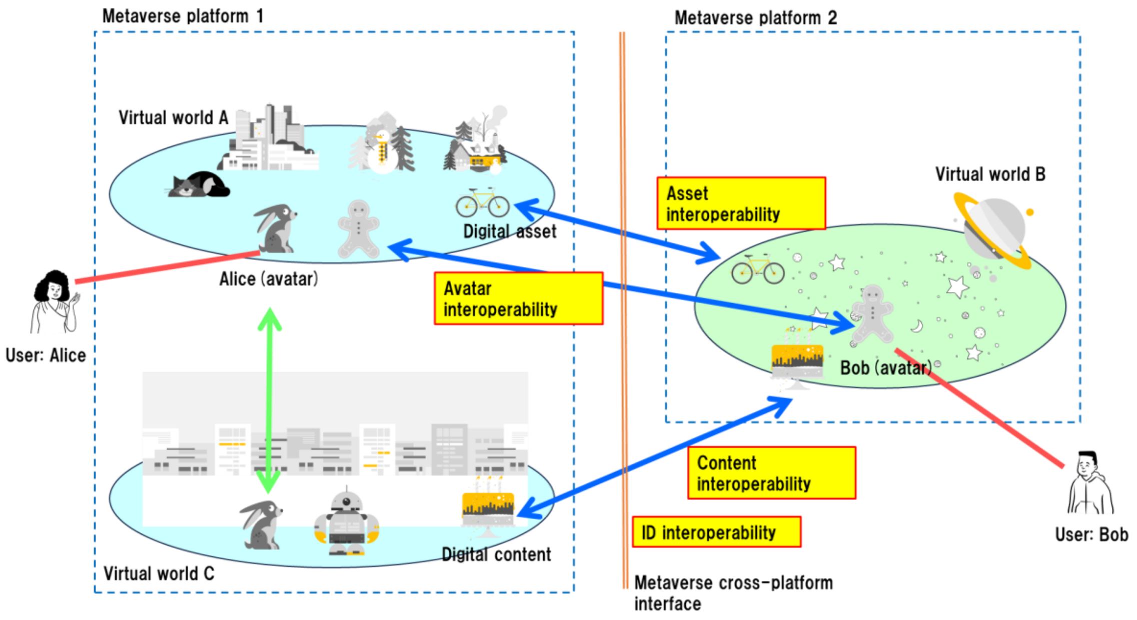


Does the interaction between the user avatar and the system avatar contain personal information??
YES
NO
Is there a risk that this information will be exposed or misused?
YES
NO
Does the standard or specification affect personal information?
YES
NO
Should the MSPA process be applied?
YES
NO
MSPA Needed
privacy consideration
NO MSPA Needed

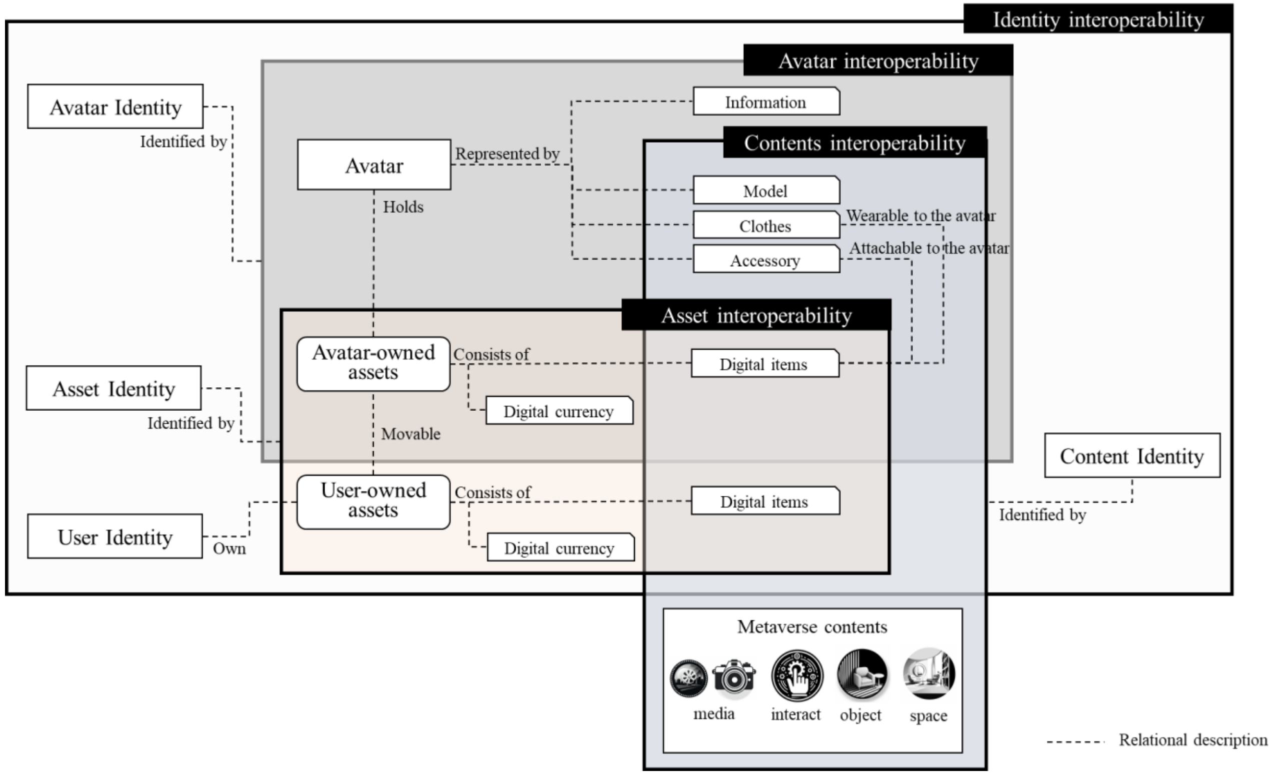
Many thanks for your attentions

[Appendix]
ITU FG-MV(Focus Group on Metaverse)

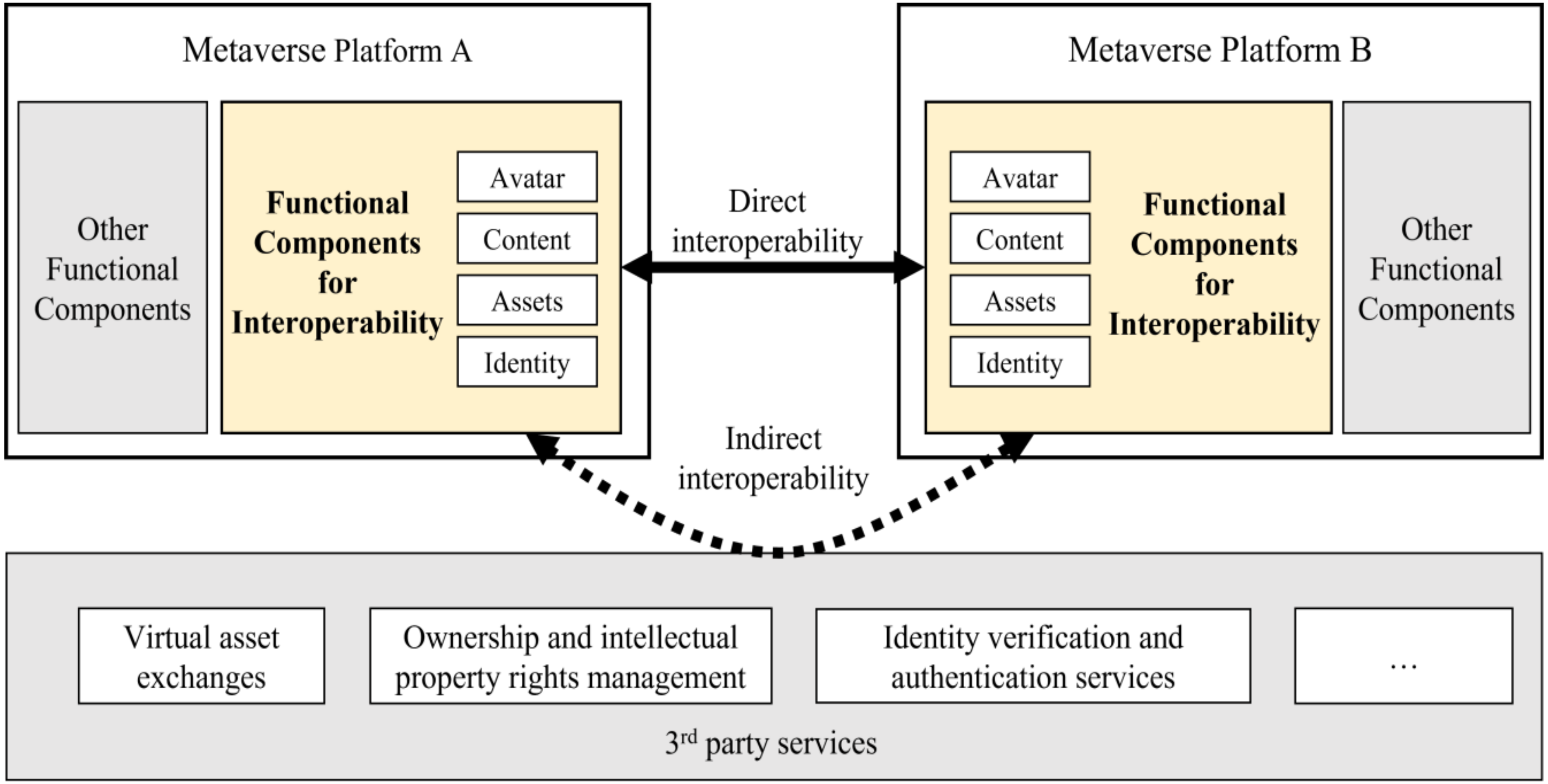
[ITU-T] FG-MV(Focus Group on Metaverse) FGMV-19 “2023 - Service scenarios and high-level requirements for metaverse cross-platform interoperability”



