SEOULTECH

A Survey on Metaverse: Fundamentals, Security and Privacy (Sections 3 – 6)

2022.09.12

Presented by: Mikail Mohammed Salim

Advanced Security in Emerging ICT

Professor: 박종혁

Contents

3. Threats and Countermeasures to Authentication & Access Control in Metaverse

A. **Threats to Authentication in Metaverse-** In metaverse, identity authentication and access control play a vital role for massive users/avatars in metaverse service offering.

1. **Identity theft**: If the identity of a user is stolen in the metaverse, his/her avatars, digital assets, social relationships, and even the digital life can be leaked and lost. In 2022, the accounts of 17 users in the Opensea NFT marketplace are hacked due to smart contract flaws and phishing attacks, causing a lost of $1.7 million.
2. **Impersonation Attack:** Hackers invade the Oculus helmet and exploit the stolen behavioral and biological data gathered by the in-built motion-tracking system to create digital replicas of the use.
3. **Avatar Authentication Issue**: Compared with real-world identity authentication, the authentication of avatars (e.g., the verification of their friends' avatars) for users in the metaverse can be more challenging through verifying facial features, voice, and video footage.
4. **Trusted and Interoperable Authentication**: In the metaverse, it is fundamental to ensure fast, efficient, and trusted cross-platform and cross-domain identity authentication.

3. Threats and Countermeasures to Authentication & Access Control in Metaverse

B. Threats to Access Control in Metaverse-

1. **Unauthorized Data Access**: Complex metaverse services will generate new types of personal profiling data (e.g., biometric information, daily routine, and user habits). Massive personal information is produced and transmitted in real time, it is complicated to decide exactly what personal information to be shared, with whom, under what condition, for what purpose, and when it is destroyed.
2. **Misuse of User/Avatar Data:** In the life-cycle of data services in the metaverse, user/avatar-related data can be disclosed intentionally by attackers or unintentionally by Virtual Service Providers to facilitate user profiling and targeted advertising activities. Besides, due to the potential non-interoperability of certain sub-metaverses, it is hard to trace the data misuse activities in the large-scale metaverse.

3. Threats and Countermeasures to Authentication & Access Control in Metaverse

C. **Security Countermeasures to Metaverse Authentication & Access Control**: For the metaverse, secure and efficient identity management is the basis for user/avatar interaction and service provisioning.

- Centralized Identity – digital identity authenticated and managed by a single institution, ex- Gmail
- Federated Identity - digital identity managed by multiple institutions or federations. Ex – Multiple metaverse providers sharing user identities.
- Self Sovereign Identity – digital identity which is fully controlled by individual users, i.e., shared with user consent

As shown in Fig. 1, in the metaverse, empowered by XR and Human Computer Interaction technologies, wearable devices such as Head Mounted Display and Brain Computing Interface enable user/avatar interactions and are expected as the major terminal to enter the metaverse.

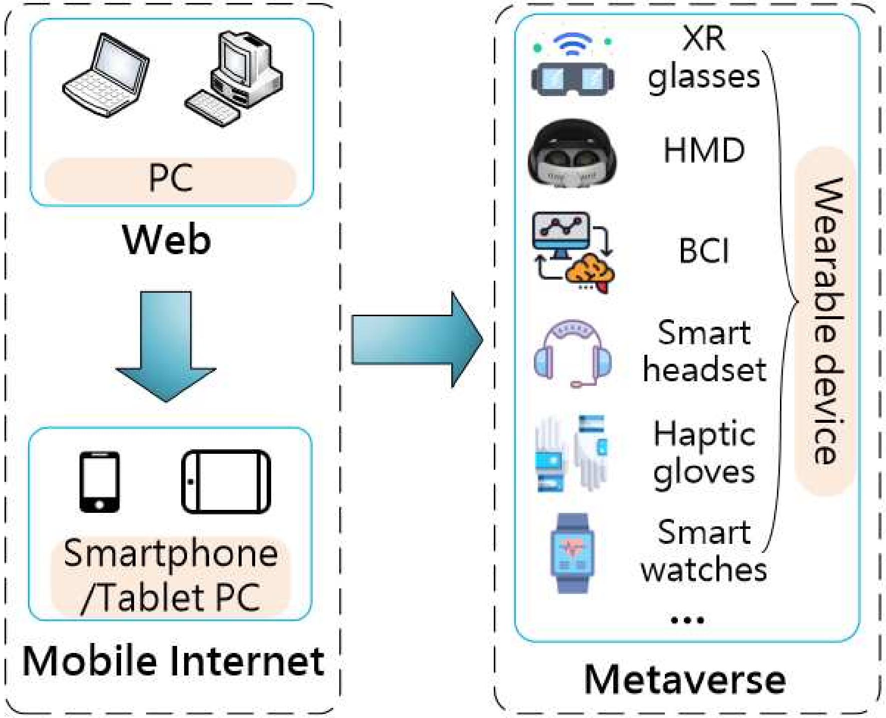


Fig. 1 Hardware terminals for entering the web, mobile Internet, and the metaverse

3. Threats and Countermeasures to Authentication & Access Control in Metaverse

C. **Security Countermeasures to Metaverse Authentication & Access Control**: We now review existing works on the metaverse in terms of key management and identity authentication for wearable devices.

1. **Key Management for wearable devices -**

- Wearable devices such as Oculus helmets and HoloLens headsets are anticipated to be the major terminal to enter the metaverse.
- Secure key management for authentication is essential for wearable devices to establish secure communication, deliver sensory data, receive immersive service.
- Existing Cryptographic based key management methods such as Diffie-Hellman cryptosystem and public key infrastructure have high device computational, bandwidth and memory resource requirements not suitable for battery operated wearable devices.

3. Threats and Countermeasures to Authentication & Access Control in Metaverse

1. **Key Management for wearable devices (contd.) -**
    - Zheng et al. [1] proposed an electrocardiogram (ECG) signal based key distribution mechanism for wearable and implantable medical devices (WIMDs). The study focuses on secure key sharing in the event of cyberattacks.
2. **Identity authentication for wearable devices -**
    - Identity authentication for wearable devices to guarantee device/user authenticity is an important research area in the metaverse.
    - As wearable devices have extremely low computing/storage capacity, Srinivas et al. [2] presented a cloud-based mutual authentication model with low system cost for wearable medical devices to prevent device impersonation in healthcare monitoring systems with password change and smart card revocation functions.
    - Zhao et al. [3] propose a novel continuous authentication model to support seamless device authentication at a low cost by extracting unique cardiac biometrics from wearable devices.

3. Threats and Countermeasures to Authentication & Access Control in Metaverse

2. **Identity authentication for wearable devices (contd.) -**
   - Jan et al. [4] design a privacy-aware mutual authentication mechanism for wearable devices, where a hidden Markov model (HMM) is devised to predict privacy risks of patient data leakage.
   - For short range communication using Bluetooth, Aksu et al. [5] focused on device authentication by implementing a smart wearable fingerprinting method tailored to Bluetooth using a series of AI algorithms.
   - Arias et al. [6] present a real attack using a hardware with attack vectors to bypass software authentications and compromise the two devices. The study states that it is necessary to secure all update channels and disable the microcontroller's external re-programmability and any debug interface for wearable devices.

