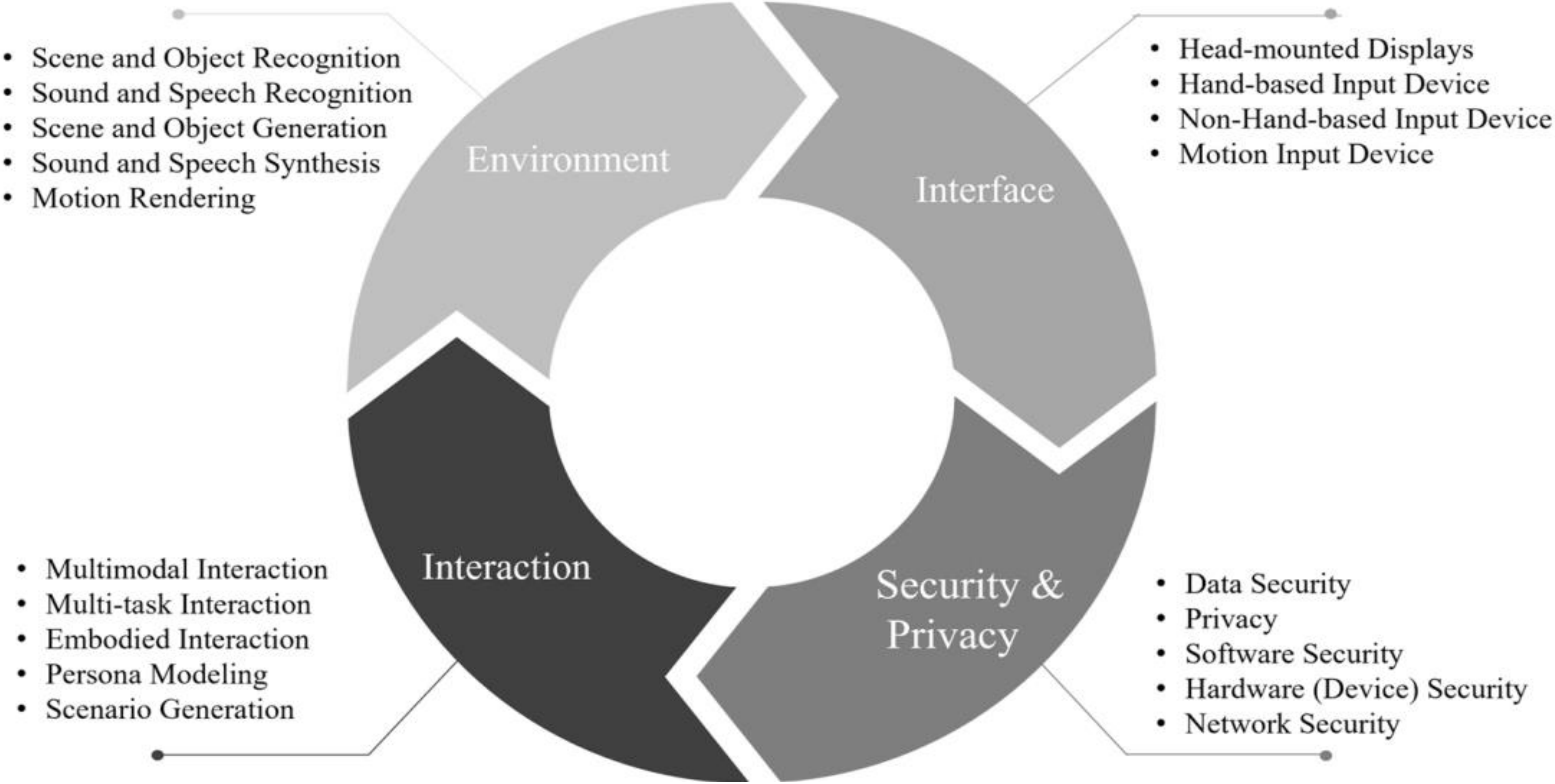
Security in the Metaverse: An Analysis of Threats and Countermeasures