< Overview of metaverse interoperability >

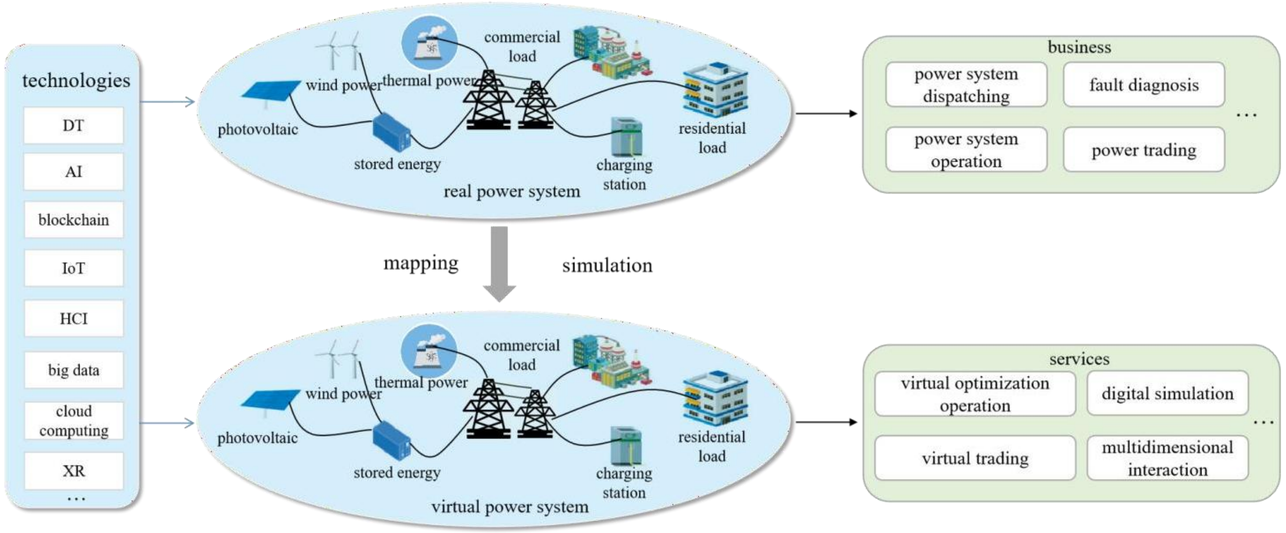


< Relationships among cross-platform interoperability aspects >

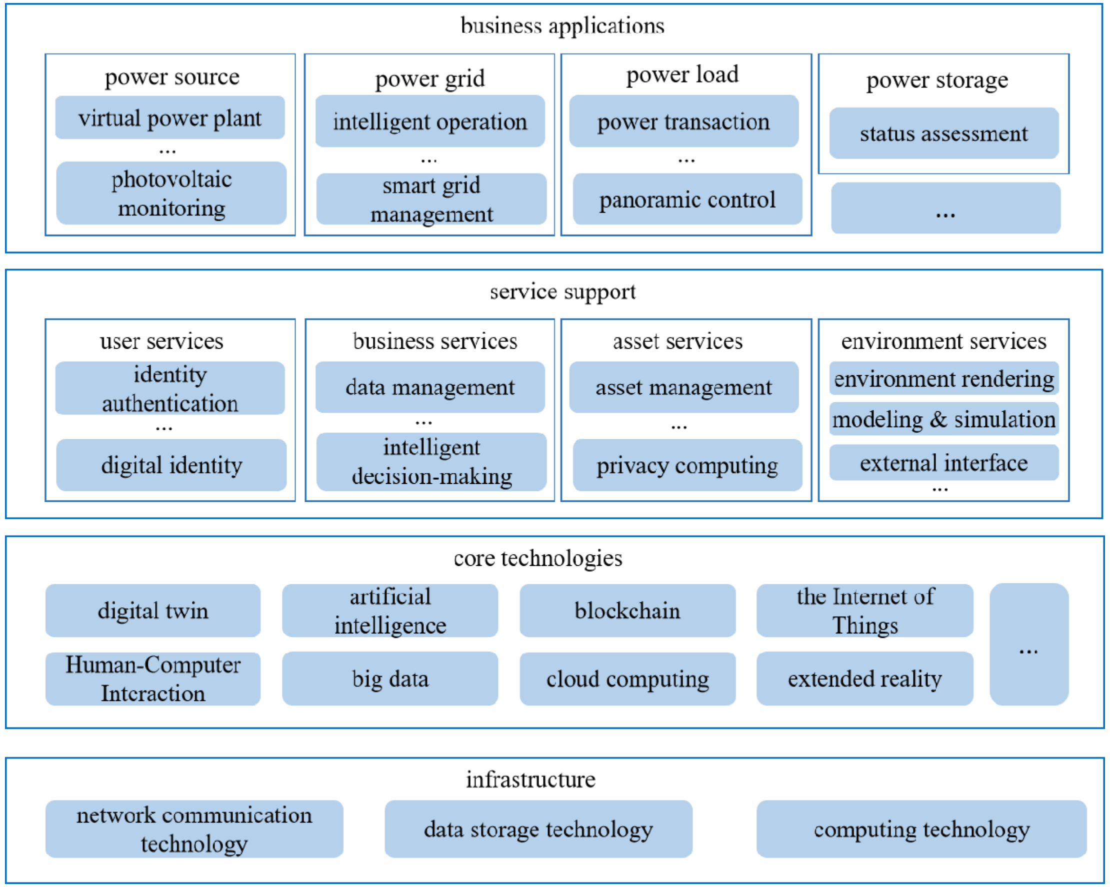

Metaverse Platform A
Other Functional Components
Functional Components for Interoperability
Avatar
Content
Assets
Identity
Direct interoperability
Metaverse Platform B
Avatar
Content
Assets
Identity
Functional Components for Interoperability
Other Functional Components
Indirect interoperability
Virtual asset exchanges
Ownership and intellectual property rights management
Identity verification and authentication services
…
3rd party services

< Concept of metaverse cross-platform interoperability>

[ITU-T] FG-MV(Focus Group on Metaverse) FGMV-27 "2024 - Guidelines for metaverse application in power system"



Mapping mode of the real and virtual power system



business applications

- power source: virtual power plant … photovoltaic monitoring
- power grid: intelligent operation … smart grid management
- power load: power transaction … panoramic control
- power storage: status assessment …

service support

- user services: identity authentication … digital identity
- business services: data management … intelligent decision-making
- asset services: asset management … privacy computing
- environment services: environment rendering, modeling & simulation, external interface …

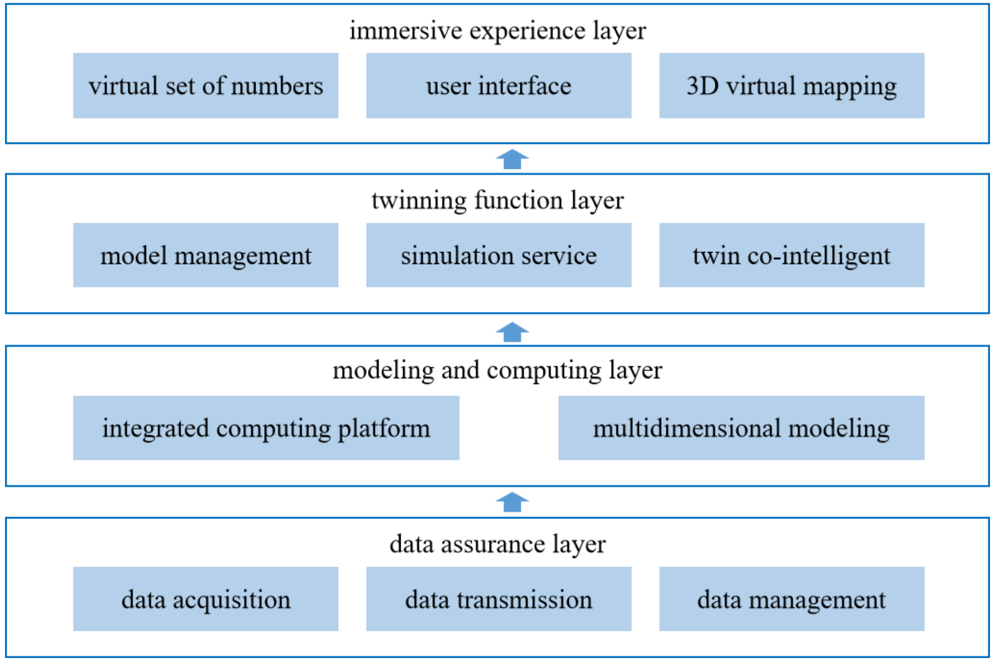
core technologies

digital twin, artificial intelligence, blockchain, the Internet of Things, Human-Computer Interaction, big data, cloud computing, extended reality, …

infrastructure

network communication technology, data storage technology, computing technology

Framework of Power Metaverse


immersive experience layer

virtual set of numbers | user interface | 3D virtual mapping

twinning function layer

model management | simulation service | twin co-intelligent

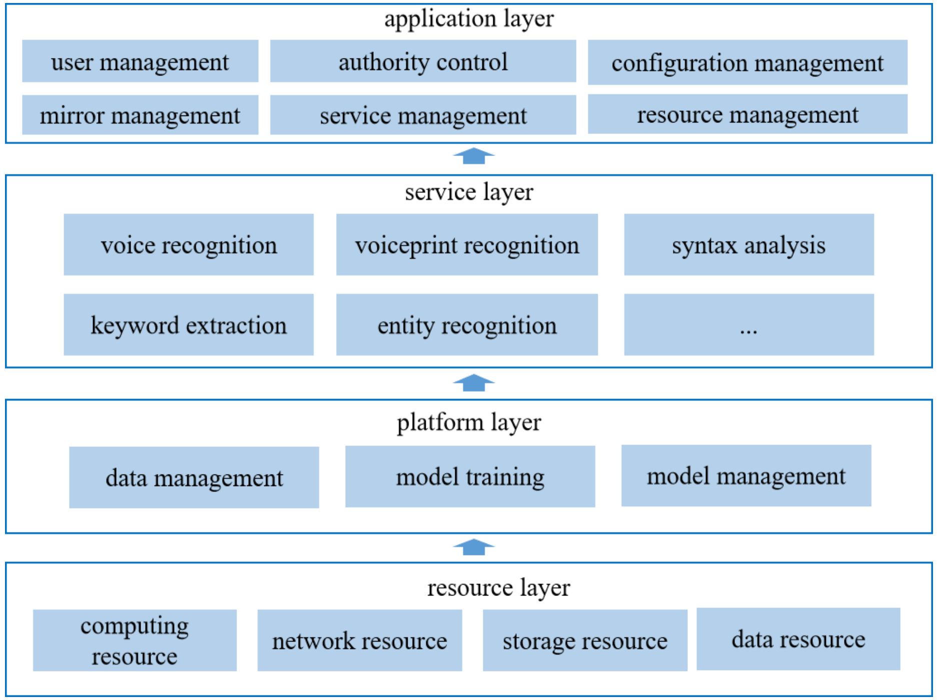
modeling and computing layer

integrated computing platform | multidimensional modeling

data assurance layer

data acquisition | data transmission | data management

Technical framework of digital twin


application layer

user management | authority control | configuration management

mirror management | service management | resource management

service layer

voice recognition | voiceprint recognition | syntax analysis

keyword extraction | entity recognition | ...