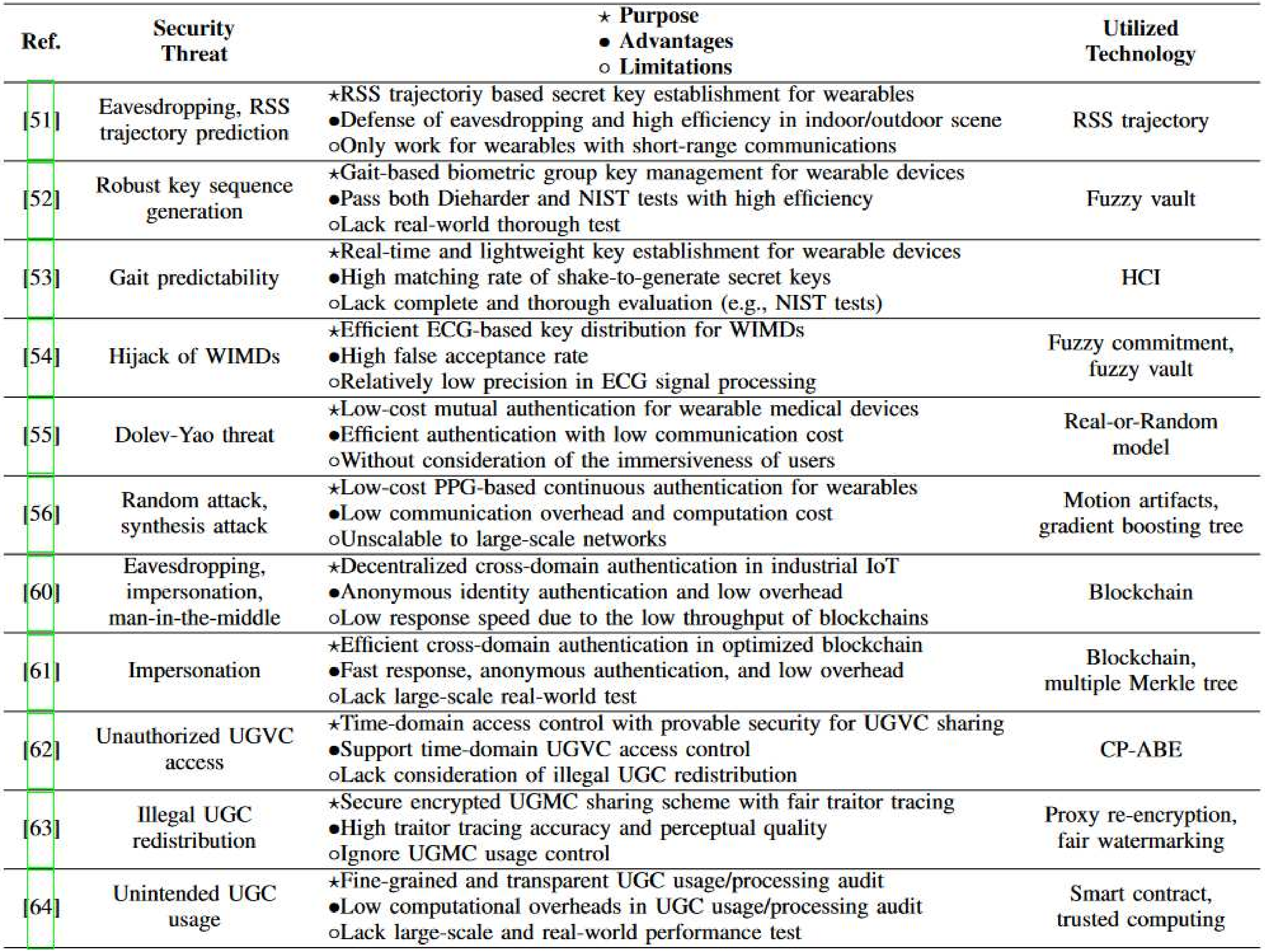
3. Threats and Countermeasures to Authentication & Access Control in Metaverse

3. **Cross-Domain Identity Authentication -**

- Identity authentication across different Metaverse virtual service providers is critical to deliver seamless metaverse services for users/avatar.
- Shen et al. [7] implemented consortium blockchain technology to design a decentralized and transparent cross-domain authentication scheme for industrial IoT devices in different domains. Device authentication is established using device identity-based encryption method. Domain specific data are transferred to respective side-chains to reduce stress on the Blockchain system.
- Chen et al. [8] proposed an Blockhain based efficient cross-domain authentication scheme named XAuth. An anonymous authentication protocol based on zero-knowledge proof is also devised to ensure privacy protection. The study uses Blockchain for privacy-preserving cross domain authentication among different Metaverse service providers.

3. Threats and Countermeasures to Authentication & Access Control in Metaverse

4. **Fine-grained Access Control and Usage Audit for Wearables and User Generated Content -**
   - The massive personally identifiable information handled by wearables can pose a huge risk of unauthorized exposure.
   - Yang et al. [9] propose a time-domain attribute-based access control mechanism with provable security for sharing user-generated video contents in the cloud. Time slots are stamped in both the cipher text and the keys shared by users ensuring only authorized users can access data based on their assigned time slot.
   - To prevent piracy of user generated data by authorized users, Zhang et al. [10] proposed a novel secure encrypted User Generated Media Content sharing scheme with traitor tracing in the cloud and watermarking mechanism.
   - We observe from the above studies that blockchain can be used to build trust-free digital identities for metaverse users. Identity authentication and access control in the metaverse can be managed by fusing wearable signals such as accelerometer data with key based encryption methods.



Ref.	Security Threat	⋆ Purpose • Advantages ◦ Limitations	Utilized Technology
[51]	Eavesdropping, RSS trajectory prediction	⋆RSS trajectoriy based secret key establishment for wearables •Defense of eavesdropping and high efficiency in indoor/outdoor scene ◦Only work for wearables with short-range communications	RSS trajectory
[52]	Robust key sequence generation	⋆Gait-based biometric group key management for wearable devices •Pass both Dieharder and NIST tests with high efficiency ◦Lack real-world thorough test	Fuzzy vault
[53]	Gait predictability	⋆Real-time and lightweight key establishment for wearable devices •High matching rate of shake-to-generate secret keys ◦Lack complete and thorough evaluation (e.g., NIST tests)	HCI
[54]	Hijack of WIMDs	⋆Efficient ECG-based key distribution for WIMDs •High false acceptance rate ◦Relatively low precision in ECG signal processing	Fuzzy commitment, fuzzy vault
[55]	Dolev-Yao threat	⋆Low-cost mutual authentication for wearable medical devices •Efficient authentication with low communication cost ◦Without consideration of the immersiveness of users	Real-or-Random model
[56]	Random attack, synthesis attack	⋆Low-cost PPG-based continuous authentication for wearables •Low communication overhead and computation cost ◦Unscalable to large-scale networks	Motion artifacts, gradient boosting tree
[60]	Eavesdropping, impersonation, man-in-the-middle	⋆Decentralized cross-domain authentication in industrial IoT •Anonymous identity authentication and low overhead ◦Low response speed due to the low throughput of blockchains	Blockchain
[61]	Impersonation	⋆Efficient cross-domain authentication in optimized blockchain •Fast response, anonymous authentication, and low overhead ◦Lack large-scale real-world test	Blockchain, multiple Merkle tree
[62]	Unauthorized UGVC access	⋆Time-domain access control with provable security for UGVC sharing •Support time-domain UGVC access control ◦Lack consideration of illegal UGC redistribution	CP-ABE
[63]	Illegal UGC redistribution	⋆Secure encrypted UGMC sharing scheme with fair traitor tracing •High traitor tracing accuracy and perceptual quality ◦Ignore UGMC usage control	Proxy re-encryption, fair watermarking
[64]	Unintended UGC usage	⋆Fine-grained and transparent UGC usage/processing audit •Low computational overheads in UGC usage/processing audit ◦Lack large-scale and real-world performance test	Smart contract, trusted computing

4. Threats and Countermeasures to Data Management in Metaverse

A. **Threats to Data Management in Metaverse-** The data collected or generated by wearable devices and users/avatars may suffer from threats in terms of data tampering and false data injection.

