ITUPublications

International Telecommunication Union

Standardization Sector

ITU Focus Group Technical Report

(06/2024)

ITU Focus Group on metaverse
(FG-MV)

FGMV-44

Security for things across metaverses in aspects of data processing and management

Working Group 6: Security, Data & Personally identifiable information (PII) Protection

PREPUBLISHED

Version

Technical Report ITU FGMV-44

Security for things across metaverses in aspects of data processing and management

Summary

In Internet of Things (IoT) [ITU-T Y.4000], each physical/virtual thing (such as sensors, IoT devices, IoT systems, IoT gateways) manages and processes its data independently, directly by itself or via relevant IoT systems. If a thing is mapped into a metaverse, actively or passively, its data will be transferred into the target metaverse. Usually, a metaverse may manage and process data of its entities by itself. And when there are a large number of entities and data, it may use external computing resources and services to manage and process relevant data. A thing may be mapped into multiple metaverses. In this case, there are more challenges to manage and process the data of things, including to protect data security.

This Technical Report analyses and provides solutions about security for things across metaverses in aspects of data processing and management, including at least relevant technical features, requirements and reference frameworks of security for things across metaverses in aspects of data processing and management.

Keywords

data management; data processing; Internet of Things (IoT); metaverse; security; thing

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.

Change Log

This document contains Version 1.0 of the ITU Technical Report on "*Security for things across metaverses in aspects of data processing and management*" approved at the 7th meeting of the ITU Focus Group on metaverse (FG-MV) held on 12-13 June 2024.

Acknowledgements

This Technical Report was researched and written by Xiaojun Mu (China Unicom, China), Xiongwei Jia (China Unicom, China), Keng Li (China Information Communication Technologies Group,China) and Heung Youl Youm (Soonchunhyang University, Korea (Republic of)) as contributors to the ITU Focus Group on metaverse (FG-MV). The development of this document was coordinated by Vincent Affleck (DSIT, United Kingdom), as FG-MV Working Group 6 Chair, and Mr Christian Alvarez (UNICEF) and Ms Hanna Linderstål (EARHART Business protection agency), as Chairs of the Task Group on cybersecurity.

Additional information and materials relating to this report can be found at: https://www.itu.int/go/fgmv. If you would like to provide any additional information, please contact Cristina Bueti at tsbfgmv@itu.int.

Editor:	Xiaojun Mu China Unicom China	**Tel:**+ 86 13292090213 **E-mail:** muxj@chinaunicom.cn
Editor:	Xiongwei Jia China Unicom China	Tel:+86 15611092296 E-mail: jiaxw9@chinaunicom.cn
Editor:	Keng Li China Information Communication Technologies Group China	E-mail: kli@fiberhome.com
Editor:	Heung Youl Youm Soonchunhyang University Korea (Republic of)	Tel:+82-41-530-1328 E-mail: hyyoum@sch.ac.kr
WG6 Chair:	Vincent Affleck DSIT United Kingdom	E-mail:Vincentaffleck2@hotmail.com
TG Co-Chair:	Christian Alvarez UNICEF	E-mail: calvarez@unicef.org
TG Co-Chair:	Hanna Linderstål EARHART Business protection agency	E-mail: hanna.linderstal@earhart.se

Table of Contents

Page

Technical Report ITU FGMV-44

Security for things across metaverses in aspects of data processing and management

1 Scope

This Technical Report analyses and provides solutions about security for things across metaverses in aspects of data processing and management.

The scope of this Technical Report includes:

- Overview of security for things across metaverses in aspects of data processing and management.
- Technical features and requirements of security for things when across metaverses in aspects of data processing and management.
- Reference framework of security for things when across metaverses in aspects of data processing and management.

Use cases and analysis on the security for things across metaverses in aspects of data processing and management are provided in the appendices.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of the Technical Report.

[ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things.*

[ITU-T X.1352] Recommendation ITU-T X.1352 (2022), *Security requirements for Internet of things devices and gateways.*

[ITU-T Y.4464] Recommendation ITU-T Y.4464 (2020), *Framework of blockchain of things as decentralized service platform.*

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.1252]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 application [b-ITU-T Y.2091]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

3.1.3 authentication [b-ISO/IEC 18014-2]: Provision of assurance of the claimed identity of an entity.

3.1.4 avatar [b-ISO/IEC 23005-4]: Entity that can be used as a (visual) representation of the user inside the virtual environments.

