Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
00 (2025) 1–75

UMetaBE-DPPML: Urban Metaverse & Blockchain-Enabled Decentralised Privacy-Preserving Machine Learning Verification And Authentication With Metaverse Immersive Devices

Kaya Kuru[a,*], Kaan Kuru[a]

[a]*School of Engineering and Computing, University of Central Lancashire, Preston, PR1 2HE, UK*

Abstract

It is anticipated that cybercrime activities will be widespread in the urban metaverse ecosystem due to its high economic value with new types of assets and its immersive nature with a variety of experiences. Ensuring reliable urban metaverse cyberspaces requires addressing two critical challenges, namely, cybersecurity and privacy protection. This study, by analysing potential cyberthreats in the urban metaverse cyberspaces, proposes a blockchain-based Decentralised Privacy-Preserving Machine Learning (DPPML) authentication and verification methodology, which uses the metaverse immersive devices and can be instrumented effectively against identity impersonation and theft of credentials, identity, or avatars. Blockchain technology and Federated Learning (FL) are merged in the developed DPPML approach not only to eliminate the requirement of a trusted third party for the verification of the authenticity of transactions and immersive actions, but also, to avoid Single Point of Failure (SPoF) and Generative Adversarial Networks (GAN) attacks by detecting malicious nodes. The developed methodology has been tested using Motion Capture Suits (MoCaps) in a co-simulation environment with the Proof-of-Work (PoW) consensus mechanism. The preliminary results suggest that the built techniques in the DPPML approach can prevent unreal transactions, impersonation, identity theft, and theft of credentials or avatars promptly before any transactions have been executed or immersive experiences have been shared with others. The proposed system will be tested with a larger number of nodes involving the Proof-of-Stake (PoS) consensus mechanism using several other metaverse immersive devices as a future job.

Keywords: Metaverse, cybercommunity, urban twins, cybersecurity, collaborative deep learning, federated learning, blockchain

1. INTRODUCTION

The metaverse, which aims to build high-fidelity (e.g. real-data, structural, and physics engine fidelities) virtual worlds with which to interact, can be engaged within the Smart City (SC) ecosystem with high immersive Quality of Experiences (QoE) leading to increased Quality of Life (QoL) [1]. Urban metaverse worlds – an extension of residents and urban society, where the virtual and the physically real blend and are more organically integrated within

*Corresponding author
Email address: kkuru@uclan.ac.uk (Kaya Kuru)

the Cybercommunity of Wisdom (CoW) and where real-person resident avatars, government avatars, governmental entities, organisations, businesses, and avatars driven by Artificial Intelligence (AI) (i.e. AI bots or virtual users) can interact – would impact urban ways of living significantly on a global scale, with many practical implementations by democratising skills/assets within an urban ecosystem. The techniques under "Internet of Everything (IoE)" and Automation of Everything (AoE) [2] combine people, organisations, processes, things, and data into a tangible, coherent framework known as Cyber-Physical Systems (CPSs). CPSs are employed to create Cyber-Physical Social Systems (CPSSs) that work together to create a smarter, more interconnected world [3]. Accurate digital replication of real-world fragments of urbanisation (SC Digital Twins (DTs) (i.e., Urban Twins (UTs)) at various granularities can be achieved in the virtual plane through UTs [4]. Numerous urban metaverse use cases have already been adopted by urban life to improve QoL by overcoming spatial and temporal constraints, and the trend suggests that this will accelerate exponentially in the years to come.

The success of urban metaverse communities, augmented with the CoW, depends on the quality of data-driven SC DTs – UTs, the seamless exchange of data between cyber and physical urban worlds (e.g. between residents and their counterparts "3D Avatars" – pseudo-physical presence) and the processing of the data effectively and efficiently with no vicious interventions and threats. The potential risks and threats in this ecosystem that incorporates Web3 can be extremer than the ones in Web2, since we are immersed with multiple tightly coupled wearable sensor-rich devices perceiving the blend of the real and the virtual – with possible imminent negative experiences, if these platforms are not designed well to mitigate these potential hazards. The metaverse, with its enriched sets of capabilities, has the potential to affect its users dramatically beyond the digital environment in a variety of aspects where users would spend more time in urban metaverse cyberspaces as metaverse technologies improve and immersive cyberspaces, with a rich set of experiences, grow. Cybersecurity and privacy protection are the two crucial challenges in making secure and reliable urban cyberspaces thrive, as cybercrime activities are expected to be rampant in this ecosystem with trillion dollars of economic value in the years to come. Ensuring seamless connectivity, data accuracy, and user privacy are critical aspects that need further attention for the efficacy of urban metaverse cyberspaces, particularly, from technical, legislative, and ethical standpoints. The use of advanced infusion metaverse technologies (e.g. VR/AR headset, full haptic body suits, i.e. MoCaps) increases the quality of resident experiences in the urban ecosystem. On one hand, the incorporation of these immersive devices into urban metaverse worlds involves technical, security, and privacy challenges (Fig. 2). Privacy in the parallel urban metaverse cybercommunities with multiple diverse objectives and users with varying expectations is a crucial issue because of their immersive nature and the wide array of a new level of Web3 communication and data collection (e.g., biometric and behavioural patterns, and real-time experiences and emotional responses via immersive wearable devices and meta-humans (i.e. avatars)) to enable and

enhance the user experience. It's imperative to build robust privacy-enhancing mechanisms to mitigate the risks in those granular socialisation parallel words where a variety of experiences as well as virtual business practices with huge economic values are run. In this treatise, the abilities of immersive devices can be instrumented to improve privacy and security when combined with other technologies such as blockchain and AI. Our research question in this study can be summarised as: How can metaverse and urban ecosystems be moulded to generate safe and secure urban metaverse cyberspaces? Can the concepts of Web3, "you control your identity" and "you control your own data"', work in this moulded ecosystem as intended in the metaverse concept to alleviate privacy concerns? What are the possible risks and cyberthreats in this cybercommunity, and how can these threats be addressed? In this direction, this paper, by analysing potential cyberthreats in the urban metaverse cyberspaces, proposes a blockchain-based authentication technique, which uses the metaverse immersive devices and can be instrumented effectively against unreal transactions, identity impersonation and theft of credentials, identity, or avatars. Particular contributions in this paper can be outlined as follows.

- The essential building blocks of the urban metaverse ecosystem – the so-called MetaCyberCity – are surveyed concisely to visualise strengths in cybersecurity and shortcomings towards cyberthreats.
- The possible cyberthreats for the urban metaverse cyberspaces are revealed, and how these threats can be addressed with a series of countermeasures is analysed.
- A blockchain-based authentication approach, which uses metaverse-immersive devices to generate Decentralised Privacy-Preserving Machine Learning (DPPML) models, is designed. This design, by avoiding Single Point of Failure (SPoF) and Generative Adversarial Networks (GAN) attacks and eliminating a trusted third party for the verification of the authenticity of models, can be instrumented effectively against unreal transactions, identity impersonation and theft of credentials, identity, or avatars within urban metaverse cyberspaces – without renouncing targeted functional abilities of the immersive devices and the essential objectives of the urban metaverse cyberspaces.

The organisational structure of the paper is presented in Fig. 1.

2. LITERATURE SURVEY

2.1. METAVERSE CONCEPT AND AI

The leading, gigantic companies such as Meta, Microsoft, NVIDIA (e.g. VMware Workspace ONE XR Hub, NVIDIA CloudXR), Intel, Apple, and Samsung – as well as many others – are investing heavily in developing advanced metaverse technologies and different metaverse ecosystems; other major companies such as Nike, Coca-Cola,

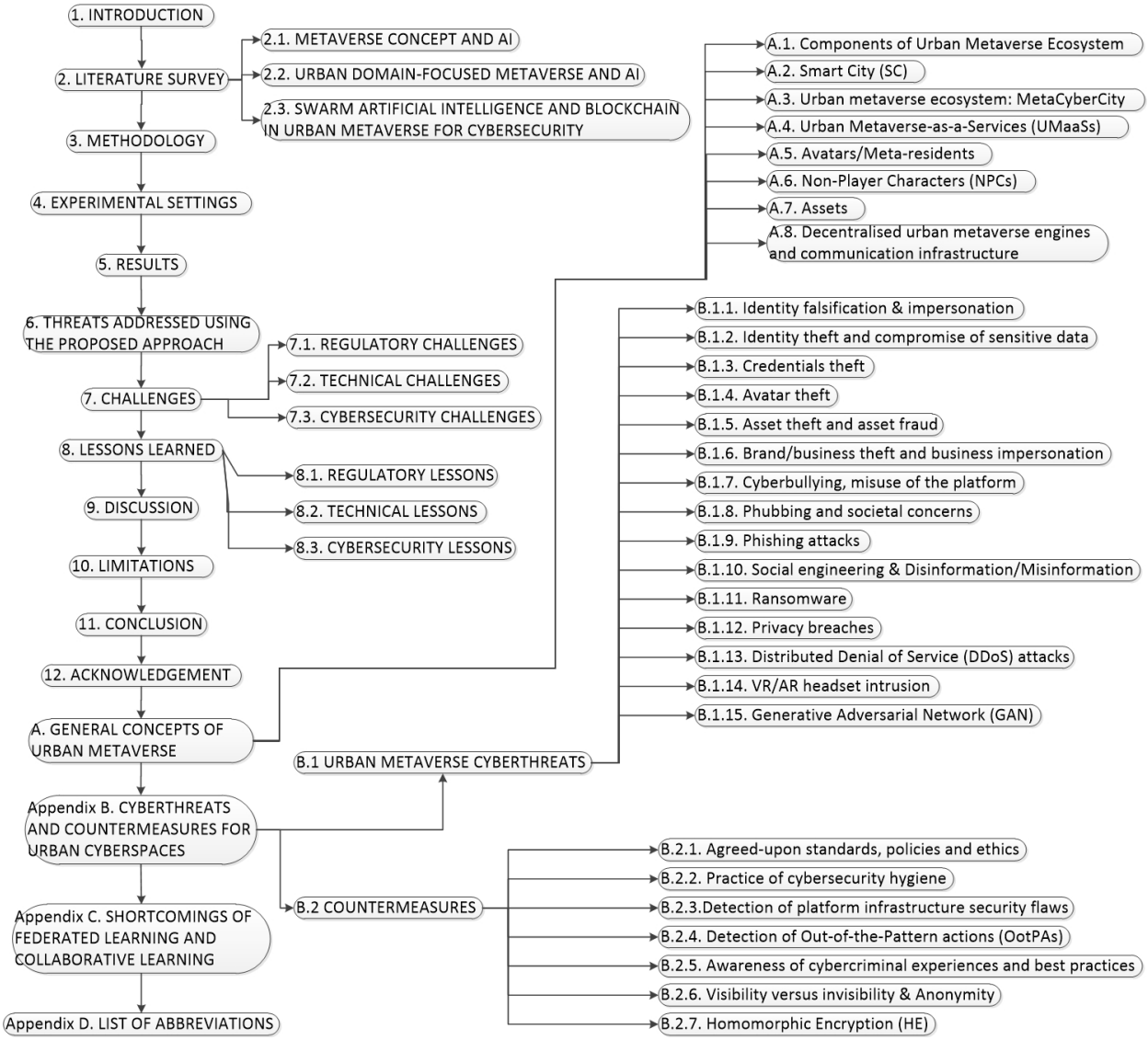

Figure 1. Organisational structure of the paper.

and Gucci are also transporting their business into the metaverse environment to create immersive experiences for their customers to interact with their products, with high QoE. This immense involvement with the metaverse will carry this 3D elevation of linear Internet (i.e. second-generation of the Internet) to the next level in which more people would be immersed in virtual worlds augmented with reality [1]. The metaverse taxonomy, definitions, architecture, applications, challenges, issues, solutions, and future trends are reviewed in [5], [6], [7]. AI approaches specific to the development of metaverse items are surveyed in [8] and the fusion of blockchain and AI with the metaverse is surveyed in [9]. Blockchain-empowered service management for the decentralised Metaverse of Things (MoTs) is analysed in [10] at aiming to resolve the problem of synchronised data transmission and service provision through

multiple devices to ensure immersive engagement of end users via all the available means of sensing and visualisation. A basic metaverse framework is analysed from the aspects of graphics, user interactions and visual construction of metaverse worlds as well as the construction of visual DTs in [11]. Building metaverse cyberspaces using DTs at all scales, states, and relations is examined in [12]. Some of the key issues, required in order to realise metaverse services based on DTs, are discussed in a short paper in [13]. Intelligent wireless sensing technology, integrating AI, can serve as an intelligent, flexible, non-contact way to access the metaverse and expedite the establishment of a bridge between the real physical world and the metaverse [14].

2.2. URBAN DOMAIN-FOCUSED METAVERSE AND AI

From an SC perspective, the fundamental technologies for SCs in relation to the metaverse are surveyed in a restrictive concept as a short paper in [15]. The vision of using Non-Fungible Tokens (NFTs) – blockchain-based tokens – in SCs is explored in [16]. More specifically, the main components of NFTs (i.e. cryptographic properties) and how SC applications, such as smart governance, smart services, smart economy, smart industry, smart environment, and smart mobility and transportation, can benefit from them are described in the study. A survey on current metaverse applications in healthcare regarding the SC health and welfare domain is performed in [17], [18], [19]. A theoretical framework by reviewing literature and synthesising best practices in designing metaverse learning environments regarding the SC education domain is proposed in [20]. An extensible SC metaverse tourism platform is disclosed in [21]. The metaverse applications built for specific SC domains are elaborated in [1] with a framework – MetaOmniCity – that derives a conceptual infrastructure instilled with AI for the development of urban metaverse parallel worlds upon UTs by encouraging citizen cooperation with experiences. MetaOmniCity, as the logical extension of UTs, demonstrates the ways of practical implementations of metaverse technologies in the urban ecosystem and makes the residents feel the city nerves in collaborative and immersive 3D spaces where two worlds can be more tangibly connected and interact in real-time.

2.3. SWARM ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN IN URBAN METAVERSE FOR CYBERSECURITY

The shortcomings of the widely employed Federated Learning (FL) and Collaborative Learning (CL) techniques in Swarm AI (SAI) are presented in Appendix C for interested readers. Privacy-Preserving Machine Learning (PPML) or more specifically, Privacy-Preserving Deep Learning (PPDL) schemes have been developed and employed to further preserve sensible data and privacy while performing FL/CL. Multiple distributed encrypted data points can be uploaded by their owners to a central server, collected by the platform, or processed data models using specific agreed-upon transparent DL training models, which are then later aggregated to establish the global model without sharing the data itself. The Homomorphic Encryption (HE) scheme allows data to be processed without needing to decrypt

it as elaborated in Section Appendix B.2.7. SEALion, CryptoNet [22], and CryptoDL are the early implementation examples (trained networks) of the PPDL scheme via encrypted outputs using HE. A PPDL system in which many learning participants perform NN-based DL over a combined dataset of all, without revealing the participants' local data to a central server is presented in [23] using asynchronous stochastic gradient descent, in combination with HE. An FL-enabled network data analytics function architecture with partial HE to secure ML model sharing with privacy-preserving mechanisms is proposed in [24]. A full HE scheme to the standard DNN, ResNet-20, is applied in [25] to implement PPML. A universal multi-modal vertical FL framework is proposed in [26] to effectively acquire cross-domain semantic features on homomorphic-encrypted data. FL mechanism is introduced into the deep learning of medical models in Internet of Things (IoT)-based healthcare system in [27] in which cryptographic primitives, including masks and HE, are applied for further protecting local models, so as to prevent the adversary from inferring private medical data by various attacks such as model reconstruction attack or model inversion attack or model inference attacks. Considering a specific application of Human Activity Recognition (HAR) across a variety of different devices from multiple individual users, the vertical FL scheme is developed to integrate shareable features from heterogeneous data across different devices into a full feature space, while the horizontal FL scheme is developed to effectively aggregate the encrypted local models among multiple individual users to achieve a high-quality global HAR model in [28], in which a computationally efficient scheme resembling HE is then improved and applied to support the parameter aggregation without giving access to it, which enables heterogeneous data sharing with privacy protection across different personal devices and multiple users in building a more precise personalised HAR model. An adversary detection-deactivation method for metaverse-oriented CDL is proposed in [29].

Cybersecurity threats against the metaverse as well as privacy concerns are analysed in [30], [31], [32], [33]. These threats and the basic measures to address some of these threats (Fig. 5) as well as the main components of privacy (Fig. 2) are explored in Appendix B. The techniques and approaches for cybersecurity to address security and privacy safeguarding concerns are being developed as cyberattacks are taking place every day for citizens in the human-cyber-physical world. Different from the cybersecurity risks faced by standard internet users, the metaverse has created new security challenges due to its different structure; for example, virtual identities, digital currencies, and NFTs (i.e. unique digital identities representing all types of assets) are interesting economic targets for hackers [31]. There is a risk of blockchain-related fraud in financial institutions [31]. NFTs can be used to represent digital assets in a SC that are required to be immutable, secure, and traceable, and they are not a stand-alone technology, as they require a well-configured blockchain and an efficient off-chain data storage solution in order for them to function properly [16]. Every NFT is associated with a particular piece of art/asset (e.g. photographs, books, videos) to certify ownership and authenticity. The blockchain records its origin and history, which lowers the possibility of counterfeiting and confirms

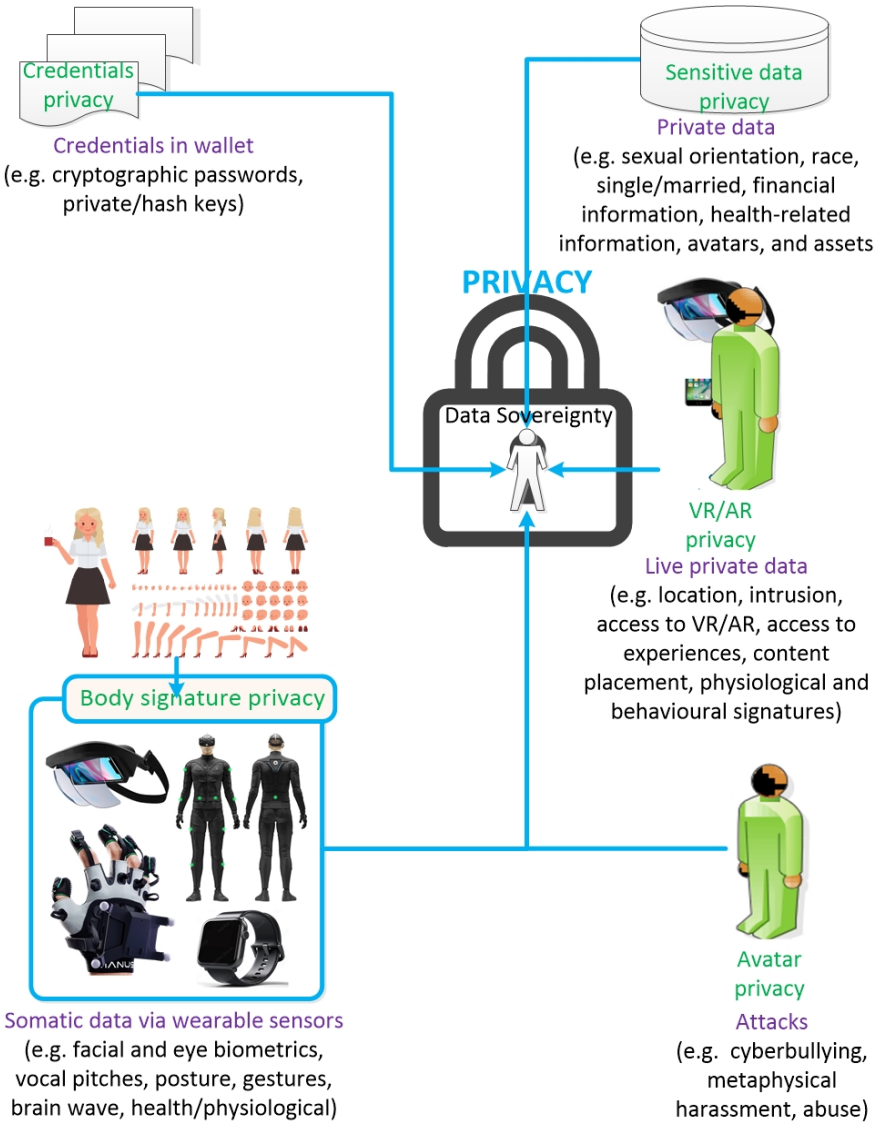

Figure 2. Main components of privacy in the urban metaverse ecosystem (elaborated in Appendix B).

the legitimacy of digital assets by ensuring authenticity and tracking provenance. Multiple ownership of NFTs is also allowable through fractional ownership, particularly, for high-value assets (e.g. real estate, collectibles) using smart contracts. NFTs facilitate simple ownership transfers via blockchain transactions. A smooth and safe ownership transfer without a trusted third party is ensured by recording the new owner on the blockchain after the transfer. To restrict access, usage, and distribution of digital content and guarantee that only verified owners have access, NFTs can be integrated with Digital Rights Management (DRM) systems. The genuinity of the individuals can be ensured using the techniques proposed in this research even if with stolen credentials as elaborated in Section 3. The concept of smart contracts aims to ensure that transactions are completed safely. It is noteworthy to emphasise that genuine

artworks can be easily stolen and sold in the form of NFTs without the knowledge of the original creator. It may be difficult to settle disagreements over NFT ownership within a decentralised blockchain ledger due to the varying legal frameworks in different countries.

Wearable hardware, which is one of the most important components of the metaverse, can also create new threats. With the increase in the use of virtual reality glasses and headsets which may serve as suitable access points for hackers, or augmented reality devices in which the biometric data of users are stored may become ideal targets for attacks. Implementing advanced multiverse realms with smart wearables is analysed in [34]. Wireless sensing technologies, such as radio-frequency identification (RFID), Wi-Fi, ultrasonic, and infrared sensors, can be used to track the movements of users in real time, enabling them to navigate and interact with the metaverse; these technologies can also be applied to tracking eye movements, facial expressions, gestures, and even body posture [14]. Due to the expected massive number of connected devices and network tenants, the 6G ecosystem would tend to be highly prone to Distributed Denial of Service (DDoS) attacks [35]. DDoS attacks and theft of avatars, particularly for wearable metaverse devices, are two main cybersecurity concerns in metaverse environments. Prevention of privacy intrusions without reducing overall QoE along with real socialising needs to be ensured. Blockchain technology has been recently introduced to mitigate these concerns in urban use cases. A design of a secure mutual authentication scheme for metaverse environments using a blockchain scheme is proposed in [36]. A framework that uses blockchain technologies was proposed in [37] for DTs to ensure the security of transactions during the data streaming between virtual and physical entities. Similar security frameworks are expected to be developed in parallel with the increasing number of metaverse use cases in the years to come. With a collaborative privacy-preserving learning method, multiple parties holding sensitive data can collaboratively learn a model across all of their datasets while minimising exposure and leakage of their data [38]. Urban metaverse cyberspaces should facilitate the exchange of information in a trusted way through the metaverse ecosystem built on decentralised blockchain technologies. Blockchain, with its privacy-preserving mechanisms by verifying the training process securely, has been recently employed to enable the secure generation of SAI in a distributed manner. Various studies, by merging blockchain technologies and FL, aim to address the shortcomings of FL against cyberattacks such as GAN attacks and SPoF. A blockchain FL (BlockFL) mechanism, enabling on-device ML without any centralised, training data or coordination by utilising a consensus mechanism is proposed in [39] to generate local models on mobile devices by exchanging and verifying the parameter updates via blockchain to avoid the aforementioned concerns. BlockFL shows that a malicious miner will never form a new blockchain whose length is longer than a blockchain formed by honest miners and the overtake probability goes to zero if just a few blocks have already been chained by honest miners. Although a malicious miner begins the first Proof-of-Work (PoW) – consensus hash generation mechanism – with the honest miners, the larger number of miners prevents the overtake. Some

recent studies in the literature aim at reducing the cyberthreats using automated detection and prevention approaches. Chen et al. [40] aim to address the threat from GAN attacks pose to CDL and propose a model-preserving CDL framework, called MP-CLF, which can effectively resist the GAN attack. An adversary detection-deactivation method for metaverse-oriented CDL is proposed in [29] to avoid GAN attacks. A blockchain-based, fair and differentially private decentralised deep learning framework (FDPDDL), which enables parties to derive more accurate local models in a fair and private manner, is proposed in [41]. A privacy-preserving two-party distributed algorithm of backpropagation which allows a neural network to be trained without requiring either party to reveal the individual data to the other is presented in [42]. More references that are specific to the particular subjects analysed in this study are provided in the related sections below. There is a research gap in revealing potential cyberthreats in urban metaverse worlds and addressing these threats using SAI in an automated manner. This paper, by proposing a blockchain-based PPML authentication and verification approach with immersive devices, aims to fill this gap, helping the metaverse concept mature within a secure urban metaverse ecosystem by prioritising the privacy of residents.

3. METHODOLOGY

The readers, who are not families with the components of the metaverse are referred to Appendix A for more information, in particular, the general concepts of the urban metaverse ecosystem. This section focuses on the developed techniques to build the proposed blockchain-enabled DPPML verification and authentication approach - the so-called UMetaBE-DPPML.

A large numbers of daily transactions and actions, taking place in a short period of time, require an efficient way of authentication, while the complexity of transactions and, more importantly, the complexity of cyberattacks is significantly increasing with newly developed metaverse technologies, particularly with wearable immersive metaverse devices. No third-party entity, including a centralised server/government, is trusted – considering semi-honest parties or honest but curious parties on the encryption-based and fully decentralised blockchain architecture in which data is supposed to be owned by its producers and is not managed by a centralised authority – which makes this ecosystem an ideal target for cybercriminals to exploit maliciously. Adverse events need to be detected in real-time to avoid dire circumstances such as losing individual data, NFTs, virtual real estate, cryptocurrency, or a breach of privacy on the blockchain in which traceability of transactions and actions is difficult to follow, due to the nature of the blockchain ecosystem with high level of data sovereignty and privacy. It needs to be assured that effective AI-based cybersecurity solutions are in place to defend residents from attacks without renouncing this nature. AI approaches can learn patterns with ML models that indicate a normal or abnormal transaction/action or cyberthreats. The modelling with ML and its real-time counteraction abilities in the urban metaverse ecosystem is conceptualised in a broader perspec-

tive in Figs. B.12 and B.13. Automated solutions with privacy-preserving mechanisms can mitigate the cyberthreats (Section Appendix B.1) effectively within the urban metaverse ecosystem. SAI, merged with blockchain, can play a prominent role in securing transactions and all other actions with a high level of privacy. Authentication of residents and verifying their true identities without a third party or a central authority is imperative in developing private and secure urban metaverse cybercommunities. Regular identity checks are crucial to both address fake avatars or avatars that have been stolen via unauthorised access to user credentials and avoid their imminent adverse consequences – such as breach of privacy and loss of assets. Individual data that can be used for authentication is composed of i) biographic identification data such as name, surname, date of birth, and ii) biometric identification data as biological characteristics (DNA, facial features, height, fingerprints, iris features, vein features, and palm features) and behavioural/gesture patterns (facial expressions, movement patterns (gait), lip motion, emotion expression or reactions to interactions using physiological responses, voice pitch patterns/prints, and speech patterns). Automated Emotion Recognition (AER) and Automated Behaviour Recognition (ABR) technologies can detect humans' emotional/behavioural states in real-time using facial expressions, voice attributes, text, body movements, and neurological signals and have a broad range of applications across many sectors [43]. Using these features to train networks and models raises privacy and ethical concerns in various aspects. Privacy and ethical concerns in applying AI for learning expressions and patterns using the aforementioned individual features, which is out of the scope of this research, are explored in [44] for interested readers.

