Review of Biometric Personal Information Protection in Metaverse Environment

ByungGook Lee (Dongseo Univ.)
Hoon Jae Lee (Dongseo Univ.)
Dae-Ki Kang (Dongseo Univ.)

DCN: 3079-24-0025-01-0003

Title: Review of Biometric Personal Information Protection in Metaverse Environment

Date Submitted: February 1, 2024

Authors or Source(s): ByungGook Lee (Dongseo Univ.)

Hoon Jae Lee (Dongseo Univ.)

Dae-Ki Kang (Dongseo Univ.)

Presented by Dae-Ki Kang (Dongseo Univ.)

Re: IEEE 3079 Session #29 in Jeju, Korea

Abstract: Contribution report for IEEE 3079 session #29

Purpose: Reviewing report and confirm to motions in this session

Biometric Personal Information Protection in Metaverse Environment

Date: 2024-02-01

Author(s):

Name	Affiliation	Phone [optional]	Email [optional]
ByungGook Lee	Dongseo Univ.	+82 10 9331 1453	lbg@dongseo.ac.kr
Hoon Jae Lee	Dongseo Univ.	+82 10 2801 3735	hjlee@dongseo.ac.kr
Dae-Ki Kang	Dongseo Univ.	+82 10 7557 2944	dkkang@dongseo.ac.kr

Biometric Personal Information Protection in Metaverse Environment

IEEE 3079

[Scope] We review the latest technological level related to biometric personal information threats in the metaverse environment and propose standardization to protect personal information accordingly. The scope of application is biometric personal information protection in the metaverse environment.

[Definition] Biometric personal information: It is comprehensively defined, including not only general biometric information such as face and fingerprint, but also biometric information such as brain and senses collected through advanced wearable devices such as HMD, hologram device, and BCI device in the metaverse.

Privacy Framework for Games & Interactive Media

IEEE 3079

A Privacy Framework for Games & Interactive Media

Peter M. Corcoran, Claudia Costache
College of Engineeing & Informatics
National University of Ireland Galway
Galway, Ireland
peter.corcoran@nuigalway.ie

Abstract— Privacy is a concept that is intertwined with data security, but its scope is significantly broader. Often considerations of privacy in the context of consumer devices are limited to a consideration of the security of the data stored in those devices. In this work a broader perspective taken and privacy is defined in terms of new classes which consider the wider context of individuals and groups of persons. The implications for games & interactive media (G&IM) devices and systems is discussed. Finally, some ideas for an improved privacy framework for G&IM are outlined and explained in the context of the literature and current state-of-art.

Index Terms—Privacy, Games, Interactive Media, Wearables, Digital Media, Consumer Devices, Entertainment Devices.

II. Related Works & Literature

In recent years there have been an increasing number of publications focusing on privacy for connected devices & services. Many of these focus on personal data [1]–[5], the need for a regulatory and legal framework [6]–[8] or the integrity of our computing devices and networks [9]–[11]. Typically a fairly narrow interpretation is given to the meaning of privacy – simply, that we should be in control of our personal data. In this work we take a broader perspective on what privacy means and consider not just data security, but the additional usage modalities of a connected G&IM device and associated network services.

P.M. Corcoran, et.al, "A Privacy Framework for Games & Interactive Media, " IEEE Games, Entertainment, Media Conference(GEM), 2018 College of Engineeing & Informatics , National University of Ireland Galway, Galway, Ireland

Privacy Framework for Games & Interactive Media

IEEE 3079

Classes of Privacy

1) Privacy of The Physical Person :

- This refers specifically to the privacy of the body. This class of privacy encompasses elements of biometrics, physically embedded devices such as RFID chips and physical implants and extending to sensing devices designed to detect body signals. As one example, consider recent progress in technologies to directly interface with electrical signals in the brain. User interfaces that employ such technology introduce new privacy challenges related to the physical person.