3.1.5 blockchain [b-ITU-T X.1400]: A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

3.1.6 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.7 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.8 decentralized system [b-ITU-T X.1400]: Distributed system wherein control is distributed among the persons or organizations participating in the operation of system.

3.1.9 distributed ledger [b-ITU-T X.1400]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

3.1.10 distributed ledger technology (DLT) [b-ITU-T X.1400]: Technology that enables the operation and use of distributed ledgers.

3.1.11 entity [b-ITU-T X.1252]: Something that has separate and distinct existence and that can be identified in a context.

NOTE – For the purposes of this Recommendation, entity is also used in the specific case of something that is claiming an identity.

3.1.12 Internet of things (IoT) [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.13 ledger [b-ITU-T X.1400]: Information store that keeps final and definitive (immutable) records of transactions.

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

3.1.15 thing [ITU-T Y.4000]: With regard to the Internet of things, this is an object of the physical world (physical things) or of the information world (virtual things), which is capable of being identified and integrated into the communication networks.

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

IoT Internet of things

DPM Data Processing and Management

5 Conventions

None.

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

With regard to a standalone and silo metaverse, its entities and their data are only available in it, and there is no consideration for entity roaming to other metaverses. In Internet of things (IoT) [ITU-T Y.4000], each physical/virtual thing (such as sensors, IoT devices, IoT systems, IoT gateways)

manages and processes its data independently, directly by itself or via relevant IoT systems. If a thing is mapped into a metaverse, actively or passively, its data will be transferred into the target metaverse. Usually, avatars in metaverse may manage and process the data of its entities by themselves. And when there are a large number of entities and data, avatars may use external computing resources and services to manage and process relevant data (see figure 6-1).

The metaverse is a complex cyber-physical-social system that can bridge the gap between virtual world and physical world [b-ITU-Journal]. An IoT thing [ITU-T Y.4464] can be connected to or mapped into one or multiple metaverses. In this case, there are more challenges to manage and process the data of things, including to protect data security.

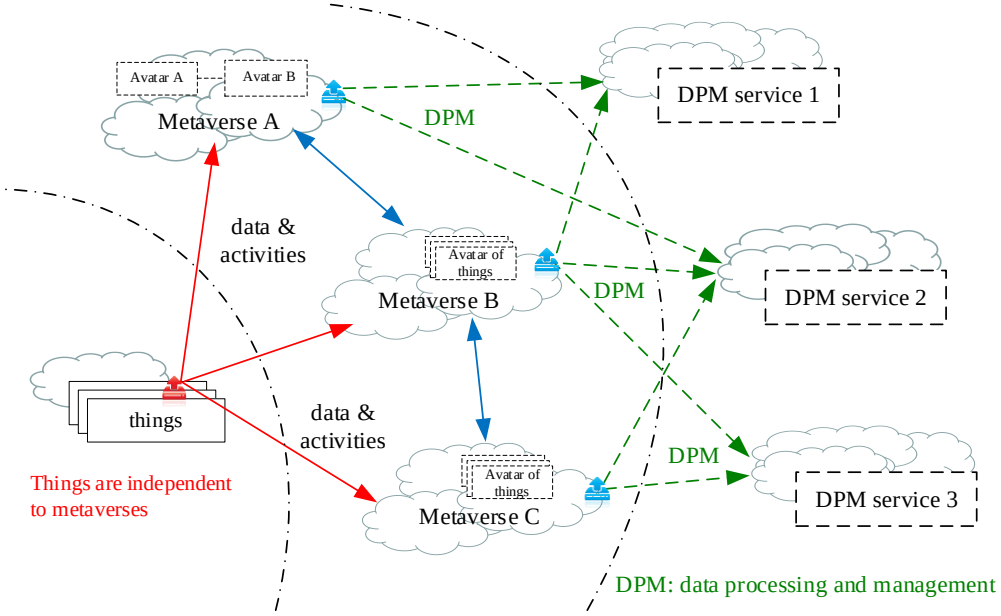

Figure 6-1 – Overview of security for things across metaverses in aspects of data processing and management

7 Technical features and requirements of security for things across metaverses in aspects of data processing and management

7.1 Technical features of security for things across metaverses in aspects of data processing and management

7.1.1 Independent data storage

Each physical/virtual thing (e.g., sensors, IoT devices, IoT systems, IoT gateways) stores its data independently, directly by itself or via relevant IoT systems.

Each avatar stores its data independently. When there are a large number of entities and data, it may use external computing resources and services to manage and process relevant data. External computing resources and services are also independent with things and avatars.