1. **Data Tampering attack:** Data integrity is at risk when shared between different virtual worlds. Attackers aim to modify or replace user credentials to hinder the normal day activities of users and reduce the quality of service of the Metaverse service provider.
2. **False Data injection Attack:** Attackers can inject falsified information such as false messages and wrong instructions to mislead metaverse systems. Ex- poisoning attacks in decentralized AI models. The returned wrong feedbacks or instructions may also threaten the safety of physical equipment and even personal safety.
3. **Issues in Managing New Types of Metaverse Data:** The metaverse requires new hardware and devices to gather various new types of data (e.g., eye movement, facial expression, and head movement). New challenges include in collecting, managing, and storing these enormous user-sensitive metaverse data, and the cyber/physical security of metaverse devices.

4. Threats and Countermeasures to Data Management in Metaverse

A. Threats to Data Management in Metaverse- (contd.)

4. **Threats to the data quality of User Generated Content and Physical Input:** Uncalibrated wearable sensors can generate inaccurate and even erroneous sensory data to mislead the creation of digital twins in the metaverse, causing poor user experience.
5. **Threats to User Generated Content Ownership and Provenance:** Due to the lack of authority, it is hard to trace the ownership and provenance of various UGCs produced by massive avatars under different virtual worlds in the metaverse.
6. **Threats to Intellectual Property Protection:** Severe challenges may arise in defining and protecting intellectual property (e.g., Avatars, User Generated Contents and AI Generated Content) in the new metaverse ecology, as the geographic boundaries of countries are broken down in the metaverse.

4. Threats and Countermeasures to Data Management in Metaverse

B. **Security Countermeasures to Metaverse Data Management -** Information security is an important prerequisite for the development and prosperity of the metaverse. In the following, we discuss the data security in metaverse in terms of data reliability, and quality.

1. **Data Reliability of AIGC, Digital Twin, and Physical Input:** Uncalibrated wearable sensors can generate inaccurate and even erroneous sensory data to mislead the creation of digital twins in the metaverse, causing poor user experience.
    - In the metaverse, AI can help generate high-quality dynamic game scenarios and context images, but also poses security threats such as adversarial and poisoned samples which is hard to detect for humans.
    - Data reliability of Digital Twins is essential and thus Gehrmann et al. [11] formally defined the synchronization consistency as a metric of the robustness of digital twin synchronization.
    - Liao et al. [12] leverage permissioned blockchain technology for trusted digital twin (DT) service transactions between VSPs and service requesters in intelligent transportation systems. To facilitate users, customized DT services, an on-demand DT-as-a-service (DTaaS) architecture is presented for fast response to meet diverse DT requirements in ITS.

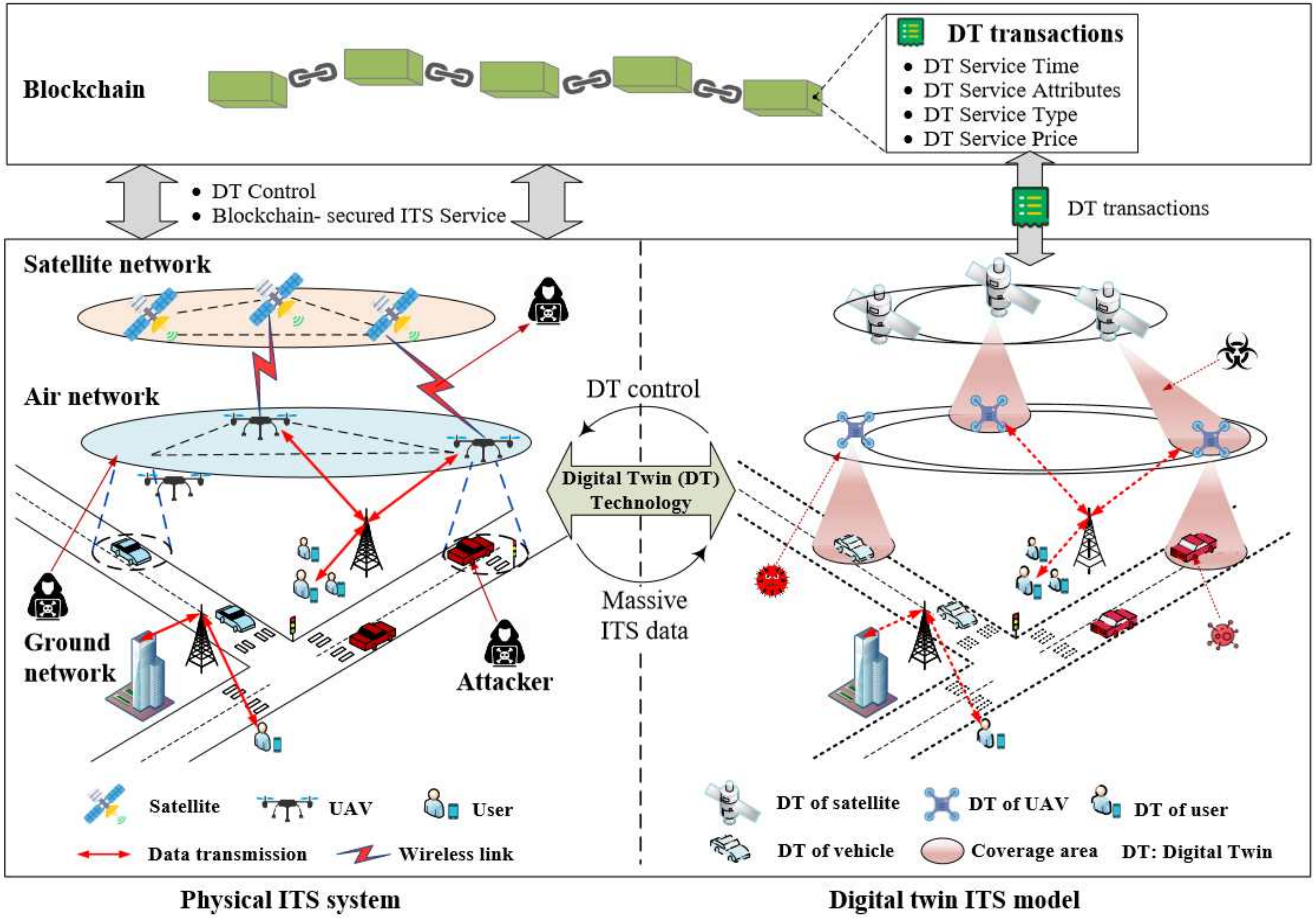


Fig. 2 Illustration of blockchain-enabled digital twin (DT)-as-a-service

4. Threats and Countermeasures to Data Management in Metaverse

1. **Data Reliability of AIGC, Digital Twin, and Physical Input: contd.**
    - Jot et al. [13] designed an interactive audio engine based on 6-degree-of-freedom (6DoF) object for parametric audio scene programming (i.e., controllable acoustic orientation, size, orientation, and other properties) in audiovisual metaverse experiences.

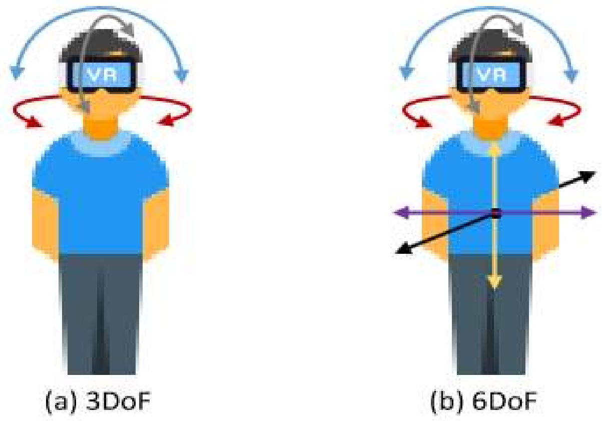


Fig. 3 Illustration of (a) 3DoF and (b) 6DoF. 3DoF means an object can rotationally move around the 3D space (i.e., x, y, and z axes), while 6DoF has additional translational movement along those axes (i.e., moving forward/backward, up/down, and left/right)

4. Threats and Countermeasures to Data Management in Metaverse

2. **Data Quality of UGC and Physical Input:** Low-quality data input from physical sensors and the UGCs produced by avatars can deteriorate the quality-of-service (QoS) of metaverse services and the QoE of users.
   - Dickinson et al. [14] give a user study on 68 participants in a VR environment and show that user perception of character believability is influenced positively by behavioral features while negatively by visual elements.
   - Su et al. [15] proposed a deep RL (DRL)-based incentive mechanism to encourage users high-quality model contribution in distributed AI paradigms with consideration of both non-IID effects and collaboration between edge/cloud servers.
   - Du et al. [16] propose an optimal targeted advertising strategy for the Virtual Service Providers to maximize its payoff in offering high-quality access services for end-users while attaining close-to-one detection error for attackers.