AI-enabled wireless sensing is a growing field that plays a crucial role in creating immersive experiences in the metaverse, a shared, virtual space that is accessible via the internet; it allows us to perceive and interact with the digital world in a more intuitive and natural way, by enabling accurate position tracking, motion detection, gesture recognition [14]. The way of building DL gesture models should consider these privacy and ethical concerns as well as the regulatory framework (Fig. B.10). Human beings, with their body and behavioural/gesture signatures, are drastically different from each other in many ways, and they can be identified based on their biological or behavioural/gesture characteristics with a high level of identification assurance. It is worth mentioning that physics-based character skills of individuals can be gained through RL, which can improve the realism of individuals in regard to avatars [45] as well. Every action or transaction during the immersive interaction of individuals can be copied into the metaverse ecosystem. These consecutive actions or transactions generate particular patterns, in other words, a cyber identity of individuals, that differentiates them from other users. Within this context, metaverse immersive devices can help residents protect the boundaries of their privacy despite the security and privacy challenges that come with these devices, particularly VR/AR headsets, which are elaborated in Section Appendix B.1.14. The capabilities of these devices can be instrumented to improve privacy and security when combined with other technologies such as blockchain and

SAI as explained earlier in Sections 1 and 2. The actions of residents can be profiled through their bodies, coupled with advanced multiple sensory technologies that are based on a variety of body signatures, while interacting with the metaverse ecosystem, particularly by using VR headsets and full haptic body suits, i.e. MoCaps, equipped with multi-sensory abilities enabling tactile sensation. Users immerse themselves with full-body haptic suits including finger and full-body tracking sets, by which every motion can be replicated in virtual worlds and the real world with a bidirectional haptic interaction (e.g. touch, and handshake in a virtual environment). A sequence of these motions can build our unique body features by extracting the patterns from users' gesture cues, which leads to patterns distinguishing us from the rest of the world. These patterns, as well as the aforementioned distinctive individual signatures, can be utilised effectively for authentication purposes via a diverse range of metaverse technologies (e.g. VR/AR headsets, MoCaps, haptics gloves, Hand Tracking Toolkit (HTT), and different types of many other Wearable Sensors (WSs)), which are improving with larger sets of options and a diverse range of attributes. For instance, Wearable Resistive Sensors (WRSs) that could directly characterise joint movements are one of the most promising technologies for hand gesture recognition due to their easy integration, low cost, and simple signal acquisition [46].

The urban metaverse cyberspaces and associated entities are distributed on the decentralised public and private ledgers (Fig. B.11). AI models are required to be trained at the edges locally and encrypted update gradients need to be transferred to construct larger or global models regarding the principles of CL/FL as expressed earlier in Section 2.3. In order to improve collaboration in learning, the privacy concerns of each data subject should be addressed by extending the concept of privacy protection to the original learning entity. In this vein, a DPPML scheme, based on transparency and personal consent (Fig. B.10), is developed using the cyber gesture signature with wearable immersive devices to protect users' privacy while verifying the authenticity of the subject, where the data subjects in more control with further security measures. All the symbols in the techniques and algorithms have been presented in Table 1. Cyber signatures, which make the subject different from other subjects, can be built through their body language using tightly coupled immersive wearable metaverse devices as visualised in Fig. 3. The pseudo codes of model training with a MoCap device are presented on blockchain in Algs. 1 and 2. More specifically, Alg. 1 shows the local training of the model with epochs fed by the particular online instant features acquired from the device, which is worn by one of the active nodes on the blockchain whereas Alg. 2 displays the global model update with the blockchain operations for verification of the update gradients acquired from all the active nodes on the blockchain through blockchain mining. Alg. 1 is run by each node individually at the edges locally whereas Alg. 2 is run on blockchain by all the active nodes where current nodes can leave and new nodes can join at any time. It is imperative to employ a technique to determine if adding the candidate blocks to the chain is appropriate or not. Only trustworthy blocks with

[2]Readers are referred to https://teslasuit.io/blog/teslasuit-motion-capture-system/ for the MoCap and to https://freedspace.com.au/tracklab/products/brands/manus-vr/optitrack-gloves-by-manus/ for the HTT images.

Table 1. Nomenclature for the techniques and algorithms (Algs. 1, 2, 3, 4).

No	Symbols	Definitions
1	α	Step size at each iteration of the gradient descent algorithm
2	A	Attributes
3	$Blockchain(ID_{MoCap}).genesis$	First block created for ID_{MoCap}, that stores info for transactions
4	$Blockchain(ID_{MoCap}).lastblock$	Last block in the blockchain for ID_{MoCap}
5	$Blockchain(ID_{MoCap}).ledger$	Ledger where the blockchain is created
6	$Blockchain(ID_{MoCap}).newblock$	New block added to the ledger
7	$Blockchain(ID_{MoCap}).newhash$	Hash generated smaller than $PoW.difficulty$ for ID_{MoCap}
8	$Blockchain(ID_{MoCap}).newhash.state$	"False" if hashing continues; else "True" to stop current mining
9	$Blockchain(ID_{MoCap}).nodes$	Active nodes in the network for ID_{MoCap}
10	$Blockchain(ID_{MoCap}).nodes.candidateblocks$	Candidate blocks of all active nodes before mining next block
11	$Blockchain(ID_{MoCap}).nodes(meR).candidateblock.body(meR)$	Candidate block of the individual user
12	F	Feature set
13	$F = A_1, A_2, \ldots, A_{size}$	Acquired attributes in a feature set
14	ϵ	Very small value indicating weight difference specified to stop training
15	$epoch$	Feature set size for training
16	ID_{MoCap}	Identification code of the MoCap
17	$ID_{HeadSetFace}$	Identification code of the headset (VR/AR) for face features
18	$ID_{HeadSetLip}$	Identification code of the headset (VR/AR) for lip features
19	$ID_{HandTrackingSet}$	Identification code of the hand tracking set
20	ID_{size}	Identification code of the last immersive device
21	$ID_{MoCap}.IP$	IP address of the MoCap device
22	$ID_{MoCap}.Port$	Port number of the MoCap device
23	$ledger$	Public blockchain distributed ledger
24	$M_{ID_{MoCap}}$	Model in the blockchain for ID_{MoCap}
25	meR	Individual user
26	$meR.Data$	Individual user data array ($ID_{MoCap}.IP$, $ID_{MoCap}.Port$, $meR.credentials$)
27	$meR.ID$	User unique identification code
28	$meR.M$	Particular gesture model per immersive device
29	$meR.M_{ID}$	Identification code of the particular gesture model, $meR.M_{ID}$
30	$R_{me_{(M_{ID_{MoCap}})}}.meR.hash$	Hash key of individual user for model, $meR.M_{ID}$
31	meR.PrivateKey	Private key of individual user
32	PoW	Proof-of-Work
33	$PoW.difficulty$	Consensus hash difficulty
34	$PoW.Operations$	Hash generation to achieve a hash smaller than $PoW.difficulty$
35	$R_{1_{(M_{ID_{MoCap}})}}$	First individual model created in blockchain for ID_{MoCap}
36	$R_{me_{(M_{ID_{MoCap}})}}$	Individual model of a particular individual in blockchain for ID_{MoCap}
37	$R_{me_{(M_{ID_{MoCap}})}}.LearningState$	"NotSufficientlyTrained" if $\lvert w^G - w^{G-1}\rvert \leq \epsilon$; "Sufficient" otherwise
38	$S = F_1, F_2, \ldots, F_{epoch}$	Sets of features for training
39	$S = F_1, F_2, \ldots, F_k$	Instant sets of features for validation of individual user
40	$timestamp$	10 digit number of operation time in the Unix system
41	$UpdateQueue$	Individual updates in the queue to update the global model
42	$UpdateQueue.updateparameters$	Update parameters of one line of the updates in the queue
43	$UpdateQueue.Size$	Size of the updates waiting in the queue to update the global model
44	$VotingThreshold$	Agreed threshold (%) required to validate the genuinity of transactions
45	w^L	Local weights
46	w^G	Global updated weights

updates are allowed to continue forward with the subsequent consensual block thanks to the distributed validation mechanism, i.e., the voting scheme in Alg.3 by avoiding GAN attacks and SPoF. To put it another way, Alg. 3, enabling other nodes to reject altered data rapidly using hashes (i.e., signatures of data), combines the voting results with the corresponding local models and stores them in the successive consensual block if the voting consensus is higher than the predetermined threshold value (e.g. 50% in order to avoid being overtaken by more malicious miners) (i.e., $VotingPercentage > VotingThreshold$) based on the accumulated votes as shown in Alg. 2. From a

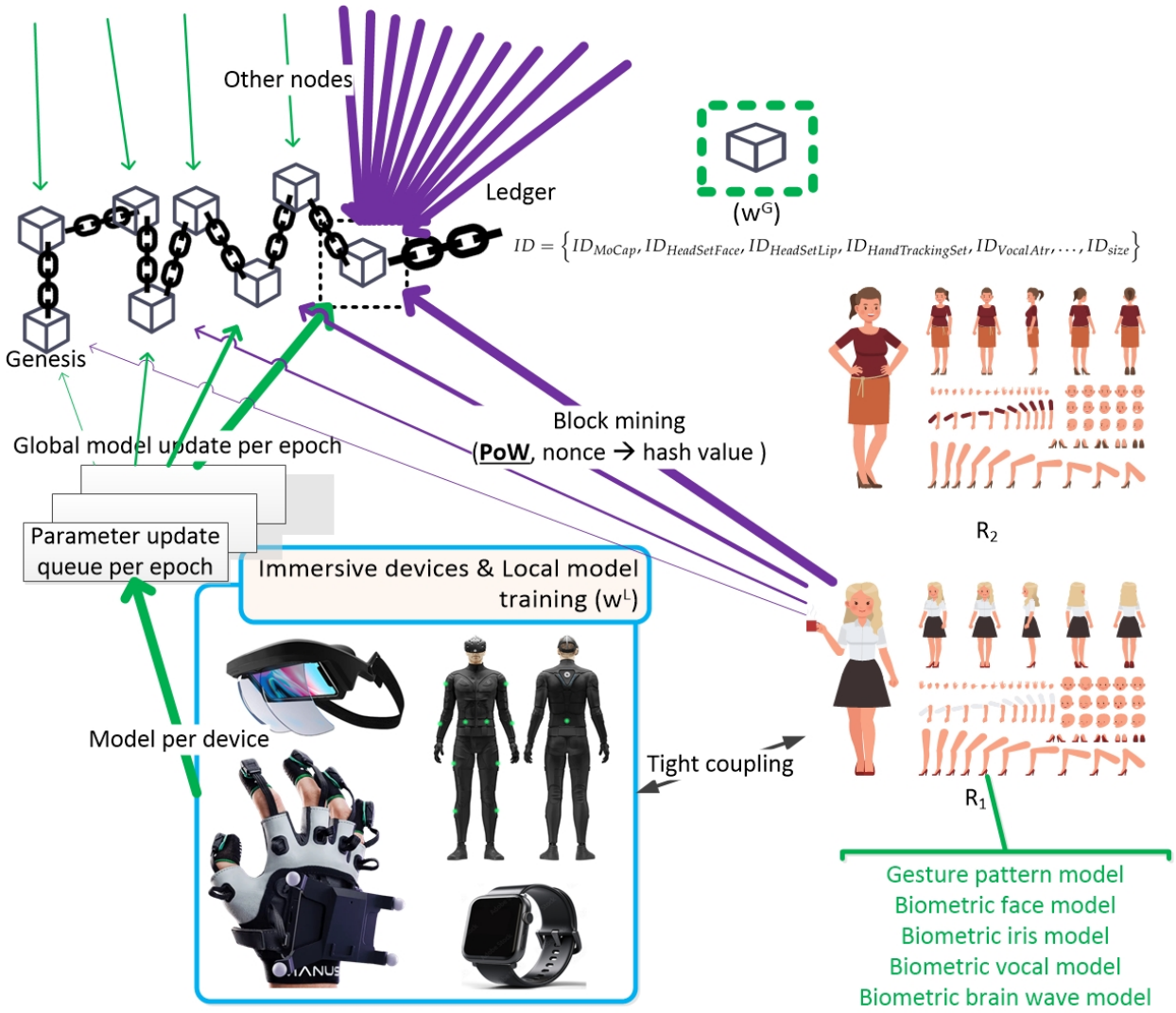

Figure 3. User-based DPPML model generation using immersive metaverse devices. The next block which is being added to the distributed ledger has the most recent model update whereas the last block has the final model itself.[2]

more technical standpoint, the gesture feature set for particular attributes, $F = \{A_1, A_2, \ldots, A_{size}\}$, of resident entities, $R = \{R_1, R_2, \ldots, R_{size}\}$, need to be trained per individual with an epoch sample size, $S = \{F_1, F_2, \ldots, F_{epoch}\}$. Local weights ($w^L$) and global weights ($w^G$) are synchronously updated after every epoch iteration to generate particular vocal or gesture models, M_{ID}, per immersive device, ID, as displayed in Eq. 1.

$$ID = \{ID_{MoCap}, ID_{HeadSetFace}, ID_{HeadSetLip}, ID_{HandTrackingSet}, ID_{VocalAtr}, \ldots, ID_{size}\} \quad (1)$$

Residents, R, perform the PoW operations with a block generation rate of λ and whoever is successful in reaching a hash key, by finding a nonce that is smaller than the target value based on the difficulty of PoW, places the

Algorithm 1: Individual authentication modelling per immersive device: Local training (ID $=\{ID_{MoCap}, ID_{HeadSetFace}, ID_{HeadSetLip}, ID_{HandTrackingSet}, \ldots, ID_{size}\}$.

Data: System input: ID_{MoCap}.IP & ID_{MoCap}.Port & *meR*.ID
Data: Instant input: $F = \{A_1, A_2, \ldots, A_{size}\}$ & $S = \{F_1, F_2, \ldots, F_{epoch}\}$
Result: Alg. 2 < −− ($UpdateQueue$ & ID_{MoCap} & *meR*.id & ContinueUpdate)

int iteration = 0;
bool ContinueUpdate = true;
=> Start data streaming from the device and parameter selection;
UDPServer udpserver = new UDPServer();
=> Thread for streaming data from ID_{MoCap};
Thread serverThread = new Thread(() => udpserver.Listen());
=> Thread for filtering targeted attributes, $F = \{A_1, A_2, \ldots, A_{size}\}$;
Thread dataHandlerThreadAtr = new Thread(() => SubscribeToEvent(udpserver));
=> ID_{MoCap} gesture parameters and local model training;
while *ContinueUpdate == true* **do**
    => Start streaming from the device;
    [*meR*.Data]= serverThread.Start(ID_{MoCap}.IP, ID_{MoCap}.Port, *meR*.credentials);
    => Start filtering for attribute selection;
    [F] = dataHandlerThreadAtr.Start(*meR*.Data);
    => Add filtered attributes to data samples until reaching the epoch size;
    S += [F];
    => Continue training until weight differences is very small as such $|w^L - w^{L-1}| \leq \epsilon$;
    if *($S.size == epoch$) && ($|w^L - w^{L-1}| > \epsilon$)* **then**
        iteration += 1 ;
        => Feed the local model training with $S = \{F_1, F_2, \ldots, F_{epoch}\}$;
        [$\alpha_{iteration}, w_{iteration}$] = localTrain($S$);
        => place the obtained update parameters in queue;
        $UpdateQueue$ += ($\alpha_{iteration}, w_{iteration,timestamp}$);
        => Empty the sample array, S, for the next epoch feed;
        S = "";
    else
        => Training has reached a satisfactory level, quit local training and global uodates;
        ContinueUpdate = false;
    end
end

candidate block with their locally trained, updated model gradient parameters along with the other emerging models updated successfully by other nodes similarly with the previous PoW operations. Then, they continue mining with the agreed-upon PoW and update their model parameters likewise obtained from the next local epoch operations until their models converge to a solution (with a minimised loss function) that satisfies a targeted accuracy rate, Acc, (i.e. $|w^G - w^{G-1}| \leq \epsilon$ where ϵ is a very small value). The last blocks during the training process with block mining, which stores each resident's individual aggregated local model updates, are added to the blockchain with their block headers and block bodies as a distributed ledger (Fig. 3), and downloaded by other residents, R, as nodes in the blockchain to carry on the next PoW operations with a newly generated candidate block. The body of the block has the last generated hash key corresponding to the individual resident model. In other words, all the updated particular models are transferred to the last block with the hash keys that are used to update the gradients for those models. All candidate blocks belonging to the nodes in the network are owned by all other nodes (i.e. CandidateBlocks = Blockchain(ID_{MoCap}).nodes.candidateblocks) as well as the last successfully added block (i.e.

Algorithm 2: Individual authentication and verification modelling per immersive device: Global update with blockchain.

Data: System input: *meR* & ID_{MoCap} & Blockchain(ID_{MoCap}).genesis & PoW & VotingThreshold
Data: Instant input: Blockchain(ID_{MoCap}).nodes & $UpdateQueue$ & ContinueUpdate
Result: & $meR.M_{ID}$ & ledger

```
=> Blockchain node assignment;
Blockchain(ID_MoCap).nodes += meR;
=> Nonce mining and global model update;
while (ContinueUpdate == true) || (UpdateQueue.Size > 0) do
    if (UpdateQueue.Size > 0)) then
        => Get the gradient updates from the queue with FIFO;
        UpdateParameters = UpdateQueue.updateparameters;
        => Download the last added block;
        LastAddedBlock = Blockchain(ID_MoCap).lastblock;
        => Get all the candidate blocks from nodes;
        CandidateBlocks = Blockchain(ID_MoCap).nodes.candidateblocks;
        => Place the global updates in the candidate block;
        Blockchain(ID_MoCap).nodes(meR).candidateblock.body (meR) = UpdateParameters;
        => Send the candidate block to all nodes in the blockchain PoW;
        Blockchain(ID_MoCap).nodes.candidateblocks += Blockchain(ID_MoCap).nodes(meR).candidateblock;
        => Run consensus hash generation mechanism to achieve a hash smaller than the target value based on the difficulty of PoW;
        while (ContinueUpdate == true) || (UpdateQueue.Size > 0) do
            hash = PoW.Operations;
            if (hash < PoW.difficulty) then
                => Hashing is achieved. Inform all other nodes;
                Blockchain(ID_MoCap).newhash == hash;
                Blockchain(ID_MoCap).newblock = Blockchain(ID_MoCap).nodes(meR).candidateblock; => New block is added to the
                  ledger if it is authentic;
                VotingPercentage <== Alg. 3 <== (LastAddedBlock & Blockchain(ID_MoCap).newblock);
                if (VotingPercentage > VotingThreshold) then
                    Blockchain(ID_MoCap).ledger += Blockchain(ID_MoCap).newblock;
                    => Delete the updated parameters from queue;
                    UpdateQueue.first.Delete;
                else
                    => Block is not added as new block;
                    message("The block is not found as authentic and not added as new block");
                end
            else if (Blockchain(ID_MoCap).newhash.state == true) then
                => Hashing is achieved by another node;
                => New block is added to the ledger;
                Blockchain(ID_MoCap).ledger += Blockchain(ID_MoCap).newblock;
            end
            else
                => Continue hashing;
            end
        end
end
```

LastAddedBlock = Blockchain(ID_{MoCap}).lastblock) before performing the next PoW operations and the added next last block with the successful hashing cannot be altered by adversaries, which is an obligation in our algorithms to add the successful candidate block to the distributed ledger and to continue the following PoW operations (i.e., $VotingPercentage > VotingThreshold$). GAN attacks, where malicious model weights with ungenuine epochs are generated by adversaries to compromise/poison the integrity of targeted models or to create synthetic identity, are prevented using the majority voting mechanism and placing the genuine candidate block with genuinely trained weights on the blockchain. In this way, the acceptance of altered candidate blocks generated by GAN attacks or malicious

Algorithm 3: Determining the authenticity of the added nodes by detecting malicious nodes.

```
Data: System input: Blockchain(ID_MoCap).nodes
Data: Instant input: LastAddedBlock & Blockchain(ID_MoCap).newblock
Result: VotingPercentage
AuthenticityNum = 0;
=> Voting by nodes for the trustworthiness of the new block;
foreach node ∈ Blockchain(ID_MoCap).nodes do
    if (LastAddedBlock ∈ Blockchain(ID_MoCap).newblock) then
        => The block is tagged as "authentic";
        AuthenticityNum += 1;
    else
        => Malicious node;
        AuthenticityNum -= 1;
    end
end
return VotingPercentage = (AuthenticityNum * 100) / num(nodes));
```

nodes is avoided by detecting altered candidate blocks. Moreover, SPoF is prevented where genuine copies of model updates with the candidate blocks as well as the last added block are owned by all nodes and the most recent model updates are already placed on the distributed architecture (distributed ledgers) of the blockchain. All the other residents/miners quit the current PoW operations when they receive the new block that is added to the blockchain to download this block and start the PoW operations from scratch, with the most recent updates using their candidate blocks with their updates, which are distributed to all other nodes. During this process, every resident, who performs the PoW for his/her model update parameters with a successful hashing, verifies all the previous model updates with the previous PoW operations as well, which are updated by other residents for their model training. The residents whose models have converged to a solution either stop the PoW operations and leave the mining as a node or continue as is to verify other residents' model updates with their current, successful updates, without providing further input updates – considering that the mining reward is still applicable even though data reward is no longer offered. The creation of blocks in chronological order, through the PoW consensus mechanism per ID, stops when no resident remains as an active node, where all the models of residents – per ID – that are expected to be completed as new nodes get added to the blockchain to build their models. Local model updates for all residents as nodes are aggregated at the last block separately, leading to final global models that correspond to individual residents. In other words, the blockchain expands further when new residents join the MetaCyberCity or UMaaSs. Users are not allowed to be successful for two consecutive PoW hashing in order not to verify their own model updates, which aims to include multiple verifications with distributed ledgers with timestamps. The final block is composed of the final aggregated individual models of residents per ID as in Eq. 2 for ID, MoCap, until new nodes join.

$$M_{ID_{MoCap}} = \left\{ R_{1_{(M_{ID_{MoCap}})}}, R_{2_{(M_{ID_{MoCap}})}}, R_{3_{(M_{ID_{MoCap}})}}, \ldots, R_{size_{(M_{ID_{MoCap}})}} \right\} \tag{2}$$

Residents upload their local true gradient updates (w^L) to form their model truthfully online epoch by epoch as instances are generated, with the required timestamp history where models, generated using false parameters, cannot result in authenticating the model owners during the use of the particular immersive device. Every entity feeds the DL model training process with the model-specific encrypted parameters until the model converges to a desired solution within a UMaaS or MetaCyberCity. The original user data is retained with the data owner and not shared with third parties and all the communicated packets are delivered between the entities using P2P/E2E ciphertexts (Fig. B.11) to avoid any possible data leakage, which aims to preserve both the data's sovereignty – and privacy, to a certain extent. Updated gradients may reveal individual private or actual information when associated with data attributes and structures. Therefore, encryption mechanisms provide further privacy protection even though the updated gradients or communicated packets have been anonymised. The above operations are repeated for all ID using different blockchain forms. The above operations, i.e., the creation of models per immersive device, needs sophisticated high-powered computing devices due to the intensive computations and significant energy consumption as discussed in Section 9. All of these operations cannot be performed on battery- and computation-constrained wireless wearable and immersive devices alone. Therefore, in our training model, only instances with attributes are acquired using the immersive devices and the remaining work is offloaded to the high-powered GPU-supported computing devices as elaborated in Section 4.

Global gesture models, which are verified by other residents in the MetaCyberCity or UMaaSs and employ a PoW consensus mechanism, are employed to be used for authentication mechanisms as proof, which has been implemented in Alg. 4, regularly during the metaverse immersive actions/activities, when requested by any active user in UMaaSs, or when required under particular circumstances such as before completing asset transactions to ensure the identity of the other party. While the training process requires sophisticated hardware as elaborated above, the implementation of identity checks using the pre-trained model does not require high-computing power and ordinary wearable and immersive devices can be employed to perform the authenticity of transactions and identity verification of the citizens using the models in the last block. In our approach, the use of the model to authenticate a resident with the blockchain-based model can be allowed by the resident using the private key and the last hash key that is associated with the particular user-/device-based model in the body of the block. Here, the blockchain is employed to provide trust among entities in modelling gestures using every online training phase automated by ID, i.e. epoch, by avoiding SPoF regarding the training in a central server and not requiring a trusted third party for the verification of the authenticity of the model and data from which the model is generated. From a more technical standpoint, the gesture feature set for particular attributes from the particular immersive device, $F = \{A_1, A_2, \ldots, A_{size}\}$, of the resident entity, $R = meR$, need to be run with the model using a couple of sample size, $S = \{F_1, F_2, \ldots, F_k\}$. The model results in either

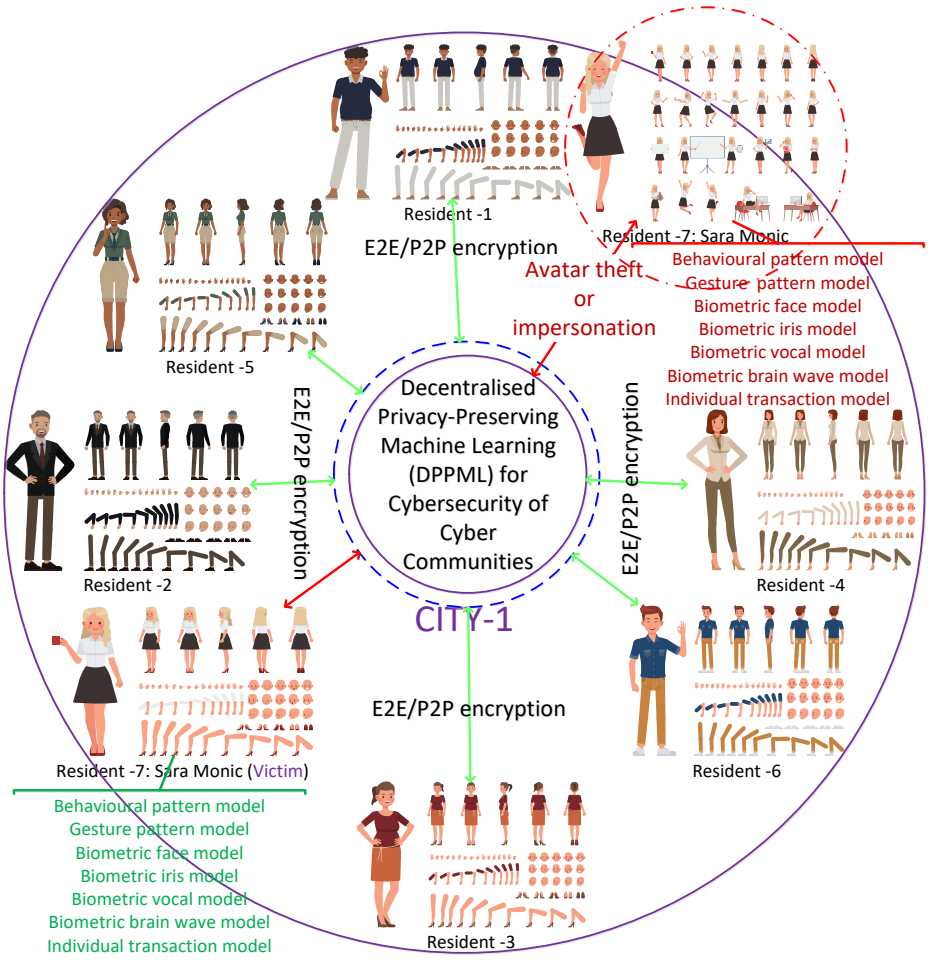

Figure 4. Detection of avatar theft (Section Appendix B.1.4) and identity impersonation (Section Appendix B.1.1). Quarantine of a harmful user to avoid possible cyberattacks.

providing the authentication proof with a successful outcome where one of the feature sets is recognised or rejecting the authentication with an unsuccessful outcome with no recognition for any of the attribute sets in the sample array. Each entity knows nothing about the trained data and its providers' identity while using the global ML models in an automated manner with the entity parameters to get a targeted classified outcome needed. The global model construction and use of this model should ensure that there is no adversarial entity collaborating with the process, which can be avoided using effective E2E/P2P encryption mechanisms (Fig. 4). These gesture models, aiming at authenticating the other party through the use of immersive devices, can be instrumented effectively against the theft of credentials, identity, or avatars. Regular biometric checks can be implemented with the proposed approach to ensure that the avatar in action represents the intended correct person. While using the trained models, the authenticity of the transactions is verified through real-time biometric verification and deployment of malicious AI-generated biometric models in decentralised blockchain ecosystems is prevented. To summarise, blockchain technologies and FL are

Algorithm 4: Proof of identity using blockchain-based DPPML pre-trained models with immersive devices where $ID = ID_{MoCap}$.