7.1.2 Trustworthy data storage

Use trustworthy storage to store data, including the data of things, the data of avatars, and the data of metaverses. Trustworthy storage system(s) guarantee(s) the reliability, confidentiality, integrity, consistency, availability and non-tampering of data.

7.1.3 Trustworthy data computing

The computing processes of thing and avatars are independent with each other. Data computing can be performed at the thing and avatar terminals, and if the data volume is large, the external DPM

can be used for data computing.

The data generated during the computing is stored in a trustworthy storage system as required for backup.

7.1.4 Multiple access control methods

There are two ways to access data of thing(s): autonomous access and gateway access. Full-fledged thing(s) in IoT systems can connect to metaverses directly and constrained thing(s) in IoT systems connect to metaverses by IoT gateways.

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

7.2.1 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.

7.2.2 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.

7.2.3 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.

7.2.4 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.

7.2.5 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.

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

Figure 8-1 shows reference framework about security for things across metaverses in aspects of data processing and management. The reference framework mainly includes five parts: data interoperability between IoT platforms and metaverse platforms; data interoperability across avatars in one metaverse platform; data interoperability across different metaverse platforms; trustworthy data storage; and data interoperability with external DPM. The reference framework also includes traditional security methods, important agents and reference points for connecting external things, avatars of things, entities, external storage, and so on.

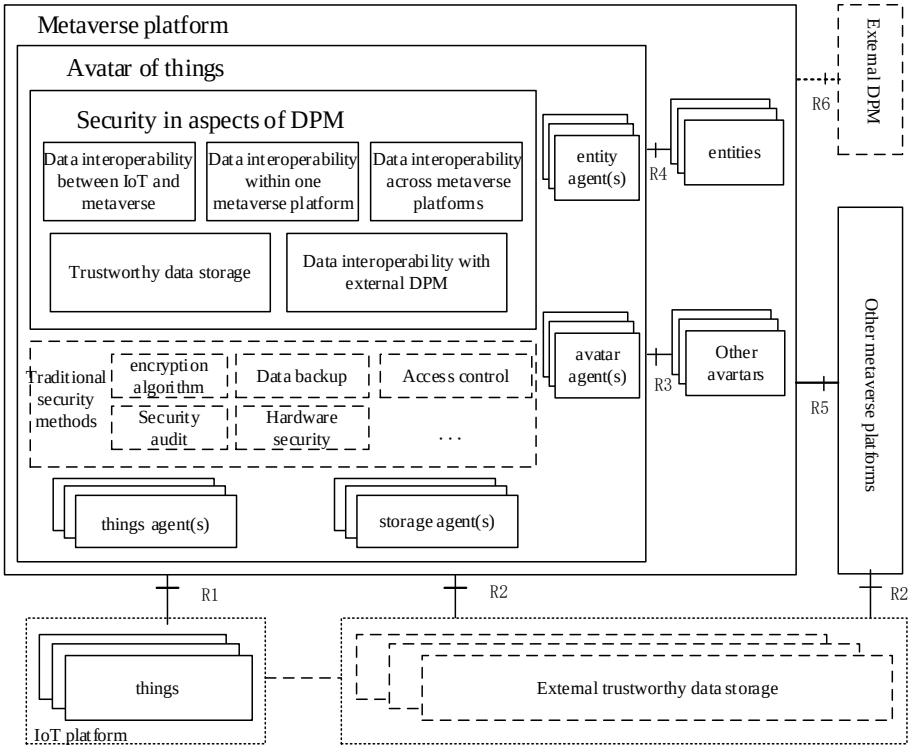

Figure 8-1 – reference framework for security for things across metaverses in aspects of data processing and management

8.1 Data interoperability between IoT platforms and metaverse platforms

Things in the IoT platform map into metaverse platforms and generate corresponding metaverse avatars. Things in IoT platforms can be mapped to one or multiple metaverse platforms. IoT platforms and metaverse platforms should provide relevant security authentication mechanisms to ensure data interoperability between IoT platforms and metaverse platforms.

The data of IoT and metaverses can be stored on external trustworthy storage, or on the metaverse platform and the IoT platform itself. If the data is stored on the external trustworthy storage, the IoT platform and metaverse platform need to provide authentication mechanisms to access the data stored in the trustworthy storage.

8.2 Data interoperability across avatars in one metaverse platform

In the same metaverse platform, different avatars of a certain thing can interoperate directly. The identity of the avatars contains the information of authentication. Data interoperability across avatars provides the security cooperation ability between multiple avatars in the same metaverse platform, including security capability assessment and security authentication before data migration, secure connection, data backup and security recovery during data migration, and so on.