P.M. Corcoran, et.al, "A Privacy Framework for Games & Interactive Media, " IEEE Games, Entertainment, Media Conference(GEM), 2018 College of Engineeing & Informatics , National University of Ireland Galway, Galway, Ireland

Privacy Framework for Games & Interactive Media

IEEE 3079

Classes of Privacy

2) Privacy of Behavior & Action :

- This class of privacy relates primarily to sensitive aspects of personal lifestyle. As examples it covers sexuality, religion, political and philosophical beliefs. Privacy is more difficult to quantify here as some individuals are more open and forthright in expressing these aspects of their life than others. Society itself can also strongly influence how this class of privacy is valued.
- As a contemporary example, same-sex partnerships were not legally recognized in many countries until quite recently. As a consequence, individuals in such partnerships would have wished to keep their relationship private. The recent reversal of this practice in many jurisdictions will have changed the established social perception on such relationships and the importance of keeping such relationships private will now be less of a concern for many.
- Infringement of this class of privacy can occur in different ways, ranging from profiling of the person to a direct interception of communications or data.

P.M. Corcoran, et.al, "A Privacy Framework for Games & Interactive Media, " IEEE Games, Entertainment, Media Conference(GEM), 2018 College of Engineeing & Informatics , National University of Ireland Galway, Galway, Ireland

Privacy Framework for Games & Interactive Media

IEEE 3079

Classes of Privacy

3) Privacy of Personal Communication :

- This class of privacy is exemplified by the classic 'wire-tap' on a phone call. From a legal perspective any privacy conversation or exchange of information through a physcial means such as a written letter or audio phone call is normally considered private between corresponding parties. But technological development has simplified, extended and commoditized personal communication through e-mail, mobile telephony and internet messaging to an extent where we generate hundreds of private messages on a daily basis. At the same time technology renders all of these communication mechanisms more vulnerable to interception than ever before.
- In one quite recent example certain TV panels with voice actuation were designed to stream audio data to a network server to decode the received voice commands [20] – a clever engineering approach to reduce computational requirements on the device itself. Unfortunately, once this voice command mode was enabled audio data was continuously streamed over the internet and could be easily intercepted. In effect the TV became an internet-enabled bugging device that could spy on private conversations in your living room.

P.M. Corcoran, et.al, "A Privacy Framework for Games & Interactive Media, " IEEE Games, Entertainment, Media Conference(GEM), 2018 College of Engineeing & Informatics , National University of Ireland Galway, Galway, Ireland

Privacy Framework for Games & Interactive Media

IEEE 3079

Classes of Privacy

4) Privacy of Data & Image :

- This class of privacy was introduced by the authors of [18] primarily to cover the growing volume of image and video data generated by consumer devices and public surveillance systems. Every individual with a smartphone is now a well-equipped photo journalist and social media has created new distribution channels with high visibility for such data. In parallel, rapid advances in facial detection and recognition technology have commoditized the tracking of individuals in images and "Big Data" techniques enable the analysis of enormous image datasets and "profiling" of individuals on a scale that was simply not possible less than a decade ago. It is not difficult to see that new privacy challenges are created by this rapid evolution in technology and recent news scandals involving Camebridge Analytics and Facebook show how real and serious these challenges are.

P.M. Corcoran, et.al, "A Privacy Framework for Games & Interactive Media, " IEEE Games, Entertainment, Media Conference(GEM), 2018 College of Engineeing & Informatics , National University of Ireland Galway, Galway, Ireland

Privacy Framework for Games & Interactive Media

IEEE 3079

Classes of Privacy

4) Privacy of Data & Image :

The 7 Types of Privacy

1. Privacy of the Individual
2. Privacy of Behavior and Action
3. Privacy of Communication
4. Privacy of Personal Data
5. Privacy of Thoughts and Feelings
6. Privacy of Location and Space
7. Privacy of Association

[18] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in European Data Protection: Coming of Age, 2013, pp. 3–32.

Privacy Framework for Games & Interactive Media

IEEE 3079

Classes of Privacy

5) Privacy of Thoughts & Feelings :

- Another 'new' class of privacy, again introduced with a view to reflect very recent developments in technology. A few years ago it was still possible to feel very comfortable in the privacy of one's own thoughts & feelings. Today this class of privacy is increasingly challenged by sophisticated monitoring technologies and advanced methods of data analysis. As examples, facial analysis can evaluate your emotions; voice analysis can detect stress levels and video analysis can detect and monitor blood flow in your face and extremities. Combining these, and other biometric signals & behavioral analysis cues enables aspects of our mental state to be predicted quite accurately. And today we are bringing new consumer devices such as 'smart speakers' into our homes – devices that are key actors in providing access to the raw data that can enable such predictions on a real-time basis.