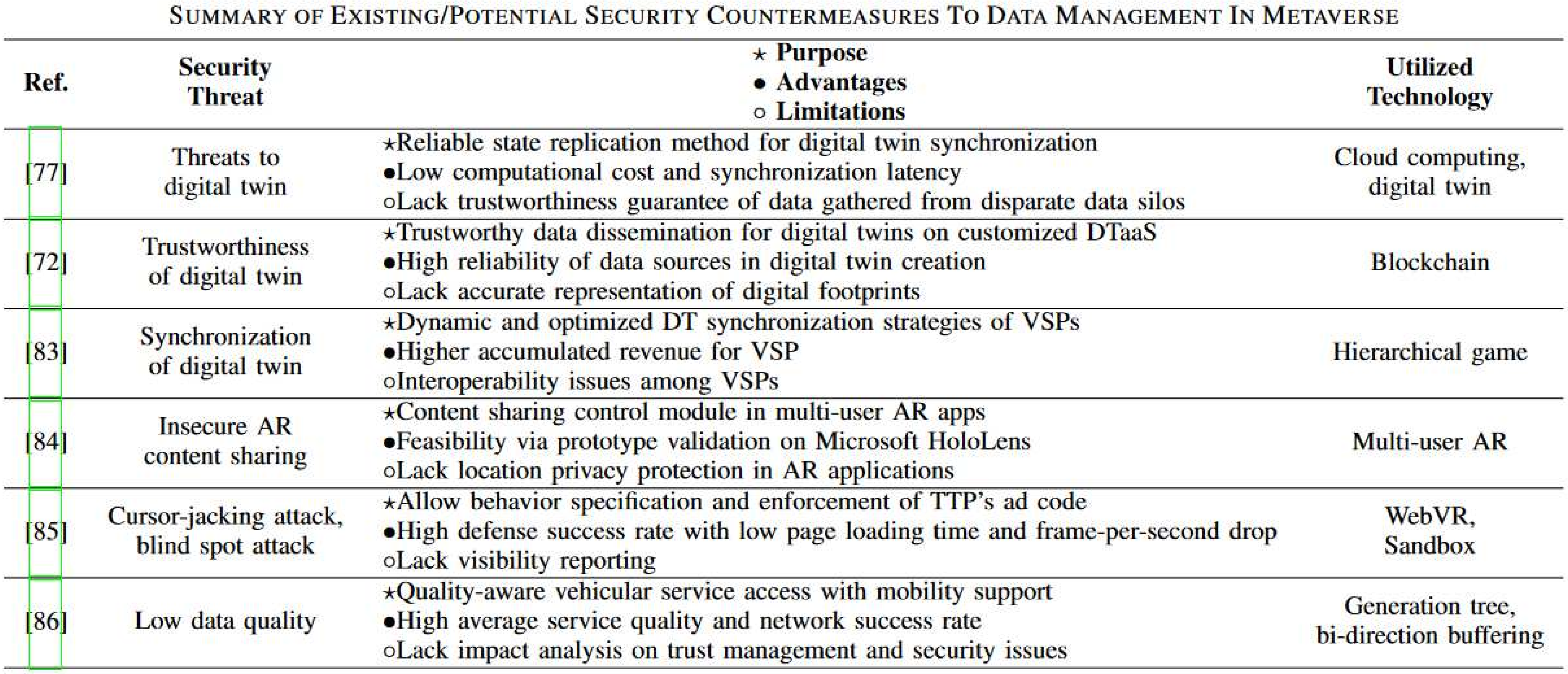
4. Threats and Countermeasures to Data Management in Metaverse

3. **Data Quality of UGC and Physical Input:** Metaverse applications are usually multi-user such as multi-player gaming and remote collaboration.
   - Aimed for secure content sharing under multi-user AR applications, Ruth et al. [17] study an AR content sharing control mechanism and implement a prototype on HoloLens to allow AR content sharing among remote or co-located users with inbound and outbound control.
   - Lee et al. [18] identify three new ad fraud threats (i.e., blind spot tracking, gaze and controller cursor-jacking, and abuse of an auxiliary display) in content sharing. A defense mechanism named AdCube is presented via visual confinement of 3D ad entities and sandboxing technique.

4. Threats and Countermeasures to Data Management in Metaverse

4. **Provenance of UGC:** Data provenance can realize the traceability of historical archives of a piece of UGC, which is essential to evaluate data quality, trace data source, reproduce data generation process, and conduct audit trail to quickly identify data responsible subjects.
   - Satchidanandan et al. [19] design a dynamic watermarking technique which exploits indelible patterns imprinted in the medium to detect misbehaviors (e.g., signal tampering) of malicious sensors or actuators.
   - Liang et al. [20] present a blockchain-based cloud file provenance architecture named ProvChain with three stages, i.e., collection, storage, and verification of provenance information. ProvChain ensures source tamper resistance, user privacy, and reliability of cloud storage.
   - For multi-hop IoT, Mohsin et al. [21] design a lightweight protocol to enable data provenance in wireless communications, where the RSS indicator of the communicating IoT node is exploited to produce the unique link fingerprint.

4. Threats and Countermeasures to Data Management in Metaverse



Summary of Existing/Potential Security Countermeasures To Data Management In Metaverse

Ref.	Security Threat	⋆ Purpose • Advantages ◦ Limitations	Utilized Technology
[77]	Threats to digital twin	⋆Reliable state replication method for digital twin synchronization •Low computational cost and synchronization latency ◦Lack trustworthiness guarantee of data gathered from disparate data silos	Cloud computing, digital twin
[72]	Trustworthiness of digital twin	⋆Trustworthy data dissemination for digital twins on customized DTaaS •High reliability of data sources in digital twin creation ◦Lack accurate representation of digital footprints	Blockchain
[83]	Synchronization of digital twin	⋆Dynamic and optimized DT synchronization strategies of VSPs •Higher accumulated revenue for VSP ◦Interoperability issues among VSPs	Hierarchical game
[84]	Insecure AR content sharing	⋆Content sharing control module in multi-user AR apps •Feasibility via prototype validation on Microsoft HoloLens ◦Lack location privacy protection in AR applications	Multi-user AR
[85]	Cursor-jacking attack, blind spot attack	⋆Allow behavior specification and enforcement of TTP's ad code •High defense success rate with low page loading time and frame-per-second drop ◦Lack visibility reporting	WebVR, Sandbox
[86]	Low data quality	⋆Quality-aware vehicular service access with mobility support •High average service quality and network success rate ◦Lack impact analysis on trust management and security issues	Generation tree, bi-direction buffering

5. Privacy Threats and Countermeasures in Metaverse

A. **Pervasive Data Collection -** When enjoying digital lives in the metaverse, user privacy including location privacy, habit, living styles, and so on may be offended during the life-cycle of data services including data perception, transmission, processing, governance, and storage.

1. **Privacy in Metaverse Games:** To immersively interact with an avatar, it requires pervasive user profiling activities at an unreasonably granular level including facial expressions, eye/hand movements, speech and biometric features, and even brain wave patterns.
2. **Privacy Leakage in Data Transmission:** In metaverse systems, abundant personally identifiable information collected from wearables (e.g., Head Mounted Displays) are transferred via wired and wireless communications, the confidentiality of which should be prohibited from unauthorized individuals/service.
3. **Privacy Leakage in Data Processing:** In metaverse services, the aggregation and processing of massive data collected from human bodies and their surrounding environments are essential for the creation and rendering of avatars and virtual environments, in which users' sensitive information may be leaked.