Maedeh Mosharraf

Faculty of computer science and engineering, Shahid Beheshti University

Email: m_mosharraf@sbu.ac.ir



Environment

- Scene and Object Recognition
- Sound and Speech Recognition
- Scene and Object Generation
- Sound and Speech Synthesis
- Motion Rendering

Interface

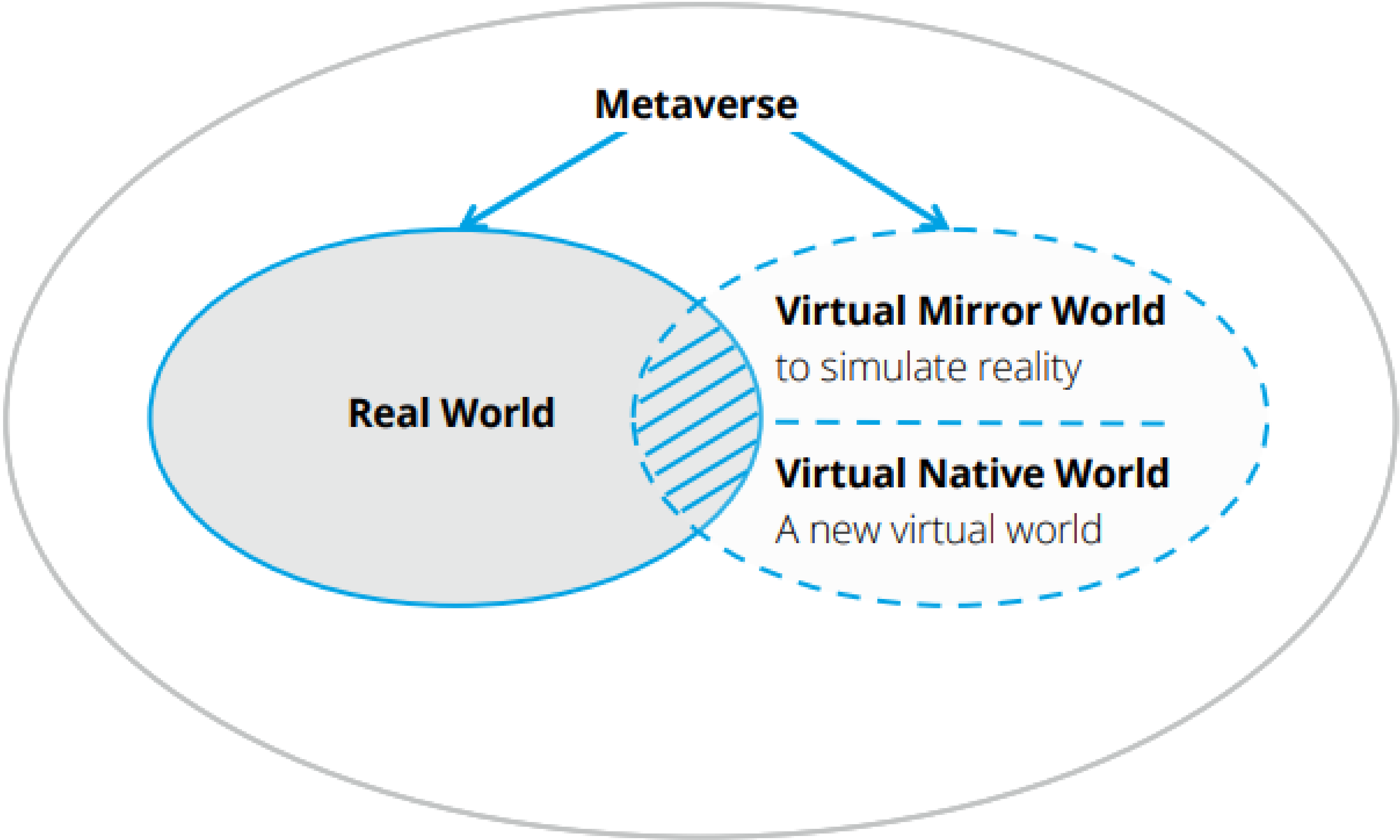
- Head-mounted Displays
- Hand-based Input Device
- Non-Hand-based Input Device
- Motion Input Device