P.M. Corcoran, et.al, "A Privacy Framework for Games & Interactive Media, " IEEE Games, Entertainment, Media Conference(GEM), 2018 College of Engineeing & Informatics , National University of Ireland Galway, Galway, Ireland

Privacy Framework for Games & Interactive Media

IEEE 3079

Classes of Privacy

6) Privacy of Location & Space :

- This overlaps to some degree with Data & Image privacy, but the focus here is on the loss of privacy in public spaces. Today, from local corner stores to airports, train stations and shopping malls we are exposed to constant surveillance. And where there is not a dedicated surveillance system you can be easily recorded on the images or video captured by others in a public space. The tracking of an individual via their consumer device(s) can also be considered as an aspect of this class of privacy.
- With recent advances in drone technology the potential now exists to follow and observe an individual beyond fixed public surveillance networks and so the significance of this class of privacy continues to grow. There was a time when it was said that people came to the big city to hide in the crowd, but in a smart-city that will no longer be possible.

P.M. Corcoran, et.al, "A Privacy Framework for Games & Interactive Media, " IEEE Games, Entertainment, Media Conference(GEM), 2018 College of Engineeing & Informatics , National University of Ireland Galway, Galway, Ireland

Privacy Framework for Games & Interactive Media

IEEE 3079

Classes of Privacy

7) Privacy of Association & Group Membership :

- Privacy of association allows people of like mind to gather together and build communities, even when their views and philosophy is not mainstream. It is a freedom we expect in a progressive society. Today social media has enabled us to build communities more easily than in the past and to reach out and engage with audiences, small and large, sharing a similar perspective. The focus can be personal via a Facebook page, or more structured via Google+ or LinkedIn but the goal is similar - to build and gather like-mined groups of people.
- For social media systems privacy and trust have become key components of their services. Some of these efforts were driven by EU legislation, but it is fair to say that a growing awareness among the user base of social media has led to a broad re-engineering in the past few years. Today social media infrastructure is increasingly sensitive to the user's need for control over the level of privacy associated with their activities. While it is not yet clear at what levels social media and IoT will interact there can be little doubt that the widespread adoption of IoT will introduce some new challenges to user privacy in this area.

P.M. Corcoran, et.al, "A Privacy Framework for Games & Interactive Media, " IEEE Games, Entertainment, Media Conference(GEM), 2018 College of Engineeing & Informatics , National University of Ireland Galway, Galway, Ireland

Privacy Framework for Games & Interactive Media

IEEE 3079

Classes of Privacy

8) Privacy of Personal Experience :

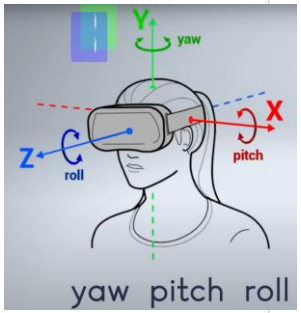
- This last category of privacy was introduced by Clarke (http://www.rogerclarke.com/DV/Intro.html#Priv) to consider the growing trend to monitor a user's preferences when they access an online service, employing this information to learn about their personal preferences.
- Consider as an example Spotify where samples of new music are offered to users based on their listening preferences. Arguably the user discovers new artists that they enjoy and most find this a helpful way to explore new music. But consider if this idea were applied to medical records to offer new experimental treatments for diseases – how would patients feel about such a service, even though it could offer significantly greater personal benefits than a music service? Although the underlying concept is almost identical the difference is that users are typically happy to declare their music preferences publicly, but not their medical history.