5. Privacy Threats and Countermeasures in Metaverse

A. Pervasive Data Collection – contd.

4. **Privacy Leakage in Cloud/Edge Storage:** In 2006, a customer database of the Second Life (a metaverse game) was hacked, and the user data was breached including unencrypted usernames and addresses, as well as encrypted payment details and passwords.
5. **Rogue or Compromised End Devices:** The use of rogue or compromised wearable end devices (e.g., VR glasses) in the metaverse is becoming an entryway for data breaches and malware invasions, and the problem may be more severe with the popularity of wearable devices for entering the metaverse.
6. **Threats to Digital Footprints:** s the behavior pattern, preferences, habits, and activities of avatars in the metaverse can reflect the real statuses of its physical counterpart, attackers can collect the digital footprints of avatars and exploit the similarity linked to real users to facilitate accurate user profiling and even illegal activities.
7. **Identity Linkability in Ternary Worlds:** As the metaverse assimilates the reality into itself, the human, physical, and virtual worlds are seamlessly integrated into the metaverse, causing identity linkability concerns across the ternary worlds.

5. Privacy Threats and Countermeasures in Metaverse

A. **Pervasive Data Collection – contd.**

8. **Threats to Accountability:** Wearable devices intrinsically gather more sensitive data such as locations, behavior patterns, and surroundings of users than traditional smart devices. The accountability in the metaverse is important to ensure users' sensitive data are handled with privacy compliance.
9. **Threats to Customized Privacy:** Similar to existing Internet service platforms, distinct users generally exhibit customized privacy preferences for different services or interaction objects. Example- a user in Roblox may be more sensitive to monetary trading activities than social activities.

5. Privacy Threats and Countermeasures in Metaverse

B. Privacy countermeasures in Metaverse–

1. **Privacy in Metaverse Games:** AR/VR games are the current most popular metaverse application for users. AR/VR games usually contain three steps: the game platform (i) collects sensory data from users and their surroundings, (ii) identifies objects according to these contexts, and lastly (iii) performs rendering on game senses for immersiveness.
   - Laakkonen et al. [22] introduced privacy-by-design principles in digital games from both qualitative and quantitative perspectives, where nineteen privacy attributes divided into three levels are accounted for privacy evaluation.

2. **Privacy-Preserving User Generated Content Sharing and Processing:**
   - Zhang et al. [23] present a FL-based secure data collaboration framework where wearable sensors periodically send local model updates trained on their private sensory data to the server which synthesizes a global abnormal health detection mode.
   - Guan et al. [24] utilize Zero Knowledge Proof to empower current account-model blockchains (e.g., Ethereum) with privacy preservation functions in terms of hiding sender-recipient linkage, account balances, and transaction amounts.

5. Privacy Threats and Countermeasures in Metaverse

B. Privacy countermeasures in Metaverse– contd.

2. Privacy in Metaverse Games: contd.

- Wang et al. [25] leveraged the trusted computing technique to design a privacy- preserving off-chain data processing mechanism, where private User Generated Content datasets are processed in an off-chain trusted enclave and the exchange of processed results and payment are securely executed via the designed fair exchange smart contract.

3. Confidentiality Protection of User Generated Content and Physical Input:

- The confidentiality of UGCs (inside the metaverse) along with physical inputs (to the metaverse) should be ensured to prevent private data leakage and sensitive data exposure.
- For confidentiality of physical inputs, Raguram et al. [26] propose a novel threat named compromising reflections, which can automatically reconstruct user typing on virtual keyboards, thereby compromising data confidentiality and user privacy.

5. Privacy Threats and Countermeasures in Metaverse

B. Privacy countermeasures in Metaverse– contd.

4. Digital Footprints Protection:

- In the metaverse, privacy inside avatars' digital footprints can be classified into three types: (i) personal information (e.g., avatar profiling), (ii) virtual behaviors, and (iii) interactions or communications between avatars or between avatar and NPC.
- A potential solution is disguise by periodically changing avatar's appearance to confuse attackers, or mannequin by replacing the avatar with a single clone (e.g., bot) which imitates user's behavior and teleport user's true avatar to another location when being tracked.

5. Personalized Privacy-Preserving Metaverse:

- Existing works on personalized privacy computing mainly based on similarity, randomized response [27], and personalized Federated Learning. With the growth of metaverse, more research on new personalized privacy preservation methods is required to serve new applications and the new ecology in the metaverse.

5. Privacy Threats and Countermeasures in Metaverse

B. Privacy countermeasures in Metaverse– contd.

6. Privacy-Enhancing Advances in Industry:

- In the metaverse, there have been incidents such as VR groping and VR sexual harassments in Horizon World. In the real world, people potentially keep an appropriate distance from others to maintain personal spaces when socializing.
- Psychologist Stanley Hall quantified and divided four types of personal spaces: public area (350-750 cm), social area (125-350 cm), personal area (50-125 cm), and intimate area (within 50 cm)

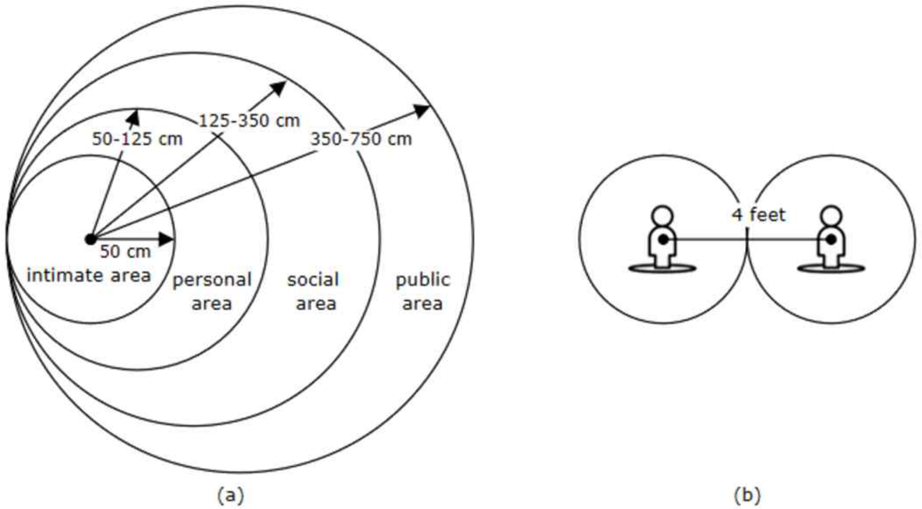
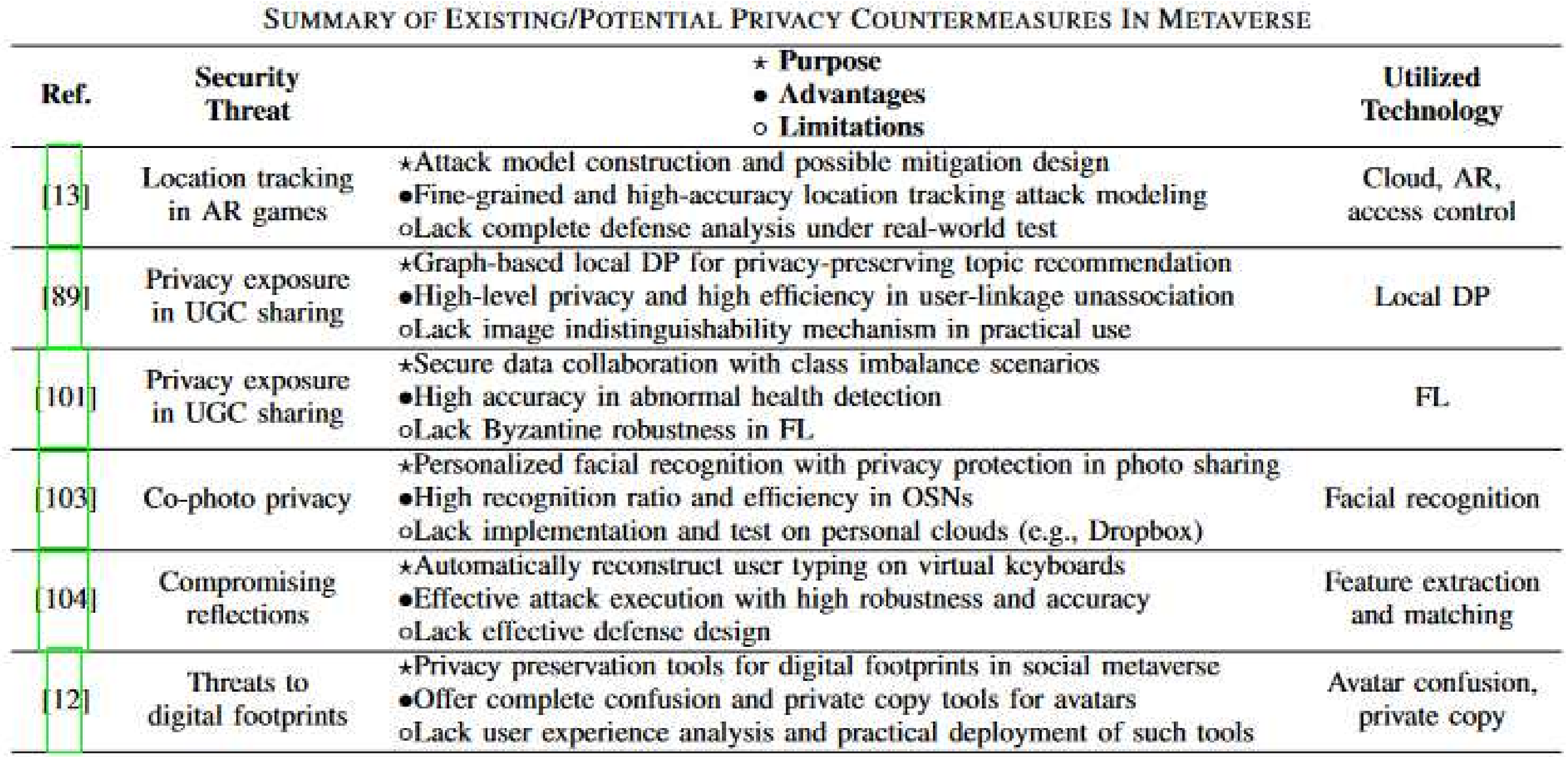


