Blockchain-Based Decentralised Privacy-Preserving Machine Learning Authentication and Verification With Immersive Devices in the Urban Metaverse Ecosystem

Kaya Kuru * and Kaan Kuru

Posted Date: 6 February 2024

doi: 10.20944/preprints202402.0317.v1

Keywords: Metaverse; Smart City (SC); Digital Twins (DTs); cybersecurity; Swarm Artificial Intelligence (SAI); Collaborative Deep Learning (CDL); Federated Learning (FL); Privacy-Preserving Machine Learning (PPML); blockchain; avatar

Article

Blockchain-Based Decentralised Privacy-Preserving Machine Learning Authentication and Verification With Immersive Devices in the Urban Metaverse Ecosystem

Kaya Kuru [1,*,†] and Kaan Kuru [1,†]

[1] School of Engineering and Computing, University of Central Lancashire, Preston, PR1 2HE, UK
* Correspondence: kkuru@uclan.ac.uk
† These authors contributed equally to this work.

Abstract: 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 worlds, an extension of residents and urban society where the virtual and the physically real blend and are more organically integrated, are meant to mirror the fabric of urban life with no harm to their residents. The success of urban metaverse cybercommunities depends on the quality of data-driven Smart City (SC) Digital Twins (DTs), the seamless exchange of data between cyber and physical worlds (e.g. between residents and their counterpart "Avatars") and the processing of the data effectively and efficiently with no vicious interventions. The potential risks in this ecosystem that incorporates Web3 can be extremer than the ones in Web2 since users are immersed with multiple tightly coupled wearable sensor-rich devices perceiving the blend of the real and the virtual with possible imminent negative experiences. This study, by analysing potential cyberthreats in the urban metaverse cyberspaces, proposes a blockchain-based Decentralised Privacy-Preserving Machine Learning (DPPML) authentication and verification technique, which uses the metaverse immersive devices and can be instrumented effectively against identity impersonation and theft of credentials, identity, or avatars.

Keywords: metaverse; Smart City (SC); Digital Twins (DTs); cybersecurity; Swarm Artificial Intelligence (SAI); collaborative deep learning (CDL); Federated Learning (FL); Privacy-Preserving Machine Learning (PPML); blockchain; avatar

1. Introduction

"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 [1]." 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 [2]. 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 worlds – cybercommunities – are meant to mirror the fabric of urban life by providing virtually inhabitable cities with no harm to their residents. The metaverse, which aims to build high-fidelity 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) [3]. Urban metaverse worlds – an extension of residents and urban society, where the virtual and the physically real blend and are more organically integrated and where real-person resident avatars, government avatars, governmental entities, organisations, businesses, and avatars driven by Artificial Intelligence (i.e. AI bots or virtual

 doi:10.20944/preprints202402.0317.v1

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 success of urban metaverse communities, augmented with wisdom, depends on the quality of data-driven SC Digital Twins (DTs), the seamless exchange of data between cyber and physical worlds (e.g. between residents and their counterpart "3D Avatars" – pseudo-physical presence) and the processing of the data effectively and efficiently with no vicious interventions and threats. An urban metaverse ecosystem framework – MetaOmniCity – was designed in [3] to demonstrate a variety of insights and directions for policymakers, city planners and all other stakeholders about how to transform data-driven SCs with DTs into virtually inhabitable cities with a network of shared immersive urban experiences from a metaverse point of view. MetaOmniCity, allowing the metaversification of cities with granular virtual societies, i.e. MetaSocieties, aims to facilitate the building of community and citizen-tailored high-fidelity virtual urban metaverse cyberspaces for future sustainable smart urbanism in which the city productivity, wealth, and QoL can be increased – thus substantially benefiting every citizen, enabling innovation, and economic development within a city.

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. Motion Capture Suits (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. On the other hand, the abilities of these 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 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 the metaverse-immersive devices to generate Privacy-Preserving Machine Learning (PPML) models, is designed. This design, by avoiding single point failure and eliminating a trusted third party for the verification of the authenticity of models, can be instrumented effectively against identity impersonation and theft of credentials, identity, or avatars within urban metaverse cyberspaces – without renouncing

 doi:10.20944/preprints202402.0317.v1

targeted functional abilities of the immersive devices and the essential objectives of the urban metaverse cyberspaces.

The remainder of this paper is organised as follows. The related works are presented in Section 2. The components of urban metaverse cyberspaces are summarised in Section 3. Cyberthreats and basic countermeasures for urban cyberspaces is explained in Section 4. The proposed methodology is introduced in Section 5. Section 6 discloses the essential challenges in revealing and addressing cyberthreats within urban metaverse worlds. The lessons learned are unfolded in Section 7. Discussion along with open issues is provided in Section 8. Finally, Section 9 concludes the key findings and outlines potential future directions.