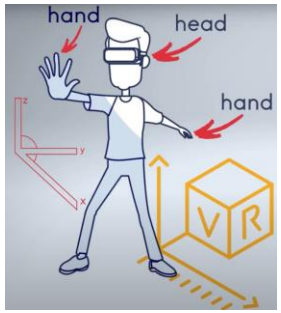
P.M. Corcoran, et.al, "A Privacy Framework for Games & Interactive Media, " IEEE Games, Entertainment, Media Conference(GEM), 2018 College of Engineeing & Informatics , National University of Ireland Galway, Galway, Ireland

Personal identifiability of user tracking data

www.nature.com/scientificreports

scientific reports





Check for updates

OPEN

Personal identifiability of user tracking data during observation of 360-degree VR video

Mark Roman Miller✉, Fernanda Herrera, Hanseul Jun, James A. Landay & Jeremy N. Bailenson

Virtual reality (VR) is a technology that is gaining traction in the consumer market. With it comes an unprecedented ability to track body motions. These body motions are diagnostic of personal identity, medical conditions, and mental states. Previous work has focused on the identifiability of body motions in idealized situations in which some action is chosen by the study designer. In contrast, our work tests 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. We argue these results show nonverbal data should be understood by the public and by researchers as personally identifying data.

Mark Roman Miller et al.(Stanford U.)," Personal identifiability of user tracking data during observation of 360-degree VR video," Nature, 2020.

Personal identifiability of user tracking data

IEEE 3079

❖ Personal identifiability of user tracking data during observation of 360-degree VR video

- Virtual reality (VR) is a technology that is gaining traction in the consumer market. With it comes an unprecedented ability to track body motions. These body motions are diagnostic of personal identity, medical conditions, and mental states. Previous work has focused on the identifiability of body motions in idealized situations in which some action is chosen by the study designer. In contrast, our work tests 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. We argue these results show nonverbal data should be understood by the public and by researchers as personally identifying data.

Mark Roman Miller et al.(Stanford U.)," Personal identifiability of user tracking data during observation of 360-degree VR video," Nature, 2020.

Personal identifiability of user tracking data

- **Personal identifiability of user tracking data during observation of 360-degree VR video**

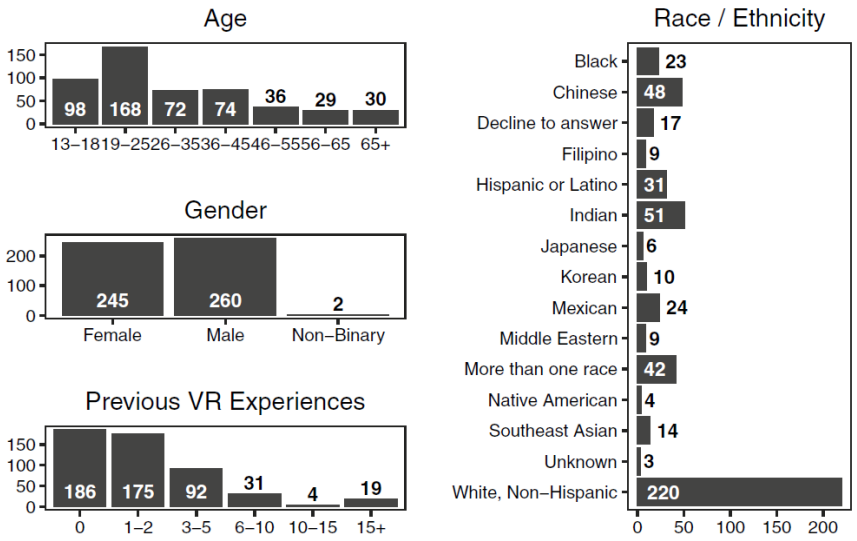


Figure 1. Histograms of demographic information (age, gender, number of previous VR experiences, and race and ethnicity) of study participants.