Fig. 4 (a) Illustration of personal space in real and virtual worlds. (b) Meta’s personal boundary function for avatars with default private border of 2-foot.

5. Privacy Threats and Countermeasures in Metaverse



SUMMARY OF EXISTING/POTENTIAL PRIVACY COUNTERMEASURES IN METAVERSE

Ref.	Security Threat	⋆ Purpose ● Advantages ○ Limitations	Utilized Technology
[13]	Location tracking in AR games	⋆Attack model construction and possible mitigation design ●Fine-grained and high-accuracy location tracking attack modeling ○Lack complete defense analysis under real-world test	Cloud, AR, access control
[89]	Privacy exposure in UGC sharing	⋆Graph-based local DP for privacy-preserving topic recommendation ●High-level privacy and high efficiency in user-linkage unassociation ○Lack image indistinguishability mechanism in practical use	Local DP
[101]	Privacy exposure in UGC sharing	⋆Secure data collaboration with class imbalance scenarios ●High accuracy in abnormal health detection ○Lack Byzantine robustness in FL	FL
[103]	Co-photo privacy	⋆Personalized facial recognition with privacy protection in photo sharing ●High recognition ratio and efficiency in OSNs ○Lack implementation and test on personal clouds (e.g., Dropbox)	Facial recognition
[104]	Compromising reflections	⋆Automatically reconstruct user typing on virtual keyboards ●Effective attack execution with high robustness and accuracy ○Lack effective defense design	Feature extraction and matching
[12]	Threats to digital footprints	⋆Privacy preservation tools for digital footprints in social metaverse ●Offer complete confusion and private copy tools for avatars ○Lack user experience analysis and practical deployment of such tools	Avatar confusion, private copy

6. Network related Threats and Countermeasures in Metaverse

A. **Threats to Metaverse network-** In the metaverse, traditional threats to the communication networks can also be effective, as the metaverse evolves from the current Internet and incorporates existing wireless communication technologies.

1. **Single Point of Failure:** The Metaverse implements cloud-based system for user/avatar management. DDoS attacks on centralized servers result in damage to physical root servers, and raise data trust and transparency challenges
2. **DDoS:** As the metaverse includes massive tiny wearable devices, adversaries may compromise these metaverse end-devices and make them part of a botnet (e.g., Mirai) to conduct DDoS attacks to make network outage and service unavailability.
3. **Sybil attacks:** Sybil adversaries may manipulate multiple faked/stolen identities to gain disproportionately large influence on metaverse services.

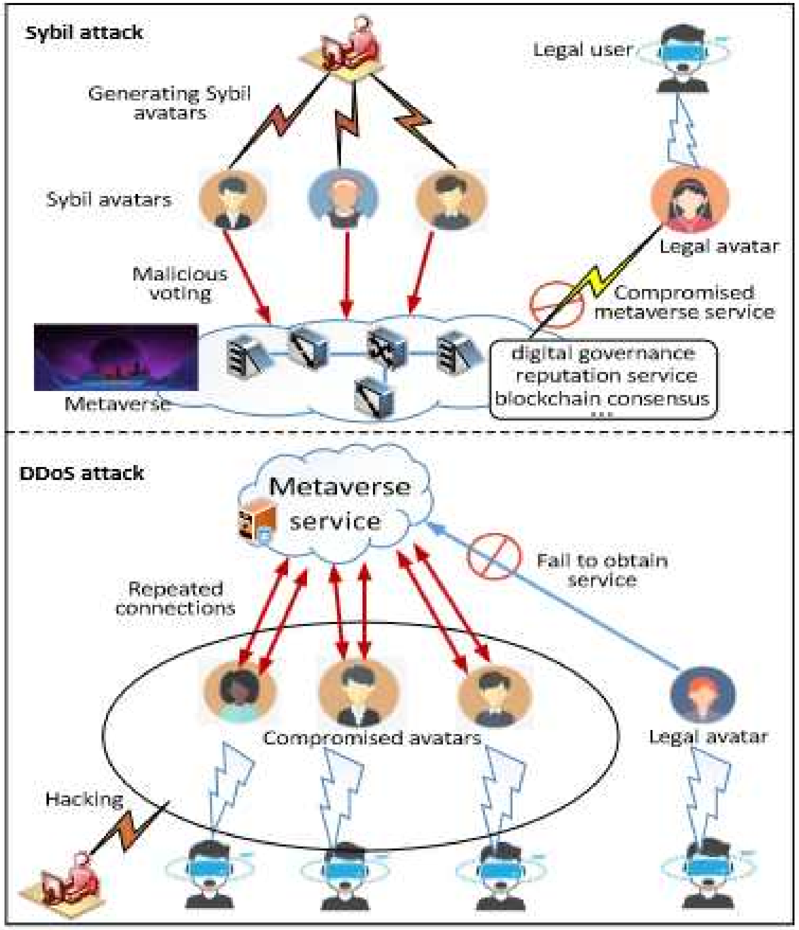


Fig. 5 Illustration of Sybil and DDoS attacks on the Metaverse

6. Network related Threats and Countermeasures in Metaverse

B. **Situational Awareness in Metaverse-** Situational awareness is an effective tool for security monitoring and threat early-warning in large-scale complex systems such as the metaverse. In the metaverse, local situational awareness is essential for monitoring a single security domain and global situational awareness can assist early-warning of large-scale distributed threats targeted at multiple sub-metaverses.