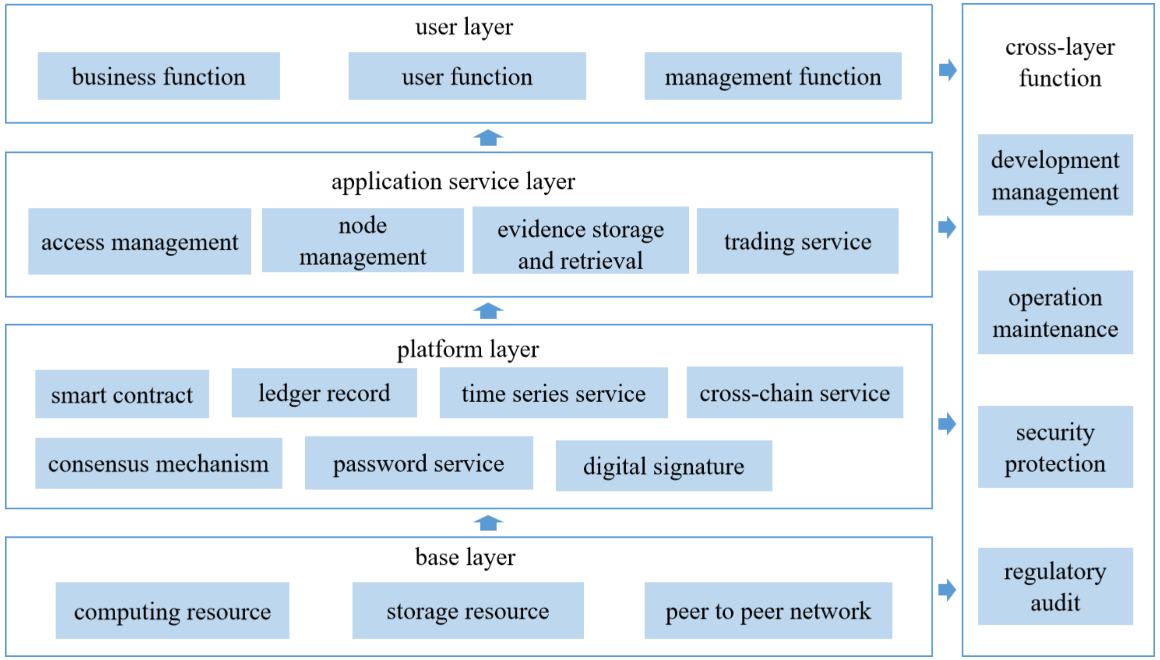
platform layer

data management | model training | model management

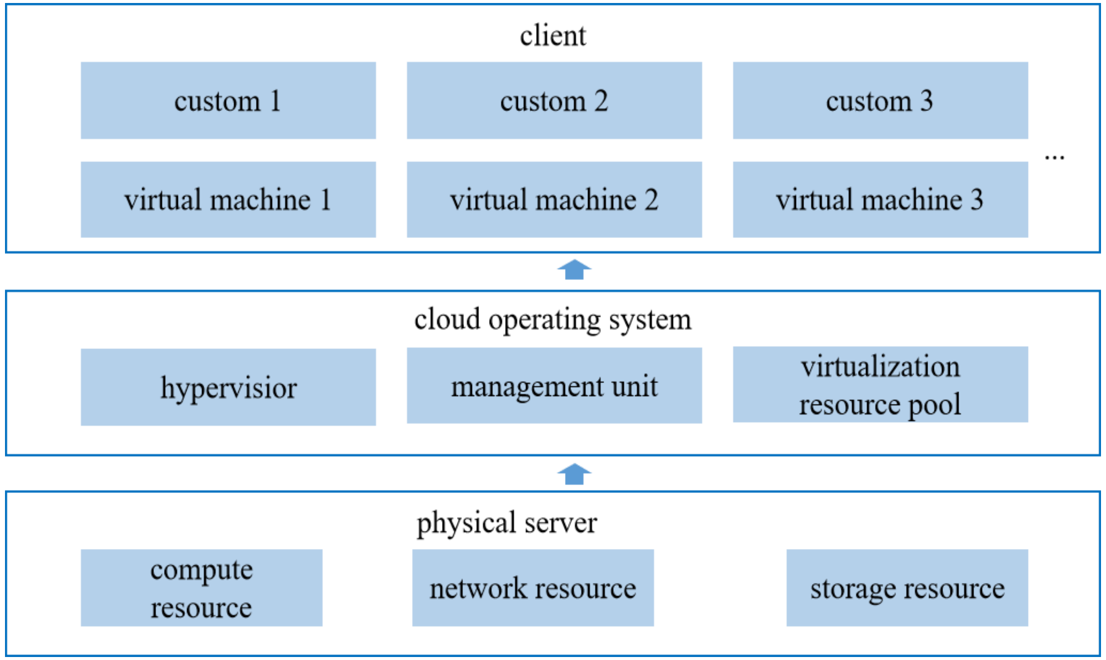
resource layer

computing resource | network resource | storage resource | data resource

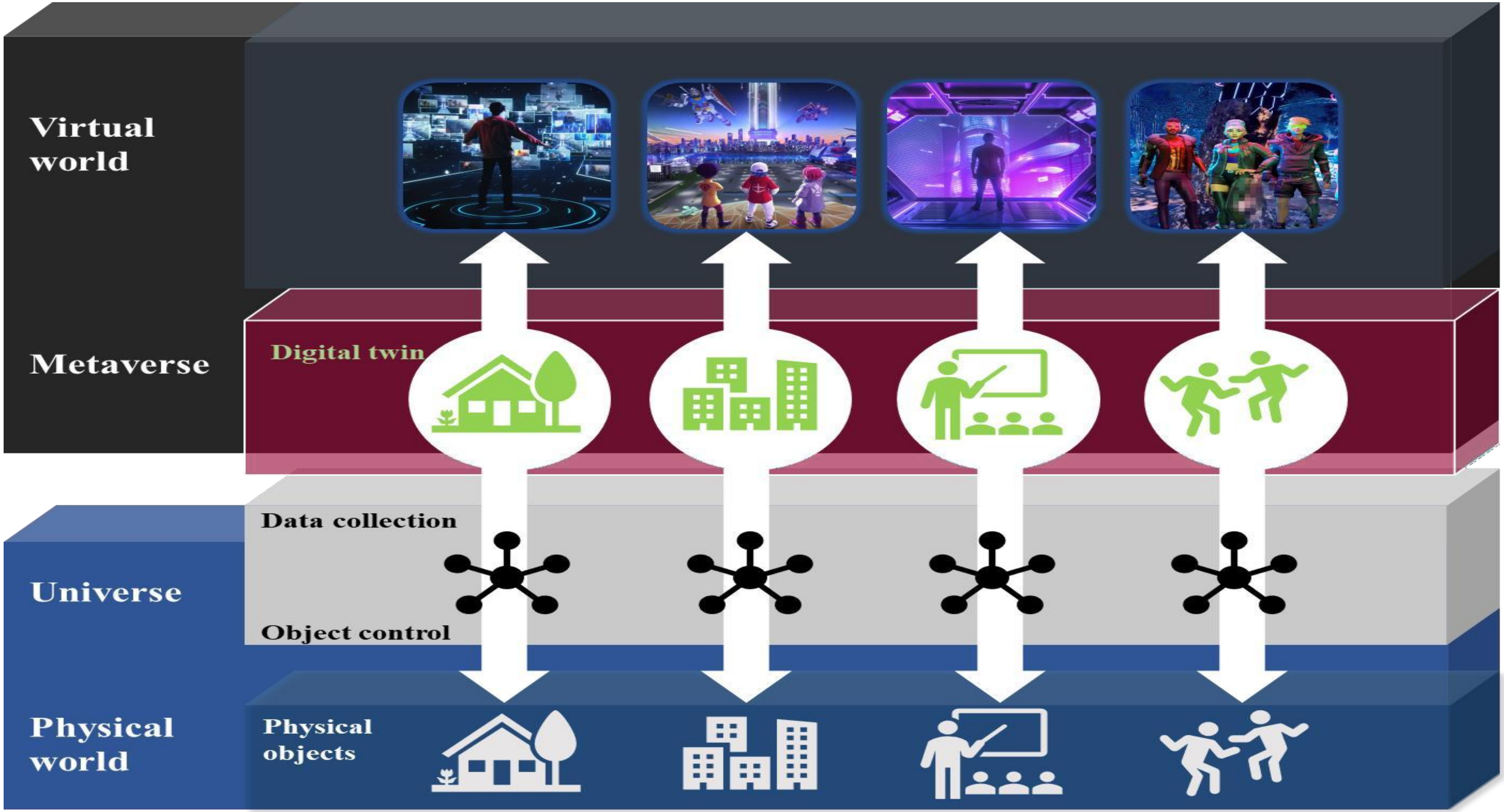
Technical framework of artificial intelligence



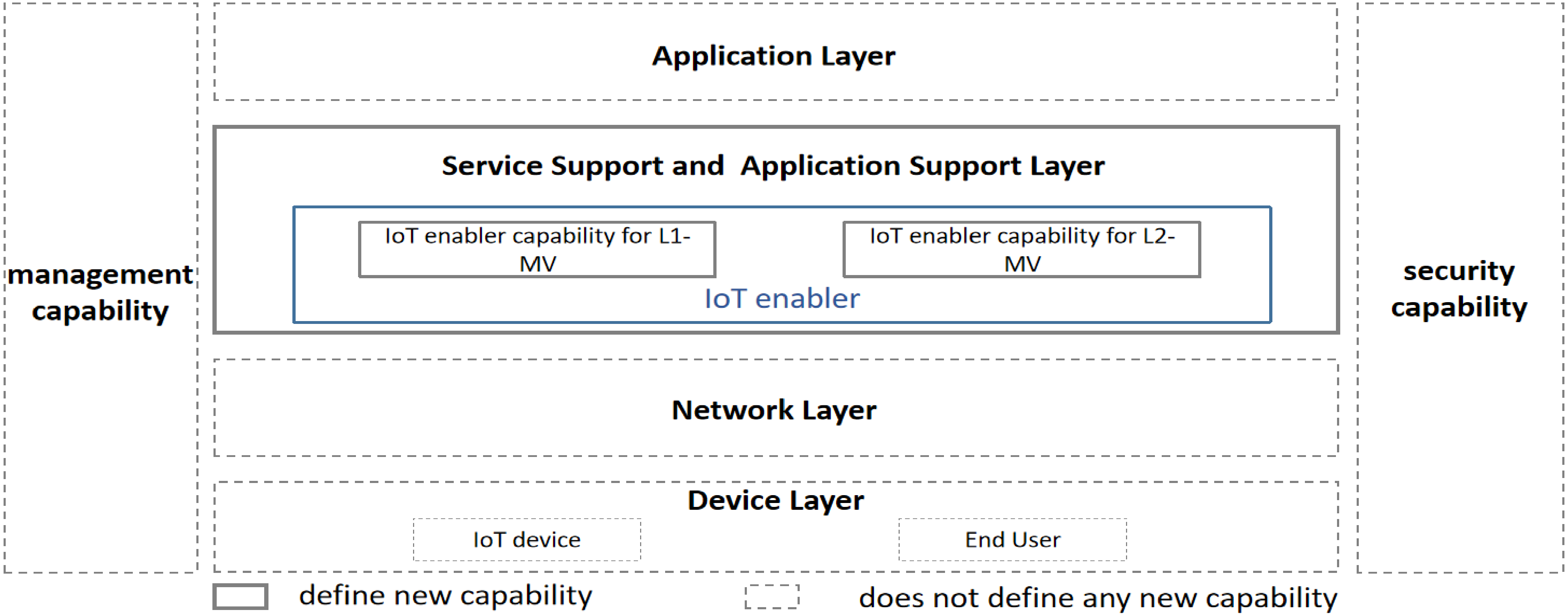
Technical framework of blockchain



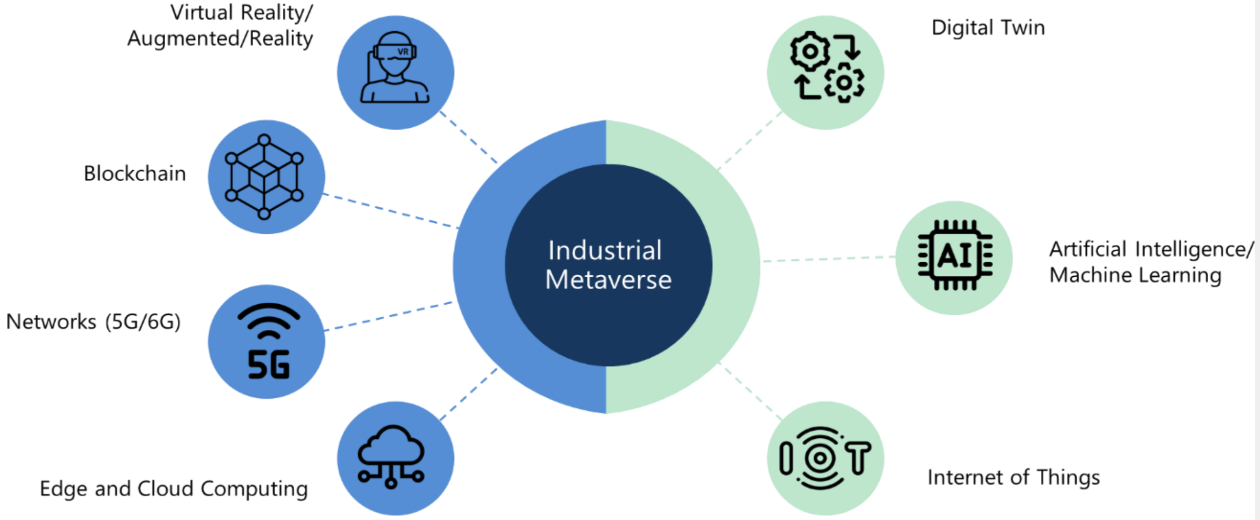
Technical framework of cloud computing



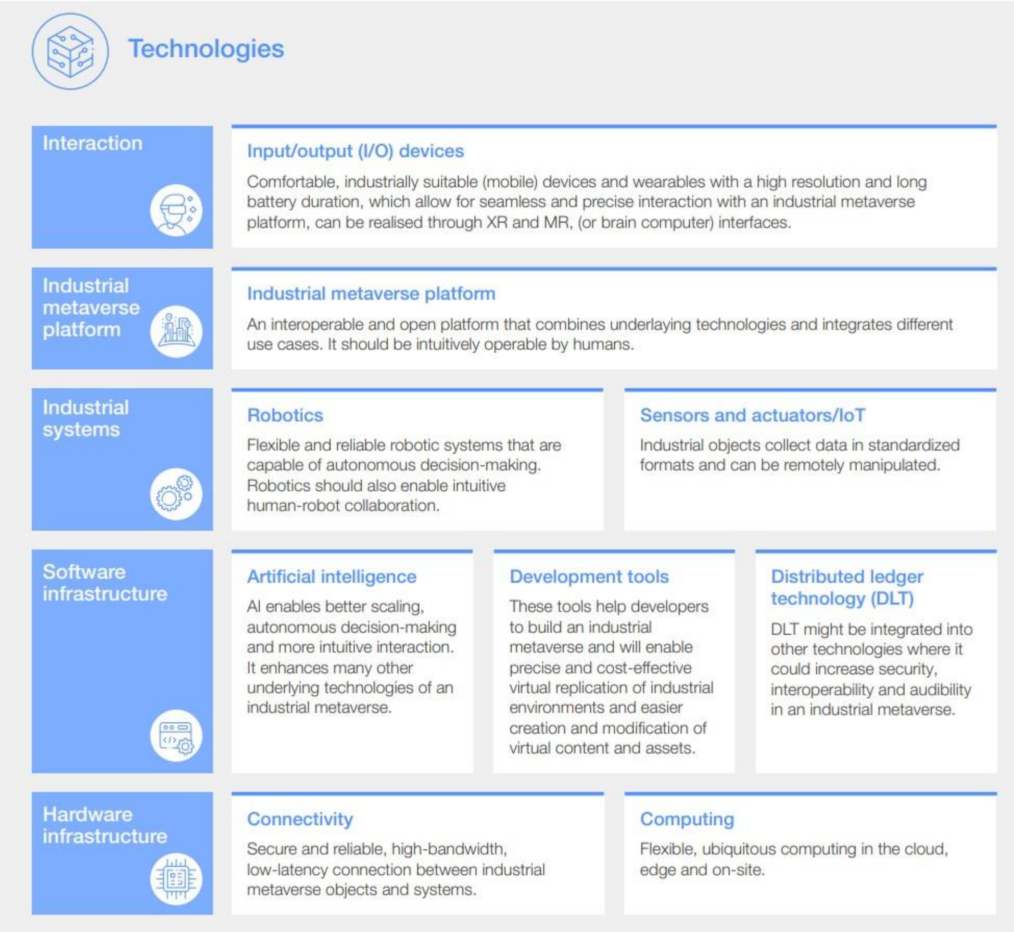
Concept of the digital twin-based integration between virtual and physical worlds


Application Layer
management capability
Service Support and Application Support Layer
IoT enabler capability for L1-MV
IoT enabler capability for L2-MV
IoT enabler
security capability
Network Layer
Device Layer
IoT device
End User
define new capability
does not define any new capability

The functional framework of MVIoT (Four Layers)



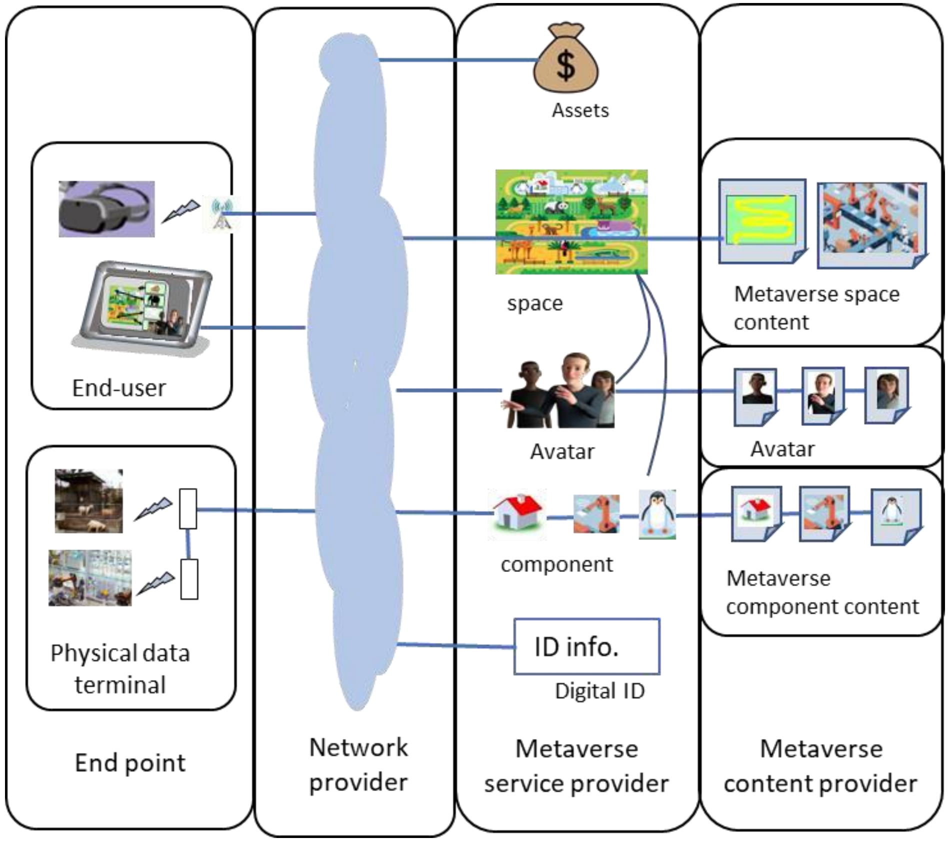
Technologies that support the industrial metaverse