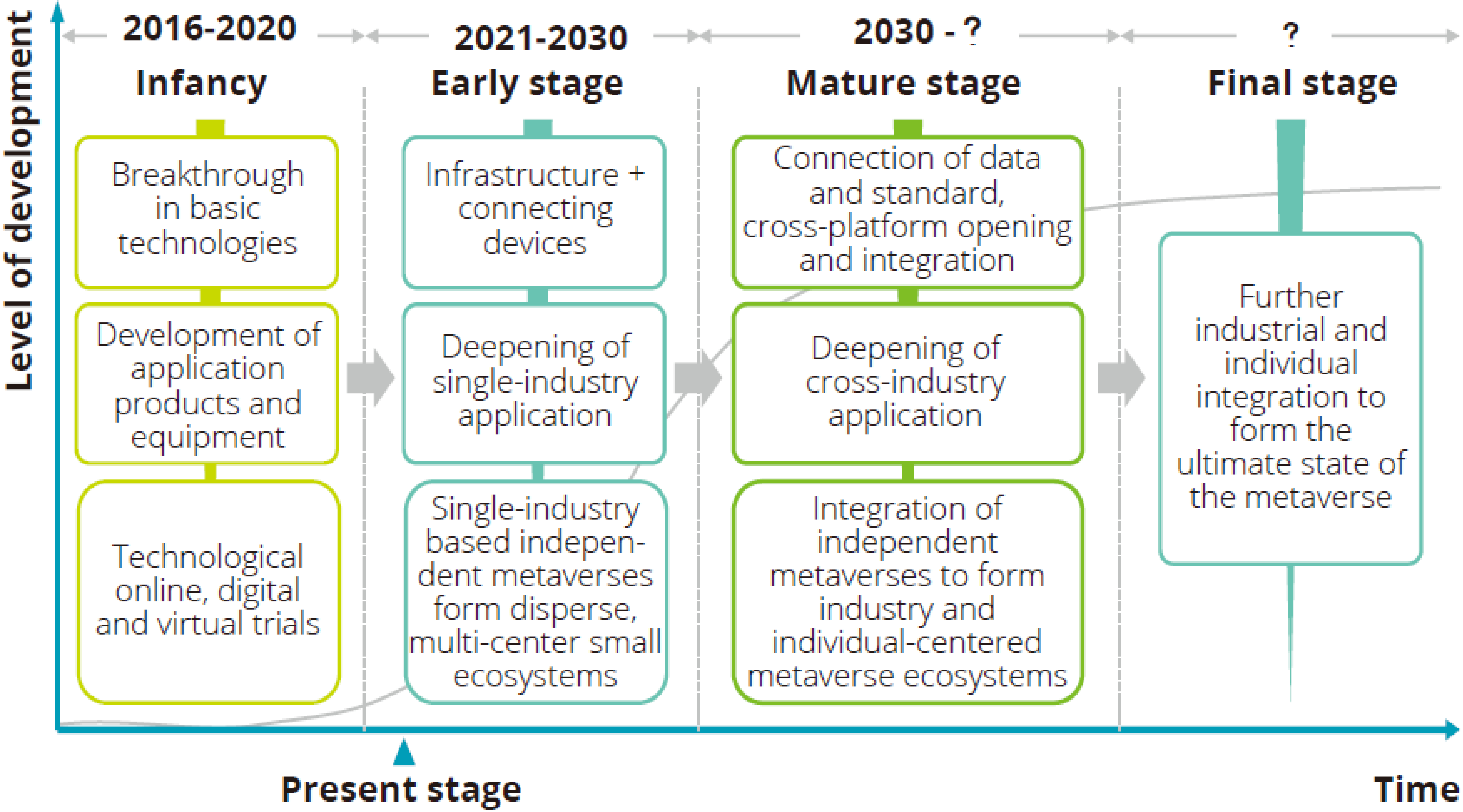
Security & Privacy

- Data Security
- Privacy
- Software Security
- Hardware (Device) Security
- Network Security