8.3 Data interoperability across different metaverses platforms

Data interoperability across metaverse platforms includes the ability of collaboration between different metaverse platforms. Authorization and certification are required before the data interoperability across metaverses platforms. Data security for DPM across metaverse platforms requires double verification of the metaverse platforms and the avatars.

8.4 Data interoperability with external DPM

Metaverse data can be processed and calculated by the metaverse platform itself. But when the data volume is large and the computing requirements are high, external DPM resources are needed. The data needs to be encrypted and encapsulated before external processing.

8.5 Trustworthy data storage

The data generated by the IoT platform and metaverse platform can be stored either on the IoT platforms and metaverse platforms or on external trustworthy storage systems. Both things and avatars are configured with data access permissions based on requirements to ensure secure storage requirements. Metaverse data may be stored on metaverse platforms or external trustworthy storage according to the policies of metaverse platforms, which provides a reliable and secure connection between metaverse platforms and external trustworthy storages for data transmission and utilization.

8.6 Traditional security methods

The traditional security method provides some basic security methods for things across metaverses in aspects of data processing and management. These security methods are some general data security processing methods to help ensure the data security across the metaverses.

Note: Traditional security methods are out of the scope of this technical report.

8.6.1 Encryption algorithm

Encryption algorithm provides full lifecycle encryption and storage of data in metaverse, realizes peer-to-peer connection and end-to-end encrypted exchange of sensitive data, prevents private data leakage and man-in-the-middle attacks, and requires controllable and traceable data usage records to protect data privacy.

8.6.2 Data backup

When data is lost or damaged, data backup can quickly recover the data to avoid incalculable losses caused by data damage. Backup data can be stored in devices such as the cloud or an external hard drive.

8.6.3 Access control

Authentication and authorization ensure that only the right users have access to enterprise data. Once the users have proven their identities, authorization will determine whether the users have the appropriate permissions to access and interact with specific data. By authorizing users, they can gain permission to read, edit, and write to different resources within the metaverse.

8.6.4 Security audit

Security audit is an approach to monitoring and managing security that monitors activity in the network and detects unusual behaviour to detect and prevent cyberattacks. Security audit usually includes log audit, vulnerability scan, security check, and so on.

8.6.5 Hardware security

Hardware-based security involves the physical protection of devices, rather than relying solely on the software installed on the hardware. Hardware security refers to the installation of security modules in the chip to ensure that the device is safely protected.

8.7 Agent(s)

8.7.1 Things agent(s)

Things agents interact with IoT platform, which provide capabilities related to security for things, as follows:

- Interacting with things; one things agent can serve one or more things.
- Supporting things to store, use and transfer data across metaverses in a secure and reliable way.
- Supporting things to manage policy related to IoT data process across metaverses, such as where to store data across metaverses; how to collect, use and transmit data across metaverses; how to ensure data security and when to transmit across metaverses, and so on.
- Supporting things to interact with avatars or other entities safely.

8.7.2 Avatar agent(s)

Avatar agents interact with avatars of things from the same or other metaverse platforms, which provides capabilities related to security for things across metaverses, as follows:

- Interacting with avatars of things; one avatar agent can serve one or more avatars.
- Supporting avatars to store, use and transfer data across metaverses in a secure and reliable way.
- Supporting avatars to manage policy related to data flow of avatars across metaverses such as where to store data across metaverses; how to collect, use, transmit data across metaverses, how to ensure data security and when to transmit across metaverses, and so on.
- Supporting avatars to interact with each other mutually and safely.

8.7.3 Entity agent(s)

Entity agents interact with external entities, which provide capabilities as follows:

- Interacting external entities (such as things, digital humans and functional components); one entity agent can serve one or more entities.
- Connecting external DPM to process and manage data when connecting to metaverses.

8.7.4 storage agent(s)

Storage agents interact with external trustworthy storage, which provides capabilities as follows:

- Connecting external trustworthy storage to store and retrieve data across metaverses.
- Connecting external trustworthy storage to store and retrieve modules for data management and security across metaverses.

8.8 External entities

8.8.1 IoT platforms

The metaverse platform uses IoT sensors and devices to collect and transfer massive real-time data in the physical world to build and update its virtual world. IoT platform is not only a data acquisition terminal in the real world, but also an interactive interface for users to access the metaverse. Users can interact with the metaverse through IoT devices such as browsing virtual scenes through smart glasses and manipulating virtual items through smart gloves.