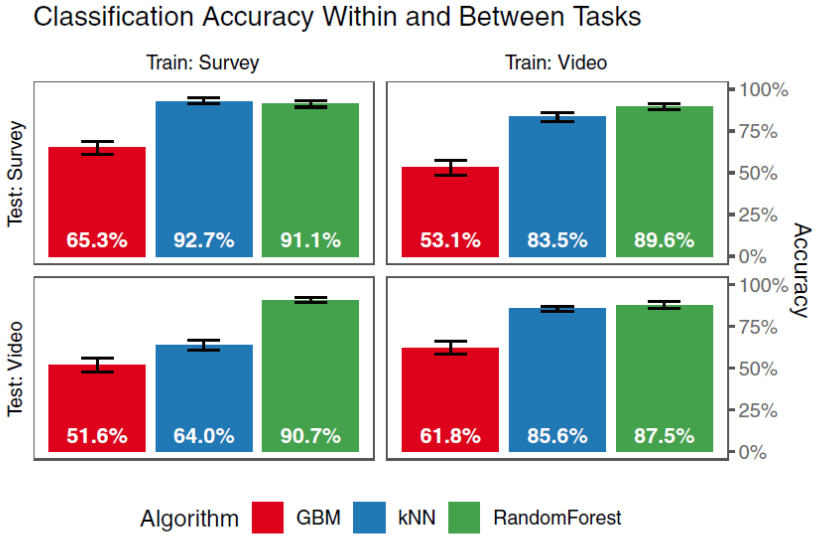


Figure 4. Accuracy within and between tasks. Error bars show the range of all 20 Monte-Carlo cross-validations.

Mark Roman Miller et al.(Stanford U.)," Personal identifiability of user tracking data during observation of 360-degree VR video," Nature, 2020.

Personal identifiability of user tracking data

❖ **Personal identifiability of user tracking data during observation of 360-degree VR video**

- For example, the y position is relative to the floor, so what is the distance between the headset and the floor where the user is standing? How far is the headset from the floor? What is the user's height? How droopy is your head? You can see how often you move your head up and down, which is the biggest identifying factor for identifying you.

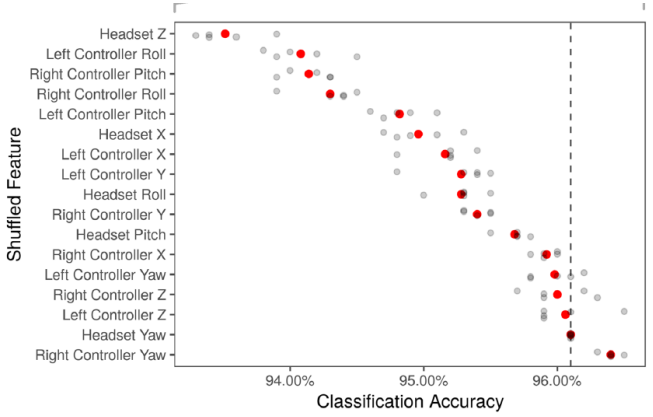


Figure 5. Feature importance displayed as Mean Decease in Accuracy. Black dashed line represents accuracy upon the unshuffled data. Bottom panel is a magnified section of the top panel.

Mark Roman Miller et al.(Stanford U.)," Personal identifiability of user tracking data during observation of 360-degree VR video," Nature, 2020.