Interaction

- Multimodal Interaction
- Multi-task Interaction
- Embodied Interaction
- Persona Modeling
- Scenario Generation


Metaverse
Real World
Virtual Mirror World
to simulate reality
Virtual Native World
A new virtual world



Level of development

2016-2020

Infancy

Breakthrough in basic technologies

Development of application products and equipment

Technological online, digital and virtual trials

2021-2030

Early stage

Infrastructure + connecting devices

Deepening of single-industry application

Single-industry based independent metaverses form disperse, multi-center small ecosystems

2030 - ?

Mature stage

Connection of data and standard, cross-platform opening and integration

Deepening of cross-industry application

Integration of independent metaverses to form industry and individual-centered metaverse ecosystems

?

Final stage

Further industrial and individual integration to form the ultimate state of the metaverse

Present stage

Time

Metaverse Drivers

Technology

Readiness of underlying technology

Networks
Rollout of 5G and fibre to more communities

Economic enablers
Rise of cryptocurrencies and NFTs

Digital infrastructure
Cloud, blockchain, etc

Virtual platforms
e.g., Sandbox, Unreal Engine, Roblox, Decentraland

Access technology
AR/VR headsets, browsers, smartphones

Culture

Mindset shift to drive acceptance and adoption

- From online work and education now conducted through video calls, to virtual socials and events on video game platforms, the COVID-19 pandemic has supercharged the role of digital in our lives.
- This has also improved the digital literacy of people across generations, leading to a level of comfort with new platforms and technologies, and an added appetite to try new experiences.