2. Literature Survey

2.1. Metaverse Concept and AI

The leading, gigantic companies such as Meta, Microsoft, NVIDIA, 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, 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 Internet) to the next level in which more people would be immersed in virtual worlds augmented with reality [3]. The metaverse taxonomy, definitions, architecture, applications, challenges, issues, solutions, and future trends are reviewed in [4], [5], [6]. AI approaches specific to the development of metaverse items are surveyed in [7] and the fusion of blockchain and AI with the metaverse is surveyed in [8]. Blockchain-empowered service management for the decentralised Metaverse of Things (MoTs) is analysed in [9] 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 visualization. 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 [10]. Building metaverse cyberspaces using DTs at all scales, states, and relations is examined in [11]. Some of the key issues, required in order to realise metaverse services based on DTs, are discussed in a short paper in [12].

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 [13]. The vision of using Non-Fungible Tokens (NFTs) – blockchain-based tokens – in SCs is explored in [14]. 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 [15], [16], [17]. A theoretical framework by reviewing literature and synthesising best practices in designing metaverse learning environments regarding the SC education domain is proposed in [18]. An extensible SC metaverse tourism platform is disclosed in [19]. The metaverse applications built for specific SC domains are elaborated in [3] with a framework – MetaOmniCity – that derives a conceptual infrastructure instilled with AI for the development of urban metaverse parallel worlds upon SC DTs by encouraging citizen cooperation with experiences. MetaOmniCity, as the logical extension of SC DTs, 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.

 doi:10.20944/preprints202402.0317.v1

2.3. Swarm Artificial Intelligence (SAI) And Blockchain in Urban Metaverse for Privacy and Security

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 [20]. 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 interchangeability in the literature to train global models using SAI. The concepts and applications of FL is analysed in [21]. With the increasing need for collaborative work, as well as the increasing concern in data privacy, the Collaborative Deep Learning (CDL) has become much more common [22] 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 [23]. 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 [24]. 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 [25]. 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. [26]) 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].

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 4.2.7. SEALion, CryptoNet [28], 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 [29] 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 [30]. A full HE scheme to the standard DNN, ResNet-20, is applied in [31] to implement PPML. A universal multi-modal vertical FL framework is proposed in [20] 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

 doi:10.20944/preprints202402.0317.v1

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 [32], 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 personalized HAR model. An adversary detection-deactivation method for metaverse-oriented CDL is proposed in [22].

Cybersecurity threats against the metaverse as well as privacy concerns are analysed in [33], [34], [35], [36]. 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 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 identities representing all types of assets) are interesting economic targets for hackers [34]. 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 standalone technology, as they require a well-configured blockchain and an efficient off-chain data storage solution in order for them to function properly [14]. There is a risk of blockchain-related fraud in financial institutions [34]. The concept of smart contracts aims to ensure that transactions are completed safely. 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 [37]. 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 [38]. 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 [39]. A framework that uses blockchain technologies was proposed in [40] 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 minimizing exposure and leakage of their data [41]. 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 secure generation of SAI in a distributed manner. A blockchain FL (BlockFL) mechanism, enabling on-device ML without any centralised, training data or coordination by utilizing a consensus mechanism is proposed in [42] 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 the 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. [24] aim to address the threat from Generative Adversarial Network (GAN) attacks pose to collaborative deep learning (CDL) and propose a model-preserving CDL framework, called MP-CLF, which can effectively

 doi:10.20944/preprints202402.0317.v1

resist the GAN attack. An adversary detection-deactivation method for metaverse-oriented CDL is proposed in [22] to avoid GAN attacks. A blockchain-based, differentially private, decentralised DL framework, which enables parties to derive more accurate local models in a fair and private manner, is proposed in [25]. 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 [43]. 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 privacy of residents.

3. Components of the 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 [3]. 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.