Data: System input: $M_{ID_{MoCap}} = \left\{R_{1_{(M_{ID_{MoCap}})}}, R_{2_{(M_{ID_{MoCap}})}}, R_{3_{(M_{ID_{MoCap}})}}, \ldots, R_{size_{(M_{ID_{MoCap}})}} <-- Blockchain(ID_{MoCap})\right\}$
Data: Instant input: $F = \{A_1, A_2, \ldots, A_{size}\}$ & $S = \{F_1, F_2, \ldots, F_k\}$ & $R_{me_{(M_{ID_{MoCap}})}}$ & $meR.PrivateKey$ & $R_{me_{(M_{ID_{MoCap}})}}.meR.hash$
Result: True & False & NoModel & NotSufficientlyTrained

```
bool ModelVal = False;
=> Find the user model;
R_me(M_ID_MoCap) = Blockchain(ID_MoCap) <-- (meR.ID);
=> Proceed only if the user has a trained model;
if (R_me(M_ID_MoCap) = Null) then
    => The user has no pre-trained model for this immersive device;
    return null;
    exit;
else
    => Proceed only for the authorised user with correct credentials;
    IsCredentials = R_me(M_ID_MoCap) <-- (meR.PrivateKey, R_me(M_ID_MoCap).meR.hash);
    if (IsCredentials = True) then
        => Check if the model is trained sufficiently (Acc, (i.e. |w^G − w^(G−1)| ≤ ϵ);
        if (R_me(M_ID_MoCap).LearningState == NotSufficientlyTrained)) then
            return NotSufficientlyTrained;
            exit;
        else
            => Test the samples with their features until it returns a true value;
            foreach (F ∈ S) do
                ModelVal = R_me(M_ID_MoCap) <-- F = {A_1, A_2, ..., A_size};
                if (ModelVal == True)) then
                    => Identity is proved;
                    return ModelVal;
                    exit;
                else
                    => Continue testing with next features (F) in samples (S);
                end
            end
            => False is assigned to ModelVal if no true value is not returned for any attribute set;
            => Most probably, the credentials have been stolen;
            return ModelVal;
        end
    else
        => The user credentials are not verified to run the model;
        => Either the credentials are wrongly entered or the avatar is impersonated;
        return 0;
        exit;
    end
end
```

merged using the metaverse immersive devices in the developed methodology (i.e. UMetaBE-DPPML) not only to eliminate the requirement of a trusted third party for the verification of the authenticity of transactions and immersive actions, but also, to avoid SPoF with the distributed architecture of the blockchain and GAN attacks by detecting malicious nodes.

4. EXPERIMENTAL SETTINGS

The experiment was designed to test a cybercommunity environment with 30 independent nodes in a co-simulated environment. 2 users with MoCaps, indicating 2 nodes (Node-A and Node-B) were incorporated into the co-simulation. Miners were rewarded with 20 cybercommunity crypto coins for each mined block. 2 powerful laptops (processor: 13th Gen Intel(R) Core(TM) i9-13950HX, 2.20 GHz; RAM: 32 GB; cores: 24) were used by Node-A and Node-B and 1 workstation (processor: Intel Xeon Platinum 8280; RAM: 2.70 GHz; RAM: 128 GB; cores: 28; boosted: NVIDIA RTX 8000) server was employed to simulate the remaining 28 nodes in the co-simulated environment. Each simulated node was assigned to one of the cores of the workstation as an individual device. The nodes first trained their local models and then the global models as explained in Section 3. After exchanging and confirming every local model update, miners/nodes execute the PoW. After reaching the PoW successfully, a new block, that records the verified local model updates, is created. Ultimately, the block that is created and contains the total number of local model updates is added to the distributed ledger. The candidate blocks of the other nodes, that cannot reach a successful PoW, are discarded and the last added block to the blockchain is downloaded by nodes for the next PoW execution. The process ended when the gesture models of Node-A and Node-B converged to a solution where the gesture training accuracies were over 0.95. The gesture models for other simulated nodes were not trained for mined blocks while they were mining. The training was conducted using the off-the-shelf Bidirectional Long Short-Term Memory Recurrent Neural Networks (Bi-LSTM-RNN) technique with the parameters presented in Table 2. As a kind of RNN and against the regular RNN suffering, vanishing and exploding gradients, LSTM-RNN was first introduced by Hochreiter et al. [47]. LSTM-RNN can memorise long-term dependencies between consecutive time steps of a sequence [48] using three gates network structure as an inherent memory storing the past information, namely, input, forget and output, by which the information at the cell state used for maintaining long-term information in the hidden layer can be updated selectively using a “receive” and “delete” dynamic process within LSTN-RNN. Furthermore, Bidirectional LSTM RNN (Bi-LSTM-RNN) with forward and backward manner introduced by Schuster and Paliwal [49] can observe complete information and establish temporal dependencies from past and future information in each sequence. Readers are referred to our previous study [50] for more information about the Bi-LSTM-RNN technique. The PoW difficulty (Line 19 in Alg. 2) is reduced significantly to decrease the PoW operation latency and complete all the operations readily in the simulation. It is worth noting that this difficulty can be adjusted accordingly with respect to the number of residents in a real-world cybercommunity considering the block generation rate.

Table 2. Parameters in Bi-LSTM-RNN [50].

Parameters	Values	Explanation
Layers	- sequenceInputLayer = 1 - bilstmLayer =100, - OutputMode = last - fullyConnectedLayer(2) - softmaxLayer - classificationLayer	- sequence input with 1 dimensions - bidirectional with 100 hidden features - output the last element of the sequence - 2 fully connected layer, two classes - softmax layer - classification layer
Epochs	- MaxEpochs = 40	- 40 times over the training dataset
Batch size	- MiniBatchSize = 50	- 50 Iteration (training pulses) per epoch
Learning rate	- InitialLearnRate = 0.01	- accelerate the learning process
Sequence length	- SequenceLength = 1000	-split the input pulse into smaller sizes, -easier processing by computing device
Curve threshold	- GradientThreshold = 1	- prevent the curve from getting too large
Environment	- ExecutionEnvironment = GPU	- use GPU for processing
Process monitoring	- plots = training-progress	- show the training iterations as processed
Progress	- Verbose = true	- show the data output

5. RESULTS

The required number of epochs to train the models of Node-A and Node-B was 47 to reach the desired accuracy rate of 0.95. All nodes, mining the blocks, almost received a fair distribution of rewards/coins. The system checks the gesture models when the nodes connect to the system or before every transaction. The system can trigger an alert when Node-A connects to the system using the credentials of Node-B and vice versa it can detect Node-B when connected by the credentials of Node-A. The system can discern genuine nodes and impersonated users by analysing their gesture models without requiring a third party to authenticate.

6. THREATS ADDRESSED USING THE PROPOSED APPROACH

The cyberthreats in the urban metaverse ecosystem and the basic measures to mitigate some of these threats are explored in Appendix B in detail. The main threats that can be launched in urban cybercommunities are demonstrated in Fig. 5 (highlighted in red). The threats that can be addressed as well as the threats that cannot be addressed by the proposed approach in this paper are summarised in Table 3.

Table 3 also shows the researchers where to focus their future research efforts to mitigate the other remaining gaps. The proposed approach can address the first four cyberthreats in Table 3, namely, “identity falsification & impersonation”, “identity theft and compromise of sensitive data”, “credentials theft”, and “avatar theft” whereas the remaining 11 threats cannot be addressed. These 11 threats, requiring individual attention and robust technical infrastructure abilities, can be mitigated with “practice of cybersecurity hygiene”, “agreed-upon standards, policies and

Table 3. Evaluation of the proposed approach in addressing the potential threats elaborated in Appendix B.

#	CYBERTHREATS	✓/-	NOTES
1	Identity falsification & impersonation	✓	Fake avatars and impersonated users may pretend to be another avatar or another person (i.e. identity forgery, dual identity) using biometrics such as facial features, and voice.
2	Identity theft and compromise of sensitive data	✓	High volumes of sensitive personal data (e.g. biometrics for generating fake avatars, financial information, health-related information, sexual orientation and race for spear phishing and generating identity forgery) can be stolen and exploited severely, particularly for financial gain, posing a high risk to users' real-world identities.
3	Credentials theft	✓	Stolen encrypted credentials including wallets with assets on the blockchain can be used to make unauthorised purchases and to launder money through stolen metaverse accounts.
4	Avatar theft	✓	Stolen avatars, i.e. virtual persona, can be controlled by cybercriminals in the name of the persona to be used for cyberattacks, harassing other users, spreading misinformation, or engaging in other harmful activities, tarnishing the reputation of the avatar's real counterpart, and money laundering purposes with cryptocurrencies.
5	Asset theft and asset fraud	-	Assets like digital currencies, NFTs, virtual items, and real estate purchases will be the primary targets of money-driven cybercriminals for the purposes of theft and fraud. The falsification of digital assets (i.e. virtual forgery) for fraudulent transactions can be readily performed using high-level imitation technologies. Fake digital assets such as non-existent properties, services, and fraudulent cryptocurrencies can be traded with promises of unrealistic returns.
6	Brand/business theft and business impersonation	-	Virtual businesses can be hijacked for the purpose of ransom. Hijacked businesses/stores can be used to obtain user financial gains and credentials. The false version of shops can be created either to damage the brand's reputation or to exploit the reputation from a financial perspective.
7	Cyberbullying, misuse of the platform	-	An urban metaverse ecosystem is an ideal space for antisocial behaviours such as cyberbullying, sexual assault, and fraud. These crimes, impacting emotional and mental health, can be committed by avatars with fake identities and may not be traceable regarding data sovereignty.
8	Phubbing and societal concerns	-	The reduction of real, urban physical social interactions replaced by virtual experiences using avatars within urban metaverse worlds may cause unforeseen negative effects and new types of psychological problems (e.g. the feeling of loneliness, social segregation, social exclusion).
9	Phishing attacks	-	Cybercriminals might create fake metaverse platforms that mimic popular metaverse cyberspaces using AI-generated bots and then use phishing techniques to trick residents into providing sensitive information, such as financial details.
10	Social engineering & Disinformation/Misinformation	-	Residents can be manipulated into taking malicious actions based on their interests, their sensitive information and their way of thinking. It might be difficult to distinguish between truth and disinformation/misinformation as urban metaverse spaces look like realistic environments.
11	Ransomware	-	The strategy for a ransomer is to gain access to a system, insert their software which takes control of the system, and demand payment in exchange for not deleting the information. Urban metaverse worlds, businesses, assets and even avatars can be hijacked for ransomware purposes.
12	Privacy breaches	-	Body signatures (i.e. digital footprint) based on the somatic data, physiological emotion recognition and behavioural signatures (e.g. emotion recognition, reactions to developing events) are inevitably exposed as we engage in using highly immersive technologies, particularly, with VR/AR/XR headsets, leading to serious privacy violations (e.g., advertisements, content management). Physical privacy (e.g. personal boundaries) can be invaded using avatars.
13	Distributed Denial of Service (DDoS) attacks	-	Metaverse urban cyberspaces composed of distributed devices and services using wireless communication technologies can be interrupted easily using jammer-type devices, leading to severe prolonged signal outages.
14	VR/AR headset intrusion	-	Vital signs (e.g. heart and respiratory rates) can be detected through smart devices and AR/VR sets. The privacy of users will be violated substantially when a hacker gains access to a user's VR/AR headset, sharing your life with you and seeing every part of your life.
15	Generative Adversarial Networks (GAN)	✓	GAN, using generative AI approaches, may cause the generation of unhealthy, highly realistic synthetic trained models, which can disrupt/interrupt automated metaverse services and infiltrate behind/through services to gain access to the environment to exploit sensitive, private data.

ethics", "automated detection of platform infrastructure security flaws", "automated detection of OotPAs", "awareness of cybercriminal experiences and best practices", and HE as elaborated in Appendix B.2. What makes the first four threats (Table 3) most vulnerable and not readily addressable with the aforementioned measures is that we can

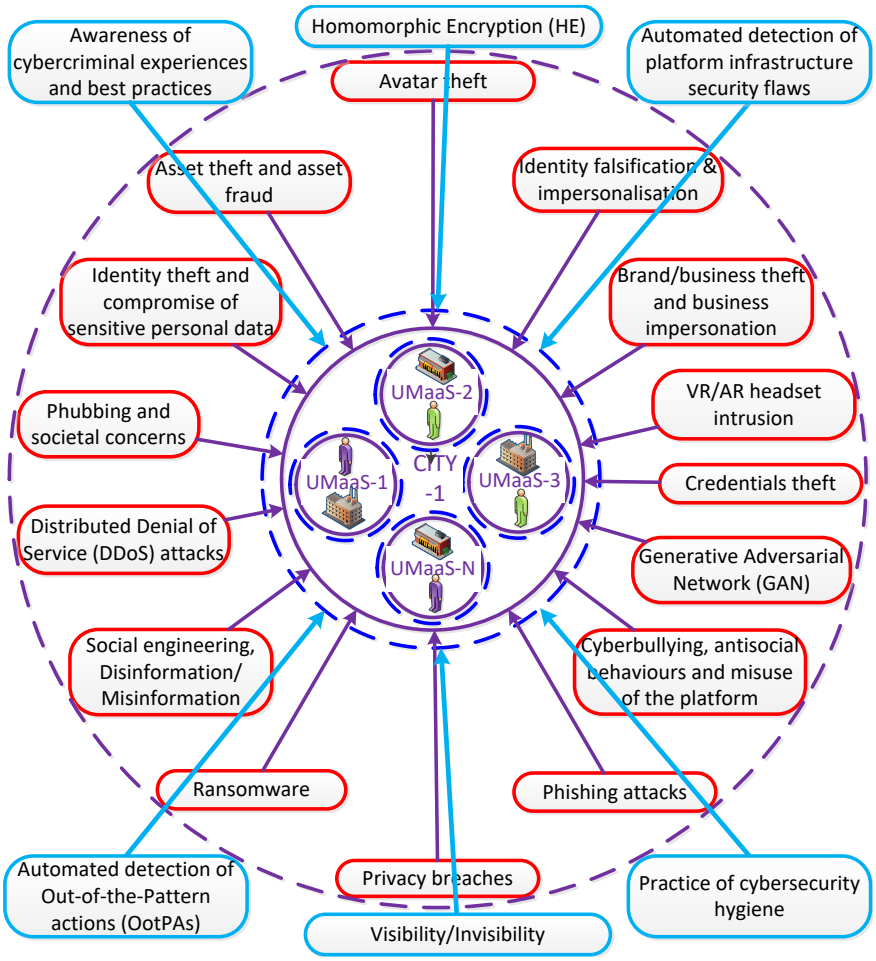

Figure 5. Cyberthreats against urban metaverse cyberspaces (red) and basic countermeasures (blue) (elaborated in Appendix B).

easily incline in the demands of our friends, colleagues, relatives, thinking that we are safe around them, leading to let down our guards. In this direction, this paper focuses on the solutions to the threats that cannot be readily addressed by the aforementioned measures (Appendix B.2, measures highlighted in blue in Fig. 5).

7. CHALLENGES

Cybersecurity measures in the urban metaverse cyberspaces encounter a unique set of challenges due to the immersive nature of these spaces. Major regulatory, technical, and cybersecurity challenges can be summarised as follows:

7.1. REGULATORY CHALLENGES

- The regulatory framework in performing user profiling, which processes the biological and biometric data, changes from one region to another and from one country to another. For instance, the General Data Protection

Regulation (GDPR)[3] in the EU, the California Consumer Privacy Act (CCPA) in the USA, and Cyber Security Law and the General Principles of Civil Law in China, in which entities are supposed to comply with certain rules, regulations, and permissions before processing personal data, are performed to protect the privacy and security of individuals. Implementing those diverse ranges of regional regulatory frameworks eases data sharing on a regional base, but data sharing and user profiling are extremely difficult in decentralised urban metaverse worlds by processing individual-specific data scattered all around the world on a global base. A global cross borders/nations consensus on data protection policies between regions/countries would ease the upholding of accountability and responsibility of stakeholders. Furthermore, these cross-border regulatory frameworks should regulate the features of the metaverse immersive devices and tools at the developer side, e.g. what they can do and what they can't do considering privacy, security and accountability.

- The other related laws such as copyright, intellectual property, and consumer protection should be updated to encompass the metaverse technology to protect the digital rights (e.g. digital assets, NFTs, crypto money) of the users.
- How avatars and their counterparts regarding accountability and responsibility are required to be treated from a legal standpoint is still unknown, which is not a question that can be readily answered by legal authorities alone, but other authorities and disciplines such as philosophers, and psychologists as well.
- Furthermore, the aforementioned similar regulatory framework, in which data transfer from the EU to outside and from outside to the EU is restricted, hinders the interoperability of the metaverse cyberspaces through which avatars and their associated data, as well as assets, are supposed to teleport for seamless management of diverse metaverse cyberspaces. For instance, a resident of a city in a country should be able to be a resident of another city in another country using his/her avatar as a guest/visitor resident for touristic purposes or attending events (e.g. concerts) or using the democratised skills/assets (e.g. DAOs).

7.2. TECHNICAL CHALLENGES

- Metaverse comes with a challenge, who is going to control it? Does it need to be controlled? What happens to the service provider if the user gets damaged physically, psychologically or financially from the perspective of accountability with responsible metaverse?
- QC, with easy-to-decrypt abilities, can help hackers in cracking blockchain-based hash keys, reaching our wallets, and sensitive data.

[3] https://gdpr-info.eu

- Only the centrally owned data can be processed to generate global models in urban metaverse communities where user-owned data cannot be included in decision-making without their consent regarding the data sovereignty, which may reduce the efficacy of ML models in decision-making and can cause overfitting in real-world use cases.

- Apart from the adversary attacks, CL, using distributed gradient updates from multiple entities, may suffer from "accuracy loss" compared to the processing and training of data centrally, which may lead to the overhitting of learning networks in real-life implementations as well. This shortcoming may be compensated by inputting more data instances with high-quality attributes.

- The urban metaverse cyberspaces may not be scalable enough to accommodate many avatars to immerse. It might be extremely difficult to provide the continuity of urban cyberspaces concerning the high number of residents in a city. Furthermore, AI-generated avatars (i.e. bots) submitted to cyberspace, by cyber attackers as a malicious attempt can disrupt services easily.

- Gesture signatures can be changed depending on the diverse range of metaverse immersive technologies (e.g. VR/AR headsets, MoCaps, haptics gloves, HTT, different types of WSs), which employ different types of sensors, sensor parameters, and calculation parameters. Therefore, pre-trained DL gesture models, which are used for authentication purposes, need to be trained from scratch when the immersive devices have been replaced with other brands to ensure that the correct models are evaluating the correct attributes acquired from the correct parameters. Industrial standardisation of immersive technologies would make the metaverse life extremely easy in many aspects.

- Transaction throughput, transaction confirmation delay, and block capacity are the three key challenges in moulding AI and blockchain technologies in an effective way [51]

7.3. CYBERSECURITY CHALLENGES

- The metaverse cybercommunities, using decentralised data structures on private and public ledgers and interoperability architecture, may not be managed by a single entity which makes it more difficult to track down and stop attackers. Therefore, it is more important to detect possible cyberattacks and avoid deceptive activities proactively, with preventive solutions where it may not be possible to take fraudulent transactions back. This objective was the main motive of this research.

- In scenarios with stronger privacy protection requirements, some cryptographic schemes with higher security are applied to the blockchain system, which improves the degree of privacy protection and reduces the transaction efficiency of the blockchain system [51].

8. LESSONS LEARNED

The main regulatory, technical, and cybersecurity lessons learned during this research can be summarised as follows:

8.1. REGULATORY LESSONS

- The urban metaverse ecosystem is evolving rapidly and national, regional, and global regulatory frameworks are presently incapable of being adaptive to the developments of this ecosystem. The regulatory framework within a resilient evolution path can be adjusted to meet the requirements of the very dynamic nature of this ecosystem in a way of encouraging the development of this technology towards change and closing the door for cybercriminals. In this direction, the metaverse urban society, businesses, stakeholders with conflicting objectives, and universities, including psychologists and philosophers, should be engaging with the regulators in order to create a better vision for the society and to guide them properly not only from a technological perspective but also from a societal perspective in upgrading the regulatory framework appropriately.

- A collective global legislative framework is essential to provide residents with trustworthy cyber worlds by preventing harm and by punishing the people who are accountable for their improper actions, particularly on the public ledger, especially considering the guest residents with their avatars all around the world.

- Incorporating data, especially for training purposes, into the processing of SAI should be based on laws and regulatory frameworks in the sense of protecting users' privacy and anonymity.

- Governmental policies should be regulated to encourage the development of metaverse cyberspaces and help remove the barriers in front of the development of functional urban metaverse worlds.

8.2. TECHNICAL LESSONS

- New digital products and services, that we do not know of yet, will be presented in urban cyberspaces. New business models will emerge within urban metaverse cyberspaces, where the way of doing business both digitally and physically will change significantly with new products and services.

- AI-generated bots equipped with advanced speech recognition abilities will be replacing the governmental and business-type staff to perform many types of procedures, which may decrease service costs and increase the quality of services 24/7 basis.

- The infrastructure of urban cyberspaces should be tested before accommodating immersive experiences with an increasing number of avatars using AI-generated avatars concerning the high computational resource requirements to process the 3D nature of the urban metaverse worlds, high volume of data for insights and instant bidirectional flow of interaction to measure if the scalability is sufficient for the targeted experiences.

- In urban metaverse cyberspaces, residents should decide how their data would be managed and processed through individual policies where residents are the owners of their data stored on public and private ledgers, not governments. More explicitly, personal data is the property of individuals and residents of urban cyberspaces can decide who is allowed to enter their property.

- The urban metaverse industry must work together in a fruitful collaboration to create robust security frameworks for wearable immersive metaverse devices such as VR/AR devices or MoCaps, cyberspaces, and applications.

- SAI suffers from the inaccurate global aggregation of BD due to privacy and security concerns. The approaches, an example of which proposed in this study, which protects the privacy and security of users will be a primary incentive to contribute to the global models where users can benefit from generated global models considerably, if they become a part of these models with their small scale of contributions.

- Existing 5G technologies are still far from supporting real-time holographic video streaming [52]. The fuse of QC with an exponentially increasing computation power and 6G technologies is expected to provide the residents with highly powerful computing and communication environments, which would boost the QoE significantly with urban metaverse worlds, particularly with worlds requiring high-quality edge computing and edge intelligence – such as holographic construction, emulation, and communication [1].

- 6G, expected by 2030 [35], as a key pillar in developing metaverse technologies, would significantly enhance seamless genuine immersive experiences [4], -[53] along with QC, paving the way for fast data processing for wisdom/insight extraction at the edge. In other words, the integration of 6G-enabled AI with FL as next-generation wireless E2E intelligence communication would integrate us with more realistic, real-time intelligence by unlocking the potential of BD [1].

8.3. CYBERSECURITY LESSONS

- As users create and share a large amount of personal information within the urban metaverse cyberspaces, privacy becomes a top priority for users, developers, and platform operators. With this in mind, developers and platform operators must implement strong data protection, secure data storage and comply with relevant privacy regulations. Privacy protection in urban metaverse worlds will be an active research field (Ex: [54]) where generated data is owned individually by their producers.

- Both decryption and encryption of personal data by utilising strong encryption protocols are paramount to protect oneself from data leakages and unauthorised access. The use of biometric identities will increase in the future for establishing better authentication systems, particularly on public ledgers. This issue is the main focus of this research.

- Multiple-factor authentication (MFA) and sophisticated Identity Management Systems (IMS), one of which is proposed in this paper, can help protect users from unauthorised access or identity theft.

- Since the metaverse allows users to create content, it's important to have content management tools equipped with AI in place to stop the spread of inappropriate content in real time and appropriate precautions should be taken against the sources of these types of content by using robust AI-driven monitoring techniques and detecting suspicious activities and incidents in an automated manner.

- Urban metaverse cyberspaces should allow performing a diverse range of cybersecurity checks to measure the system's cybersecurity level, leading to revealing the weak points to improve.

- Urban metaverse cyberspaces need to ensure that every resident can access the cybercommunity, regardless of their social position, income or technical skills and they are protected against cybercriminals.

- All the assets can be lost if the private key, which is kept in the individual wallet, is lost or a mistakenly approved transaction cannot be taken back, where there is no central authority to intervene. Therefore, cybersecurity is more important in this platform on Web3 when compared to Web2.

- Improving the system throughput of public blockchains (e.g. supply chain, healthcare) is highly demanded [55] where distributed consensus protocols for blockchain networks can execute a limited number of transactions in a period (i.e., Bitcoin and Ethereum, can only process around 9 and 29 transactions per second, respectively) caused by the bottleneck problem in blockchain sharding, i.e. cross-shard transaction processing [55], [56]). For instance, Jiang et al. [55] propose an approach in public blockchains to securely perform an increasing

number of transactions in a short time in parallel with increased throughput by solving the shard scheduling problem in polynomial time. Similar studies will help incorporate blockchain technologies into a wide range of public domains.

- We can visualise an urban metaverse ecosystem in which insurance companies will take their indispensable part as in real life, particularly for ransomware attacks to protect the assets of users and businesses, which, in turn, will boost investments in metaverse cybersecurity solutions.