Market

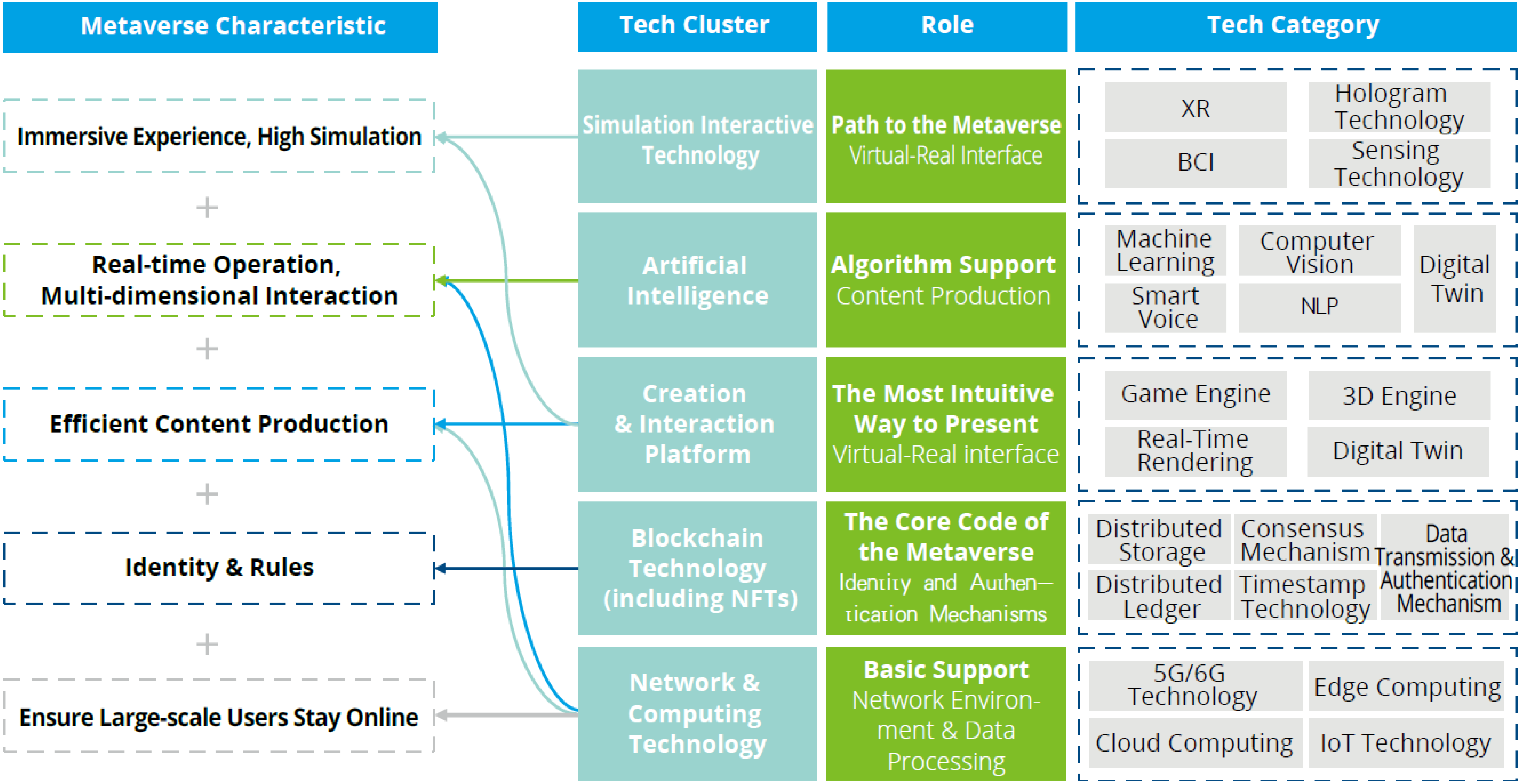
Supporting market activity and trends

Firm initiatives
New products, patents, processes, etc., launched by leading technology, OEM, entertainment and media companies

Immersive experiences
Live sporting games, concerts, and social events broadcasted and hosted by leading sports agencies and platforms

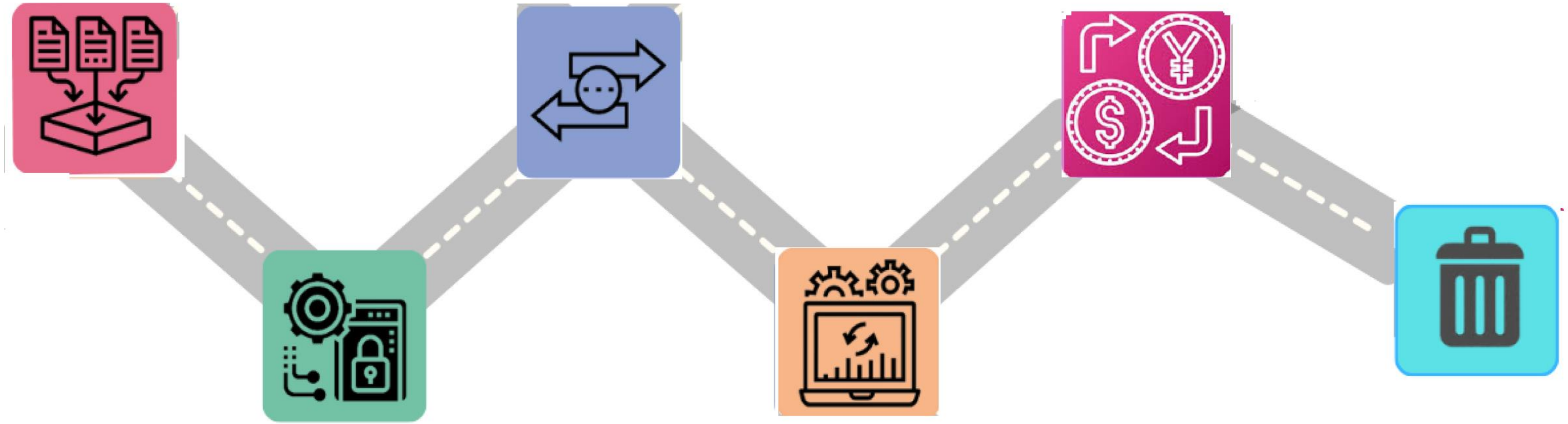
M&A and partnerships
Major partnerships and acquisitions across technology, gaming, and entertainment players globally