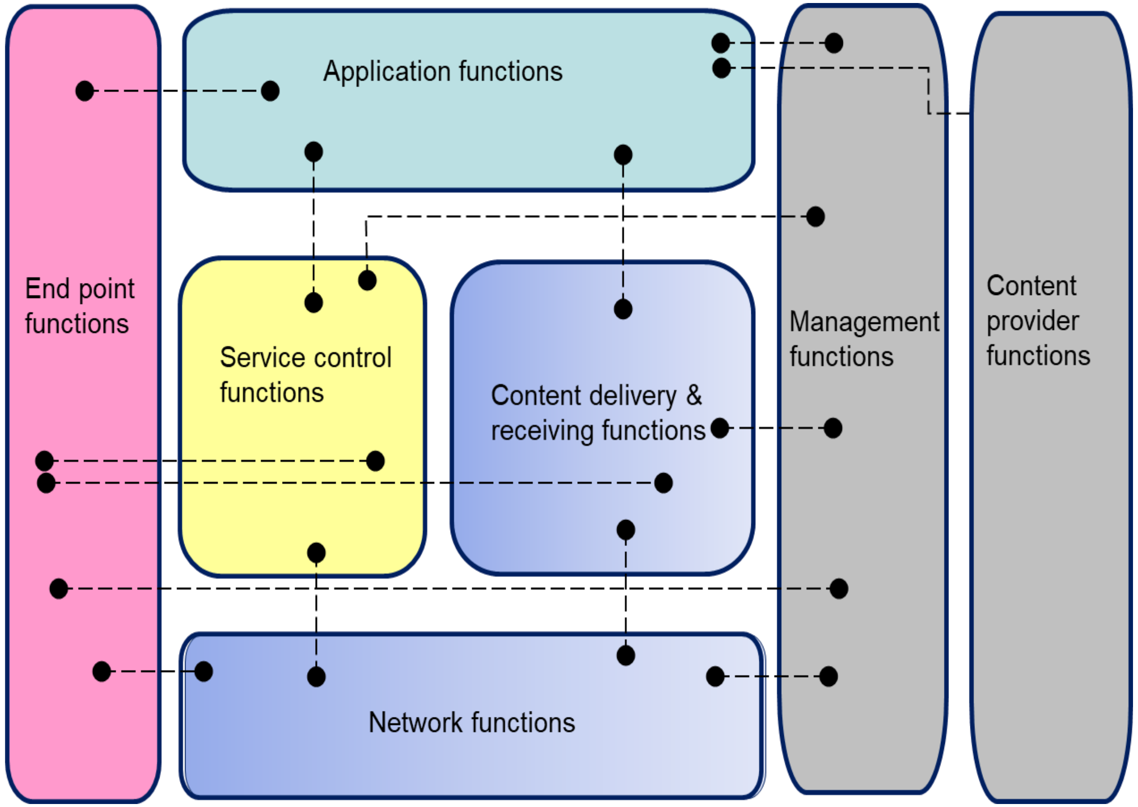
Technologies

Layer	Technology	Description
Interaction	Input/output (I/O) devices	Comfortable, industrially suitable (mobile) devices and wearables with a high resolution and long battery duration, which allow for seamless and precise interaction with an industrial metaverse platform, can be realised through XR and MR, (or brain computer) interfaces.
Industrial metaverse platform	Industrial metaverse platform	An interoperable and open platform that combines underlaying technologies and integrates different use cases. It should be intuitively operable by humans.
Industrial systems	Robotics	Flexible and reliable robotic systems that are capable of autonomous decision-making. Robotics should also enable intuitive human-robot collaboration.
	Sensors and actuators/IoT	Industrial objects collect data in standardized formats and can be remotely manipulated.
Software infrastructure	Artificial intelligence	AI enables better scaling, autonomous decision-making and more intuitive interaction. It enhances many other underlying technologies of an industrial metaverse.
	Development tools	These tools help developers to build an industrial metaverse and will enable precise and cost-effective virtual replication of industrial environments and easier creation and modification of virtual content and assets.
	Distributed ledger technology (DLT)	DLT might be integrated into other technologies where it could increase security, interoperability and audibility in an industrial metaverse.
Hardware infrastructure	Connectivity	Secure and reliable, high-bandwidth, low-latency connection between industrial metaverse objects and systems.
	Computing	Flexible, ubiquitous computing in the cloud, edge and on-site.

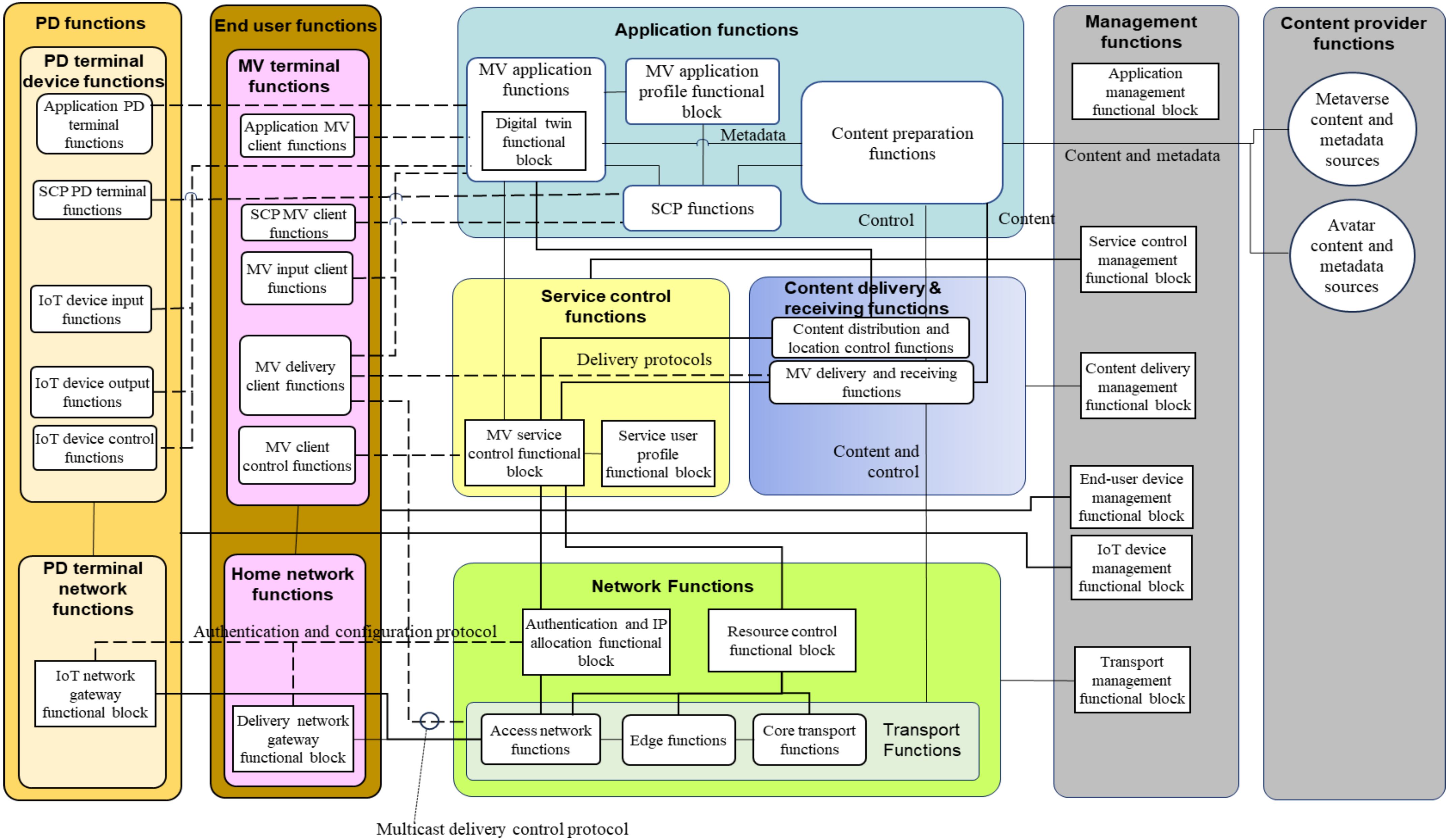
Emerging technologies within the five-layer technology framework



Metaverse domain


Application functions
End point functions
Service control functions
Content delivery & receiving functions
Management functions
Content provider functions
Network functions