9. DISCUSSION

"When she leans back away from Da5id, his face has changed. He looks dazed and expressionless. Maybe Da5id really looks that way; maybe Snow Crash has messed up his avatar somehow so that it's no longer tracking Da5id's true facial expressions. But he's staring straight ahead, eyes frozen in their sockets [57]." Those exposed to unfathomable "Snow Crash" – a mysterious new drug and a linguistic/computer virus that has surfaced in both the virtual and the real world – in the metaverse experience their virtual avatars being "hacked" and rendered useless, which induces a state of catatonia in reality, making users susceptible to mind control and manipulation [58]. Through the development of the metaverse concept from the Sumerian myth (5500 - 1800 BC) and mind-altering novel, "Snow Crash" in 1992, to today's information age, human- and society-centred urban metaverse (HSCUM) worlds, i.e., human-cyber-physical worlds – an extension of residents and urban society where the virtual and the physically real blend and are more organically integrated within the CoW with CPSSs, are meant to mirror the fabric of urban life with no harm to their residents. Today, and every day, worldwide, one million more people are born-into or move-into a city [59]. The global population is expected to double by 2050 [60] and more than 68% of the population will be living in an urban environment by 2050 [61] with a population of 5 billion [62]. Metaverse worlds, enabling rich communication channels, have already become a part of our daily routine and an increasing number of people are embracing the growing number of metaverse worlds with immersive metaverse devices. Recent advances in metaverse technologies are providing many opportunities and urging city governments and all other stakeholders within an urban life to change the way of managing cities and doing business more intelligently in location and time-independent, high-fidelity virtual worlds [1] to alleviate the problems of rapid urbanisation with limited urban resources, such as increasing population, pollution, traffic, noise, real-estate/office prices, and mobility difficulties. Urban life has already embraced many urban metaverse use cases with future objectives (as elaborated in [1]) to increase the QoL by overcoming temporal and spatial restrictions, and the trend indicates that this would expedite exponentially in the years to come. Cybercommunities instilled with metaverse technologies should provide their residents with functional, safe, secure, and private worlds with high QoE to readily evolve and mitigate the problems of urbanisation. The near

future will embrace more metaverse applications fuelled by advancing immersive metaverse technologies, leading to a change in the way of doing business in the urban ecosystem [1]. Urban metaverse cyberspaces, as the main communication/interaction channel, will be connecting urban places and residents not only to one another within a city but also to the rest of the world. We visualise that residents will be spending most of their daily life in urban metaverse cyberspaces compared to real life for governmental interactions, socialising, or doing business in the years to come. Cities and their residents, who have abilities/skills/assets, can socialise, be creative and monetise their assets and time through this channel. These cyber worlds will be a target for cybercriminals to exploit as the economic value of these cyber worlds increases with their assets, and as the urge to reveal privacy via immersive devices is becoming a reality for residents, while controlling the boundaries of privacy is getting difficult with these devices. Municipalities are building their future with the concept of the metaverse and future urban cyber worlds are expected to evolve to be more immersive with advanced, real-time, data-driven, virtual/augmented dynamic platforms, devices, and hyper-realistic MetaHumans [1]. Our research question was if we can turn the abilities of these immersive metaverse devices into the residents' advantage in providing their security and avoiding a breach of privacy. In a broader perspective, if it is possible to build a trustworthy, urban metaverse cybercommunity, without requiring a centralised government to protect our privacy or a third party to mediate between entities, e.g. for a transaction. Regular identity authentication during interactions or before executing transactions in the urban metaverse worlds is crucial to address transaction authenticity, identity impersonation and theft of credentials, identity, or avatars and avoid their imminent adverse consequences. In this treatise, while the urban metaverse ecosystem is flourishing, this research analyses cyberthreats and basic cybersecurity control measures against those cyberthreats comprehensively within the urban metaverse ecosystem. It reveals the cybersecurity gaps within these environments in the literature and real-world implementations. Additionally, it designs a novel blockchain-based DPPML authentication and verification approach – the so-called UMetaBE-DPPML – to fill these gaps, based on physics-based characters of individuals (i.e. body cyber footprint/identity – e.g. facial expressions, movement patterns (gait), lip motion, emotional expression or reactions to experiences using physiological responses, voice pitch patterns/prints, and speech patterns) obtained from immersive metaverse wearable devices (e.g. VR/AR headset, MoCaps, haptics gloves, HTT). In this way, cyber signature models, with a diverse range of attributes, are built step by step, verified by other residents and placed in blockchain ledgers to be employed whenever needed to verify the authenticity of the residents/avatars even if all the credentials are in the hands of cybercriminals.

PPML/PPDL schemes in the literature have been introduced in Section 2.3. As explained in the literature, standard FL/CL model generation tools based on wearable devices can be provided by the main urban city, or the developers of the metaverse devices, to users to train their models in a standard way, through which messages can be communicated

Table 4. Comparison of the proposed approach with the developed methods in the literature.

Method		Technical aspects					Using					Measures against				
	Literature	No trusted third party	Data sovereignty	User privacy	Avoiding GANs	Avoiding SPoF	Body signature	Immersive devices	Online attribute capture	Alternative models	Reward	Identity impersonation	Theft of credentials	Theft of identity	Theft of avatars	Unreal Transactions
FL	[63]	-	✓	✓	-	-	-	-	-	✓	-	-	-	-	-	✓
	[29]	-	✓	✓	-	-	-	-	-	✓	-	-	-	-	-	✓
	[64]	-	✓	✓	-	-	-	-	-	✓	-	-	-	-	-	✓
	[40]	-	✓	✓	-	-	-	-	-	✓	-	-	-	-	-	✓
Metaverse oriented FL	[42]	-	✓	✓	✓	-	-	-	-	✓	-	-	-	-	-	-
	[65]	-	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-
Metaverse oriented blockchain based FL	[39]	✓	✓	✓	✓	✓	-	-	-	✓	✓	-	-	-	-	-
	[41]	✓	✓	✓	✓	✓	-	-	-	✓	✓	-	-	-	-	-
	[66]	-	-	✓	✓	-	-	-	-	-	-	✓	-	-	-	✓
	[67]	✓	✓	✓	✓	✓	-	-	-	-	-	-	-	-	-	✓
	[68]	✓	✓	✓	-	✓	-	-	-	-	-	✓	-	-	-	✓
	[69]	✓	✓	✓	✓	✓	-	-	-	-	✓	✓	-	-	-	✓
	[70]	✓	-	✓	-	✓	-	-	-	-	-	✓	-	-	✓	-
	[71]	-	✓	✓	-	✓	-	-	-	-	✓	-	-	-	-	-
UMetaBE-DPPML (Metaverse + Blockchain + FL)	Proposed	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

between the entities in an automated manner using advanced AI techniques. However, updated gradients may reveal individual private or actual information when associated with data attributes and structures. Therefore, encryption mechanisms provide further privacy protection. Secure queries on sensitive private data through the aforementioned models without revealing their contents are possible using an agreed-upon, encrypted subset of the feature vector. The content of the query or input for trained models can be verified, allowing for computation and then the result is returned based on an authentication mechanism, e.g. HE (Sections Appendix B.2.7). However, in addition to the inefficiency of homomorphic-based encryption, the authenticity of local or global models cannot be guaranteed without the authentication of a trusted third party. But, every third party within the urban metaverse ecosystem is untrusted, concerning privacy in particular, considering semi-honest parties or honest but curious parties. Moreover, the locally or globally pre-trained gesture models can be replaced by cybercriminals with their recently trained models instantly, particularly when the credentials of a user are hijacked. Therefore, a blockchain-based approach, which is elaborated in the following subsection, is proposed in this research. In this sense, the main urban entity (i.e. MetaCyberCity) and its cybercommunity entities (i.e. UMaaSs) (Fig. A.9) should be addressing the concerns of its residents appropriately, privacy concerns in particular, without requiring the authentication of a third party, while immersing themselves with urban experiences and executing their transactions. The proposed blockchain-based DPPML authentication and verification approach (i.e. UMetaBE-DPPML) in this research addresses those aforementioned concerns effectively and efficiently.

Considering the management of the identity definitions of an avatar/user, a balance should be established between

privacy and security without compromising privacy. Centralised systems (controlled by either a single organisation or a couple of organisations – i.e. federated), which control all the identity definitions of an avatar's single authentication token, have the obvious drawback of having a single target for malicious actors to focus their efforts on when compared to the management of SSI that is owned and controlled by the user in metaverse worlds. Although SSI is the targeted objective that gives all types of freedom and resilience to the user and the user is supposed to be privileged to fully control user-defined information and to have all the data related to this identity, trust in SSI within multiple metaverse cyberspaces along with the interoperability is the major challenge considering the generation of safe and interconnected metaverse worlds where audit trails are highly difficult to perform, if not impossible. Authentication of SSI by trusted cross-platforms and the interoperability of SSI through diverse metaverse cyberspaces will be the key research questions to be answered in the years to come in metaverse environments to realise the primary objectives of the metaverse.

Will a single authentication avatar token allow the user to access multiple metaverse virtual, urban worlds by enabling the user to travel between different metaverse cities? We do not have the red pill from "Snow Crash" to gain the ability to distinguish the illusion the Matrix creates from reality while engaging in cyber worlds. It is worth emphasising that it will be more difficult to differentiate what is real and what is not, where the real and the synthetic blend and are not readily distinguishable, due to the fact of experiencing events in metaverse environments with multiple of our sensors interacting with the events, leading to an increased susceptibility to manipulation. Therefore, users should be properly and appropriately trained based on their objectives in this ecosystem to be vigilant, particularly against frauds and to cope with the predicaments, particularly bullying and harassment. Then, the striking question comes forward: do we want to use the red pill to distinguish the real from the imaginary or the blue pill to remain ignorant so as to make ourselves more immersed in the environment?

Our research question was if we can turn the abilities of immersive metaverse devices into the residents' advantage in providing their security and avoiding a breach of privacy. In a broader perspective, if it is possible to build a trustworthy, urban metaverse cybercommunity, without requiring a centralised authority/government to protect our privacy or a third party to mediate between entities, e.g. for a transaction. We would like to point out the main contributions of our proposed approach considering the blockchain-enabled approaches in the literature elaborated earlier in Section 2.3. First and foremost, to the best of our knowledge, the proposed approach in our work is the first one in the literature employing metaverse immersive devices with blockchain technologies instilled with AI to authenticate users in urban metaverse environments. The following paragraphs elaborate on how our techniques differentiate from the main developed techniques in the literature and off-the-shelf techniques.

The approaches such as FL/CDL ([63], [29], [64], [40]) (elaborated in Section 2.3) provide the opportunity to

protect user privacy and data sovereignty while leveraging the combined intelligence of several dispersed nodes. However, they, requiring a third trusted body, suffer from GAN attacks and SPoF concerning the central aggregator server by relying on a single central server, which is vulnerable to the server's malfunction, which not only may put the entire process of thorough learning at risk, but also, may jeopardise the timely and trustworthy authentication and verification. Moreover. these approaches do not reward the local devices without providing rewards/compensation, such a device is less willing to federate with the other devices [39], which requires the generation of robust models. This research designs a novel blockchain-facilitated authentication and verification approach, based on physics-based characters of individuals (i.e. body cyber footprint/identity – e.g. facial expressions, movement patterns (gait), lip motion, voice pitch patterns/prints, and speech patterns) obtained from immersive metaverse wearable devices (e.g. VR/AR headset, MoCaps, haptics gloves, HTT). In this way, cyber signature models, with a diverse range of attributes, can be built step by step, verified by other residents and placed in blockchain ledgers to be deployed whenever needed to verify the authenticity of the residents/avatars by avoiding GAN attacks and SPoF even if all the credentials are in the hands of cybercriminals as explored earlier in Sections 4 and 5. Local modes are rewarded for their collaborations for the sake of the generation of robustly working systems as emphasised in Section 5.

In MP-CLF [40] and in the metaverse-oriented CDL approaches [29], the focus is on mitigating data leakage of CDL under the GAN attacks. Based on fully connected neural network learning, MP-CLF employs a matrix blinding technology to break the local modelling of the GAN attack by blinding specific model parameters and trainers' data, which is easily implementable and has strong security. Besides, MP-CLF builds a user partition model pre-training to improve training quality and strengthen model protection. The performed experiments demonstrate that MP-CLF can completely resist the GAN attack with good computational efficiency. In the metaverse-oriented CDL [29] using an adversary detection-deactivation method, malicious participants can hide within the major innocent and silently upload deceptive parameters to degenerate the model performance, or they can abuse the downloaded parameters to construct GAN to acquire the private information of others illegally. To compensate for these vulnerabilities, the approach proposes an adversary detection-deactivation method that can limit and isolate the access of potential malicious participants as well as quarantine and disable the GAN attack or harmful backpropagation of received threatening gradients. A detailed protection analysis is conducted on a multiview CDL case, and results show that the protocol can effectively prevent harmful access by heuristic manner analysis and can protect the existing model by swiftly checking received gradients using only one low-cost branch with an embedded firewall. In the privacy-preserving two-party distributed algorithm of backpropagation proposed in [42], the privacy concern of each data holder is preserved by extending the privacy preservation notion to original learning algorithms using multilayer neural networks, which allows training without requiring either party to reveal her data to the other. However, SPoF and the

requirement of trusted third parties are the main drawbacks of these approaches where no blockchain technologies are incorporated into the techniques. [65] proposes trustworthy semantic communications for the metaverse relying on federated learning.

In BlockFL, where the blockchain network enables exchanging devices' local model updates while verifying and providing their corresponding rewards, [39] locally trained ML models using the particular agreed-upon data instances are aggregated on the blockchain to build the targeted larger model to increase the accuracy compared to the locally trained models, aiming to avoid overfitting. To summarise, in BlockFL, the server entity in FL is substituted with a blockchain network. Although the data privacy is preserved with local model updates (i.e., learning model's weight and gradient parameters, from which the raw data cannot be derived) and SPoF is avoided in this way, the authenticity of local models cannot be verified (despite a validation process of the local training results utilised) regarding the genuinity of data instances if nodes are malicious. Moreover, in those types of approaches, the combined established models are accepted as correct and do not go through further verifications regarding any GAN attacks during the training process. In the blockchain-based FDPDDL [41], the developed techniques enable parties to derive more accurate local models fairly and privately by using the developed two-stage scheme. During the initialisation stage, artificial samples generated by differentially private GAN are used to mutually benchmark the local credibility of each party and generate initial tokens. During the update stage, differentially private stochastic gradient descent is used to facilitate collaborative PPDL and local credibility and tokens of each party are updated according to the quality and quantity of individually released gradients. The experimental results on benchmark datasets under three realistic settings demonstrate that FDPDDL achieves high fairness, yields comparable accuracy to the centralised and distributed frameworks, and delivers better accuracy than the stand-alone framework. It focuses on achieving higher accuracies in models. The blockchain-based Metaverse-AKA developed by [66] designs a lightweight and privacy-preserving seamless cross-metaverse authentication and key agreement scheme to realize the seamless cross-metaverse authentication and assure the users' privacy by achieving anonymity and unlinkability through a trusted issuer, enabling resistance to multiple attacks like impersonation attack, man-in-the-middle attack and replay attack. No training using FL is used to construct user-based models in Metaverse-AKA. [67] proposes an FL privacy-preserving approach (i.e. DRL-based DDA) in virtual industrial IoT (IIoT) blockchain technology to realize secure transactions by detecting attacks during operations. The developed virtual mobile device-based Metaverse scenario works on the privacy-preserving context inside an environment of IIoT supply-chain and achieves any transaction process without risking user private data. [72] presents a blockchain and a DT-enabled IoT software-defined networking (SDN) integrated framework for offering decentralised and secure data operations in IoT networks to address the generation of a vast amount of data, posing storage, processing, and security concerns, leading to significant improvements in latency and throughput.

[68] uses the blockchain concept to generate a hashed identifier from the node's IP and passes between nodes inside the path during the route discovery that provides assurance about the identity of the node and keeps the integrity of the exchanged information. More specifically, it proposes a secure wireless routing protocol based on blockchain technology to provide authentication and integrity to the network without adding extra processing that degrades the network's performance with extra overhead. As a secure system, the blockchain architecture and its properties provide verification features to the nodes and detect impersonation acts by a chaining mechanism. [69] proposes a secure blockchain-empowered FL framework with decentralised model aggregation (i.e., BF-Meta) to mitigate the negative influence of malicious users and provide secure virtual services in the metaverse by monitoring malicious clients with a real-virtual combined credit system based on the behaviours of the users and users' honest updates during training (i.e., the documentation of illegal behaviours). [70] develops a privacy-preserving, interoperable and decentralised authentication scheme for metaverse environments. [71] develops blockchain-inspired collaborative cyberattack detection for securing the metaverse. The proposed federated IDS implements a hybrid client selection (HCS) technique, considering the accuracy and reputation of client histories, to select high-quality metaverse edge devices.

The features of the above-mentioned similar studies in the literature are compared with the proposed approach (UMetaBE-DPPML) in this paper in multiple criteria. In our approach, every node creates his/her body signature model using the data instances that are generated automatically by immersive devices online. In other words, every epoch during training is verified by other nodes and weights in epochs are authenticated using the immersive device that is currently in use by nodes. The built models in our approach are verified by nodes with the newly created body signature datasets using immersive devices to find out if the model belongs to the individual. The main objectives in our approach are significantly different from those mentioned approaches in the literature. The main purpose of our approach is to build an approach (by preserving privacy and avoiding SPoF and GAN attacks without requiring trusted third parties) that checks if an active avatar/user in the metaverse ecosystem represents the genuine counterpart. Regarding the protection of privacy specific to the urban metaverse ecosystem, our methodology aims to preserve the multidimensional aspects of privacy as delineated in Fig. 2 whereas the above-mentioned approaches in the literature aim to cover the data privacy (i.e., contents of data instances and their attributes) during the training of models. What makes our approach heads and shoulders is its enabling measures against unreal transactions, identity impersonation and theft of credentials, identity, or avatars.

It is worth emphasizing that the PoW is integrated into our experiments during the test of the proposed approach in the study. The PoW mechanism is known for its significant energy consumption considering block times and transaction propagation and relatively high latency considering intensive computations requiring powerful GPUs compared to alternatives. In this regard, the processing of the PoW on the hardware of wireless wearable and immersive devices is

a challenging issue concerning their computation and battery limitations. To compensate for energy consumption and latency in our tests, the computation is offloaded to the high-powered GPU-supported computing devices as elaborated in Section 4 and the PoW difficulty (Line 19 in Alg. 2) is reduced significantly to decrease the PoW operation latency and complete all the operations readily in the simulation. The difficulty can be adjusted accordingly with respect to the number of residents in a real-world cybercommunity considering the block generation rate. Alternative consensus mechanisms like Proof-of-Stake (PoS) have emerged as more energy-efficient and potentially faster. The use of the PoS mechanism with our techniques will be performed in our future work as specified in Section 11. The concerns over energy consumption and latency are expected to be mitigated significantly with the use of the PoS. Still, the processing needs to be offloaded to high-powered computing devices from battery- and hardware-constrained wearable and immersive devices. On the other hand, while the model training process requires sophisticated hardware, the implementation of identity checks using the pre-trained model does not require high-computing power and ordinary wearable and immersive devices can be easily employed for this process.

10. LIMITATIONS

The particular DPPML gesture models may not work properly with the changing body gesture conditions, depending on the changing body structures such as broken leg, arm, or finger, varying mood states, and illness. This can be compensated through the use of alternative DPPML gesture models, which are trained separately with multiple immersive devices. The proof of identity can be obtained from the alternative model (e.g. HTT) if it does not work for a particular model (e.g. MoCap). Moreover, the proposed techniques can only address the threats against transaction authenticity, identity impersonation and theft of credentials, identity, or avatars throughout the many threats elaborated in Section Appendix B.1 (Fig. 5).

11. CONCLUSION

Urban metaverse, not an alternative to urban reality, but an immersive parallel of it, in which the physical and their equivalent virtual clones co-exist with swarms of massive immersive human-machine interactions, will be providing cities with new ways for the digital transition and societal transformation; it will respond to urbanisation with more intelligent services through the exploration and exploitation of the metaverse concept by mirroring the high-fidelity life of urban societies [1], paving the way for alleviating the problems of rapid urbanisation with limited urban resources. Virtual metaverse cyberspaces, where architecture, technology, and social dynamics are moulded with virtual and augmented reality beyond screens; where our interactions with the local and central governments, businesses, organisations, and other residents can be managed; where we can create, develop, and publish our own urban experiences

that mirror our own urban life – these are what lay ahead, with a variety of many practical applications to provide residents with a more immersive and interactive experience of their city. On one hand, these cyberspaces will be democratising all the skills/assets within an urban environment, with a huge economic value benefiting every citizen. On the other hand, granular microdata, which makes and identifies us with specific features, will be collected through these cyberspaces. The potential risks and cyberthreats in this ecosystem that incorporates Web3 can be extremer than the ones in Web2, since we are immersed with multiple, tightly-coupled, wearable, sensor-rich devices perceiving the blend of the real and the virtual – with possible imminent negative experiences, if these dynamic platforms are not designed well to mitigate these potential hazards. This research analyses risks and cyberthreats and basic cybersecurity measures against them comprehensively within the urban metaverse ecosystem. This study reveals the cybersecurity gaps within these environments in the literature and real-world implementations. The metaverse cybercommunities, using decentralised data structures on private and public ledgers and interoperability architecture, may not be managed by a single entity, which makes it more difficult to track down and stop attackers. Adverse events need to be detected in real time proactively to avoid dire circumstances such as losing individual data, NFTs, virtual real estate, cryptocurrency, or a breach of privacy on the blockchain in which traceability of transactions and actions is difficult to follow, due to the nature of the blockchain ecosystem with a high level of data sovereignty and privacy. Breach of privacy and cybersecurity leads to breach of trust and ensuring secure and reliable spaces in an automated manner, using AI solutions, is paramount for these worlds to thrive.

The metaverse is the new playground for hackers to threaten your security, breach your privacy and steal your data and assets (Fig. 2). This research mainly focuses on mitigating the cyberthreats of “credentials theft”, “identity falsification & impersonation”, “Identity theft”, and “Avatar theft”. A blockchain-based authentication and verification approach (UMetaBE-DPPML) that utilises individual behavioural/gesture signatures (i.e. digital body footprint) obtained from immersive metaverse wearable devices is designed to extend the access control, privacy and security of residents in metaverse urban cyberspaces with blockchain technologies instilled with AI. This approach can be instrumented effectively against unreal transactions, identity impersonation and theft of credentials, identity, or avatars at the time they are occurring – without renouncing the targeted functional abilities of the immersive devices and the essential objectives of the urban metaverse cyberspaces. The preliminary results prove the viability of employing the proposed techniques in realising the objectives in this report. More explicitly, the results suggest that the proposed techniques can prevent these particular cyberthreats promptly before any transactions have been executed. Moreover, from a privacy point of view, individual gesture models can be created without sharing particular body signatures with other users and trusted third parties. By using these models, users do not need to share their newly generated private body signature data with other users and third parties to prove their identities before executing transactions,

which protects their data from untrusted/semi-honest parties or honest but curious parties, leading to the protection of private data from authorised and unauthorised access. Users can share their data and live experiences with people whose identities have been verified with those models, leading to sharing their lives or doing business with genuine people. Through control settings, physical distances can be preserved from other avatars whose identities have not been verified via these models concerning the avatar or credentials theft or impersonation, leading to protection from potential cyberbullying, metaphysical harassment or abuse (Fig. 2).

To the best of our knowledge, this research is the first one in the literature that utilises the body's cyber signature in extending the protection of residents in cyber worlds by avoiding the access of unauthorised individuals to private data or assets using blockchain technologies. The secure and reliable urban metaverse cyberspaces, supported by similar verification and authentication approaches, will construct ecosystems of trust among all the entities within the urban metaverse ecosystem. By discussing the challenges and potential areas for future research, this research not only presents an overview of the current research landscape but also serves as a roadmap for future research efforts in this field. The proposed system will be tested with a larger number of nodes involving the PoS consensus mechanism using several other metaverse immersive devices. We will focus on applying the proposed approach in real-world applications, with a couple of immersive devices and with a larger number of nodes and under diverse network conditions as a future objective.

12. ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their constructive input and comments.

References

[1] K. Kuru, Metaomnicity: Toward immersive urban metaverse cyberspaces using smart city digital twins, IEEE Access 11 (2023) 43844–43868. doi:10.1109/ACCESS.2023.3272890.

[2] K. Kuru, H. Yetgin, Transformation to advanced mechatronics systems within new industrial revolution: A novel framework in automation of everything (aoe), IEEE Access 7 (2019) 41395–41415. doi:10.1109/ACCESS.2019.2907809.

[3] K. Kuru, D. Ansell, Tcitysmartf: A comprehensive systematic framework for transforming cities into smart cities, IEEE Access 8 (2020) 18615–18644. doi:10.1109/ACCESS.2020.2967777.

[4] F. Tang, X. Chen, M. Zhao, N. Kato, The roadmap of communication and networking in 6g for the metaverse, IEEE Wireless Communications (2022) 1–15doi:10.1109/MWC.019.2100721.

[5] S.-M. Park, Y.-G. Kim, A metaverse: Taxonomy, components, applications, and open challenges, IEEE Access 10 (2022) 4209–4251. doi:10.1109/ACCESS.2021.3140175.

[6] A. M. Al-Ghaili, H. Kasim, N. M. Al-Hada, Z. B. Hassan, M. Othman, J. H. Tharik, R. M. Kasmani, I. Shayea, A review of metaverse's definitions, architecture, applications, challenges, issues, solutions, and future trends, IEEE Access 10 (2022) 125835–125866. doi:10.1109/ACCESS.2022.3225638.

[7] G. D. Ritterbusch, M. R. Teichmann, Defining the metaverse: A systematic literature review, IEEE Access 11 (2023) 12368–12377. doi:10.1109/ACCESS.2023.3241809.

[8] T. Huynh-The, Q.-V. Pham, X.-Q. Pham, T. T. Nguyen, Z. Han, D.-S. Kim, Artificial intelligence for the metaverse: A survey, Eng. Appl. Artif. Intell. 117 (2023) 105581. doi:https://doi.org/10.1016/j.engappai.2022.105581.

[9] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, Z. Zheng, Fusing blockchain and ai with metaverse: A survey, IEEE Open Journal of the Computer Society 3 (2022) 122–136. doi:10.1109/OJCS.2022.3188249.

[10] T. Maksymyuk, J. Gazda, G. Bugár, V. Gazda, M. Liyanage, M. Dohler, Blockchain-empowered service management for the decentralized metaverse of things, IEEE Access 10 (2022) 99025–99037. doi:10.1109/ACCESS.2022.3205739.

[11] Y. Zhao, J. Jiang, Y. Chen, R. Liu, Y. Yang, X. Xue, S. Chen, Metaverse: Perspectives from graphics, interactions and visualization, Visual Informatics 6 (1) (2022) 56–67. doi:https://doi.org/10.1016/j.visinf.2022.03.002.

[12] Z. Lv, S. Xie, Y. Li, M. Shamim Hossain, A. El Saddik, Building the metaverse by digital twins at all scales, state, relation, Virtual Reality & Intelligent Hardware 4 (6) (2022) 459–470. doi:https://doi.org/10.1016/j.vrih.2022.06.005.