Virtual storefronts
Leading luxury and consumer brands providing offerings through stores in virtual worlds across industries and categories



Metaverse Characteristic	Tech Cluster	Role	Tech Category
Immersive Experience, High Simulation	Simulation Interactive Technology	**Path to the Metaverse** Virtual-Real Interface	XR Hologram Technology BCI Sensing Technology
+ Real-time Operation, Multi-dimensional Interaction	Artificial Intelligence	**Algorithm Support** Content Production	Machine Learning Computer Vision Digital Twin Smart Voice NLP
+ Efficient Content Production	Creation & Interaction Platform	**The Most Intuitive Way to Present** Virtual-Real interface	Game Engine 3D Engine Real-Time Rendering Digital Twin
+ Identity & Rules	Blockchain Technology (including NFTs)	**The Core Code of the Metaverse** Identity and Authentication Mechanisms	Distributed Storage Consensus Mechanism Data Transmission & Authentication Mechanism Distributed Ledger Timestamp Technology
+ Ensure Large-scale Users Stay Online	Network & Computing Technology	**Basic Support** Network Environment & Data Processing	5G/6G Technology Edge Computing Cloud Computing IoT Technology

Secure Data Lifecycle in Metaverse



Acquisition

- Techniques and methods
- Partnerships for data collection
- Impact of Technology & big data

Storage

- Storage cost & Maintenance
- Storage & Retention Policies
- Method For Data Security

Transformation

- Communication & Transparency
- Coordination
- Cost & Maintenance
- Access and Visualization

Process

- Techniques
- Data Quality Metrics

Exchange

- New Method tools & Uses

Destruction

- Data statute of limitations

Existing Threats in Data Acquisition

- Vulnerability of edge nodes
  - Disabling edge nodes
  - Turning edge nodes to botnet to carry out DDoS attack
  - Using edge nodes for eavesdropping
  - Modifying input data before sending
  - Uncalibrated wearable sensors
  - Deepfake and impersonation attack
- Input data tampering
  - False data injection
  - Replay attack
  - Zero dynamics attack
- Malicious/ low quality UGC
  - Decreasing the quality of user experience
  - Publishing malicious script

Existing Threats in Data Storage

- SPoF in centralized data storage
- Blockchain vulnerability
- Cloud vulnerability
- Breaking classical cryptography
- Side channel attack

Existing Threats in Data Transfer

- Data leakage
  - Eavesdropping
  - Man in the middle
  - Packet sniffing
  - Data interception
- Intrusion
  - DDoS
  - Syn flood
  - Packet flooding
  - Packet sniffing
  - Packet tampering
  - Ping sweeping
  - Eavesdropping

Existing Threats in Data Processing

- Attacking deep learning models
- Attacking federated learning models
  - Data poisoning
  - Attacking the effective edge nodes
  - Inference attacks
  - GAN attack
- Malware