1. **Local Situational Awareness:**
   - Lv et al. [28] present a smart intrusion detection model to detect attack behaviors on 3D VR-based industrial control systems based on support vector machine (SVM).
   - Heartfield et al. [29] propose a multi-layered lightweight anomaly detection method by exploiting radio-frequency wireless communications to/from them to identify potentially malicious transactions.
   - Reinforcement Learning methods are employed for intrusion detection in small-scale applications such as smart homes.
2. **Global Situational Awareness:** Global situational awareness can facilitate understanding global security statuses in defending large-scale attacks in the metaverse.

6. Network related Threats and Countermeasures in Metaverse

B. Situational Awareness in Metaverse- contd.

2. Global Situational Awareness: contd.

- Krishnan et al. [30] combine digital twin and SDN to build a behavioral monitoring and profiling system where security strategies are evaluated on digital twins before being deployed in the real network.
- Zarca et al. [31] further propose SDN-enabled virtual honeynet services with higher degree of scalability and flexibility.
- As shown in Fig. 6, based on specific security policies, security virtual network functions (VNFs) (e.g., virtual honeynet, IDS, IPS, and firewall) can be configured and instanced on demand reactively or proactively, coordinated by the SDN controller.

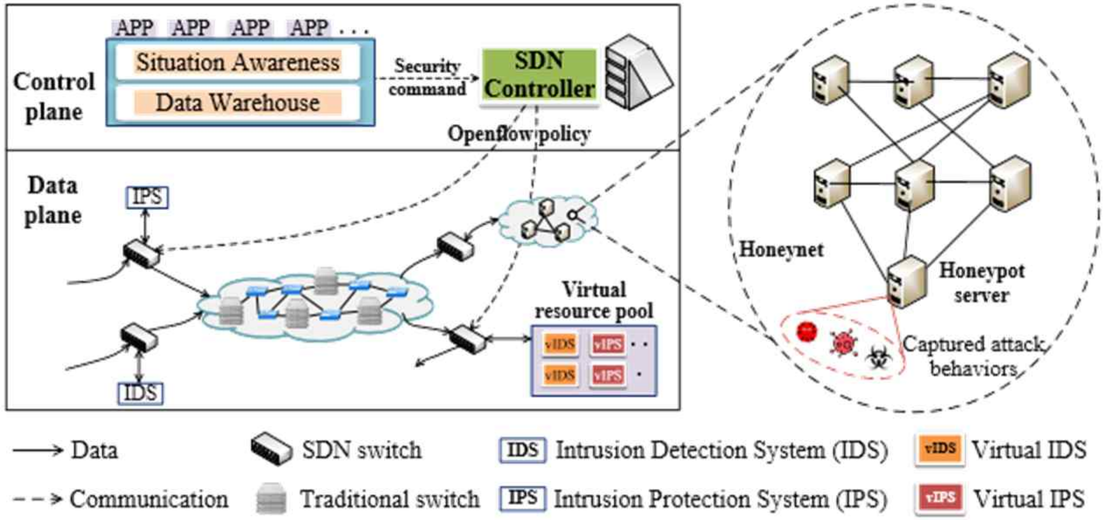


Fig. 6 Illustration of SDN-enabled virtual honeynet services for collaborative situational awareness

6. Network related Threats and Countermeasures in Metaverse

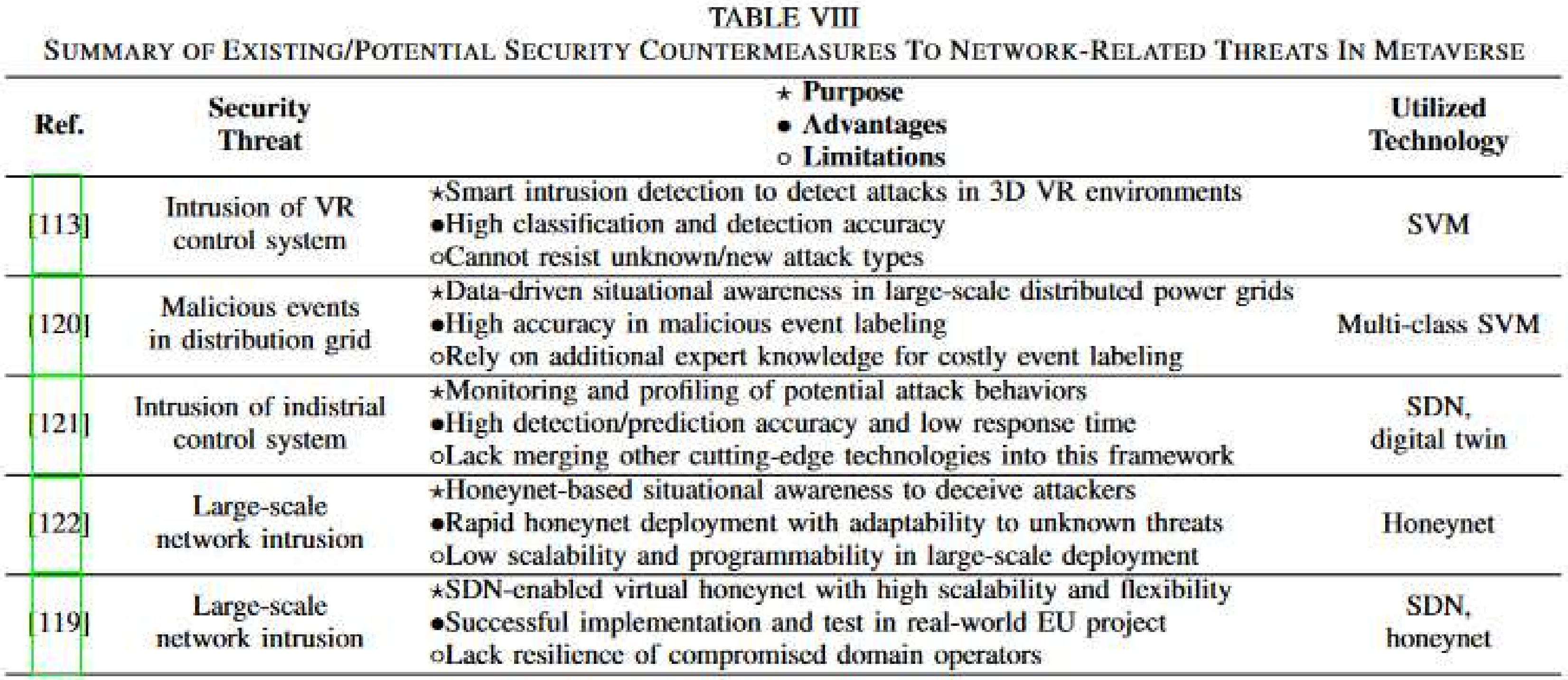


TABLE VIII
SUMMARY OF EXISTING/POTENTIAL SECURITY COUNTERMEASURES TO NETWORK-RELATED THREATS IN METAVERSE

Ref.	Security Threat	⋆ Purpose • Advantages ◦ Limitations	Utilized Technology
[113]	Intrusion of VR control system	⋆Smart intrusion detection to detect attacks in 3D VR environments •High classification and detection accuracy ◦Cannot resist unknown/new attack types	SVM
[120]	Malicious events in distribution grid	⋆Data-driven situational awareness in large-scale distributed power grids •High accuracy in malicious event labeling ◦Rely on additional expert knowledge for costly event labeling	Multi-class SVM
[121]	Intrusion of indistrial control system	⋆Monitoring and profiling of potential attack behaviors •High detection/prediction accuracy and low response time ◦Lack merging other cutting-edge technologies into this framework	SDN, digital twin
[122]	Large-scale network intrusion	⋆Honeynet-based situational awareness to deceive attackers •Rapid honeynet deployment with adaptability to unknown threats ◦Low scalability and programmability in large-scale deployment	Honeynet
[119]	Large-scale network intrusion	⋆SDN-enabled virtual honeynet with high scalability and flexibility •Successful implementation and test in real-world EU project ◦Lack resilience of compromised domain operators	SDN, honeynet