[13] M. Aloqaily, O. Bouachir, F. Karray, I. A. Ridhawi, A. E. Saddik, Integrating digital twin and advanced intelligent technologies to realize the metaverse, IEEE Consumer Electronics Magazine (2022) 1–8doi:10.1109/MCE.2022.3212570.

[14] L. Zhao, Q. Yang, H. Huang, L. Guo, S. Jiang, Intelligent wireless sensing driven metaverse: A survey, Computer Communications 214 (2024) 46–56. doi:10.1016/j.comcom.2023.11.024.
URL http://dx.doi.org/10.1016/j.comcom.2023.11.024

[15] A. T. Kusuma, S. H. Supangkat, Metaverse fundamental technologies for smart city: A literature review, in: 2022 International Conference on ICT for Smart Society (ICISS), 2022, pp. 1–7. doi:10.1109/ICISS55894.2022.9915079.

[16] A. Musamih, A. Dirir, I. Yaqoob, K. Salah, R. Jayaraman, D. Puthal, Nfts in smart cities: Vision, applications, and challenges, IEEE Consumer Electronics Magazine (2022) 1–14doi:10.1109/MCE.2022.3217660.

[17] G. Bansal, K. Rajgopal, V. Chamola, Z. Xiong, D. Niyato, Healthcare in metaverse: A survey on current metaverse applications in healthcare, IEEE Access 10 (2022) 119914–119946. doi:10.1109/ACCESS.2022.3219845.

[18] A. Almarzouqi, A. Aburayya, S. A. Salloum, Prediction of user's intention to use metaverse system in medical education: A hybrid sem-ml learning approach, IEEE Access 10 (2022) 43421–43434. doi:10.1109/ACCESS.2022.3169285.

[19] R. Chengoden, N. Victor, T. Huynh-The, G. Yenduri, R. H. Jhaveri, M. Alazab, S. Bhattacharya, P. Hegde, P. K. R. Maddikunta, T. R. Gadekallu, Metaverse for healthcare: A survey on potential applications, challenges and future directions, IEEE Access 11 (2023) 12765–12795. doi:10.1109/ACCESS.2023.3241628.

[20] M. Wang, H. Yu, Z. Bell, X. Chu, Constructing an edu-metaverse ecosystem: A new and innovative framework, IEEE Transactions on Learning Technologies 15 (6) (2022) 685–696. doi:10.1109/TLT.2022.3210828.

[21] P. Suanpang, C. Niamsorn, P. Pothipassa, T. Chunhapataragul, T. Netwong, K. Jermsittiparsert, Extensible metaverse implication for a smart tourism city, Sustainability 14 (21). doi:10.3390/su142114027.

[22] J. W. Bos, K. Lauter, J. Loftus, M. Naehrig, Improved security for a ring-based fully homomorphic encryption scheme, in: M. Stam (Ed.), Cryptography and Coding, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 45–64.

[23] L. T. Phong, Y. Aono, T. Hayashi, L. Wang, S. Moriai, Privacy-preserving deep learning via additively homomorphic encryption, IEEE Transactions on Information Forensics and Security 13 (5) (2018) 1333–1345. doi:10.1109/TIFS.2017.2787987.

[24] C. Zhou, N. Ansari, Securing federated learning enabled nwdaf architecture with partial homomorphic encryption, IEEE Networking Letters 5 (4) (2023) 299–303. doi:10.1109/LNET.2023.3294497.

[25] J.-W. Lee, H. Kang, Y. Lee, W. Choi, J. Eom, M. Deryabin, E. Lee, J. Lee, D. Yoo, Y.-S. Kim, J.-S. No, Privacy-preserving machine learning

with fully homomorphic encryption for deep neural network, IEEE Access 10 (2022) 30039–30054. doi:10.1109/ACCESS.2022.3159694.

[26] M. Gong, Y. Zhang, Y. Gao, A. K. Qin, Y. Wu, S. Wang, Y. Zhang, A multi-modal vertical federated learning framework based on homomorphic encryption, IEEE Transactions on Information Forensics and Security 19 (2024) 1826–1839. doi:10.1109/TIFS.2023.3340994.

[27] L. Zhang, J. Xu, P. Vijayakumar, P. K. Sharma, U. Ghosh, Homomorphic encryption-based privacy-preserving federated learning in iot-enabled healthcare system, IEEE Transactions on Network Science and Engineering 10 (5) (2023) 2864–2880. doi:10.1109/TNSE.2022.3185327.

[28] X. Zhou, W. Liang, J. Ma, Z. Yan, K. I.-K. Wang, 2d federated learning for personalized human activity recognition in cyber-physical-social systems, IEEE Transactions on Network Science and Engineering 9 (6) (2022) 3934–3944. doi:10.1109/TNSE.2022.3144699.

[29] P. Li, Z. Zhang, A. S. Al-Sumaiti, N. Werghi, C. Y. Yeun, A robust adversary detection-deactivation method for metaverse-oriented collaborative deep learning, IEEE Sensors Journal (2023) 1–1doi:10.1109/JSEN.2023.3325771.

[30] N. Huq, R. Reyes, P. Lin, M. Swimmer, Cybersecurity threats against the internet of experiences, Trend Micro Research.

[31] M. Pooyandeh, K.-J. Han, I. Sohn, Cybersecurity in the ai-based metaverse: A survey, Applied Sciences 12 (24). doi:10.3390/app122412993.

[32] Y. Huang, Y. J. Li, Z. Cai, Security and privacy in metaverse: A comprehensive survey, Big Data Mining and Analytics 6 (2) (2023) 234–247. doi:10.26599/BDMA.2022.9020047.

[33] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, X. Shen, A survey on metaverse: Fundamentals, security, and privacy, IEEE Communications Surveys & Tutorials (2022) 1–1doi:10.1109/COMST.2022.3202047.

[34] S. Rostami, M. Maier, The metaverse and beyond: Implementing advanced multiverse realms with smart wearables, IEEE Access 10 (2022) 110796–110806. doi:10.1109/ACCESS.2022.3215736.

[35] A. Kalla, C. De Alwis, G. Gur, S. P. Gochhayat, M. Liyanage, P. Porambage, Emerging directions for blockchainized 6g, IEEE Consumer Electronics Magazine (2022) 1–1doi:10.1109/MCE.2022.3164530.

[36] J. Ryu, S. Son, J. Lee, Y. Park, Y. Park, Design of secure mutual authentication scheme for metaverse environments using blockchain, IEEE Access 10 (2022) 98944–98958. doi:10.1109/ACCESS.2022.3206457.

[37] E. E.-D. Hemdan, A. S. A. Mahmoud, BlockTwins: A Blockchain-Based Digital Twins Framework, Springer International Publishing, 2021, p. 177–186. doi:10.1007/978-3-030-65691-1_12.
URL http://dx.doi.org/10.1007/978-3-030-65691-1_12

[38] O.-A. Kwabena, Z. Qin, T. Zhuang, Z. Qin, Mscryptonet: Multi-scheme privacy-preserving deep learning in cloud computing, IEEE Access 7 (2019) 29344–29354. doi:10.1109/ACCESS.2019.2901219.

[39] H. Kim, J. Park, M. Bennis, S.-L. Kim, Blockchained on-device federated learning, IEEE Communications Letters 24 (6) (2020) 1279–1283. doi:10.1109/LCOMM.2019.2921755.

[40] Z. Chen, J. Wu, A. Fu, M. Su, R. H. Deng, Mp-clf: An effective model-preserving collaborative deep learning framework for mitigating data leakage under the gan, Knowledge-Based Systems 270 (2023) 110527. doi:https://doi.org/10.1016/j.knosys.2023.110527.
URL https://www.sciencedirect.com/science/article/pii/S0950705123002770

[41] L. Lyu, Y. Li, K. Nandakumar, J. Yu, X. Ma, How to democratise and protect ai: Fair and differentially private decentralised deep learning, IEEE Transactions on Dependable and Secure Computing 19 (2) (2022) 1003–1017. doi:10.1109/TDSC.2020.3006287.

[42] T. Chen, S. Zhong, Privacy-preserving backpropagation neural network learning, IEEE Transactions on Neural Networks 20 (10) (2009) 1554–1564. doi:10.1109/TNN.2009.2026902.

[43] S. Latif, H. S. Ali, M. Usama, R. Rana, B. Schuller, J. Qadir, Ai-based emotion recognition: Promise, peril, and prescriptions for prosocial path (2022). arXiv:2211.07290.

[44] A. McStay, Emotional ai, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy, Big Data & Society 7 (1)

(2020) 2053951720904386. arXiv:https://doi.org/10.1177/2053951720904386, doi:10.1177/2053951720904386.
URL https://doi.org/10.1177/2053951720904386

[45] X. B. Peng, P. Abbeel, S. Levine, M. van de Panne, Deepmimic: Example-guided deep reinforcement learning of physics-based character skills, ACM Trans. Graph. 37 (4). doi:10.1145/3197517.3201311.

[46] S. Duan, F. Zhao, H. Yang, J. Hong, Q. Shi, W. Lei, J. Wu, A pathway into metaverse: Gesture recognition enabled by wearable resistive sensors, Advanced Sensor Research 2 (8) (2023) 2200054. arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/adsr.202200054, doi:https://doi.org/10.1002/adsr.202200054.
URL https://onlinelibrary.wiley.com/doi/abs/10.1002/adsr.202200054

[47] S. Hochreiter, J. Schmidhuber, Long short-term memory, Neural Comput. 9 (8) (1997) 1735–1780.

[48] M. H. Beale, M. T. Hagan, H. B. Demuth, Deep learning toolbox: User's guide (2018) [cited 20.10.2024].
URL https://dokumen.pub/MATLABdeep-learning-toolbox-users-guide-r2020anbsped.html

[49] M. Schuster, K. Paliwal, Bidirectional recurrent neural networks, IEEE Transactions on Signal Processing 45 (11) (1997) 2673–2681. doi:10.1109/78.650093.

[50] K. Kuru, D. Ansell, D. Hughes, B. J. Watkinson, F. Gaudenzi, M. Jones, D. Lunardi, N. Caswell, A. R. Montiel, P. Leather, D. Irving, K. Bennett, C. McKenzie, P. Sugden, C. Davies, C. Degoede, Treatment of nocturnal enuresis using miniaturised smart mechatronics with artificial intelligence, IEEE Journal of Translational Engineering in Health and Medicine 12 (2024) 204–214. doi:10.1109/JTEHM.2023.3336889.

[51] Z. Zhang, X. Song, L. Liu, J. Yin, Y. Wang, D. Lan, Recent advances in blockchain and artificial intelligence integration: Feasibility analysis, research issues, applications, challenges, and future work, Security and Communication Networks 2021 (2021) 1–15. doi:10.1155/2021/9991535.
URL http://dx.doi.org/10.1155/2021/9991535

[52] Y. Huang, Y. Zhu, X. Qiao, X. Su, S. Dustdar, P. Zhang, Toward holographic video communications: A promising ai-driven solution, IEEE Communications Magazine 60 (11) (2022) 82–88. doi:10.1109/MCOM.001.220021.

[53] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, Y. M. Jang, 6g wireless communication systems: Applications, requirements, technologies, challenges, and research directions, IEEE Open Journal of the Communications Society 1 (2020) 957–975. doi:10.1109/OJCOMS.2020.3010270.

[54] B. Falchuk, S. Loeb, R. Neff, The social metaverse: Battle for privacy, IEEE Technology and Society Magazine 37 (2) (2018) 52–61. doi:10.1109/MTS.2018.2826060.

[55] S. Jiang, J. Cao, C. L. Tung, Y. Wang, S. Wang, Sharon: Secure and efficient cross-shard transaction processing via shard rotation, in: IEEE INFOCOM 2024 - IEEE Conference on Computer Communications, 2024, pp. 2418–2427. doi:10.1109/INFOCOM52122.2024.10621394.

[56] Y. Xiao, N. Zhang, W. Lou, Y. T. Hou, A survey of distributed consensus protocols for blockchain networks, IEEE Communications Surveys & Tutorials 22 (2) (2020) 1432–1465. doi:10.1109/COMST.2020.2969706.

[57] N. Stephenson, Snow Crash, 1st Edition, Bantam Books, New York, USA, 1992.

[58] TheNexus, A summary of "snow crash" by neal stephenson (1992) (2023) [cited 01.01.2024].
URL https://medium.com/@exploringthenexus/a-summary-of-snow-crash-by-neal-stephenson-1992-703496c9900e

[59] P. Wilson, State of smart cities in uk and beyond, IET Smart Cities 1 (1) (2019) 19–22. doi:10.1049/iet-smc.2019.0024.

[60] Y. Sun, H. Song, A. J. Jara, R. Bie, Internet of things and big data analytics for smart and connected communities, IEEE Access 4 (2016) 766–773. doi:10.1109/ACCESS.2016.2529723.

[61] P. Kiestra, Safe cities index 2019: Urban security and resilience in an interconnected world (2019) [cited 25.10.2019].
URL https://safecities.economist.com/wp-content/uploads/2019/08/Aug-5-ENG-NEC-Safe-Cities-2019-270x210-

19-screen.pdf

[62] P. Neirotti, A. D. Marco, A. C. Cagliano, G. Mangano, F. Scorrano, Current trends in smart city initiatives: Some stylised facts, Cities 38 (2014) 25 – 36. doi:https://doi.org/10.1016/j.cities.2013.12.010.
URL http://www.sciencedirect.com/science/article/pii/S0264275113001935

[63] Q. Yang, Y. Liu, T. Chen, Y. Tong, Federated machine learning: Concept and applications, ACM Trans. Intell. Syst. Technol. 10 (2). doi:10.1145/3298981.
URL https://doi.org/10.1145/3298981

[64] B. Hitaj, G. Ateniese, F. Perez-Cruz, Deep models under the gan: Information leakage from collaborative deep learning, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS '17, Association for Computing Machinery, New York, NY, USA, 2017, p. 603–618. doi:10.1145/3133956.3134012.
URL https://doi.org/10.1145/3133956.3134012

[65] J. Chen, J. Wang, C. Jiang, Y. Ren, L. Hanzo, Trustworthy semantic communications for the metaverse relying on federated learning, IEEE Wireless Communications 30 (4) (2023) 18–25. doi:10.1109/MWC.001.2200587.

[66] Y. Yao, X. Chang, L. Li, J. Liu, J. Mišić, V. B. Mišić, Metaverse-aka: A lightweight and privacypreserving seamless cross-metaverse authentication and key agreement scheme, in: 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta), 2022, pp. 2421–2427. doi:10.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00340.

[67] S. A. O. N, P. Si, Q. Li, Research implementation of privacy-preserving blockchain based on metaverse and fl design integration, in: 2024 9th International Symposium on Computer and Information Processing Technology (ISCIPT), 2024, pp. 28–31. doi:10.1109/ISCIPT61983.2024.10672816.

[68] A. Jarjis, G. Kadir, Blockchain authentication for aodv routing protocol, in: 2020 Second International Conference on Blockchain Computing and Applications (BCCA), 2020, pp. 78–85. doi:10.1109/BCCA50787.2020.9274452.

[69] W. Liu, H. Chen, E. C. Ngai, Bf-meta: Secure blockchain-enhanced privacy-preserving federated learning for metaverse, in: 2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom), 2024, pp. 166–172. doi:10.1109/MetaCom62920.2024.00037.

[70] M. U. Hassan, Y. Abbas Bangash, W. Iqbal, A. Chehri, J. Iqbal, Prida-me: A privacy-preserving, interoperable and decentralized authentication scheme for metaverse environment, IEEE Open Journal of the Communications Society 6 (2025) 493–515. doi:10.1109/OJCOMS.2024.3523518.

[71] A. Zainudin, M. A. P. Putra, R. N. Alief, R. Akter, D.-S. Kim, J.-M. Lee, Blockchain-inspired collaborative cyber-attacks detection for securing metaverse, IEEE Internet of Things Journal 11 (10) (2024) 18221–18236. doi:10.1109/JIOT.2024.3364247.

[72] A. Bhardwaj, R. Chaudhary, A. M. Aslam, I. Budhiraja, Blockchain-based robust sdn framework for digital twin-enabled iot networks, in: 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall), 2023, pp. 1–6. doi:10.1109/VTC2023-Fall60731.2023.10333591.

[73] C. Harrison, B. Eckman, R. Hamilton, P. Hartswick, J. Kalagnanam, J. Paraszczak, P. Williams, Foundations for smarter cities, IBM Journal of Research and Development 54 (4) (2010) 1–16. doi:10.1147/JRD.2010.2048257.

[74] A. Hudson-Smith, V. Signorelli, Digital innovation for data visualisations in participatory urban planning (2022).
URL https://connected-environments.org/portfolio/vilo-platform/

[75] S. Jiang, J. Cao, H. Wu, Fast and atomic cross-blockchain asset exchange for metaverse interoperability, in: 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), 2023, pp. 177–184. doi:10.1109/MetaCom57706.2023.00044.

[76] K. Kuru, Conceptualisation of human-on-the-loop haptic teleoperation with fully autonomous self-driving vehicles in the urban environment, IEEE Open Journal of Intelligent Transportation Systems 2 (2021) 448–469. doi:10.1109/OJITS.2021.3132725.

[77] K. Kuru, W. Khan, A framework for the synergistic integration of fully autonomous ground vehicles with smart city, IEEE Access 9 (2021) 923–948. doi:10.1109/ACCESS.2020.3046999.

[78] K. Kuru, S. Worthington, D. Ansell, J. M. Pinder, A. Sujit, B. Jon Watkinson, K. Vinning, L. Moore, C. Gilbert, D. Jones, et al., Aitl-wing-hitl: Telemanipulation of autonomous drones using digital twins of aerial traffic interfaced with wing, IEEE Access 11.

[79] K. Kuru, J. M. Pinder, B. J. Watkinson, D. Ansell, K. Vinning, L. Moore, C. Gilbert, A. Sujit, D. Jones, Toward mid-air collision-free trajectory for autonomous and pilot-controlled unmanned aerial vehicles, IEEE Access 11 (2023) 100323–100342. doi:10.1109/ACCESS.2023.3314504.

[80] Z. Lv, L. Qiao, Y. Li, Y. Yuan, F.-Y. Wang, Blocknet: Beyond reliable spatial digital twins to parallel metaverse, Patterns 3 (5) (2022) 100468. doi:https://doi.org/10.1016/j.patter.2022.100468.

[81] M. Arslan, Metaverse'in akıllı kent hizmetlerine etkisi, Akademik Araştırmalar ve Çalışmalar Dergisi (AKAD) 14 (27) (2022) 292 – 303. doi:10.20990/kilisiibfakademik.1146016.

[82] J. Li, S. Wang, M. Zhang, W. Li, Y. Lai, X. Kang, W. Ma, Y. Liu, Agent hospital: A simulacrum of hospital with evolvable medical agents (2024). arXiv:2405.02957.
URL https://arxiv.org/abs/2405.02957

[83] A. Docca, Supercharge robotics workflows with ai and simulation using nvidia isaac sim 4.0 and nvidia isaac lab (2024) [cited 20.10.2024].
URL https://developer.nvidia.com/blog/supercharge-robotics-workflows-with-ai-and-simulation-using-nvidia-isaac-sim-4-0-and-nvidia-isaac-lab/

[84] J.-S. Lee, I.-C. Choi, J.-Y. Kim, A study on expression of npc colloquial speech using chat-gpt api in games against joseon dynasty settings, The Journal of The Institute of Internet, Broadcasting and Communication 24 (3) (2024) 157–162.

[85] K. Kuru, Planning the future of smart cities with swarms of fully autonomous unmanned aerial vehicles using a novel framework, IEEE Access 9 (2021) 6571–6595. doi:10.1109/ACCESS.2020.3049094.

[86] K. Kuru, D. Ansell, W. Khan, H. Yetgin, Analysis and optimization of unmanned aerial vehicle swarms in logistics: An intelligent delivery platform, IEEE Access 7 (2019) 15804–15831. doi:10.1109/ACCESS.2019.2892716.

[87] A. M. Aslam, R. Chaudhary, A. Bhardwaj, I. Budhiraja, N. Kumar, S. Zeadally, Metaverse for 6g and beyond: The next revolution and deployment challenges, IEEE Internet of Things Magazine 6 (1) (2023) 32–39. doi:10.1109/IOTM.001.2200248.

[88] G. O. Pérez, A. Ebrahimzadeh, M. Maier, J. A. Hernández, D. L. López, M. F. Veiga, Decentralized coordination of converged tactile internet and mec services in h-cran fiber wireless networks, Journal of Lightwave Technology 38 (18) (2020) 4935–4947. doi:10.1109/JLT.2020.2998001.

[89] L. Chang, Z. Zhang, P. Li, S. Xi, W. Guo, Y. Shen, Z. Xiong, J. Kang, D. Niyato, X. Q. Y. Wu, 6g-enabled edge ai for metaverse:challenges, methods,and future research directions, Journal of Communications and Information Networks 7 (2) (2022) 107. doi:10.23919/JCIN.2022.9815195.

[90] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, Y. Liu, A survey of blockchain technology applied to smart cities: Research issues and challenges, IEEE Communications Surveys Tutorials 21 (3) (2019) 2794–2830. doi:10.1109/COMST.2019.2899617.

[91] X. Xu, B. Cizmeci, C. Schuwerk, E. Steinbach, Model-mediated teleoperation: Toward stable and transparent teleoperation systems, IEEE Access 4 (2016) 425–449. doi:10.1109/ACCESS.2016.2517926.

[92] A. Ebrahimzadeh, M. Maier, Delay-constrained teleoperation task scheduling and assignment for human+machine hybrid activities over fiwi enhanced networks, IEEE Transactions on Network and Service Management 16 (4) (2019) 1840–1854. doi:10.1109/TNSM.2019.2937020.

[93] K. Kuru, Joint cognition of remote autonomous robotics agent swarms in collaborative decision-making & remote human-robot teaming.

[94] K. Kuru, Platform to test and evaluate human-in-the-loop telemanipulation schemes for autonomous unmanned aerial systems, in: IEEE/ASME MESA 2024 – 20th Int. Conference on Mechatronic, Embedded Systems and Applications, 2024.

[95] K. Kuru, Human-in-the-loop telemanipulation schemes for autonomous unmanned aerial systems, in: 4. Interdisciplinary Conference on Electrics and Computer (INTCEC 2024), 2024.

[96] D. Wang, K. Ohnishi, W. Xu, Novel emerging sensing, actuation, and control techniques for haptic interaction and teleoperation, IEEE Transactions on Industrial Electronics 67 (1) (2020) 624–626. doi:10.1109/TIE.2019.2927784.

[97] IEEE, P1918.1 - tactile internet: Application scenarios, definitions and terminology, architecture, functions, and technical assumptions (2018) [cited 20.02.2021].
URL https://standards.ieee.org/project/1918_1.html

[98] C. S. Punla, R. C. Farro, Are we there yet?: An analysis of the competencies of BEED graduates of BPSU-DC, International Multidisciplinary Research Journal 4 (3) (2022) 50–59.

[99] A. M. Aslam, A. Bhardwaj, R. Chaudhary, Quantum-resilient blockchain-enabled secure communication framework for connected autonomous vehicles using post-quantum cryptography, Vehicular Communications 52 (2025) 100880. doi:https://doi.org/10.1016/j.vehcom.2025.100880.

[100] K. Kuru, K. Kuru, Urban metaverse cyberthreats and countermeasures against these threats, in: Proceedings of IEEE Sixth International Conference on Blockchain Computing and Applications (BCCA 2024), 2024.

[101] K. Kuru, K. Kuru, Blockchain-enabled privacy-preserving machine learning authentication with immersive devices for urban metaverse cyberspaces, in: 2024 20th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications (MESA), 2024, pp. 1–8. doi:10.1109/MESA61532.2024.10704877.

[102] K. Kuru, K. Kuru, Urban metaverse cyberspaces & blockchain-enabled privacy-preserving machine learning authentication with immersive devices, in: Proceedings of IEEE Sixth International Conference on Blockchain Computing and Applications (BCCA 2024), 2024.

[103] K. Kuru, K. Kuru, Urban metaverse cyberthreats and countermeasures to mitigate them.

[104] L. Cui, J. Liu, Virtual human: A comprehensive survey on academic and applications, IEEE Access 11 (2023) 123830–123845. doi:10.1109/ACCESS.2023.3329573.

[105] D. Z. Morris, Coindesk turns 10: 2016 - how the dao hack changed ethereum and cryptob (2023) [cited 15.05.2023].
URL https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto

[106] I. Vladimirov, M. Nenova, D. Nikolova, Z. Terneva, Security and privacy protection obstacles with 3d reconstructed models of people in applications and the metaverse: A survey, in: 2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST), 2022, pp. 1–4. doi:10.1109/ICEST55168.2022.9828791.

[107] S. Frenkel, K. Browning, The metaverse's dark side: Here come harassment and assaults (2021) [cited 05.02.2023].
URL https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html

[108] V. Sharma, Introducing a personal boundary for horizon worlds and venues (2022).
URL https://www.oculus.com/blog/introducing-a-personal-boundary-for-horizon-worlds-and-venues/

[109] B. K. Wiederhold, Metaverse games: Game changer for healthcare?, Cyberpsychology, Behavior, and Social Networking 25 (5) (2022) 267–269, pMID: 35549346. arXiv:https://doi.org/10.1089/cyber.2022.29246.editorial, doi:10.1089/cyber.2022.29246.editorial.

[110] TheWachowskis, (2023) [cited 20.088.2023].
URL https://www.sparknotes.com/film/matrix/themes/#:~:text=The%20Relationship%20Between%20Body%2C%

20Brain,out%20to%20be%20an%20illusion

[111] D. Eckhoff, I. Wagner, Privacy in the smart city—applications, technologies, challenges, and solutions, IEEE Communications Surveys Tutorials 20 (1) (2018) 489–516. doi:10.1109/COMST.2017.2748998.

[112] S. S. Yau, H. G. An, A. B. Buduru, An approach to data confidentiality protection in cloud environments, International Journal of Web Services Research 9 (3) (2012) 67–83. doi:10.4018/jwsr.20120701041.

[113] R. Podschwadt, D. Takabi, P. Hu, M. H. Rafiei, Z. Cai, A survey of deep learning architectures for privacy-preserving machine learning with fully homomorphic encryption, IEEE Access 10 (2022) 117477–117500. doi:10.1109/ACCESS.2022.3219049.

[114] C. Dwork, F. McSherry, K. Nissim, A. Smith, Calibrating noise to sensitivity in private data analysis, in: S. Halevi, T. Rabin (Eds.), Theory of Cryptography, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006, pp. 265–284.

[115] K. Kuru, Management of geo-distributed intelligence: Deep insight as a service (dinsaas) on forged cloud platforms (fcp), Journal of Parallel and Distributed Computing 149 (2021) 103–118. doi:https://doi.org/10.1016/j.jpdc.2020.11.009.

Appendix A. GENERAL CONCEPTS OF URBAN METAVERSE

Appendix A.1. Components of Urban Metaverse Ecosystem

Many of the potential urban metaverse worlds are yet to be discovered and developed and the ready-to-use off-the-shelf SC twins and newly built twins are expected to expedite the development of more resilient metaverse implementations in the SC ecosystem [1]. We would like to shed light on the main building blocks of the urban metaverse ecosystem before addressing our research question. In this direction, the background of this research regarding the unpinning of urban metaverse cyberspaces is summarised in this section.