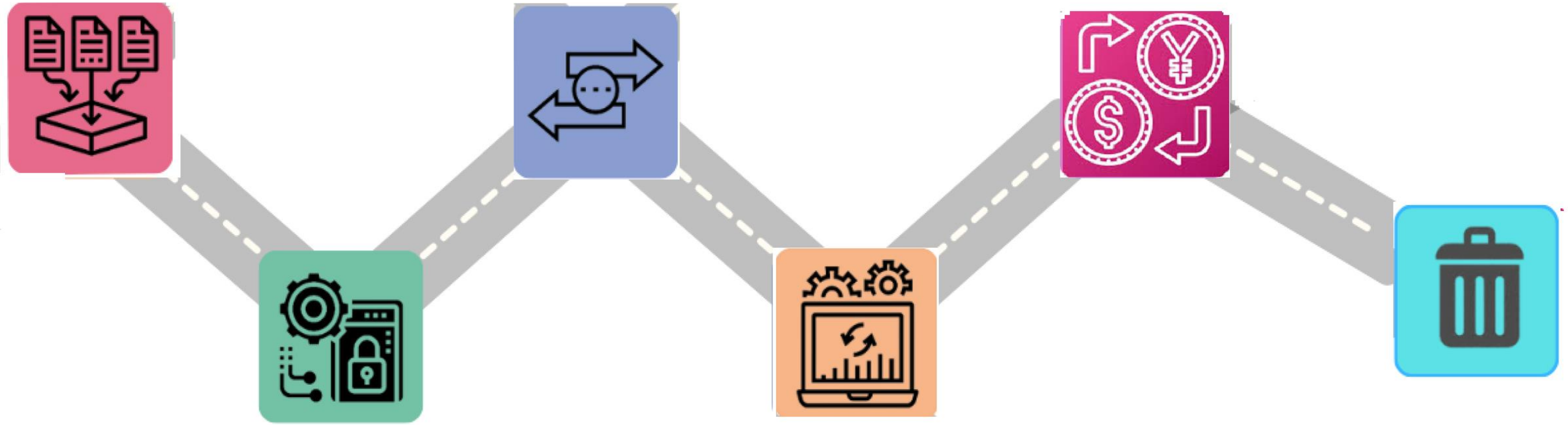
Existing Threats in Data Transaction

- Digital twin vulnerabilities
  - Digital twin data leakage
  - Digital twin unauthorized tampering
  - Information theft from digital twin
- Digital asset vulnerabilities
  - Threat to privacy
  - Theft of asset ownership
  - Attacking smart contract
- Man in the room and VR worm

Existing Threats in Data Destruction

- Malicious data non removal due to blockchain immutability
- Metaverse governance by handful organization

Secure Data Lifecycle in Metaverse



Acquisition

- Techniques and methods
- Partnerships for data collection
- Impact of Technology & big data

Storage

- Storage cost & Maintenance
- Storage & Retention Policies
- Method For Data Security

Transformation

- Communication & Transparency
- Coordination
- Cost & Maintenance
- Access and Visualization

Process

- Techniques
- Data Quality Metrics

Exchange

- New Method tools & Uses

Destruction

- Data statute of limitations

Data Acquisition Security Countermeasures

- Authentication and integrity verification of input nodes
- Management of edge nodes
- Input quality assurance
- Ensuring data provenance through the utilization of IoT techniques

Data Storage Security Countermeasures

- Data protection laws
- Blockchain utilizing quantum resistance encryption
- Achieving scalability while ensuring blockchain security
- Securing stored data in cloud

Data Transfer Security Countermeasures

- Using digital twins
- Encryption and access control mechanisms

Data Processing Security Countermeasures

- Resistance to adversarial models/ inputs
- Segmentation of the XR processing environment
- Malware detection

Data Exchange Security Countermeasures

- Distributed ledger infrastructure
- Protecting digital footprints
- Protecting digital twins

Data Destruction Security Countermeasures

- Removing from blockchain
- Secure removing from cloud or central database

Other Security Challenges

- New data security challenges
- Extremely large and diverse data volume
- Algorithmic challenges: Bias, lack of transparency, and vulnerability
- Interactions with synthetic content and fake users
- The "Darkverse" concept and its heightened hazards

THANK YOU