References

1. G. Zheng, R. Shankaran, W. Yang, C. Valli, L. Qiao, M. A. Orgun, and S. C. Mukhopadhyay, “A critical analysis of ECG-based key distribution for securing wearable and implantable medical devices,” IEEE Sensors Journal, vol. 19, no. 3, pp. 1186–1198, Feb. 2018.
2. J. Srinivas, A. K. Das, N. Kumar, and J. J. Rodrigues, “Cloud centric authentication for wearable healthcare monitoring system,” IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 5, pp. 942–956, Sept.-Oct. 2018.
3. Zhao, Y. Wang, J. Liu, Y. Chen, J. Cheng, and J. Yu, “Trueheart: Continuous authentication on wrist-worn wearables using PPG-based bio-metrics,” in IEEE Conference on Computer Communications (INFOCOM), Jul. 2020, pp. 30–39.
4. M. A. Jan, F. Khan, R. Khan, S. Mastorakis, V. G. Menon, M. Alazab, and P. Watters, “Lightweight mutual authentication and privacy-preservation scheme for intelligent wearable devices in industrial-CPS,” IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5829–5839, Aug. 2021.
5. H. Aksu, A. S. Uluagac, and E. S. Bentley, “Identification of wearable devices with Bluetooth,” IEEE Transactions on Sustainable Computing, vol. 6, no. 2, pp. 221–230, Apr.-Jun. 2021.
6. O. Arias, J. Wurm, K. Hoang, and Y. Jin, “Privacy and security in internet of things and wearable devices,” IEEE Transactions on Multi-Scale Computing Systems, vol. 1, no. 2, pp. 99–109, Apr.-Jun. 2015.
7. M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, “Blockchain-assisted secure device authentication for cross-domain indus- trial IoT,” IEEE Journal on Selected Areas in Communications, vol. 38, no. 5, pp. 942–954, May 2020.
8. J. Chen, Z. Zhan, K. He, R. Du, D. Wang, and F. Liu, “XAuth: Efficient privacy-preserving cross-domain authentication,” IEEE Transactions on Dependable and Secure Computing, 2021, doi: 10.1109/TDSC.2021.3092375.
9. K. Yang, Z. Liu, X. Jia, and X. Shen, “Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach,” IEEE Transactions on Multimedia, vol. 18, no. 5, pp. 940–950, May 2016.
10. L. Y. Zhang, Y. Zheng, J. Weng, C. Wang, Z. Shan, and K. Ren, “You can access but you cannot leak: Defending against illegal content redistribution in encrypted cloud media center,” IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 6, pp. 1218–1231, Nov.-Dec. 2020.

References

11. C. Gehrmann and M. Gunnarsson, “A digital twin based industrial automation and control system security architecture,” IEEE Transactions on Industrial Informatics, vol. 16, no. 1, pp. 669–680, Jan. 2020.
12. S. Liao, J. Wu, A. K. Bashir, W. Yang, J. Li, and U. Tariq, “Digital twin consensus for blockchain-enabled intelligent transportation systems in smart cities,” IEEE Transactions on Intelligent Transportation Systems, 2021, doi: 10.1109/TITS.2021.3134002.
13. J.-M. Jot, R. Audfray, M. Hertensteiner, and B. Schmidt, “Rendering spatial sound for interoperable experiences in the audio metaverse,” in International Conference on Immersive and 3D Audio (i3DA), Sep. 2021, pp. 1–15.
14. P. Dickinson, A. Jones, W. Christian, A. Westerside, and A. Parke, “Experiencing simulated confrontations in virtual reality,” in ACM CHI Conference on Human Factors in Computing Systems (CHI), May 2021, pp. 1–10.
15. Z. Su, Y. Wang, T. H. Luan, N. Zhang, F. Li, T. Chen, and H. Cao, “Secure and efficient federated learning for smart grid with edge-cloud collaboration,” IEEE Transactions on Industrial Informatics, vol. 18, no. 2, pp. 1333–1344, Feb. 2022.
16. H. Du, D. Niyato, J. Kang, D. I. Kim, and C. Miao, “Optimal targeted advertising strategy for secure wireless edge metaverse,” arXiv preprint arXiv:2111.00511, 2021.
17. K. Ruth, T. Kohno, and F. Roesner, “Secure multi-user content sharing for augmented reality applications,” in 28th USENIX Security Symposium (USENIX Security 19), Aug. 2019, pp. 141–158.
18. H. Lee, J. Lee, D. Kim, S. Jana, I. Shin, and S. Son, “AdCube: WebVR ad fraud and practical confinement of Third-Party ads,” in 30th USENIX Security Symposium (USENIX Security 21), Aug. 2021, pp. 2543–2560.
19. B. Satchidanandan and P. R. Kumar, “Dynamic watermarking: Active defense of networked cyber–physical systems,” Proceedings of the IEEE, vol. 105, no. 2, pp. 219–240, Feb. 2017.
20. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, “Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability,” in IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), May 2017, pp. 468–477.

References

21. M. Kamal and s. Tariq, “Light-weight security and data provenance for multi-hop internet of things,” IEEE Access, vol. 6, pp. 34 439–34 448, 2018.
22. J. Laakkonen, J. Parkkila, P. J ̈appinen, J. Ikonen, and A. Seffah, “Incorpo- rating privacy into digital game platform design: The what, why, and how,” IEEE Security & Privacy, vol. 14, no. 4, pp. 22–32, July-Aug. 2016.
23. D. Y. Zhang, Z. Kou, and D. Wang, “FedSens: A federated learning approach for smart health sensing with class imbalance in resource constrained edge computing,” in IEEE Conference on Computer Commu- nications (INFOCOM), May 2021, pp. 1–10.
24. Z. Guan, Z. Wan, Y. Yang, Y. Zhou, and B. Huang, “BlockMaze: An effi- cient privacy-preserving account-model blockchain based on zk-SNARKs,” IEEE Transactions on Dependable and Secure Computing, May-Jun. 2020, doi: 10.1109/TDSC.2020.3025129.
25. Y. Wang, Z. Su, N. Zhang, J. Chen, X. Sun, Z. Ye, and Z. Zhou, “SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain,” IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7688–7699, Nov. 2021.
26. R. Raguram, A. M. White, Y. Xu, J.-M. Frahm, P. Georgel, and F. Monrose, “On the privacy risks of virtual keyboards: Automatic reconstruction of typed input from compromising reflections,” IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 3, pp. 154–167, May- Jun. 2013.
27. H. Song, T. Luo, X. Wang, and J. Li, “Multiple sensitive values-oriented personalized privacy preservation based on randomized response,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2209– 2224, Dec. 2020.
28. Z. Lv, D. Chen, R. Lou, and H. Song, “Industrial security solution for virtual reality,” IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6273– 6281, Apr. 2021.
29. M. Zhang, A. Raghunathan, and N. K. Jha, “MedMon: Securing medical devices through wireless monitoring and anomaly detection,” IEEE Trans- actions on Biomedical Circuits and Systems, vol. 7, no. 6, pp. 871–881, Dec. 2013.
30. P. Krishnan, K. Jain, R. Buyya, P. Vijayakumar, A. Nayyar, M. Bilal, and H. Song, “MUD-based behavioral profiling security framework for software-defined IoT networks,” IEEE Internet of Things Journal, May 2021, doi: 10.1109/JIOT.2021.3113577.
31. A. M. Zarca, J. B. Bernabe, A. Skarmeta, and J. M. Alcaraz Calero, “Virtual IoT honeynets to mitigate cyberattacks in SDN/NFV-enabled IoT networks,” IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1262–1277, Jun. 2020.

Thank you

Presented by: Mikail Mohammed Salim