Metaverse functional architecture framework



PD functions

PD terminal device functions

Application PD terminal functions

SCP PD terminal functions

IoT device input functions

IoT device output functions

IoT device control functions

PD terminal network functions

IoT network gateway functional block

End user functions

MV terminal functions

Application MV client functions

SCP MV client functions

MV input client functions

MV delivery client functions

MV client control functions

Home network functions

Delivery network gateway functional block

Authentication and configuration protocol

Multicast delivery control protocol

Application functions

MV application functions

Digital twin functional block

MV application profile functional block

Metadata

Content preparation functions

SCP functions

Control

Content

Service control functions

Delivery protocols

MV service control functional block

Service user profile functional block

Content delivery & receiving functions

Content distribution and location control functions

MV delivery and receiving functions

Content and control

Network Functions

Authentication and IP allocation functional block

Resource control functional block

Access network functions

Edge functions

Core transport functions

Transport Functions

Management functions

Application management functional block

Content and metadata

Service control management functional block

Content delivery management functional block

End-user device management functional block

IoT device management functional block

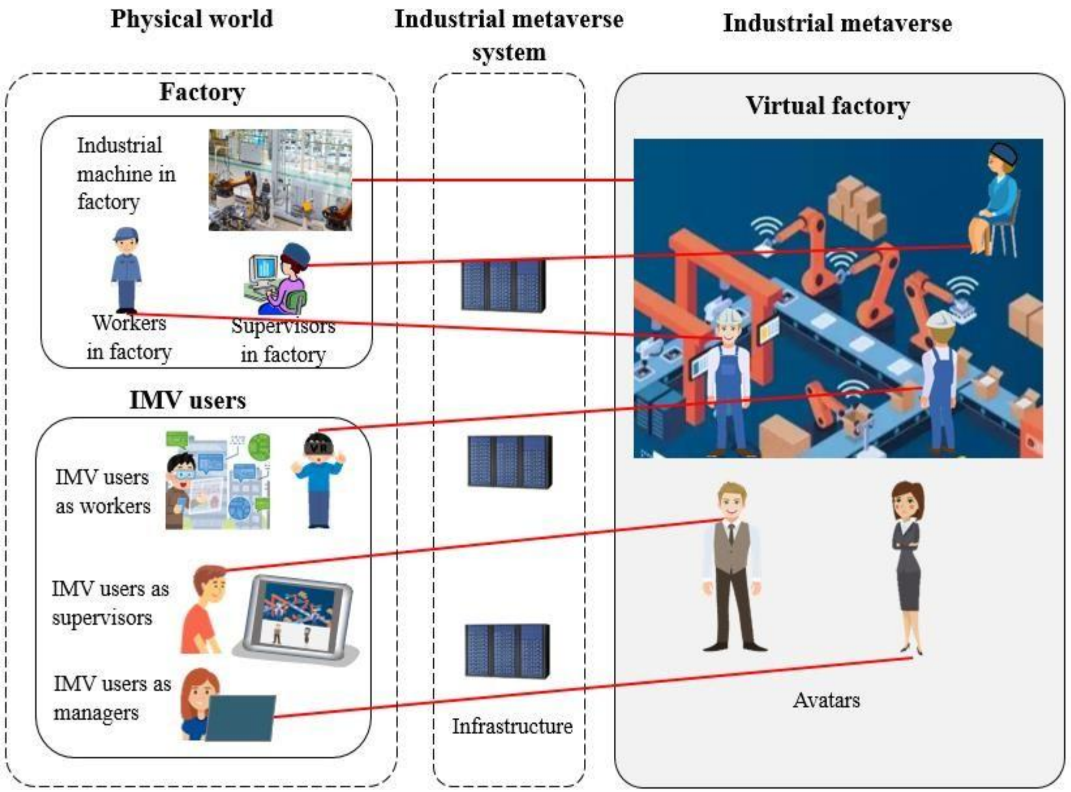
Transport management functional block

Content provider functions

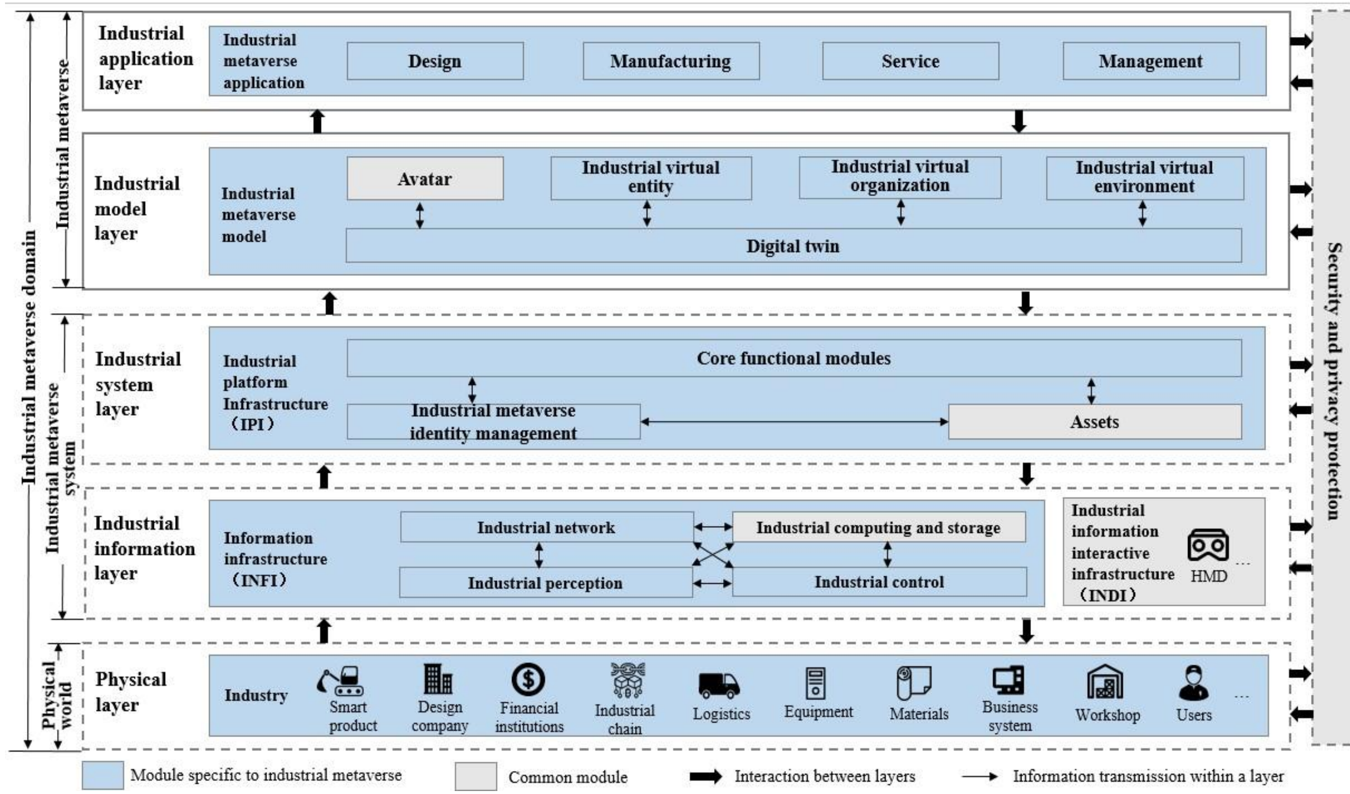
Metaverse content and metadata sources

Avatar content and metadata sources

Metaverse architectural overview (DT-IoT metaverse)

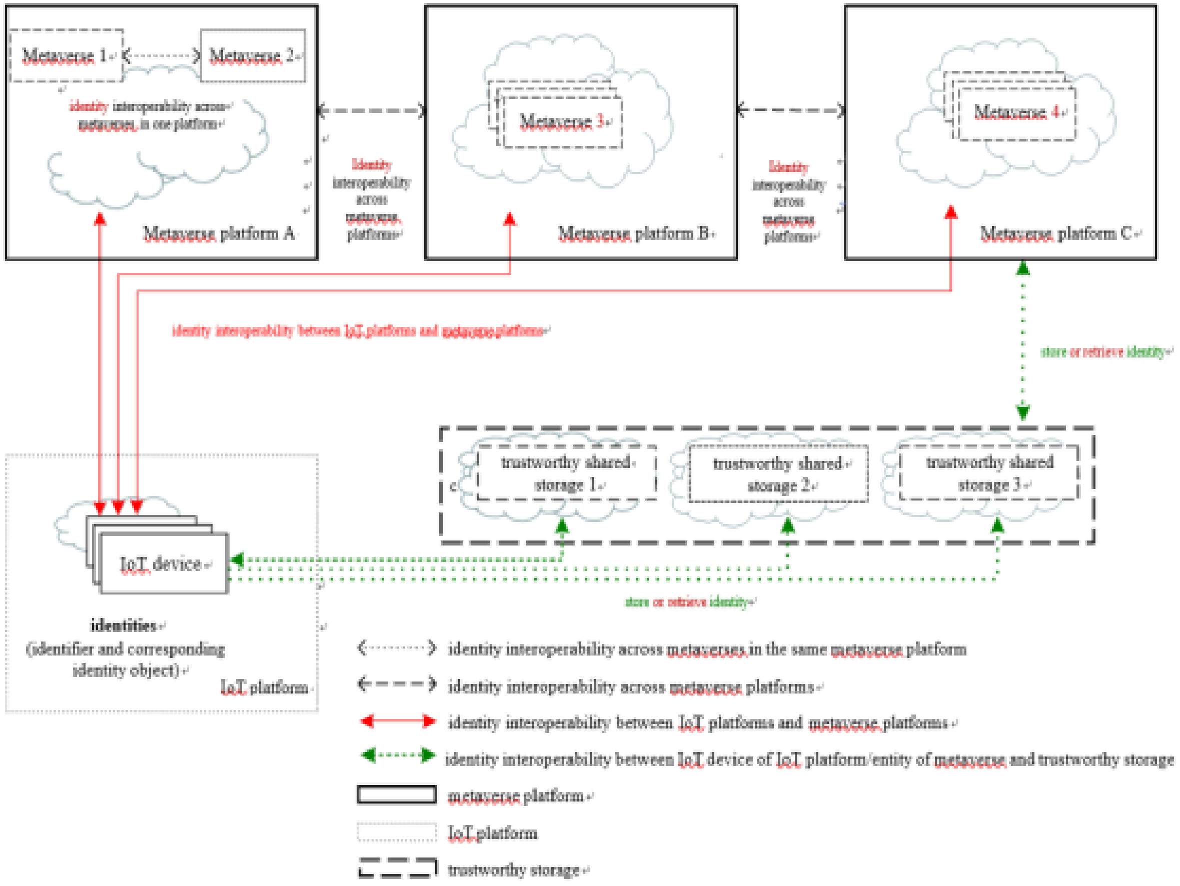


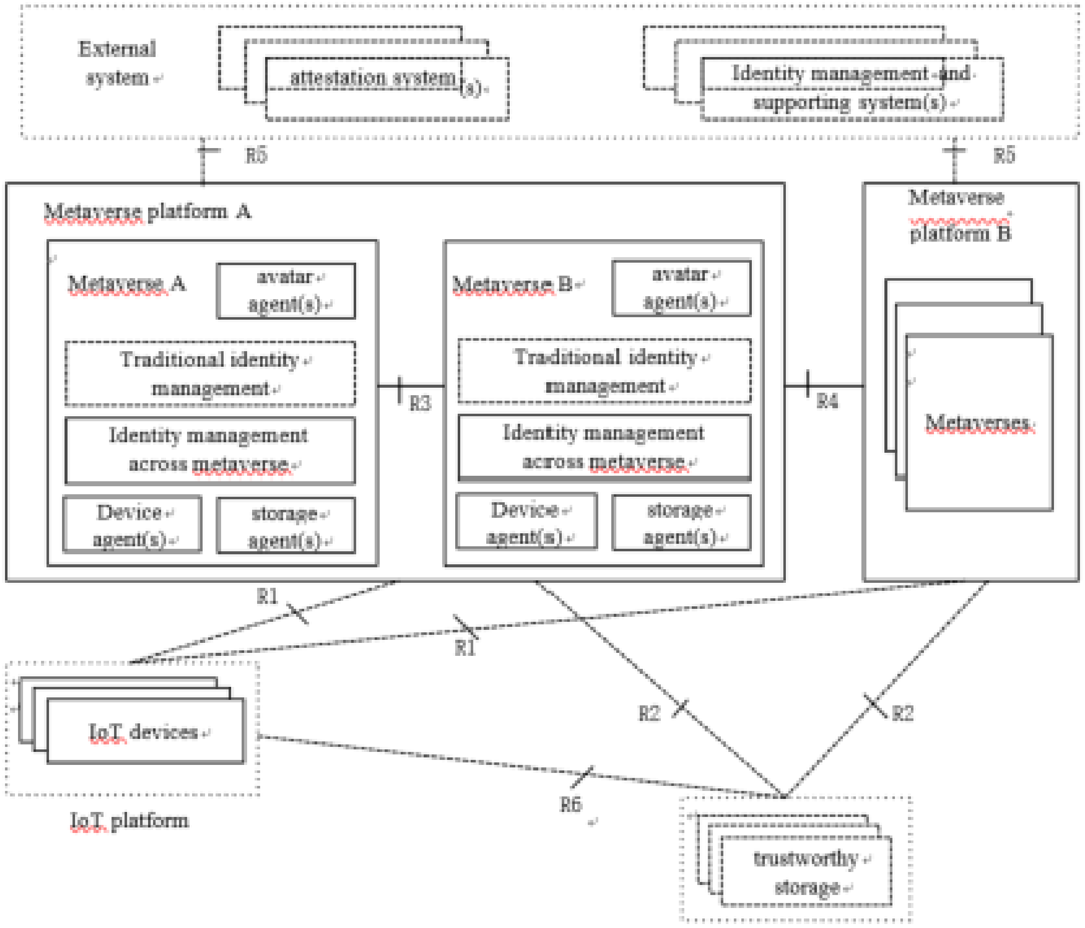
Overview of industrial metaverse domain


Industrial metaverse domain
Industrial metaverse
Industrial metaverse system
Physical world
Security and privacy protection
Industrial application layer
Industrial metaverse application
Design
Manufacturing
Service
Management
Industrial model layer
Industrial metaverse model
Avatar
Industrial virtual entity
Industrial virtual organization
Industrial virtual environment
Digital twin
Industrial system layer
Industrial platform Infrastructure （IPI）
Core functional modules
Industrial metaverse identity management
Assets
Industrial information layer
Information infrastructure （INFI）
Industrial network
Industrial computing and storage
Industrial perception
Industrial control
Industrial information interactive infrastructure （INDI）
HMD
...
Physical layer
Industry
Smart product
Design company
Financial institutions
Industrial chain
Logistics
Equipment
Materials
Business system
Workshop
Users
...
Module specific to industrial metaverse
Common module
Interaction between layers
Information transmission within a layer

Overall framework of industrial metaverse domain

[ITU-T] FG-MV(Focus Group on Metaverse) FGMV-42 “2024 - Interoperability of identity of things across metaverse platforms”

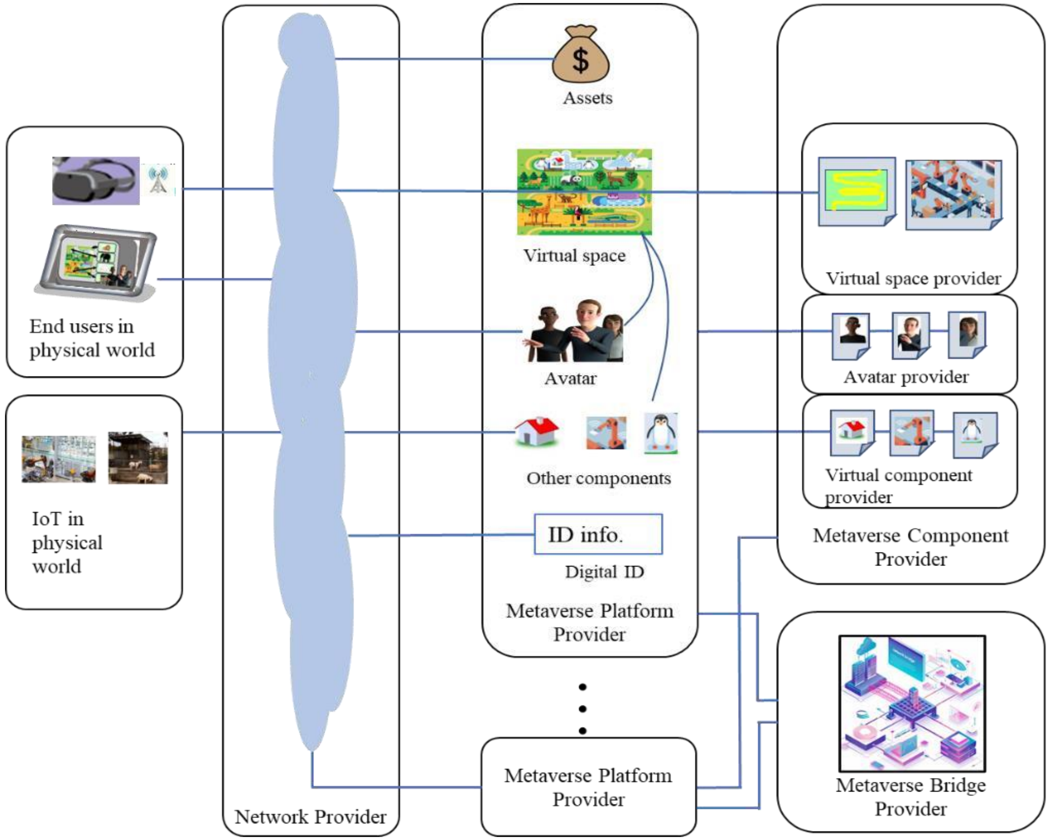

Metaverse 1
Metaverse 2
identity interoperability across metaverses in one platform
Metaverse platform A
Identity interoperability across metaverse platforms
Metaverse 3
Metaverse platform B
Identity interoperability across metaverse platforms
Metaverse 4
Metaverse platform C
identity interoperability between IoT platforms and metaverse platforms
store or retrieve identity
trustworthy shared storage 1
trustworthy shared storage 2
trustworthy shared storage 3
IoT device
store or retrieve identity
identities
(identifier and corresponding identity object)
IoT platform
identity interoperability across metaverses in the same metaverse platform
identity interoperability across metaverse platforms
identity interoperability between IoT platforms and metaverse platforms
identity interoperability between IoT device of IoT platform/entity of metaverse and trustworthy storage
metaverse platform
IoT platform
trustworthy storage