Appendix A.2. Smart City (SC)

In a broader inclusive definition, SC can be defined as an opportunistic concept that perpetually enhances harmony between the lives and the environment around those lives in a city by harnessing smart technology, enabling a comfortable and convenient living ecosystem, which paves the way towards smarter countries and a smarter planet [3]. SCs are being implemented to combine governors, organisations, institutions, citizens, environment, and emerging technologies in a highly synergistic synchronised ecosystem to increase QoL and enable a more sustainable future for urban life with increasing natural resource constraints [3]. The concepts of “IoE” and “AoE” [2] bring the people, organisations, lives, processes, data, and things into a concrete coherent structure – CPSs to develop a synergistic smarter connected globe [3]. SC connects physical infrastructures, Information Communication Technology (ICT) infrastructures, social infrastructures, and business infrastructures to leverage the collective intelligence of the city [73]. The main objectives of establishing SCs can be summarised as i) enabling the integration of the distributed services and resources in a combined synergistic fashion, ii) improving existing public services and providing new effective

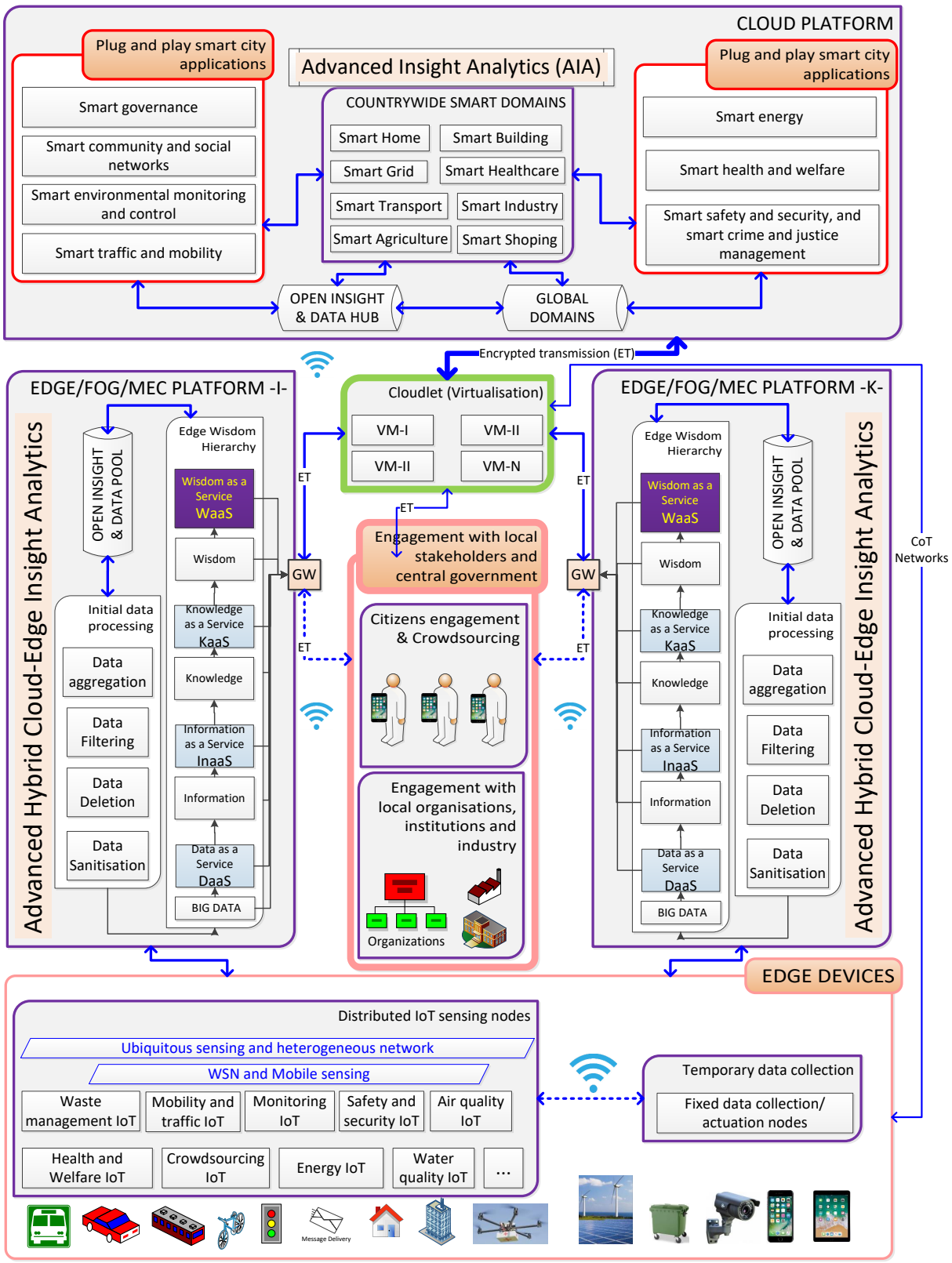

Figure A.6. Main components of SC and their interaction with each other [3].

Figure A.7. Simulation of reality through DTs: ViLO model showing live sensor data on infrastructure equipped with VR and AR [74]. A digital model of the Queen Elizabeth Olympic Park in London, UK, is enriched with real-time data streams and connected to the ViLo Digital Platform for Data Visualizations in Participatory Urban Planning. Image courtesy of The Bartlett Centre for Advanced Spatial Analysis (https://www.ucl.ac.uk/bartlett/casa).

citizen-centric, user-driven, and demand-oriented services, iii) monitoring a city with easy-to-use visualisation tools, iv) enabling near-real-time services for end-users and/or further smart actuation, v) increasing the sustainability with optimised services, vi) improving the lives and livelihoods of citizen, and vii) drive economic development, innovation and global city investment competitiveness [3]. Readers are referred to [3] for the technological infrastructure of SCs involving communication networks and further information about real-world SC use cases. To summarise (Fig. A.6), its main layers enabling proper sensing and appropriate autonomous actuation are i) strict engagement with all the stakeholders, ii) edge IoT devices and citizens to collect data and interact with the environment intelligently by harnessing large amounts of near-real-time data using sophisticated communication technologies, iii) edge/fog platforms, iv) the cloud platform involving cloudlets, and v) integration of smart domains not only within itself but also with the national and global smart domains.

Appendix A.3. Urban metaverse ecosystem: MetaCyberCity

People can hardly browse and travel across the metaverse platforms or spend assets of one metaverse in another; there is an urgent need to design protocols making metaverses interoperable [75]. DTs of physical worlds (e.g. Virtual London (ViLO) platform (Fig. A.7)), that can be established using SC components, would be the base for developing

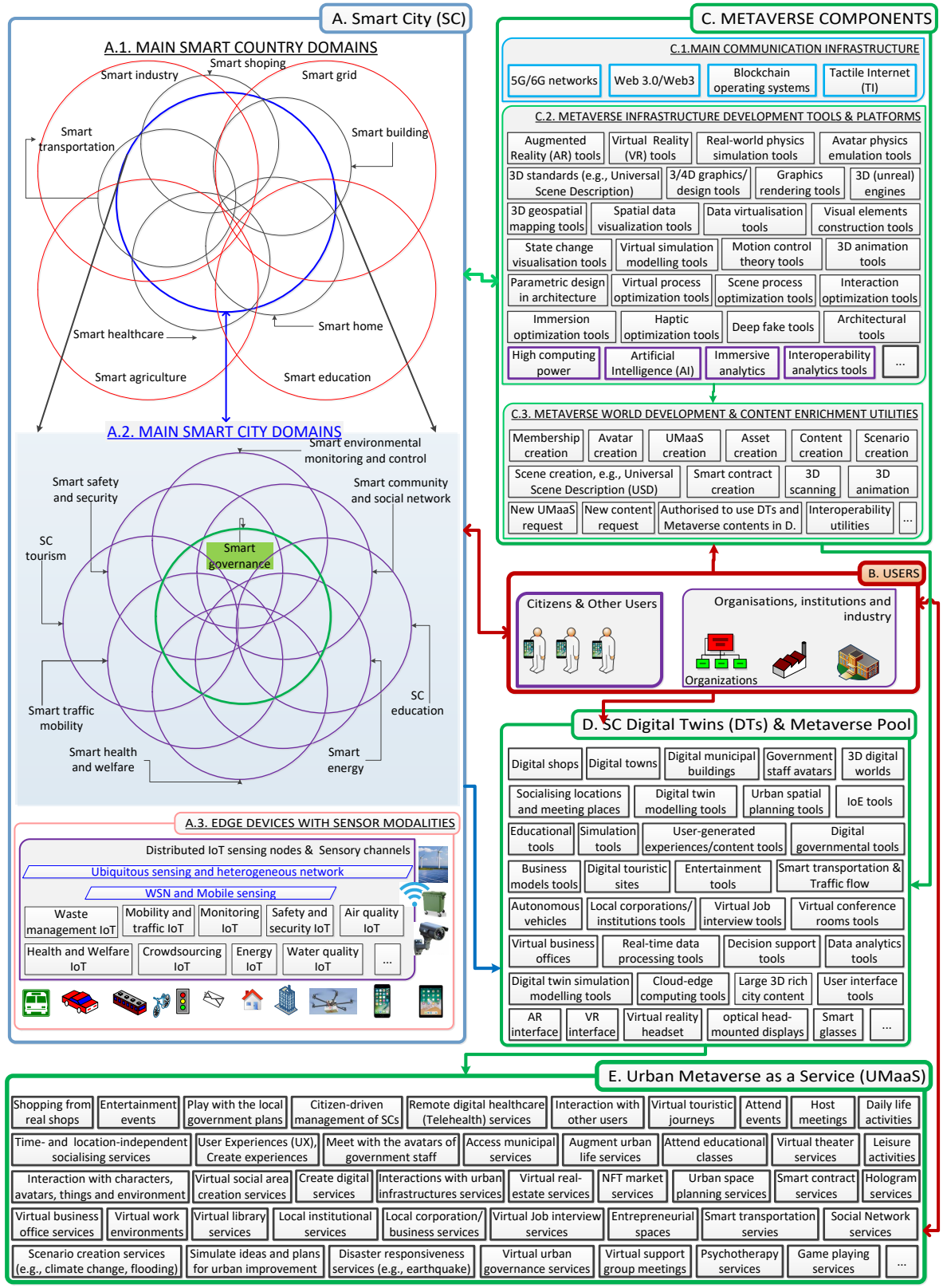

Figure A.8. Architecture of a metaverse city: Main components and their interaction with each other [1].

ultra-realistic metaverse worlds. Readers are referred to the previous studies ([76], [77], [78], [79]) for the examples of DTs developed by us. The urban metaverse ecosystem, the so-called MetaCyberCity is the interconnected network of decentralised blockchain worlds, i.e. UMaaSs, equipped with DTs and resident avatars of the MetaCyberCity can navigate from one UMaaS to another with interoperable abilities and they can build their UMaaS worlds (elaborated in Section Appendix A.4). The general infrastructure of the urban metaverse with the key enabling technologies is depicted in Fig. A.8. The framework consists of five main building blocks, namely, A. SC, B. Users, C. Metaverse components, D. SC DTs and metaverse pools, and finally E. UMaaS. These components and their intertwined interactions with each other are elaborated in [1]. A metaverse can be defined as "democratised, decentralised, user-driven virtual and augmented immersive 3D spaces where two worlds – virtual and physical existence – can be more tangibly connected and people who are not in the same physical space can come together with their avatars to feel many different types of experiences" [1]. An urban metaverse can be defined as the expansion of DTs in the fields of people and society [80]. It provides us with an immersive environment to perform our daily routines in the physical world. SCs, with DTs, are expected to significantly benefit from the promising potentials of the metaverse in the most optimum way. The combination of metaverse and SC will increase further in the forthcoming periods, and this will affect urban life by spreading to all SC applications [81]. Custodial and non-custodial wallets are the two main categories of blockchain-based storage options for private users. Custodial wallets involve entrusting a third party with both the associated private keys and associated assets along with all other stored private information. The third parties, with the responsibility for overall management of the assets including their security and maintenance, are allowed and trusted to exchange all entities in custodial wallets. It is worth noting that a range of control can be granted to individuals, from full authority delegation to total self-custody of assets in these wallets, which is open to internal mishandling if not exposed to cyberthreats. On the other hand, all assets and private keys along with all private information are managed by their owners with complete autonomy, involving their security, in non-custodial wallets. In the same direction, metaverse cyberspaces can be classified as centralised that is controlled by a central entity (e.g. Meta) and decentralised (e.g. Decentraland) that is user-owned and most of the control is in the hands of their users. Urban metaverse cyberspaces are composed of both centralised and decentralised architecture regarding the objectives of the cyberspaces, some of which are controlled by the local city governments and some of which (i..e., user-owned, user-centric) may be managed by their users or together with the local government.

Blockchain, as a distributed database, provides unique data structures (i.e. crypto worlds) that were designed to make many people interact/transact with each other without thinking about privacy too much. On the other hand, Distributed Ledger Technology (DLT) aims to incorporate privacy into the transactions further. Blockchain, a type of DLT, is implemented as a decentralised Peer-to-Peer (P2P) network and stores a digital ledger in a distributed and

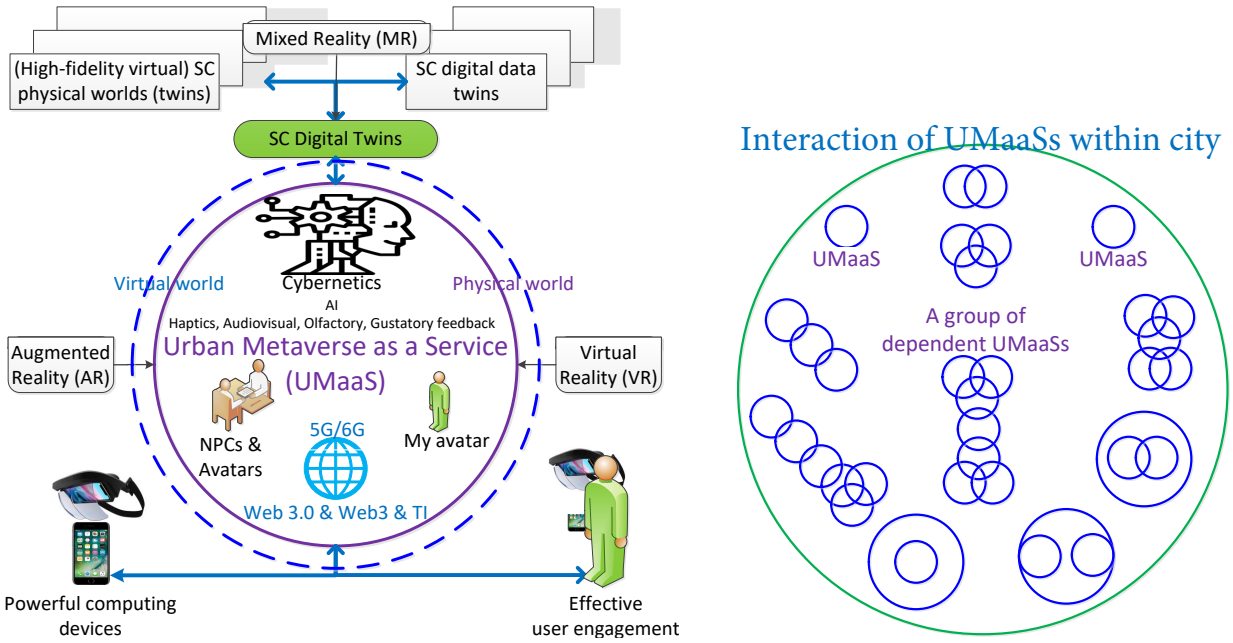

Figure A.9. Left: Pivotal components of UMaaS. Blurring borders between virtual and physical worlds. Right: Various structural design models of UMaaSs: Jointed (dependent) and unconnected (independent) spaces (Fig. A.8E) [1].

secure manner; smart contracts extend the capabilities of blockchain technology; they are executable codes with all the terms and conditions of an agreement between various entities and are deployed on the blockchain; some of the advantages provided by smart contracts are automation, access control, trust-building, and elimination of third-party execution [35]. Smart contracts are autonomously working decentralised networked systems whose governance is based on pre-established rules and usually contained within Decentralised Autonomous Organisation (DAO) (elaborated in Section Appendix A.4). Contract addresses of smart contracts are used to house assets safely. The key components of the metaverse in developing urban worlds are summarised in Fig. A.8 C.

Appendix A.4. Urban Metaverse-as-a-Services (UMaaSs)

We explained the concept of UMaaS within urban metaverse worlds for the first time in the previous research [1]. To summarise, UMaaSs are the fragmented worlds of urban life. They are parallel urban rooms within a city, allowing the efficient customisation of particular urban metaverse services. An urban metaverse is composed of a collection of metaverse urban rooms/worlds – UMaaSs as exemplified in Fig. A.8E. The main building blocks in establishing UMaaSs – moulding the physical world and virtual world within an intertwined environment – are cybernetics, avatars, assets, Non-Player Characters (NPCs) and UTs. Research on real-world human-robot dynamics is being advanced by the developing projects such as “MetaUrban” [82] and “Isaac Sim 4.0” [83] which creates complex urban environments and supports tasks like social navigation and interactions between AI agents, humanoid robots and humans

using Reinforcement Learning (RL) and Imitation Learning (IL). Granular UMaaSs provide residents with specific immersive shared observations, interactions, collaboration and social experiences via well-designed user interfaces leading to high QoE. The generation of granular UMaaSs (e.g. microcosms of real worlds) would reduce required computing resources significantly. UMaaSs, with rich activities, are the multiple urban metaverse worlds, i.e. co-existence and co-dependence between the physical world and the virtual world. UMaaSs, tailored and enriched with individuals' experiences using AR and VR tools, aim to eliminate the boundaries such as time, space and language between real worlds and their immersive counterparts. They represent isolated and jointed/integrated/composite immersive worlds (Fig. A.9 right) designed for particular and restrictive objectives and can provide an effective and flexible membership solution for avatars.

Teleoperation between UMaaSs is possible to complete various specific tasks since a resident has only a single avatar within an urban metaverse ecosystem. Physically accurate immersive worlds can be connected to generate larger virtual metaverse spaces – a group of dependent UMaaSs – or each can individually serve as a UMaaS to help meet the particular requirements of the city, city managers, residents and non-residents who are interrelated with the urban ecosystem. When created by residents to realise particular objectives such as "protecting and managing urban heritage", UMaaSs, with multiagent nodes, can be governed by the principles of DAO, by which they turn into member-owned organisations. Within a protocol, authorised participants work together to build blocks and reach consensus between linked contracts. Recently emerging DAOs are built using blockchain and Web3 technologies to provide cybercommunities with self-evolution through autonomy by avoiding any central governance intervention/dictation. They are governed by their members collaboratively on a fairness basis through blockchain smart contracts with token-based and value-added systems and data is managed on a data sovereignty basis in a trustworthy ecosystem. Residents of DAOs are as powerful in the management and decision-making as the value they create. DAOs protect the integrity and equity of their users, safeguard their privacy and safety, and enable them to make the most of their value. Governance, operational, and incentive mechanisms as well as on-chain daily activities can be determined by their users collectively through a smart contract voting system leading to a joint decision. DAOs, by incorporating other skilful experts from other regions into the organisation, can have the power to direct the policies of not only local and central governments but also other related organisations located elsewhere all around the world. Not only are the skills, talents and services democratised globally beyond the borders of the MetaCyberCity in this way within UMaaSs, but also, they are improved considerably by the global contributions with wider group intelligence.

Appendix A.5. Avatars/Meta-residents

"3D Avatars" – pseudo-physical presence (i.e. cyber teleoperation) of users – are the residents of the urban worlds. Avatars are Self-Sovereign Identity (SSI) that is governed by their owners. Avatars, DTs of residents, present

physically in UMaaSs worlds to interact with the urban environments and other avatars representing other residents allowing the feeling of being in the same room. The appearance of our avatars in expressing our reaction to events, and interaction with people and all other objects is essential in UMaaSs. In other words, our digital self and physical self are coupled to increase the immersiveness in a bidirectional physical and emotional flow of feeling (e.g. facial expression, smell, touch). Avatars will be more realistic with the development of facial expression and emotion recognition technologies. For instance, the Cambria VR headset developed by Meta enables users to readily reflect their facial expressions to their avatars via immersive eye contact, aiming to achieve visual fidelity. In the other direction, what avatars interact in UMaaS worlds are reflected back to the physical self within a bidirectional flow of tightly coupled experiences (e.g. smell, touch). The applications that allow 3D scanning using smartphones help create more realistic avatars. Residents can scan themselves with varying emotions and expressions from different angles and their realistic avatars can be created in several minutes. The current advancing technologies e.g. Epic Games, Unreal Engine, and DeepFake allow the creation of hyper-realistic MetaHumans that look like the characters of their counterparts [4] concerning the appearance, gender, age, ethnicity, manners, mimics, emotions etc. More advanced engines will enable us to create MetaHumans that look exactly like us in the years to come. Avatars are not NFTs. They are not embodied to be unique. Residents can have multiple avatars in different metaverse worlds. Avatars can use their clones to eliminate time-space restrictions further for completing different tasks in different virtual spaces at the same time. For instance, an avatar can attend a concert within a UMaaS using his/her clone while interacting with government staff within another UMaaS space.

Appendix A.6. Non-Player Characters (NPCs)

NPCs are neither avatars nor controlled by people. They are utilised to make the worlds look exactly like the real world for modelling and visualising a realistic virtual environment. For instance, all pedestrians are presented as NPCs to show real-time human mobility in the urban environment while an avatar is driving a vehicle on urban roads. NPCs, enabling visual realism, behave under a set of rules defined for them representing their real-world characteristics by fulfilling the scene anticipation with the lack of emotional intelligence and interaction. Avatars can interact with NPCs concerning the rules defined for NPCs. However, NPCs are unable to adjust to novel situations or dialogues when scripted responses are used, and static behaviours result in repetitive actions that are unaffected by user interaction or external circumstances. NPCs with dynamic, context-aware interactions are now being created using AI tools like ChatGPT [84]. Role-based NPCs (e.g. police, fireman) with unique behaviours and more flexible and dynamic actions as well as authentic scenes and emotional responses considering the dynamics of the environment will be generated

[4] Ex: https://www.youtube.com/watch?v=6mAF5dWZXcI

using the advancing AI tools (e.g. Generative Pre-trained Transformers (GPT), GAN) by enabling the capable of learning in the years to come. AI-powered digital humans will eventually be almost identical to humans in terms of their cognitive capacities with the advancing NPC realism while humans would not be sole decision-makers with their avatars.

Appendix A.7. Assets

UMaaSs have their own assets. The assets can be created while UMaaSs are being generated and they can be moulded by users during the lifetime of UMaaSs. The assets of an urban metaverse ecosystem are composed of a wide range of digital goods, services and all other virtual items including virtual real estate (virtual lands and properties to buy, rent, sell, and build structures on), digital currency (cryptocurrencies and tokens to trade), digital collectibles (NFTs: ownership and authenticity of unique digital creations such as digital arts, music, video), virtual goods and services (e.g. clothing, accessories, cars, buildings, entertainment, offices, and their values based on their rarity, utility, and aesthetic appeal), virtual businesses/shops (e.g. virtual forms of real businesses such as Nike, Coca-Cola, Gucci, the concert of Ariana Grande), digital identities (i.e. avatars), all the objects which makes a city (e.g. lands, buildings, streets, roads, NPCs, vehicles), AI-powered digital humans (e.g. digital Einstein), AI-generated avatars/bots to represent businesses and other people during their busy times and adjacency [1]. The value and popularity of urban assets can be subject to change based on market trends and community preferences. For instance, some virtual land plots can be more expensive compared to others if their locations are near popular attractions, city centres or the plots that are owned by famous people. It is noteworthy to emphasise that NFTs, while establishing ownership of unique assets, have played a significant role in the metaverse business. Smart contracts, running on transparent DLT which is the backbone of blockchain networks and tracked, verified, and validated collectively, are the tools used to buy and sell digital assets in a trustworthy ecosystem by tracking and verifying them.

Appendix A.8. Decentralised urban metaverse engines and communication infrastructure

In this section, we would like to summarise the communication infrastructure in SCs and urban metaverse ecosystems to understand the possible cyberthreats better considering the current, imminent, and future communication architectures. The communication infrastructure in cities along with urban metaverse ecosystems to establish SC applications has already been analysed in the previous research [3], [77], [85], [86]. Therefore, this subject is not elaborated in this paper and the readers are referred to these studies about a diverse set of communication technologies employed in SCs and urban metaverse ecosystems. To summarise, city communication infrastructure provides large-scale machine-type communications with a multiplicity of communication modalities using an orchestration of backhaul and fronthaul (i.e. crosshaul) mechanisms. This communication infrastructure helps a bidirectional stream

of near-real-time information, knowledge and wisdom between the physical and virtual environments of SC blended DTs. The engines of the metaverse communication infrastructure on which metaverse applications can run seamlessly are placed in Fig. A.8 C.1. The foundational pillars of this infrastructure are 5G/6G networks, Web 3.0 / Web3, blockchain operating systems and Tactile Internet (TI). More specifically, 6G is envisioned as an emerging revolutionary wireless technology and cutting-edge network architecture for tactile and haptic applications to provide high bandwidth, reliability, latency, energy efficiency, and intelligent services [87].

User-centric and decentralised Web 3.0, with rich media content, semantic immersive UX and AI capabilities, has changed our communication and interaction behaviours significantly compared to one-way text-based Web 1.0 and ubiquitous vision-based user-driven Web 2.0. Furthermore, the incorporation of blockchain technologies into Web 3.0 has created a more evolved decentralised web – Web3. Web3, using multiple operating systems, provides data sovereignty (e.g. creative asset sovereignty) for individuals allowing a more advanced user-centric decentralised network with further individual data management capabilities. While 5G technologies are taking their indispensable places in real-world implementations, it is worth mentioning that future 6G, at the expense of increased complexity, considers not only delivering another 1000x increase in data rates, but also diving into self-sustaining networks and dynamic resource utilisation; 6G will also put an end to smartphone-centric networks, introducing new system paradigms (e.g. human-centric services) [88]. 6G, not only promises to connect things with Ultra-Reliable Low Latency Communications (URLLC) (1-microsecond latency) leading to no delay in real time, but also promises to connect things intelligently with ultra-high density connections (i.e. over 100 devices per cubic metre). In this sense, the use of location awareness immersive technologies, AR/VR/XR/MR as well as holographic communication, will be eased with 6G since intelligence, as the key component of immersive technologies, is connected. The combination of blockchain and 6G allows the streamlining of a peak rate of 1 Tbit/s [35] using a Terahertz-sized frequency band to achieve a network delay with a transmission rate of less than 1 ms and the probability of communication interruption less than one in a million using spatial multiplexing technology [89] and many SC initiatives are very much familiar with Web3 by using blockchain technologies for their various applications. The more advanced immersive technologies such as TI with quality haptic feedback, the better immersive urban metaverse worlds using urban DTs leading to better urban metaverse cyberspaces [1]. Blockchain technologies, enabling individual data ownership, are already being used by cities to store, share and process the information that is under the control of the users. Readers are referred to [90] for the SC blockchain application examples. The widespread use of current blockchain technologies as well as newly developing blockchain technologies specific to the urban ecosystem in establishing UTs (i.e. digital shadows of avatars of the urban ecosystem) will boost and ease the integration of these technologies into establishing UMaaS worlds. An example of applying blockchain technologies into metaverse virtual spaces for ensuring timely

multi-scale spatial data processing using a data layer between physical worlds and their DTs is presented in [80].