8.8.2 External trustworthy storage

External trustworthy storage is used to store data of IoT and metaverse and information generated during data exchange across metaverses. External trustworthy storage provides cross-metaverse data sharing capability, and implements efficient and secure data flow between different metaverse

through secure data exchange protocols and interfaces. In general, external trustworthy storage can be achieved through distributed ledger technology.

8.8.3 External DPM

When the amount of data is large or the metaverse platform itself is difficult to process the relevant data, the external DPM can be used for data processing and management across metaverses.

8.9 reference points

There is a group of reference points to interact with avatars, including:

- R1: for things to interact with avatars in metaverses.
- R2: for trustworthy storage to store the avatars and some other information related with data management and security across metaverses.
- R3: for avatar to share and exchange data across metaverses.
- R4: for entity to interact with avatars in metaverses.
- R5: for different metaverses interact directly with each other.
- R6: for metaverse platform to interact external with DPM.

9 Security consideration

There are many security issues in the security for things across metaverses in aspects of data processing and management. For example: data leakage, authentication and authorization issues, PII challenges, and regulatory challenges. In order to deal with these security issues, a series of measures need to be taken to strengthen the security of data exchange across the metaverses. This includes strengthening data encryption and transmission security, improving identity verification and authorization mechanisms, and strengthening PII technology and policy development.

Appendix I

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

(This appendix does not form an integral part of the Technical Report.)

I.1. Smartwatch data security across metaverses

Wearable device is an important sensor of metaverse. Smartwatches utilize multiple sensor devices to capture human movements in real time from various parts of the user's body (including ankles, wrists and head) and associate them with their avatars, allowing users to create their avatars using full-body movements. Smartwatches collect a large amount of data, involving the data processing and management of the data across metaverses, is an important application scenario of data management and security across metaverses.

I.1.1. Description

Multiple sensors in a smartwatch manage and process their data independently, either directly or through related IoT systems. In a metaverses application, the sensor is actively or passively mapped to one or more metaverses, and its data are transmitted to the target metaverses. The sensor and metaverses are independent of one another, and in order to ensure the credibility of data transmission the relevant important data of the sensor and metaverses will be stored on the trustworthy storage. Typically, a metaverse can manage and process its entity's data by its own. When the number of entities and amount of data are large, external computing resources and services may be used to manage and process the relevant data. External resources (DPM services) and metaverses and thing(s) are independent of each other. The DPM service calculates and processes the data in the metaverse, and the important node information of the processing process (such as processing time and content) will also be stored on the trustworthy storage.

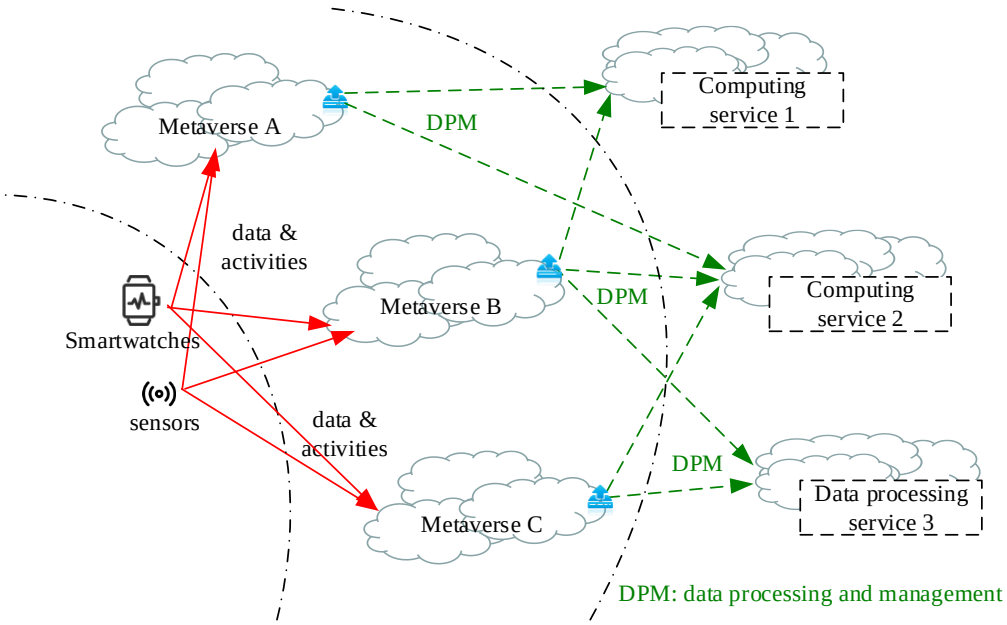

Figure I-1 – Smartwatch data security across metaverses in aspects of data processing and management

I.1.2. Assumptions

The assumptions related to this use case include the following:

– The smartwatch has multiple sensors to collect user action information.