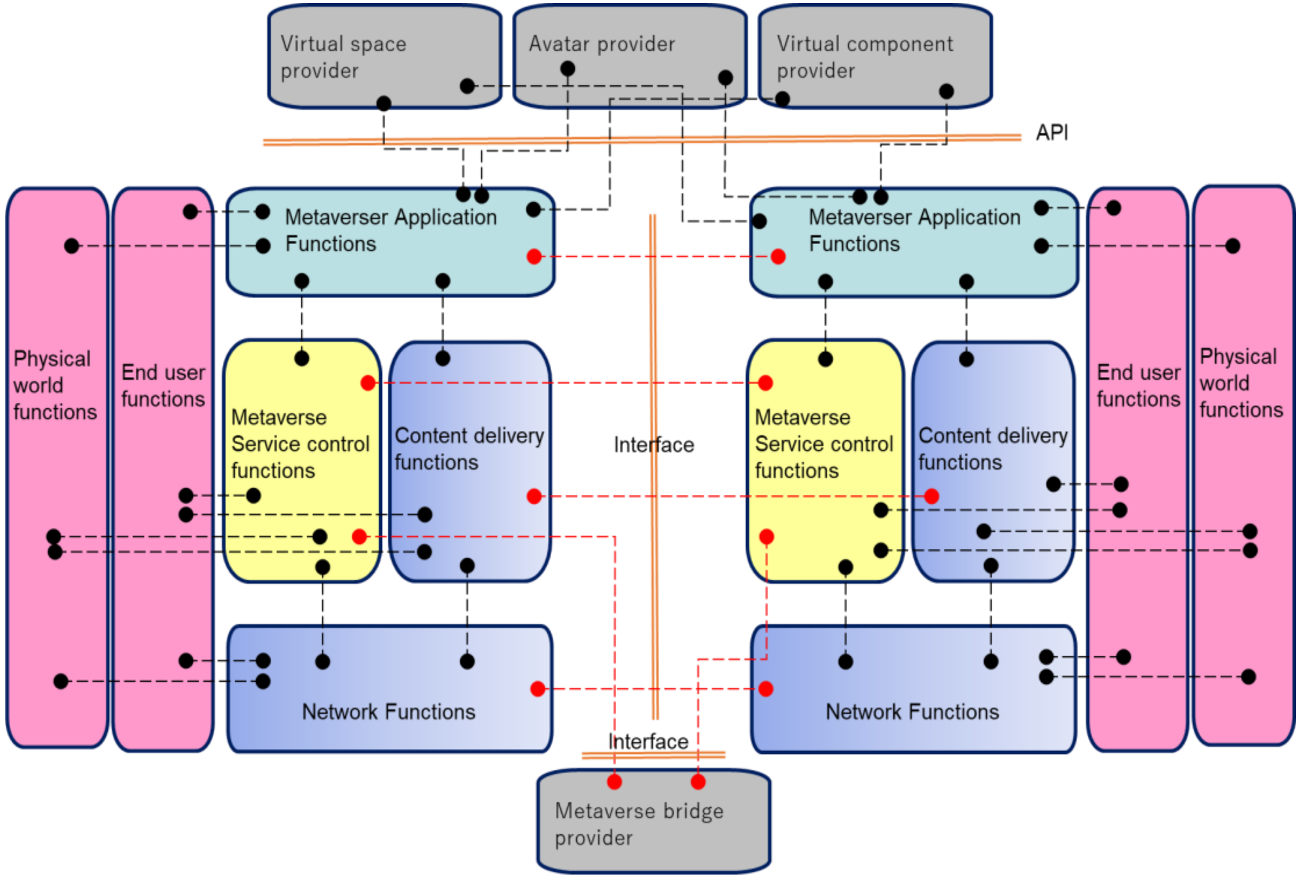


Technical feature of identity interoperability across metaverse platforms

Reference framework for identity interoperability across metaverse platforms

[ITU-T] FG-MV(Focus Group on Metaverse) FGMV-43 “2024 - High-level interoperability architecture for cross-platform metaverse”


Assets
Virtual space
Avatar
Other components
ID info.
Digital ID
Metaverse Platform Provider
Metaverse Platform Provider
End users in physical world
IoT in physical world
Network Provider
Virtual space provider
Avatar provider
Virtual component provider
Metaverse Component Provider
Metaverse Bridge Provider

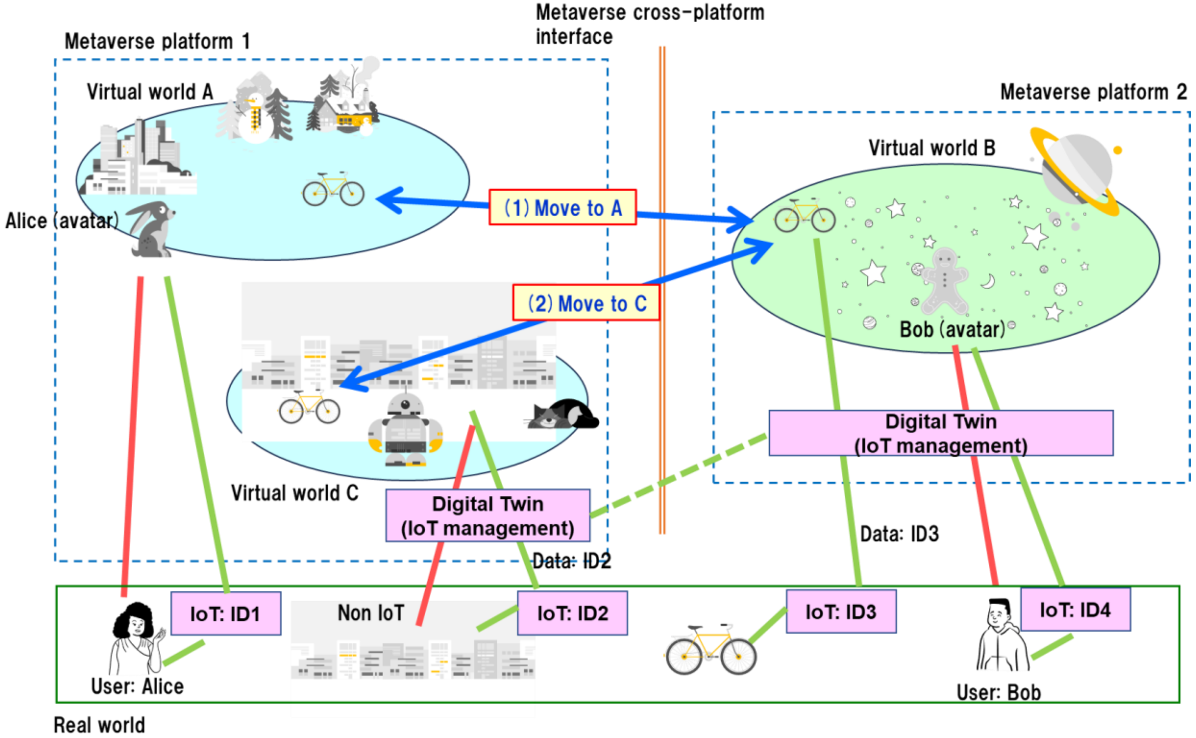

Virtual space provider
Avatar provider
Virtual component provider
API
Metaverser Application Functions
Metaverser Application Functions
Physical world functions
End user functions
Metaverse Service control functions
Content delivery functions
Interface
Metaverse Service control functions
Content delivery functions
End user functions
Physical world functions
Network Functions
Network Functions
Interface
Metaverse bridge provider

NOTE: Management functions are not shown in this figure (Red colored connections indicate interoperable connections)

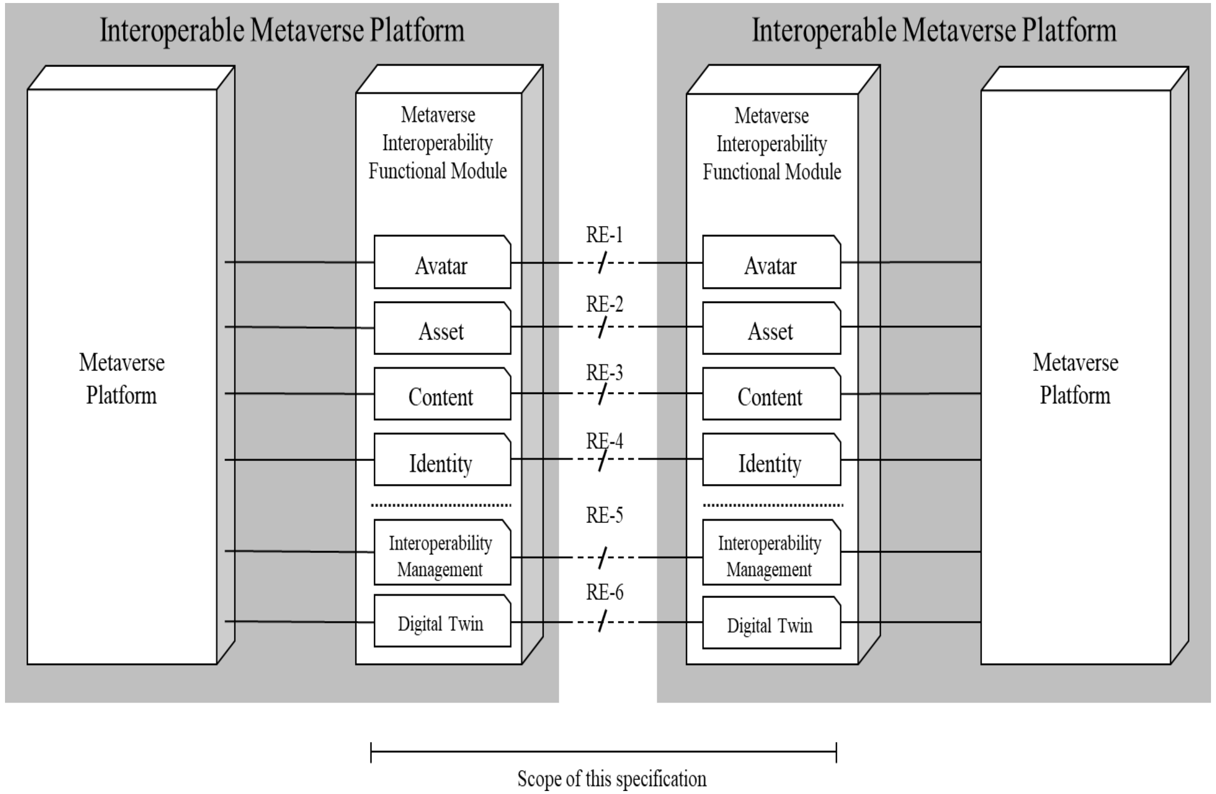
Stakeholders for metaverse cross-platform interoperability

Framework of metaverse cross-platform interoperability

[ITU-T] FG-MV(Focus Group on Metaverse) FGMV-43 “2024 - High-level interoperability architecture for cross-platform metaverse”