On the Privacy Implications of Eye Tracking

- **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

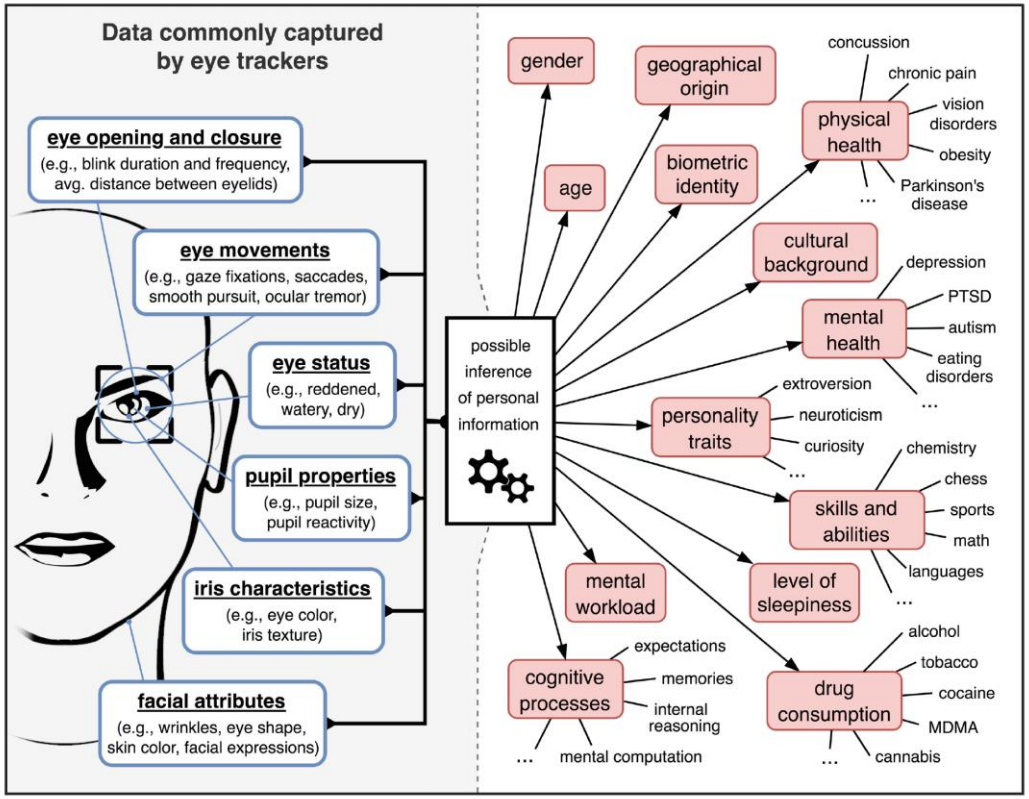


Fig. 1. Overview of sensitive inferences that can be drawn from eye tracking data.

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.

Biometrics

❖ Biometrics

- Biometrics are body measurements and calculations related to human characteristics.
  Biometric authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological characteristics which are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor/scent, voice, shape of ears and gait. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to mouse movement, typing rhythm, gait, signature, behavioral profiling, and credentials. Some researchers have coined the term behaviometrics to describe the latter class of biometrics. More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

https://en.wikipedia.org/wiki/Biometric

Biometric Personal Information Protection in Metaverse

IEEE 3079

[Scope] We review the latest technological level related to biometric personal information threats in the metaverse environment and propose standardization to protect personal information accordingly. The scope of application is biometric personal information protection in the metaverse environment.

[Definition] Biometric personal information: It is comprehensively defined, including not only general biometric information such as face and fingerprint, but also biometric information such as brain and senses collected through advanced wearable devices such as HMD, hologram device, and BCI device in the metaverse.

Biometric Personal Information Protection in Metaverse

IEEE 3079

❖ Encryption

- Use of encryption and other security measures to protect users' personal data from unauthorized access, theft, or misuse.

❖ Explicit Consent

- Users should be provided with clear and concise information about how their personal data will be collected, processed, and used in the metaverse, and they should be required to give explicit consent before any data is collected.

❖ Data Minimization

- Companies and organizations should only collect and process the minimum amount of personal data necessary to provide their services in the metaverse.

❖ Transparency and Control

- Users should be provided with transparency and control over their personal data in the metaverse, including the ability to access, correct, and delete their data.

Biometric Personal Information Protection in Metaverse

IEEE 3079

❖ **Data Breach Response Plan**
- Companies and organizations should have a clear plan in place for responding to data breaches in the metaverse and notifying users if their personal data is compromised.

❖ **Multi-factor Authentication**
- Implementing multi-factor authentication to ensure that only authorized users can access personal data in the metaverse.

❖ **Third-Party Audits**
- Conducting third-party audits to ensure compliance with data protection regulations and best practices in the metaverse.

Biometric Personal Information Protection in Metaverse

IEEE 3079

❖ **Privacy by Design**

- Adopting a privacy-by-design approach when developing and implementing metaverse technologies, meaning that privacy considerations are taken into account at every stage of the development process.

❖ **Anonymization**

- Companies and organizations can consider anonymizing personal data to protect users' identities and privacy.

❖ **User Education**

- Providing users with education and resources on how to protect their personal data in the metaverse, such as safe browsing habits and privacy settings.