– There are multiple metaverses working independently.

– There are multiple DPMS working independently.

– There is a blockchain or distributed ledger for storing data and processing information.

I.2. Games data security across metaverses

The metaverse is not a single virtual world, there are multiple independent metaverses. Taking the game industry as an example, the current development mode of metaverse games is that one metaverse game corresponds to an independent metaverse, and different games cannot interact with each other, which means that players cannot freely switch between different game worlds, and the items they obtain, such as equipment and skin, can only be used in a certain game. Players can't move assets across metaverses.

I.2.1. Description

In general, information about the user of the game, including data related to objects or sensors generated by AR/VR devices, will be mapped to a metaverse game. In the case of the across-metaverse game application scenario, the information in the real world will be mapped to multiple independent metaverses, and the target metaverses can manage and process the relevant IoT data by itself. As the number of users increases, external computing resources will be used to manage and process the relevant data. Across-metaverse games mean that data on different metaverse games can be managed and processed safely using common external resources. The external resources are not unique, but a group of infrastructures that collectively support different metaverses. Specifically, a certain player is connected to metaverse A with his or her environmental information (for example, body temperature, head movement and eye tracking information), which was sensed by IoT devices. When User's avatar moves to metaverse B, avatars may use external computing resources and services to manage and process relevant data.

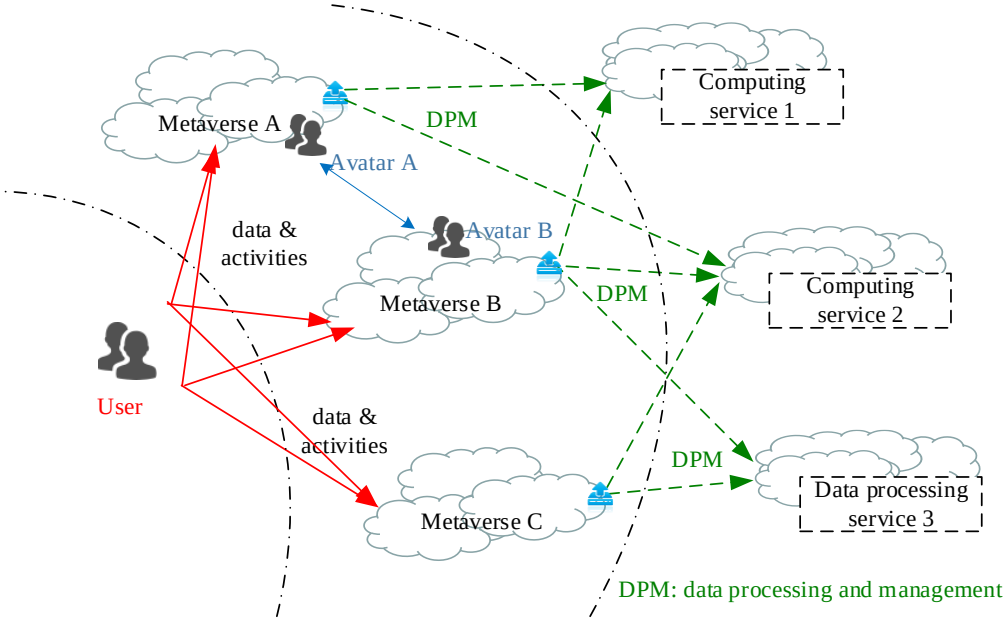

Figure I-2 – Game data security across metaverses in aspects of data processing and management

I.2.2. Assumptions

The assumptions related to this use case include the following;

– There are multiple game metaverses working independently.

– There are security mechanisms to ensure that the data is mapped across different metaverses.

– Trustworthy storage can be used for storing data and processing information.

Bibliography

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, Information technology – Security techniques – Privacy framework.

[b-ITU-Journal] ITU Journal 2023, Future and evolving technologies, *Special issue on Metaverse* https://www.itu.int/en/journal/j-fet/2023/002/Pages/default.aspx

[b-ITU-T X.800] Recommendation ITU-T ITU-T X.800(1991), Security architecture for Open Systems Interconnection for CCITT applications

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), Baseline identity management terms and definitions.

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology.*