Instant feedback through the metaverse immersive technologies (e.g. high-definition (HD) rendering, smart wearable devices, haptics (tactile and kinesthetic) (sense of touch), audiovisual modalities, olfactory (sense of smell), gustatory (sense of taste)) is going to play a pivotal role in establishing a strong immersive metaverse implementation that enables a tight interface between the physical and virtual worlds by coupling with artificial sensors and actuators. Haptics, as an extension of visual and auditory modalities, refer to both kinaesthetic and tactile information and include position, velocity, force, torque, vibration, etc [91]. With the advent of commercially available haptic/tactile sensory and display devices, conventional triple-play (i.e. audio, video, and data) communications now extend to encompass the real-time exchange of haptic information (i.e. touch and actuation) for the remote control of physical and/or virtual objects through the Internet [92], [93], [94], [95]. Furthermore, a lot of more novel, intelligent, user-friendly haptic devices are emerging with the advent of new functional materials, smart actuators and sensors, embedded computers, and the latest advances in real-time intelligence, Machine Learning (ML), cognitive science, AR/VR/MR [96], MoCaps, haptics gloves, and HTT leading to a better bilateral exchange of energy between two remote nodes. These advancements are highly supported by the standardisations of haptics on an application basis, e.g. IEEE P1918.1 [97].

Appendix B. CYBERTHREATS AND COUNTERMEASURES FOR URBAN CYBERSPACES

Possible urban cyber risks, cyberthreats, and privacy concerns are analysed in this section before exploring the proposed PPML authentication technique in Section 3. Urban metaverse cyberspaces, using the 3D elevation of linear Internet, will inevitably be a target for cybercriminals due to their economic value with valuable assets, immersive nature, and a large volumes of data, particularly, vision-based data, to be exploited in many aspects. The drivers behind cyberattacks can be for a variety of reasons such as money-driven, ego-satisfaction, curiosity, or joy-motive through privacy intrusion. Urban metaverse cyber worlds, on the new and more evolved decentralised 3D Web3, harbour new types of threats in addition to the current threats we are very much familiar with on web2 due to their immersive nature and new types of assets. Profiles of cybercriminals should be revealed to combat them in a more effective manner using appropriate tools developed for these specific profiles, which is not the scope of this paper. Vast amounts of data including movements, preferences, emotions and biometrics will be collected in the urban cybercommunities. This BD is subject to potential data breaches, unauthorised access, and misuse of sensitive information. We need to get ready to deal with these hazards while we are embracing many promising potentials within this new type of urban ecosystem. The main threats that can be launched in urban cybercommunities are demonstrated in Fig. 5 along with the basic countermeasures. These cyberthreats are intertwined with one another and it is difficult to differentiate them

with distinctive borders. We explain these threats in the following subsections. We would like to explain a couple of critical points before moving to the following subsections. Regarding the metaverse environment, quantum information technology is capable of enhancing the system's security and privacy, improving the computational scales, optimising the output, improving the communication, securing the network channels, providing absolute randomness for metaverse-based applications, and supporting ML implementations in the metaverse by integrating quantum ML [98]. For instance, [99] proposes a hybrid security solution integrating the Kyber Post-Quantum Cryptography with Adaptive Grouping Score-based Practical Byzantine Fault Tolerance for enhancing security in connected and autonomous vehicles, leading to substantial improvements in reducing latency up to 47.16%, achieving an approximate 65.6% overall reduction in computation costs and effectively increasing the average throughput by 71.44% compared to existing security solutions. Moreover, it demonstrates that the approach provides resistance to quantum computational attacks, providing a future-proof solution in anticipation of quantum computing (QC) advancements. On one hand, promising QC enables advanced immersive environments instilled with wisdom/insights that can be acquired from related BD, on the other hand, the encryption codes of blockchain, which can not be decrypted for tens or hundreds of years using the current computing power, can be decrypted in hours/days/weeks using the high power of QC. Therefore, cybersecurity in blockchain technologies should be improved in parallel with QC. Strictly speaking, blockchain platforms require significant improvement regarding crypto technologies, which is the most critical main building block. They may be replaced by other newly promising technologies integrated with 6G to mitigate these concerns where 6G networks are expected to emerge as Distributed Trust-Based Secure Networks (TBSN) where security, privacy and trust are the key pillars to meet these requirements [35]. Cyberthreats in metaverse environments, as well as the proposed solutions, are analysed in [100], [101], [102], [103].

Appendix B.1. URBAN METAVERSE CYBERTHREATS

Appendix B.1.1. Identity falsification & impersonation

Virtual human systems, i) by achieving both realistic virtual humans with face expression recognition and smooth and flexible dialogue engines with chatbots, and ii) by targeting to achieve emotional recognition and emotional empathy, typically consist of five main modules: character generation, voice generation, animation generation, audio and video synthesis display, and interaction using information technologies, such as computer graphics, motion capture, ML, high-precision rendering, and speech synthesis [104]. Convincing, false representations of individuals – by exploiting the immersive nature of the metaverse – can be created, as fake avatars using high-level imitation technologies (e.g. GAN (Section Appendix B.1.15)) to impersonate friends, other users, trusted figures, well-known individuals, or influential figures such as famous people, leading to many different forms of harm – such as scamming, virtual harassment, phishing, etc. One way that this is achieved is through the DeepFake which utilises AI to combine real

and AI-generated visual and auditory media to create a fabrication of reality – for example, given enough samples of an individual's voice, a deep-learned model of that person's unique voice can be created, which then could be made to say anything that someone likes or hates. Pretending to be another avatar (i.e. identity forgery, dual identity) using biometrics such as facial features, and voice will be easier as avatars become more realistic looking as technology progresses. In this way, the other impersonated users in the environment can be exploited to manipulate users into transferring valuable assets, revealing sensitive information or credentials, or engaging in hazardous activities. Registration of residents/avatars and businesses to the MetaCyberCity and UMaaSs using authentication tokens would mitigate these concerns, but this may not be an ideal option for residents concerning privacy regarding being tracked by the authority.

Appendix B.1.2. Identity theft and compromise of sensitive data

High volumes of sensitive personal data about us are collected through high-level tracking technologies (e.g. VR/AR headsets). This data (e.g. biometrics, financial information, health-related information, sexual orientation, race, movement patterns, voice patterns, brain waves) can be compromised and aid in executing various malicious actions. The metaverse environments can be destabilised by malicious software (i.e. Malware) that can stop us from reaching our environment, prevent us from transferring our private data, or send our credentials to other sources by penetrating our information. Spear phishing tailored to particular subjects is the main concern in deceiving the subject with more believable tactics, after sensitive, personal information is compromised. This information can be stolen and exploited severely, particularly for financial gain, posing a high risk to users' real-world identities. Stronger and more effective authentication approaches are being developed to protect users by avoiding any possible identity theft. Malicious software attacks can target vulnerabilities in metaverse platforms, leading to unauthorised access, data breaches, or disruption of services. Every once in a while, our highly sensitive personal data gets leaked and becomes compromised due to the ineffective implementation of cybersecurity measures in the online services/social media we use. Compromised identity data can be moulded to create fake avatars that mimic their counterparts to manipulate other users (Sections Appendix B.1.1).

Appendix B.1.3. Credentials theft

Users' private data including their wallets, avatars, and assets are encrypted on the blockchain. First, users should follow the practice of cybersecurity hygiene strictly (Section Appendix B.2.2) and should not share their private keys with others in cybercommunities to avoid every type of attack that is summarised in Fig. 5. The encryption approaches currently used in the blockchain seem safe to protect them against decryption approaches considering the current computing power. Nevertheless, it is noteworthy to emphasise that every encrypted code is vulnerable to

decryption and we are witnessing the theft of huge amounts of assets (e.g. crypto money) in the metaverse worlds. It is noteworthy to mention that the 2016 DAO hack [105] damaged the robustness reputation of smart contracts. Stolen credentials can be used to make unauthorised purchases and to launder money through stolen metaverse accounts.

Appendix B.1.4. Avatar theft

Avatars, with unique features, are the assets of their users and are supposed to function in urban metaverse cyberspaces to represent their counterparts. All the assets of a user are encrypted on the blockchain ledgers to fight against theft and other attacks. Attackers can use others‘ avatars in our environment to deceive us easily. Private data credentials in the metaverse could become compromised and an avatar of a user can be hijacked to take over the environment of the user and to deceive other users in the cybercommunity. The stolen avatar, i.e. virtual persona, can be controlled by cybercriminals in the name of the persona to be used for cyberattacks. Concretely speaking, a stolen avatar can be used to harass other users, spread misinformation, or engage in other harmful activities, tarnishing the reputation of the avatar's real counterpart. Stolen avatars might be used for money laundering purposes with cryptocurrencies. Vladimirov et al. [106] analyses the threats that a realistic digital clone (avatar) of a person can have in the wrong hands from the perspective of security and privacy. In his study, a network intrusion detection system, by protecting against cyberattacks, misuse, and negligence, and dynamic information flow tracking methods, by monitoring the flow of user login details, are proposed to detect unauthorised access to the metaverse platforms in an automated way to avoid avatar theft.

Appendix B.1.5. Asset theft and asset fraud

A virtual economy, containing valuable assets, within an urban cybercommunity has the potential to thrive significantly. These assets like digital currencies, NFTs, virtual items, and real estate purchases by users will be the primary targets of money-driven cybercriminals for the purposes of theft and fraud. Residents can lose their possessions if cybercriminals gain access to their digital credentials (Section Appendix B.1.3) and wallets. Moreover, the falsification of digital assets (i.e. virtual forgery) for fraudulent transactions will be another path that will be followed by cybercriminals. The genuine-like virtual forgery assets can be readily created using high-level imitation technologies – e.g. GAN with the generative and discriminator models (Section Appendix B.1.15). The securing of digital wallets for the protection of virtual assets and cybersecurity measures against virtual forgery will be the main subject within the metaverse cybercommunities. Fake digital assets such as non-existent properties, services, and fraudulent cryptocurrencies can be traded with legitimate currency with promises of unrealistic returns.

Appendix B.1.6. Brand/business theft and business impersonation

Businesses and users will create digital replicas of their real physical assets (e.g. real-world stores) in urban metaverse worlds. Virtual businesses can be hijacked for the purpose of ransom. Hijacked businesses/stores can be used to obtain user financial gains and credentials. Furthermore, the false version of shops can be created either to damage the brand's reputation or to exploit the reputation from a financial perspective. Moreover, impersonated businesses/stores that mimic legitimate companies can be used to compromise user accounts/credentials along with financial damages. For instance, criminals can create a fake store that looks identical to the real one to sell counterfeit products and the users may believe that they are buying real goods within these fake metaverse businesses. These digital businesses can be copied by cybercriminals to scam other businesses and organisations including governmental entities as well.

Appendix B.1.7. Cyberbullying, misuse of the platform

An urban metaverse ecosystem, with immersive abilities, would be an ideal space for antisocial behaviours such as cyberbullying, sexual assault, and fraud. In a virtual reality game, VRChat, a violating incident occurs about once every seven minutes [107]. Criminal actions are expected to increase as the metaverse expands with multiple application areas. These crimes will impact the victim's emotional and mental health, much like the way these crimes affect victims in the physical world [30]. These crimes, impacting emotional and mental health, can be committed by avatars with fake identities and may not be traceable regarding data sovereignty. Avatars can be registered with tokens to the MetaCyberCity and UMaaSs to mitigate these concerns, enabling the tracing of bad behaviour within the metaverse ecosystem, and leading to holding users accountable for their inappropriate actions such as cancelling their tokens. Furthermore, physical rules of avatars can be enforced using the metaverse software. For instance, Meta launched "Personal Boundary" for Horizon Worlds that will give people more control over their VR experience; the roughly 4-foot distance between an avatar and others will remain on by default for non-friends, and now an avatar can adjust his/her personal boundary from the settings menu in Horizon Worlds [108]. Moreover, the users can be exposed to racism. The interaction of children with strangers in metaverse worlds needs to be analysed before allowing children to immerse within uncontrolled virtual worlds concerning the misuse of these networks. Detection of abnormal content (e.g. inappropriate images, videos, text) in real-time using automated content profiling equipped with advanced AI tools is paramount to avoid imminent consequences of these attacks.

Appendix B.1.8. Phubbing and societal concerns

Phubbing is the act of rejecting or ignoring the company of a person in favour of a mobile phone. There is a high probability with the urban metaverse ecosystem that the level of phubbing increases within our real social environ-

ments due to its immersive virtual nature. From a cyber-dystopia point of view, the reduction of real, urban physical social interactions – intimate, real close relationships – replaced by virtual experiences using avatars within urban metaverse worlds may cause unforeseen negative effects and new types of psychological problems (e.g. the feeling of loneliness, social segregation, social exclusion) for humans, since metaverse worlds cannot be sufficient to meet the real closeness despite their immersive services, which should be analysed by related disciplines and the ways for addressing these societal concerns need to be revealed [1]. Moreover, it is well known that physical inactivity increases the risk of serious health conditions coronary heart disease, stroke, hypertension, and osteoporosis [109]. The massive use of metaverse environments may cause physical inactivity and physical activities should be incentivised within urban metaverse worlds to avoid aforementioned health problems [1].

Appendix B.1.9. Phishing attacks

In addition to the aforementioned phishing attacks mentioned in other subsections (Sections Appendix B.1.1, Appendix B.1.2), cybercriminals might create fake metaverse platforms (e.g. UMaaSs) that mimic both popular metaverse cyberspaces and avatars using AI-generated bots and then use phishing techniques to trick residents into providing sensitive information, such as login credentials or financial details while they are thinking that they are interacting with legitimate metaverse communities.

Appendix B.1.10. Social engineering & Disinformation/Misinformation

Residents can be manipulated based on the contents either created by themselves or in which they are interested. Trustworthiness and reliability of the content on social platforms have been in question all the time. The Matrix trilogy explores the interconnection between the body, the brain, and the mind, especially how that connection changes when the world turns out to be an illusion [110]. Virtual products (as a part of an advertisement) or AI-driven avatars, with their seemingly authentic stories, can be injected into the urban metaverse cyberspace as they are a part of the real environment to influence us one way or the other. Residents might be targeted for money laundering purposes. Social engineering attacks can be more convincing compared to web2, as cyber attackers can deceive users in a variety of effective approaches, particularly, using identity falsification and impersonation scams (Section Appendix B.1.1) such as the creation of realistic avatars (Sections Appendix B.1.1 and Appendix B.1.2) and businesses/stores (Section Appendix B.1.6) by exploiting the trust of others. Residents can be manipulated into taking malicious actions based on their interests, their sensitive information (single/married, sexual orientation, race) and their way of thinking. They can be drawn into fake romantic relationships and may end with huge financial losses based on the financial information revealed through well-established trusted relationships or end with physical and mental damages with real-world meetings. It might be difficult to distinguish between truth and disinformation/misinformation as urban

metaverse spaces look like realistic environments. Some checks and balances are required to validate the genuineness of actions and associated contents to be protected thoroughly.

Appendix B.1.11. Ransomware

Avatars, businesses, and assets or even urban metaverse worlds can be hijacked for ransomware purposes. Due to the information required for participation in the metaverse, malicious actors have more potential areas of information available to them to ransom. The strategy for a ransomer is to gain access to a system holding important information, insert their software which takes control of the system, and demand payment in exchange for not deleting the information. The metaverse, by the nature of its suffix, is interconnected, requiring communication between many different moving parts – meaning that the value of a single set of information has the potential to be exploited exponentially. Instant ransomware attacks to live events (e.g. concerts), while experiences are happening, are expected to increase in this ecosystem to exploit the situation by putting severe pressure.

Appendix B.1.12. Privacy breaches

Sharing experiences within metaverse cyberspaces means sharing your whole life including yourself, your emotions, and your reactions to events with the outside world. The immersive nature of the metaverse cybercommunities reveals more of us regarding the generated information using multiple sensors, which may violate our privacy out of our control. Our body signature (i.e. digital footprint) based on the somatic data (e.g. facial and eye biometrics, vocal pitches, posture, gestures, location) along with our reactions to developing events is being inevitably exposed as we engage in urban metaverse cyberspaces using highly immersive technologies, particularly, with VR/AR/XR headsets. Privacy protection or even information on privacy policies was found to be scarce in an analysis of 25 SCs with key concerns [111]. Owners of data are concerned with the risks of unauthorised usage of their sensitive data by various entities, including service providers [112] on the cloud platforms, particularly on the private cloud platform. We learned from the court cases and compensations that the technology giants governing social media had sold their user data to third parties without the consent of their users, which is a breach of privacy and security and these types of actions reduce trust in these companies. How to prevent sensitive data from unauthorised reading becomes an imperative issue in the development of cybercommunities regarding the collection of data from a highly distributed diverse computing environment and immense integration of DTs with the domains within SC, and with national and global domains [3]. Within this context, urban metaverse cyberspaces should be transparent with users about how they process the sensitive data of their users (Fig. B.10). Data sharing should be implemented using a consent-based approach where no personal data can be shared with third parties. Empowering users in the metaverse requires granular privacy controls and the ability to control what data is shared. Residents should be able to withdraw their pre-given consents

and their collected data must be deleted urgently if demanded by them. Users must be informed of the policies of the platform about what types of data can be deleted if requested concerning transparency. Residents should be able to leave the platforms as they wish without giving a reason.

The more the avatar resembles the user with advancing technologies, the more personal data such as physiological and behavioural signatures as well as the environmental space can be compromised with the sensory data transformation using immersive devices (e.g. VR/AR headset, MoCaps, haptics gloves, HTT, different types of WSs). Invasions of data privacy is one of the concerns. Privacy is supposed to be protected on Web3 where the owned data or assets are encrypted using distributed blockchain data structures and they can be shared with the other parties via smart contracts by the authorisation of the owner using private keys (i.e. cryptographic password or personal digital signature) securely within this token economy. Unauthorised access to user behaviour tracking that leads to emotion recognition for specific types of inputs could lead to serious privacy violations. For instance, users can be targeted by advertisements and they can be tracked with individual trajectory content management techniques, which can harm them mentally and financially. The invasion of physical privacy is the other concern. An avatar can be attacked (e.g. metaphysical, harassment, abuse) by other avatars in the virtual environment, which may cause psychological harm to the user of the avatar in the context that "the avatar is physically me". Personal boundaries with close friends and others should be defined in the controlled settings of immersive urban platforms as elaborated in Section Appendix B.1.7.

Appendix B.1.13. Distributed Denial of Service (DDoS) attacks

Metaverse urban cyberspaces are composed of distributed devices and services using wireless communication technologies and this wireless communication can be interrupted easily using jammer-type devices. Implementing advanced multiverse realms with smart wearables is analysed in [34]. Wearable hardware, which is one of the most important components of the metaverse, can also create new threats. With the increase in the use of VR headsets which may serve as suitable access points for hackers or AR devices in which the biometric data of residents are stored, they may become ideal targets for attacks. GPS services on which immersive devices rely can be easily spoofed or jammed and GPS signals can be lost promptly due to DoS attacks with a jammer with a reaction time in the order of a couple of microseconds, which causes severe prolonged signal outages. Due to the expected massive number of connected devices and network tenants, the 6G ecosystem would tend to be highly prone to DDoS attacks [35]. DoS attacks, theft of avatars and privacy breaches, in particular, for wearable metaverse devices, are the three main cybersecurity concerns in urban cybercommunities. Prevention of privacy intrusions without reducing overall QoE along with real socialising needs to be ensured. Blockchain technology has been introduced to mitigate these concerns in urban use cases. A framework that uses blockchain technologies was proposed in [37] for DTs to ensure the security of

transactions during the data streaming between virtual entities and physical entities. Similar security frameworks are expected to be developed in parallel with the increasing number of metaverse use cases in the years to come. Moreover, immersive services can be disrupted due to a lack of standardised metaverse security measures concerning the vulnerabilities and inconsistencies between a variety of interconnected devices and applications, which can impact users‘ experiences negatively.

Appendix B.1.14. VR/AR headset intrusion

Malicious actors can track every move of a resident through VR/AR headsets and user profiles can be built on this intrusion to be exploited. The experiences of residents can be manipulated, which can harm the users physically, mentally and financially. Facial, eye, ear, and body motion (e.g. gait motion, posture) features are transferred from VR/AR headsets to the counterpart avatars either to authenticate the user or to mimic user expressions and this is recorded on distributed or centralised ledgers on the blockchain operating systems for a variety of purposes. Furthermore, the personal surrounding is also recorded most of the time through a VR/AR headset to either determine the space to move for the avatar or to show i) where the user is going and looking, ii) whom the user is with, and iii) what the user is doing. Recording of these unique identifiers with biometric data creates serious data and identity protection risks along with privacy risks with our surroundings. Facial and eye expressions, emotions, and brain waves indicate how the user reacts to specific events or objects and they can be highly valuable data to be exploited for a variety of purposes (e.g. targeted product advertisement, DeepFake creations, identity theft (Section Appendix B.1.4). Furthermore, vital signs (e.g. heart and respiratory rates) can be detected through smart devices and AR/VR sets. Cyberattackers are inclined to exploit the vulnerabilities in VR/AR devices to steal the aforementioned sensitive personal information or to partially take control of these devices with several intrusion activities such as content placement. How we are responding to the placed items in the virtual environment can make us the target of advertisements. The privacy of users will be violated substantially when a hacker gains access to a user's VR/AR headset, sharing your life with you and seeing every part of your life. Users of VR headsets immersed in the virtual environment are in a vulnerable position, and they can be physically harmed by the manipulation of their perception and they can be directed in the wrong direction, leading to physical damage or life-threatening actions. Moreover, they, particularly children, can be mentally harmed by inappropriate content out of the context placed in virtual environments through wearable immersive devices.

Appendix B.1.15. Generative Adversarial Networks (GAN)

Several security weaknesses can threaten the safety of the CDL training process within the metaverse ecosystem, which might result in fatal attacks to either the pre-trained large model or the local sensitive data sets possessed by

an individual entity [29]. The GAN attacks have shown that poorly protected local data is vulnerable to being learned by adversaries [40]. In CDL, malicious participants in the urban metaverse cybercommunity can upload deceptive parameters to degenerate the model performance, or they can abuse the downloaded parameters to construct a GAN to acquire the private information of others illegally [29]. GAN, using generative AI approaches, may cause the generation of unhealthy, highly realistic synthetic trained models, which can disrupt/interrupt automated metaverse services and infiltrate behind/through services to gain access to the environment to exploit sensitive, private data (e.g. identity falsification & impersonation, asset fraud). Moreover, assets can be forged easily using GAN attacks. Efficient adversary detection-deactivation approaches are needed to disable the GAN attacks for a secure urban ecosystem.

Appendix B.2. COUNTERMEASURES

Appendix B.2.1. Agreed-upon standards, policies and ethics

As shown in Fig. B.10, the platform-based policies per specific cybercommunity, by considering its intended objectives and basic requirements, are moulded using i) individual policies determined by their users and businesses of cybercommunities regarding the rights of data sovereignty and ii) governmental or regional regulatory framework (e.g. GDPR). Flow of individual data, businesses and avatars between metaverse cyberspaces on the encryption-based and fully decentralised blockchain architecture is delineated in this figure. Individuals, as owners of their data, are the main actors in managing and controlling their sensitive data with little or no governmental/regional restrictions/interventions. The policies are determined and agreed upon by all stakeholders through a transparent, trustable, and ethical scheme. Individual sensitive data is not retained in cybercommunities if there is no necessity considering the regulatory framework and it is deleted instantly when the necessity is not a case any longer. Data protection measures within cybercommunities should be sufficiently assuring, and the sharing of data with third parties by cybercommunities should be consent-based - no data sharing without the ratification of data owners. Avatars and cyber businesses, along with their assets, should be teleoperating from one cybercommunity to the other within the urban metaverse ecosystem considering the interoperability of the metaverse.

Appendix B.2.2. Practice of cybersecurity hygiene

A chain is only as strong as its weakest link. Lack of metaverse awareness, regarding the understanding of the underlying cyber risks, should be mitigated. In this direction, everybody has to prepare themselves for the advantages and disadvantages of the technology by equipping themselves with some level of understanding about metaverse immersive experiences regarding the use of this developing technology before engaging in this ecosystem. The human factor is the main concern in cybersecurity measures. Therefore, first and foremost, all users of any urban metaverse

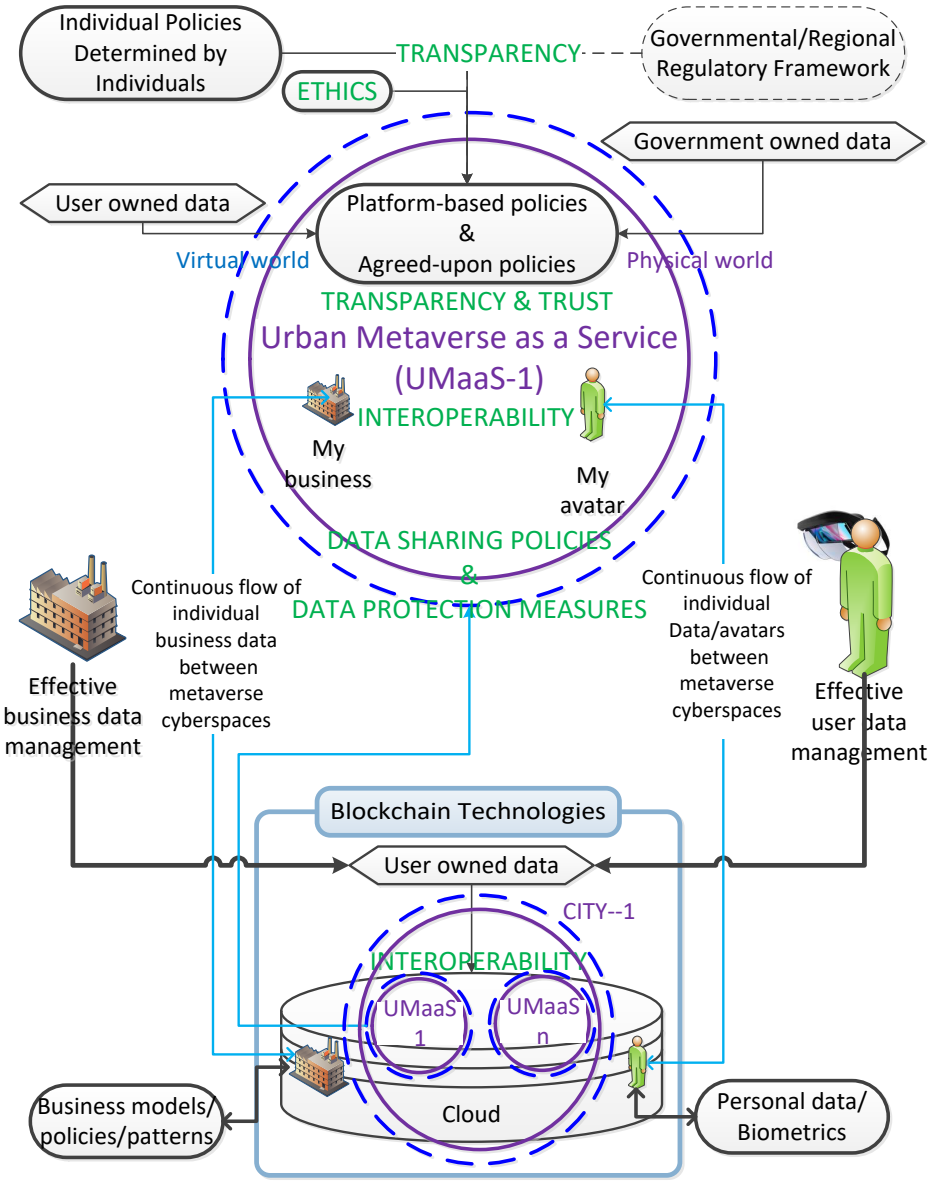

Figure B.10. Interoperability and transparency umbrella of MetaCyberCity: Flow of individual data, businesses and avatars.

platform have to be trained using the tools instilled into the platform about how to practice cybersecurity hygiene to avoid everyday cyberattacks (Section Appendix B.1) such as malware exposures or social engineering. Even the best systems can not be protected without practising cybersecurity hygiene properly.