Encryption Technology for Personal Information Protection

IEEE 3079

❖ **Encryption technology for personal information protection in the Metaverse environment**

- Purpose: In the metaverse environment where the real world and the virtual world coexist, the data transmitted through the communication network lacks or does not include encryption function. That is, some VR platforms are designed without essential security devices, and data communication is performed in an unencrypted communication between VR devices and servers. The purpose of this standard is to define the application of encryption technology between devices and servers or between nodes in a metaverse environment.

Biometric authentication devices

IEEE 3079

❖ **Fingerprint scanners**

- A fingerprint scanner is a technology that identifies and authenticates an individual's fingerprints to grant or deny access to a computer system or a physical facility.

❖ **Keystroke dynamics**

- Keystroke dynamics, also known as typing biometrics, is the automated method of identifying or confirming an individual's identity based on their typing manner and rhythm on a keyboard.

❖ **Facial pattern recognition**

- Facial recognition is a technology that can match a human face from a digital image or video frame with a database of faces to verify an individual's identity.

❖ **Iris scan identification**

- Iris recognition is an automated biometric identification method that captures unique patterns within a ring-shaped region surrounding the pupil of each eye.

❖ **Retinal scan**

- A retinal scan is a biometric technique that utilizes a low-intensity light source to map the distinctive patterns of an individual's retina.

❖ **Hand geometry recognition devices**

- Hand-geometry devices are biometric devices specifically designed for capturing the geometric characteristics of a human hand, such as the length, width, thickness, and curvature of the fingers, palm size, and distances between joints.

Metaverse Architecture

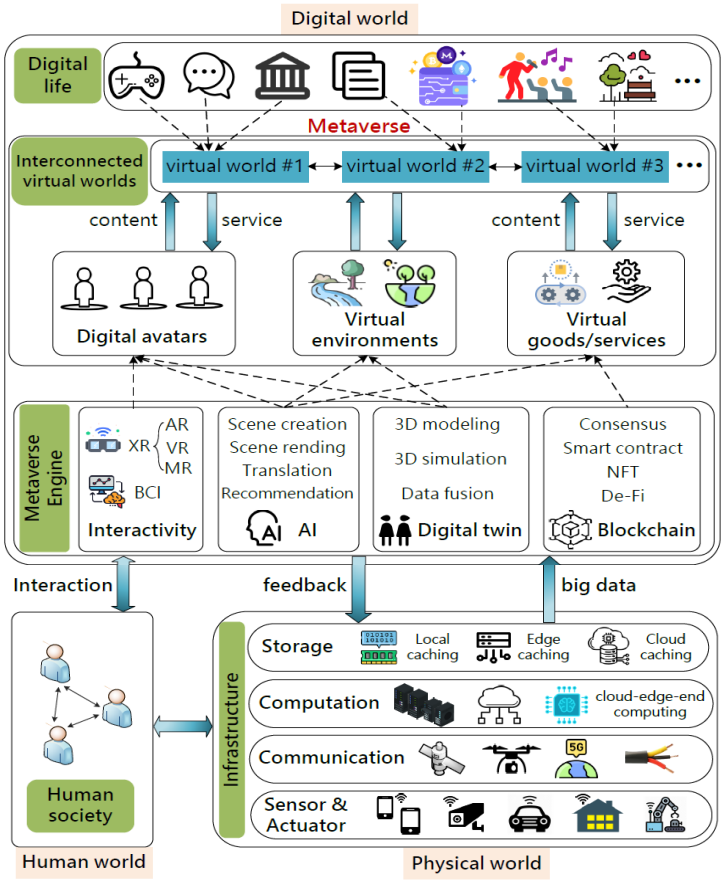


Fig. 5. The architecture of metaverse in integration of the human, physical, and digital worlds.

IEEE 2888

- **Human Society**
- **Physical Infrastructures**
  - Storage
  - Computation
  - Communication
  - Sensor & Actuator
- **Interconnected Virtual Worlds**
  - digital avatar
  - virtual environments
  - virtual goods/services
- **Metaverse Engine**
  - Interactivity: XR(AR/VR/MR), BCI
  - AI
  - Digital Twin
  - Blockchain
- **In-World Information Flow**
- **Information Flow Across Worlds**

Thank You