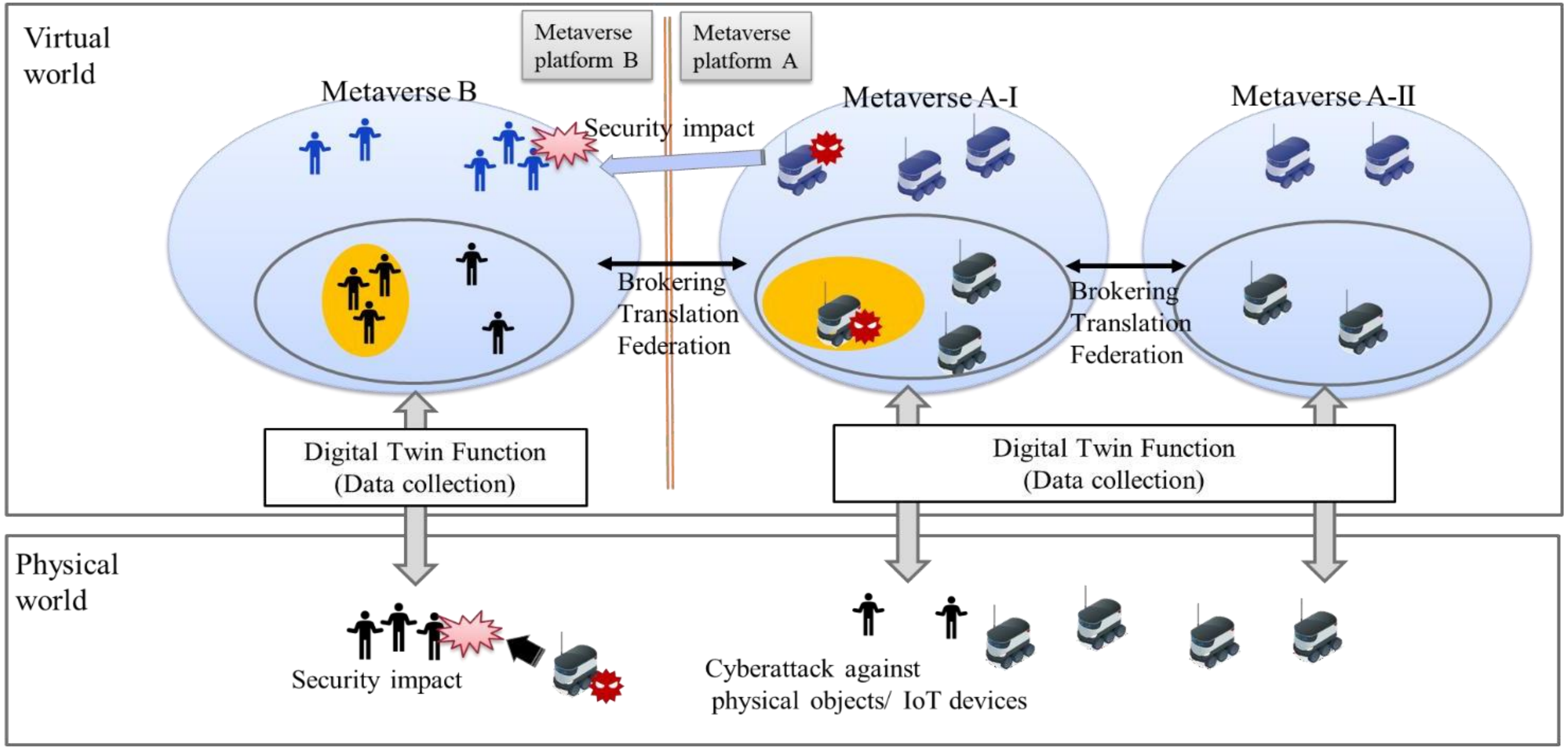
Interoperability of metaverses with both digital twins and IoT devices



Interoperable Metaverse Platform
Interoperable Metaverse Platform
Metaverse Platform
Metaverse Interoperability Functional Module
Avatar
Asset
Content
Identity
Interoperability Management
Digital Twin
RE-1
RE-2
RE-3
RE-4
RE-5
RE-6
Metaverse Interoperability Functional Module
Avatar
Asset
Content
Identity
Interoperability Management
Digital Twin
Metaverse Platform
Scope of this specification

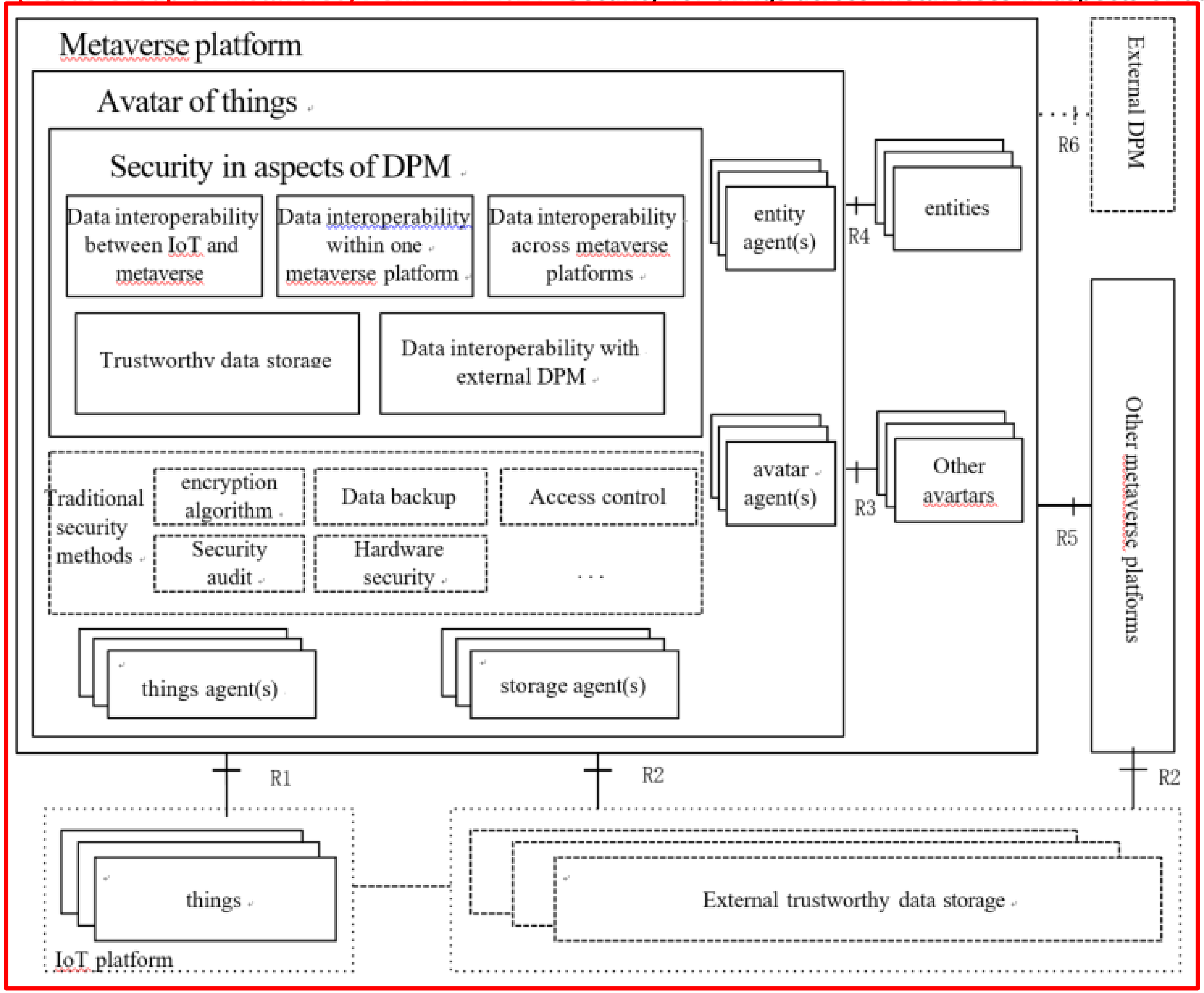
Architectural overview of interoperation between metaverse platforms

According to the discussions so far, the classification of the metaverse includes metaverse with digital twins and metaverse with IoT devices. To interoperate these metaverses securely, it is important to ensure the security of the underlying IoT devices and cyber-physical systems, as well as the cybersecurity of the metaverse stated in [ITU FGMV-10]. Since IoT devices and cyber- physical systems integrate the cyber and physical spaces, security measures should not be limited to cyberspace or individual systems but need to consider the impact on the physical space surrounding the systems. As shown in Figure, when network-connected devices are subjected to cyberattacks, it affects the surrounding physical entities, which in turn also impacts the metaverse with digital twin or IoT devices. The interoperability of digital twins is effective when evaluating the impact of cyberattacks on the physical space.



Cyberattack impact on metaverse with digital twin or IoT

[ITU-T] FG-MV(Focus Group on Metaverse) FGMV-44 “2024 - Security for things across metaverses in aspects of data processing and management”


Metaverse platform
Avatar of things
Security in aspects of DPM
Data interoperability between IoT and metaverse
Data interoperability within one metaverse platform
Data interoperability across metaverse platforms
Trustworthy data storage
Data interoperability with external DPM
Traditional security methods
encryption algorithm
Data backup
Access control
Security audit
Hardware security
. . .
things agent(s)
storage agent(s)
entity agent(s)
entities
R4
avatar agent(s)
Other avartars
R3
External DPM
R6
Other metaverse platforms
R5
R1
R2
R2
things
IoT platform
External trustworthy data storage

Reference framework for security for things across metaverses in aspects of data processing and management

Requirements of security for things across metaverses in aspects of data processing and management

(1) Security for things across metaverses in aspects of data processing

The data processing across metaverses includes data generation, data transmission and data analysis, mainly including the following aspects:

- It is required to use a unified data format (such as JavaScript Object Notation (JSON), Extensible Markup Language (XML) or Concise Binary Object Representation (CBOR)), and secure communication protocols (such as Hypertext Transfer Protocol (HTTP) or WebSocket) to ensure that the data exchange across metaverses has good compatibility and parsing.
- It is recommended to design and provide clear and complete API documents to clarify interface requirements in order to ensure that third-party developers can call services.
- It is recommended to support the identity authentication protocols across metaverses (such as Open Authorization (OAuth) or OpenID Connect (OIDC)) to achieve single sign-on (SSO) and cross-platform identification of user identity.

(2) Security for things across metaverses in aspects of data management

Lifecycle management provides data collection, storage, utilization, sharing, deletion, and so on, to ensure the transparency and controllability across metaverses.

- It is recommended to establish a data activity log system, record the whole process of data processing, and support the audit and traceability of data operations.
- It is recommended to monitor data across metaverses in real time to detect and respond abnormal data behaviours.

(3) Security for things across metaverses in aspects of data storage

When data is processed across metaverses, external trustworthy storage is used to help data exchange.

- It is recommended that data and records for data exchange and sharing are stored in a secure and tamper-resistant manner with the capability to report on it for audit purposes.
- It is recommended to provide a capability for connecting external storage to accommodate data volume growth in metaverses.

(4) Data encryption algorithms

Cryptography is a tool to provide data security, the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized use.

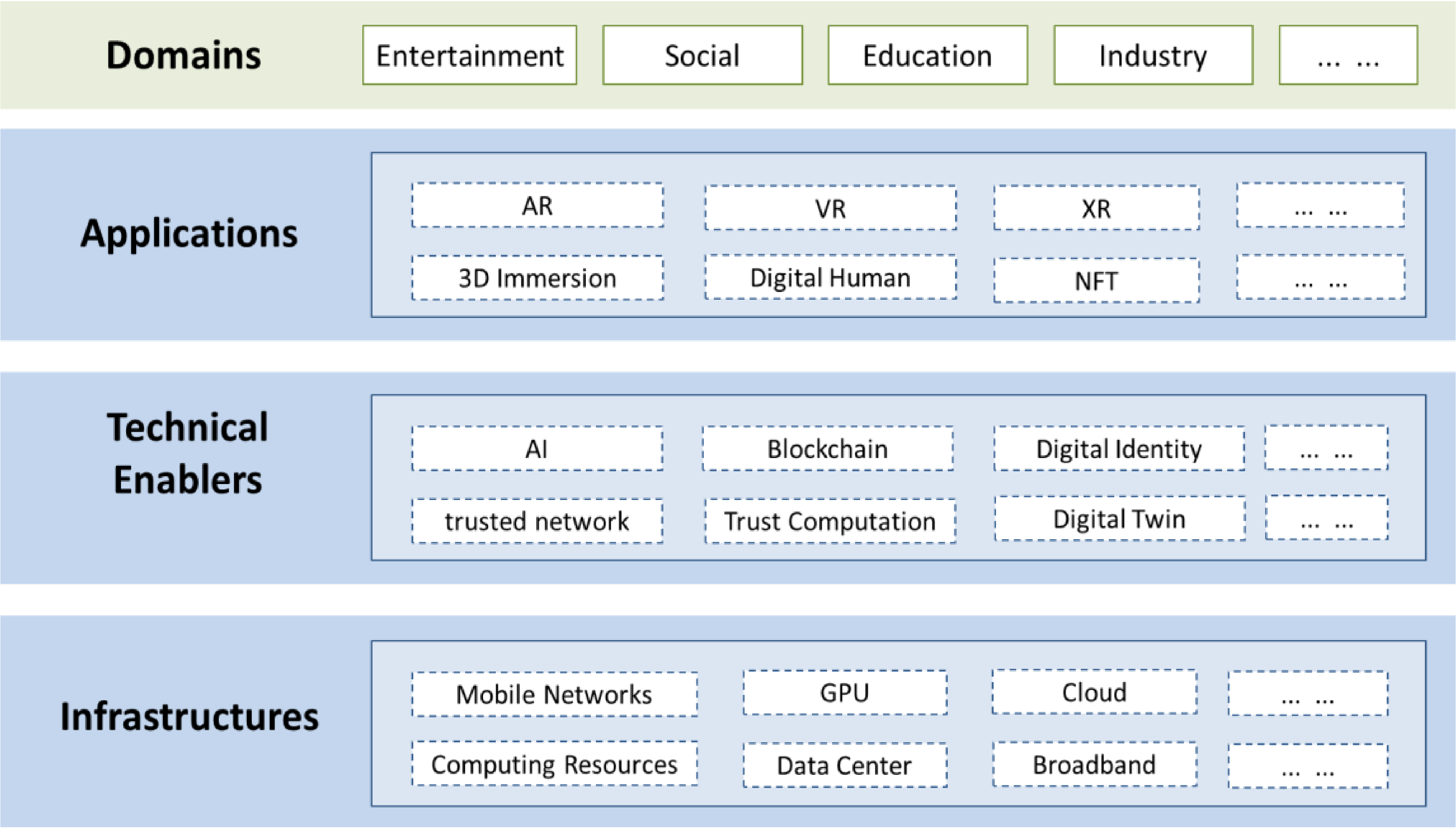
The data security dimension is composed of transmission data protection and data protection in rest, information flow control, secure session management and PII protection.