Urban metaverse cyberspaces look like our real environment, a kind of DT of it. First, we should be thinking of incorporating similar cybersecurity measures that are implemented in our real environment along with the ones in Web2 into this real and virtual blended ecosystem and, accordingly, urban metaverse cyberspaces should be protected in a similar way by their main managing bodies (i.e. city governors) with policies in place (Fig. B.10) and

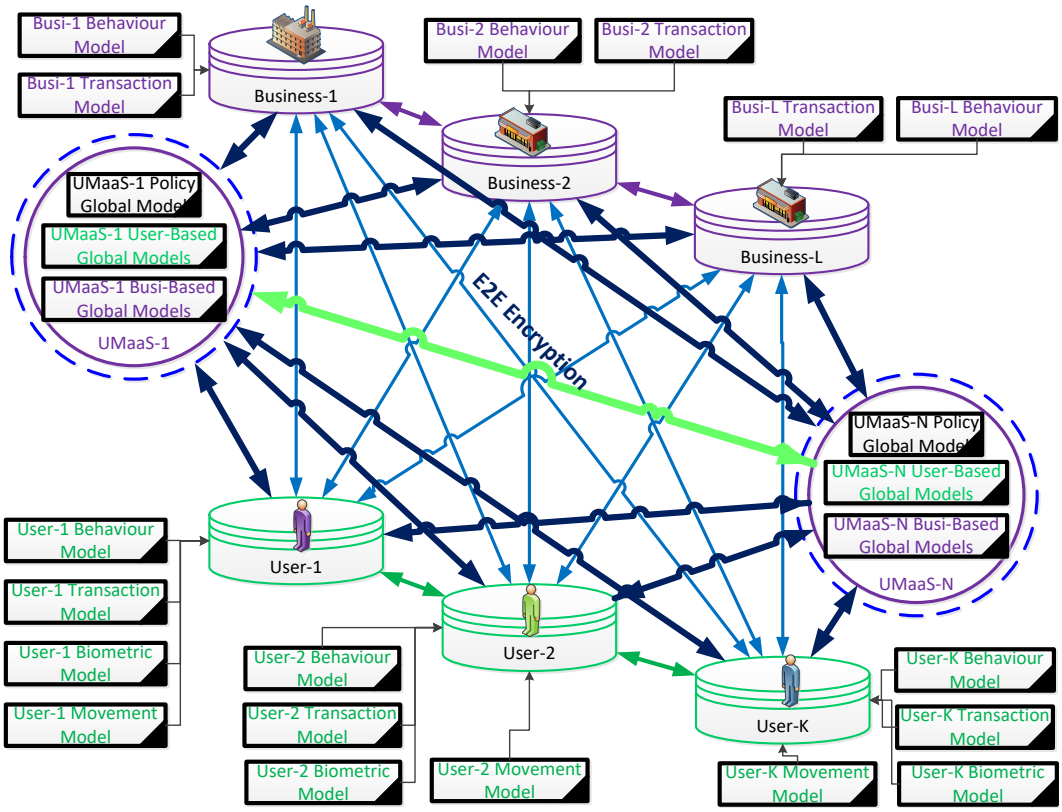

Figure B.11. Decentralised End-to-End (E2E) privacy-preserving CDL architecture: UMaaS-, Business-, and user-based local and global models.

advanced automated AI tools to detect instant attacks. For instance, strong metaverse credentials, with MFA, should be performed to protect ourselves from the most severe cyberattacks. Furthermore, we should keep in mind that this is not our real environment and further measures using novel cybersecurity techniques are required to protect ourselves from further possible cyberthreats (Fig. 5) augmented in this environment as elaborated in Section Appendix B.1. Technically speaking, the cybersecurity approaches should be specifically developed to the features and objectives of metaverse cybercommunities regarding the advantages and shortcomings of Web3. Every third-party individual entity (e.g. user, business) within the cybercommunity is untrusted, considering semi-honest parties or honest but curious parties. In this sense, the main urban entity (i.e. MetaCyberCity) and its cybercommunity entities (i.e. UMaaSs) (Fig. A.9) should be addressing the concerns of its residents appropriately, privacy concerns in particular, to provide proper cybersecurity hygiene such as: Are transactions safe? Is my data protected? Is my privacy protected in the metaverse urban spaces? Am I protected against the bad behaviours of other avatars? Etc. Having said this, it is worth emphasising that the human factor will remain the weakest point of defence, despite immense awareness efforts, meaning that the only other option is to strengthen other areas with effective AI approaches, such as the ability to monitor all AI-based attacks, as explored throughout this paper, where the platform-based generated data is in the

hands of the good to be processed by advanced AI tools in order to serve noble ends.

Appendix B.2.3. Detection of platform infrastructure security flaws

Every resident user, every business and every granular UMaaS is accepted as a private entity and all entities can communicate with each other within this design (Fig. B.11). All users, businesses, and granular UMaaSs as urban cybercommunity entities can communicate with one another whenever needed to run local automated allowed queries on local models and contribute to the construction of targeted global models of UMaaSs. The main communication scheme between entities is managed by the particular architecture of a UMaaS in which immersive experiences are taking place regarding the agreed-upon policies (Fig. B.10). Urban Metaverse cyber platforms, UMaaSs, should have effective governance and moderation policies to identify and mitigate malicious activities. Platform system attacks or insufficient resources can stop the functioning of the platform, leading to interruptions of experiences (e.g. interruption of an event such as a concert) within the platform. Finding the weak points of the system to defend better against cyberattacks is crucial in the metaverse. What cybersecurity level, that the MetaCyberCity and UMaaSs have, shall be measured regarding the resilience to the potential metaverse cyberthreats (Section Appendix B.1) before embarking on the MetaCyberCity or UMaaS. From a system engineering standpoint, a system shall adapt itself to the developing circumstances outside that surround and interact with the system to reduce risks and evolve. Urban metaverse cyberspaces should be able to detect and fix security flaws within the system in an automated manner and notify the affected data subjects where there are data breaches or other damages. Detection of flaws (e.g. abnormal resource usage) comes with protection solutions as well. The data, belonging to the particular platform, such as network trafficking, and resource usage are analysed in real time using the platform-based trained system models to improve the platform performance and to find out the abnormal activities taking place within the platform (cyberphobic attacks to avatars, malware attacks, spreading misinformation and disinformation, AI-generated bot attacks, GAN attacks, stealing and/or manipulation of system-owned data (system data breaches)). AIOps are already in place to manage the infrastructure of the metaverse worlds, particularly in managing structured and unstructured data and storing and disseminating it. More explicitly, AIOps provides event correlation capabilities by analysing real-time data and can determine deviations from typical patterns that might point to system anomalies. AI can be used effectively to predict attacks in the metaverse urban cyberspaces. ML-based trained models can help detect attacks directly to the infrastructure of the platform and defend the system from these attacks by improving its defence mechanisms with real-time effective solutions in an automated manner. Platform-based activities, interactions and experiences can be monitored in real time using automated decentralised privacy-preserving CL models, by considering the privacy of residents, to avoid any interruptions.

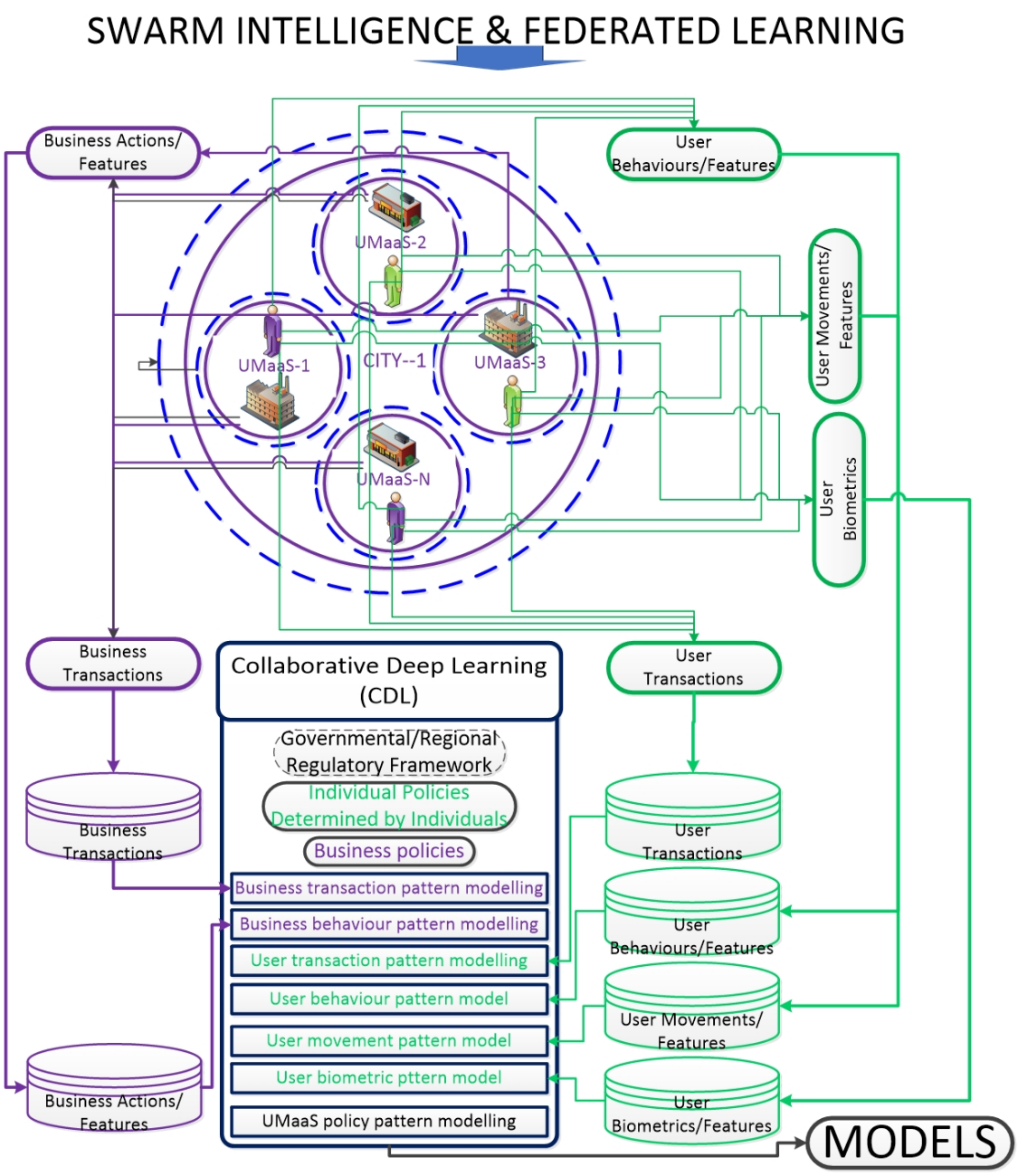

Figure B.12. MetaCyberCity: UMaaS- & Business- & User-Based AI learning and modelling.

Appendix B.2.4. Detection of Out-of-the-Pattern actions (OotPAs)

P2P/E2E interactions between entities are illustrated in Fig. B.11 within the distributed urban ecosystem. In addition to the interactions with other residents, users interact with urban businesses (e.g. via AI-driven avatars) within immersive urban metaverse cyberspaces to carry out commercial actions, such as the purchase of goods and their maintenance with smart metaverse contracts. Automated detection of outliers with inconsistencies that don't

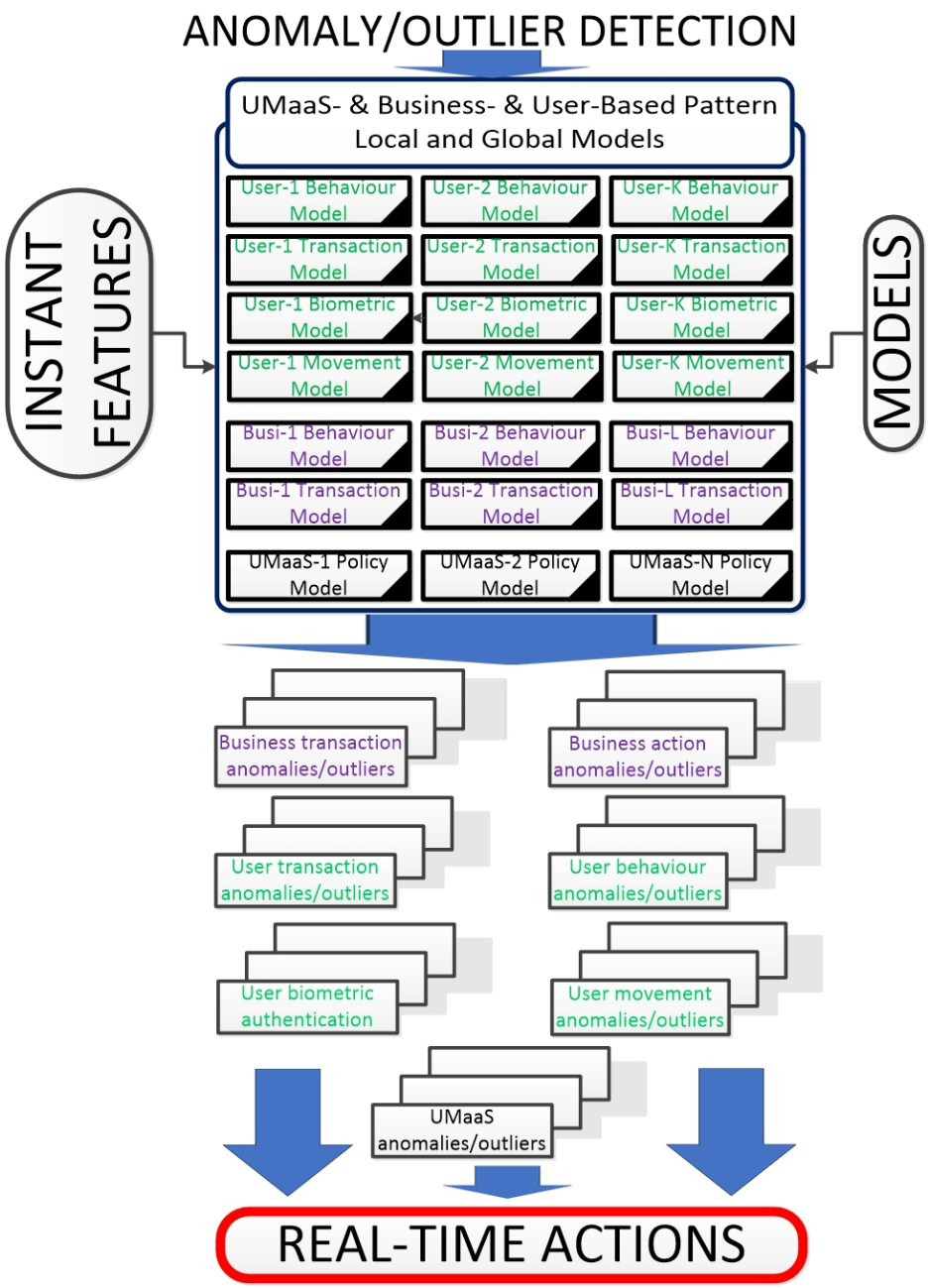

Figure B.13. MetaCyberCity: Human-out-of-the loop real-time anomaly detection to take real-time actions.

fit the real-world decent life norms or behaviours that don't match the trusted individual's or business's actions using advanced AI tools is paramount to provide residents and businesses with a secure environment with high QoE. Besides, residents with their avatars, businesses, virtual stores, and AI-generated avatars/bots can be classified with a scale of categorisation (e.g. ranging from very bad to very good) for various criteria (e.g. trust, use of language, behaviours) based on their pre-observed, pre-noted actions and the feedback obtained from the other residents and businesses in

the same metaverse cyberspace. Each entity can upgrade the other entity's credibility. Entities can hide their previous adverse actions in the real world from others but not in the urban metaverse environment where the previous actions are noted and not forgotten, considering the agreed-upon policies of the particular metaverse cyberspace (Fig. B.10). Any user should face punishment if acting against the policies of the platform virtually or legally based on the severity of the actions. They, based on their actions, can be categorised as "red", "orange", "yellow", or "green" regarding their risk profiles based on the aforementioned criteria, but always by prioritising privacy and respecting data sovereignty. Entities, with repeated, extreme adverse actions, can be tagged with colours on a red gradient to make other virtual businesses and residents vigilant against these entities. Entities can be banned from entering cybercommunities where their actions are getting severe. However, all these approaches, which are dependent on human responsible actions, are not sufficient to provide residents with completely instant, automated, and secure protection within this newly developing urban metaverse ecosystem, considering the large number of transactions and actions, which need to be authenticated and verified immediately.

CDL/FL, as elaborated in Section 2.3, can help detect OotPAs to alleviate cyberthreats. As shown in Figs. B.12 and B.13, automated platform-, user- and/or business-focused cybersecurity ML models can be generated by utilising SAI, primarily CDL to both monitor OotPAs leading to the detection of cyberattacks and address those attacks in real time using the automated cybersecurity measures (Fig. 5). A decentralised privacy-preserving CDL architecture, where every resident user, every business, and every granular UMaaS is accepted as a private entity and all entities can communicate with one another whenever needed to run local, automated, and allowed queries on local models and to contribute to the construction of targeted global models of UMaaSs within this design, is conceptualised in Fig. B.11. Nevertheless, these approaches have their shortcomings in providing the required level of privacy, authentication and verification mechanisms as explained in Section 2.3. It is worth explaining that in addition to profit-driven companies within the urban community, we extend the concept of "business entity" within this paper by including all other value-adding community organisations and institutions within an urban environment: governmental organisations and institutions (e.g. educational units, hospitals), and Non-Governmental Organisations (NGOs) (e.g. British Heart Foundation and private universities).

Appendix B.2.5. Awareness of cybercriminal experiences and best practices

A sense of urgency to gain something (e.g. crypto money, assets, tickets, membership, promotions) may pressure urban metaverse users into hasty decisions, leading to harmful consequences. Most of the cyberthreats and risks can be avoided by staying vigilant with a high level of cybersecurity hygiene (Section Appendix B.2.2) within the urban metaverse cybercommunity. The MetaCyberCity and its granular functions/organisations – UMaaSs – should have cybersecurity awareness platforms and encountered vicious events (e.g. scams, impersonation, suspicious activities,

etc.) should be reported via these platforms to raise awareness to help prevent these adverse actions. Furthermore, advanced automated cybersecurity mechanisms, which mitigate the encountered experienced cyberthreats, should be incorporated into the MetaCyberCity swiftly.

Appendix B.2.6. Visibility versus invisibility & Anonymity

Invisibility, feeling the immersive nature of the cybercommunities without being seen, and anonymity, situations where an individual's identity is unknown to other users using an anonymous avatar during the immersive interaction, are two sensitive subjects, which should be investigated in detail with respect to the objectives and requirements of specific cybercommunities and the rights of other users within the same cybercommunity. However, specific transactions and immersive communications may require the authentication of the individual's identity to avoid any potential fraudulent attacks. Technically speaking, users can make other people invisible to themselves and themselves invisible to other users. Privacy can be provided via an invisibility option that can be defined in the settings of urban cybercommunities without violating the rights of other users who join the platform actively. For instance, a person can join a metaverse meeting or a concert without being noticed by other users. Anonymity can be authenticated by the platform that knows the true identity of the user even though the individual identity is still unknown to other users for privacy and security reasons. It is noteworthy to highlight that these rights – having an invisible or anonymous avatar – can effectively be exploited by cybercriminals as well. The fact that you can make multiple avatars, which are not NFTs, and act with different levels of anonymity makes it easier for cybercriminals to get away with their crimes, making it hard to hold people or businesses responsible for their adverse behaviours. Therefore, this subject is an open issue that needs to be discussed by the research community comprehensively.

Appendix B.2.7. Homomorphic Encryption (HE)

HE enables multiple entities to perform complex queries and computations on encrypted data without compromising the privacy of data and its encryption. The processed result still may remain in encrypted form for the owner of the data to decrypt it using the private key for visualisation. Concretely speaking, sensitive data can be shared and computed without the need to decrypt, but with a large computational overhead. The ciphertext operation's computational complexity is much higher than that of the plaintext operation, both in terms of memory consumption and processing time [113]. There are three types of HE, namely: partially HE, somewhat HE, and fully HE. Fully HE produces the largest computational overhead compared to the other two HEs, while having infinite addition and multiplication operations on ciphertexts. Fully HE is being employed by many giant companies such as Microsoft to compute sensitive data in the public domain despite its computational overhead and complexity. Most importantly, it allows to training of homomorphic-based encryption structures to build larger learning models, namely CDL models, using SAI. HE's

goal is to prevent recovery of the original data in order to protect privacy and the data from unauthorised access. ML-as-a-Service (MLaaS) techniques using the processing of encrypted data with HE-like approaches will be focused on in the future, particularly, for applications which need a high level of privacy-preserving requirements on data that is stored in public domains and need to be computed by multiple entities. Another privacy preservation technique, which has captured a wide range of attention, is differential privacy which was developed in [114], by which noise is added to the data to secure the data from attacks. However, the more noise added to the data to provide further security and privacy, the less the model accuracy is obtained. This technique is out of the scope of this paper.

Appendix C. SHORTCOMINGS OF FEDERATED LEARNING AND COLLABORATIVE LEARNING

A large number of transactions and immersive experiences shall be managed in a safely automated manner in urban metaverse cyberspaces. AI can play a significant role in securing transactions through ML models equipped with Swarm AI (SAI). Federated Learning (FL), introduced by Google, has gained prominence as an effective solution for addressing data silos, enabling collaboration among multiple parties without sharing their data [26]. In FL, each entity trains its own data locally, and only the locally generated model itself is sent to the central server to aggregate all the models to form the final model for each entity to utilise. Collaborative Learning (CL) and FL have been used interchangeably in the literature to train global models using SAI. The concepts and applications of FL are analysed in [63]. With the increasing need for collaborative work, as well as the increasing concern in data privacy, Collaborative Deep Learning (CDL) has become much more common [29] regarding its successful application with Deep Neural Network (DNN) models established on Big Data (BD) – with some of these instances of success being reached on imperfect conditions. CDL models enable parties to locally train their deep learning structures and only share a subset of the parameters in the attempt to keep their respective training sets private [64]. The CDL framework allows local devices to cooperate on training models without sharing private data, which resolves the contradiction of the availability and privacy of data [40]. From a technical standpoint, DL can be performed in a collaborative manner, where a parameter server is required to maintain the latest parameters available to all parties [41]. Data, particularly BD, is distributed among multiple entities due to changing distributed architecture (e.g. cloud, metaverse), its strategic value, data privacy and security, which necessitates CL – with distributed multiple entities. In CL, a learning model is constructed using multiple distributed data points, possibly by exploiting whole data, either belonging to a single user, multiple users, a single platform, or multiple platforms to extract common features or patterns by preserving data privacy. New and effective approaches (e.g. [115]) are necessary to turn large volumes of information into wisdom/insights at their sites and to transfer the required abstract insightful form of the data to the entities which demand this – considering the privacy and security of data. Although local data is not directly shared with FL, models

trained on this data may also be spied on by malicious adversaries, semi-honest parties, or honest but curious parties, when local models are aggregated into a centre. Moreover, under the circumstance of knowing the local model, spies may adopt some attacks to restore the original data, which indirectly leads to information leakage [27].

Appendix D. LIST OF ABBREVIATIONS

ABR:	Automated Behaviour Recognition
AER	Automated Emotion Recognition
AoE	Automation of Everything
AI	Artificial Intelligence
BD	Big Data
Bi-LSTM-RNN	Bidirectional Long Short-Term Memory Recurrent Neural Networks
BlockFL	Blockchain FL
BP	Business Profiling
CA	Content Awareness
CCPA	California Consumer Privacy Act
CDL	Collaborative Deep Learning
CL	Collaborative Learning
CPSs	Cyber-Physical Systems
CPSSs	Cyber-Physical Social Systems
CoBs	Classification of Businesses
CP	Content Profiling
CoUs	Classification of Users
CoW	Cybercommunity of Wisdom
DAO	Decentralised Autonomous Organisation
DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
DNN	Deep Neural Network
DPPML	Decentralised Privacy-Preserving Machine Learning
DRM	Digital Rights Management
DTs	Digital Twins
E2E	End-to-End

FDPDDL	Fair and Differentially Private Decentralised Deep Learning Framework
FL	Federated Learning
GPT	Generative Pre-trained Transformers
GAN	Generative Adversarial Networks
GDPR	General Data Protection Regulation
GMaaS	Global Model as a Service
HAR	Human Activity Recognition
HD	High-Definition
HE	Homomorphic Encryption
HSCUM	Human- and Society-Centred Urban Metaverse
HTT	Hand Tracking Toolkit
ICT	Information Communication Technology
IL	Imitation Learning
IMS	Identity Management Systems
IoE	Internet of Everything
IoT	Internet of Things
IIoT	Industrial IoT
LMaaS	Local Model as a Service
MFA	Multi-Factor Authentication
MLaaS	ML as a Service
ML	Machine Learning
MoTs	Metaverse of Things
MoC	Metaverse of Country
MoCaps	Motion Capture Suits
MoW	Metaverse of World
NeRFs	Neural Radiance Fields
NFTs	Non-Fungible Tokens
NGOs	Non-Governmental Organisations
NPCs	hlcNon-Player Characters
QC	Quantum Computing
QoE	Quality of Experiences

QoL	Quality of Life
P2P	Peer-to-Peer
PoS	Proof-of-Stake
PoW	Proof-of-Work
PP	Platform Profiling
PPML	Privacy-Preserving Machine Learning
PPDL	Privacy-Preserving Deep Learning
RFID	Radio-Frequency Identification
RL	Reinforcement Learning
OotPEs	Out-of-the-Pattern Events
SA	Situational Awareness
SPoF	Single Point of Failure
SAI	Swarm Artificial Intelligence
SC	Smart City
SSI	Self-Sovereign Identity
TBSN	Distributed Trust-Based Secure Networks
TI	Tactile Internet
UMaaSs	Urban Metaverse-as-a-Services
UP	User Profiling
URLLC	Ultra-Reliable Low Latency Communications
UTs	Urban Twins
ViLO	Virtual London
WRSs	Wearable Resistive Sensors
WSs	Wearable Sensors