- It is required to encrypt data transmitted or stored using secure cryptographic algorithms.
- It is required to provide data security mechanisms for the support of trusted data transmission and circulation.
- It is recommended to use data encryption, digital signatures, hash function, and data fingerprints to ensure data security.

(5) Access control of metaverse platform

The access control of metaverse platform is designed to ensure the security of the platform, user privacy and the data legality.

- It is recommended to provide authentication and authorization mechanisms to ensure that users can only access the functions and services they are authorized to access.
- It is recommended to implement a multilevel rights system to distinguish different roles such as ordinary users, content creators and administrators; and each role has different access and operation rights.
- It is recommended to provide secure login mechanisms, such as multifactor authentication (MFA), one-time password (OTP), to enhance account security and prevent unauthorized access.



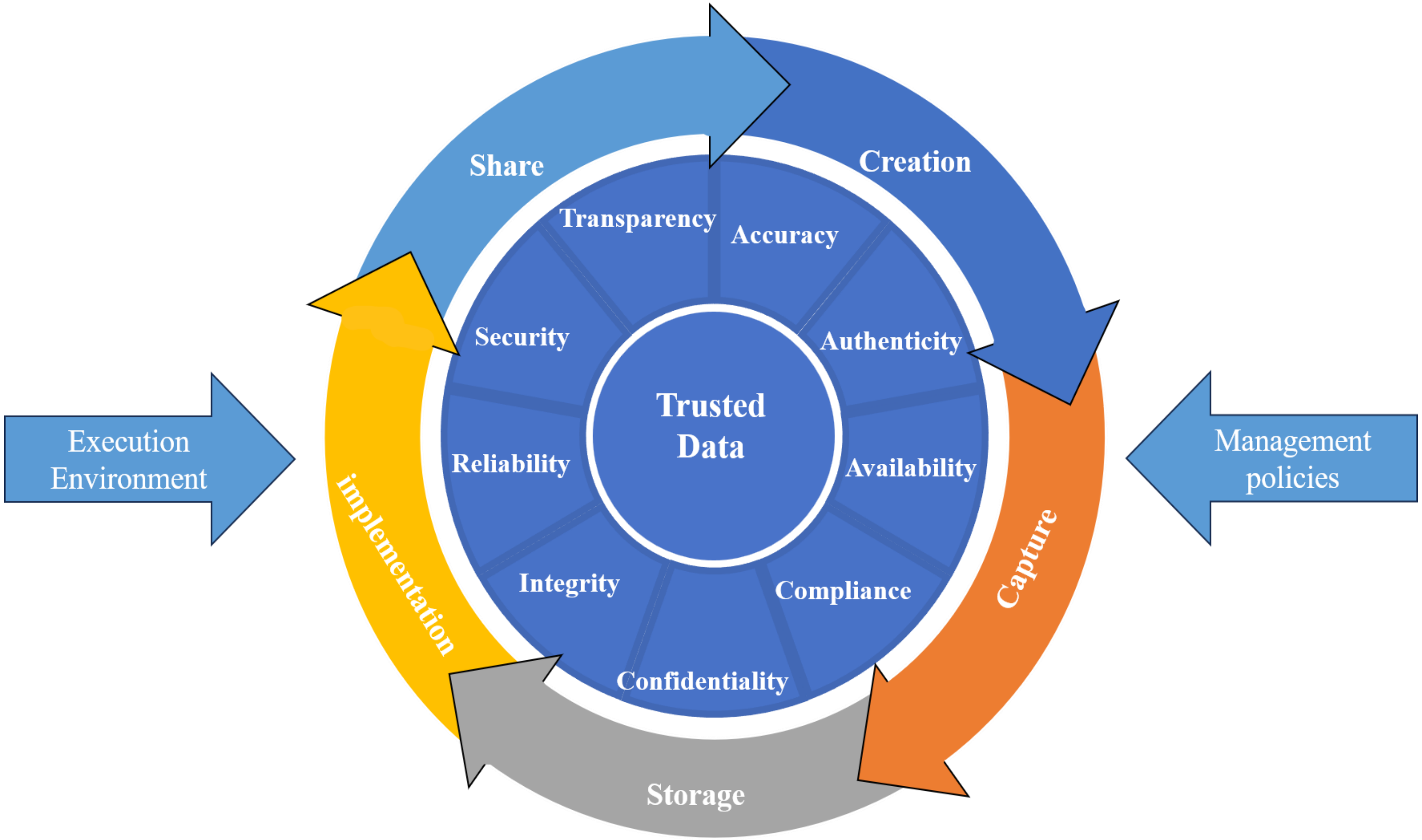
Domains: Entertainment | Social | Education | Industry | … …

Applications: AR | VR | XR | … … | 3D Immersion | Digital Human | NFT | … …

Technical Enablers: AI | Blockchain | Digital Identity | … … | trusted network | Trust Computation | Digital Twin | … …

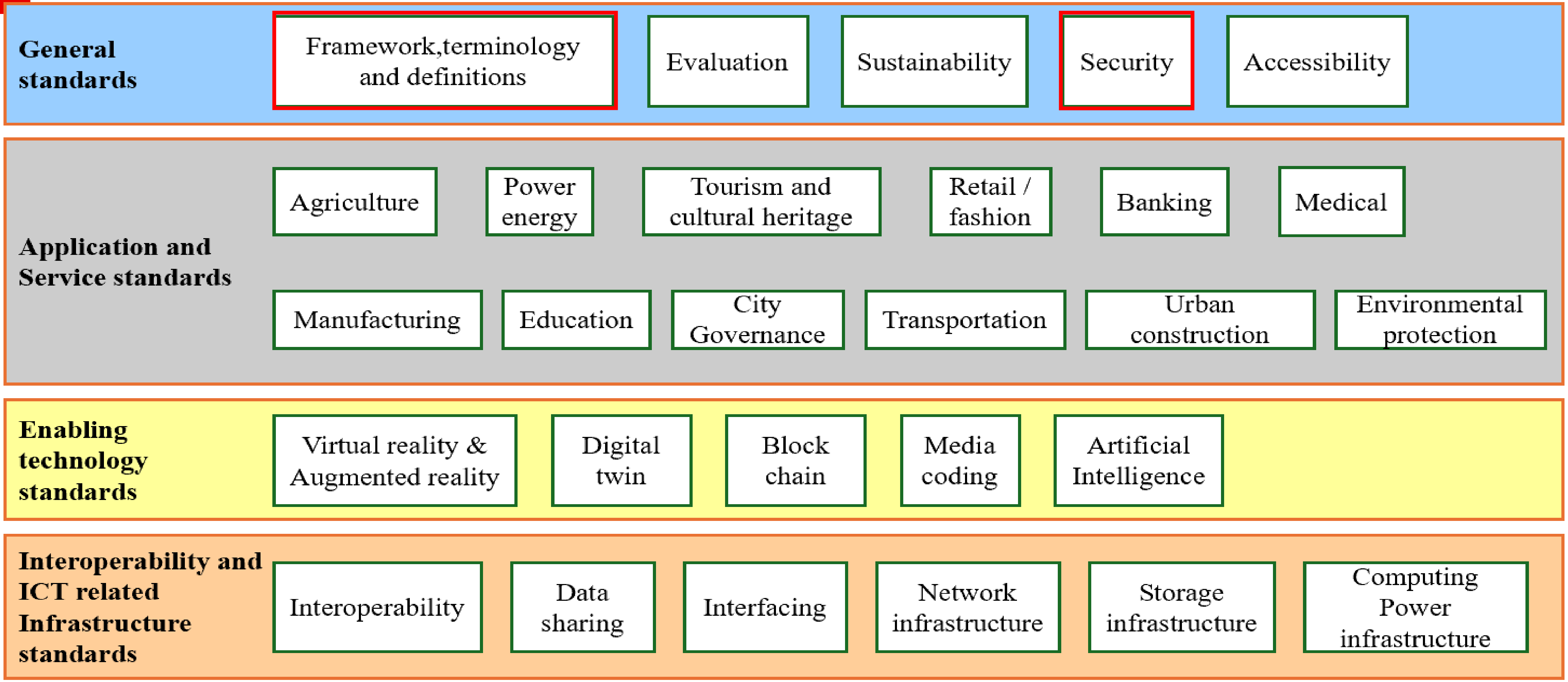
Infrastructures: Mobile Networks | GPU | Cloud | … … | Computing Resources | Data Center | Broadband | … …

A **reference model** for a trustworthy metaverse



The conceptual model of trusted data

[ITU-T] FG-MV(Focus Group on Metaverse) FGMV-51 “2024 - Standardization roadmap for metaverse”



General standards

- Framework,terminology and definitions
- Evaluation
- Sustainability
- Security
- Accessibility

Application and Service standards

- Agriculture
- Power energy
- Tourism and cultural heritage
- Retail / fashion
- Banking
- Medical
- Manufacturing
- Education
- City Governance
- Transportation
- Urban construction
- Environmental protection

Enabling technology standards

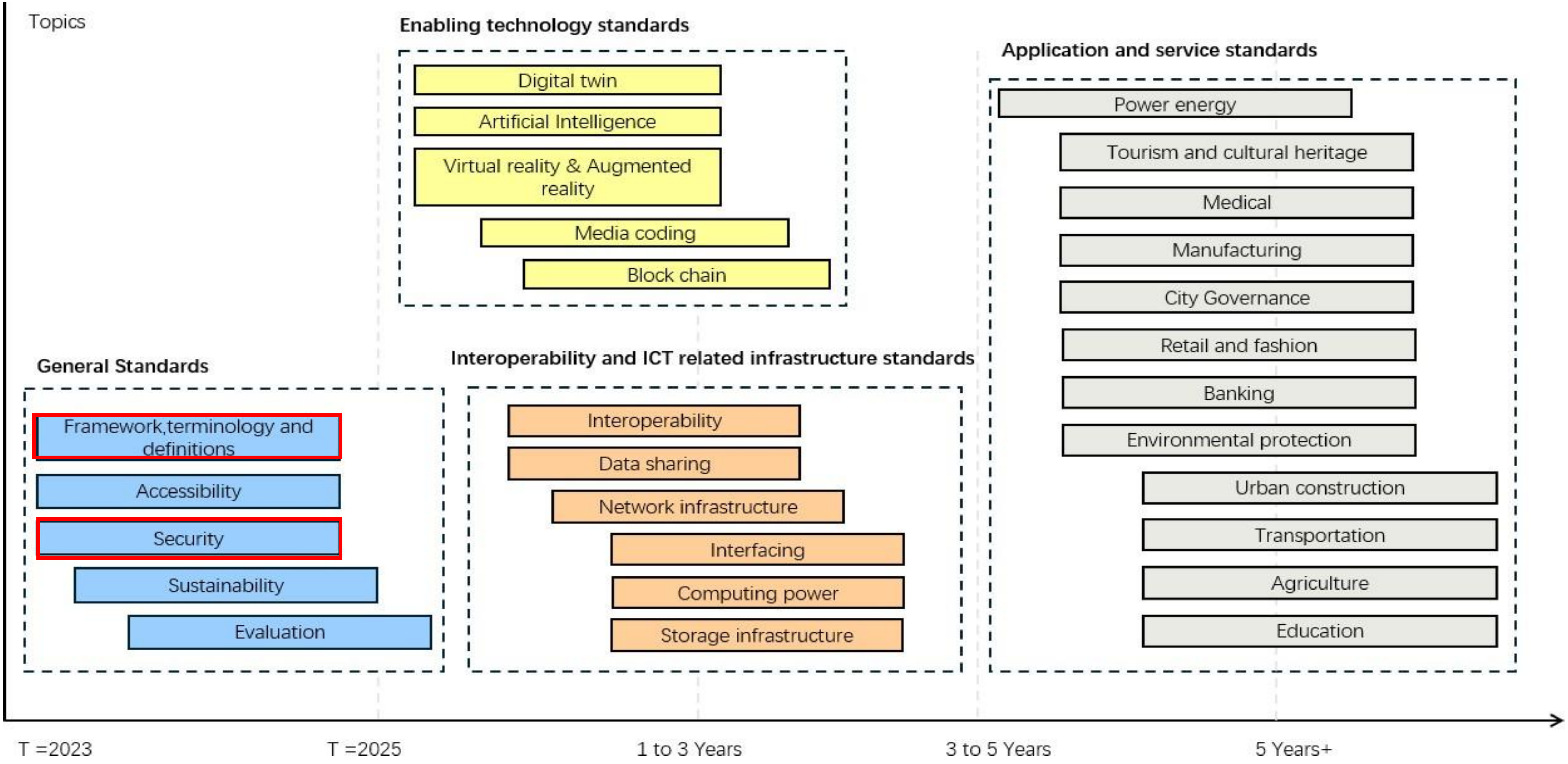
- Virtual reality & Augmented reality
- Digital twin
- Block chain
- Media coding
- Artificial Intelligence

Interoperability and ICT related Infrastructure standards

- Interoperability
- Data sharing
- Interfacing
- Network infrastructure
- Storage infrastructure
- Computing Power infrastructure

<Standards for metaverse can be generally classified into four categories>

- General standards,
- Application and service standards,
- Enabling technology standards, and
- Interoperability and ICT related infrastructure standards.



Possible timeline for standardization of metaverse