3.1. 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 [44]. 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 [44]. The concepts of "Internet of Everything (IoE)" and "Automation of Everything (AoE)" [45] bring the people, organisations, lives, processes, data, and things into a concrete coherent structure – Cyber-Physical Systems (CPSs) to develop a synergistic smarter connected globe [44]. SC connects physical infrastructures, Information Communication Technology (ICT) infrastructures, social infrastructures, and business infrastructures to leverage the collective intelligence of the city [46]. 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 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 [44]. Readers are referred to [44] for the technological infrastructure of SCs involving communication networks and further information about real-world SC use cases. To summarise (Figure 1), 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.

 doi:10.20944/preprints202402.0317.v1

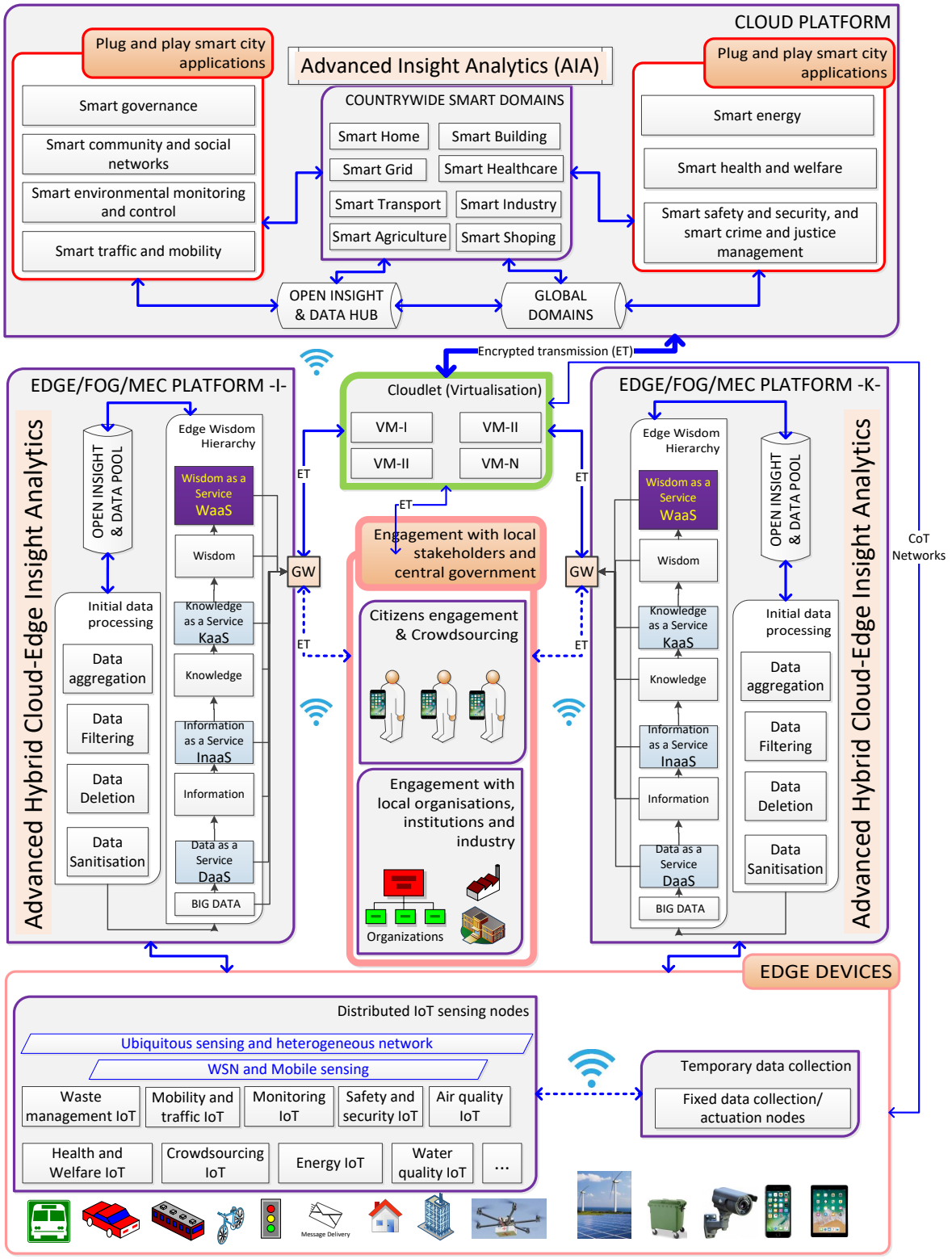

Figure 1. Main components of SC and their interaction with each other [44].

3.2. SC Digital Twins (DTs)

SC DTs are the building blocks of SCs. Through DTs, the real world can be accurately replicated in the virtual plane digitally across multiple levels of granularity and can interact dynamically and evolve synchronously with the virtual twin in the virtual plane [47]. The construction of DTs, i.e. blueprints of SCs, that facilitate the means to monitor, understand and optimise the functions and

 doi:10.20944/preprints202402.0317.v1

Situational Awareness (SA) of all physical entities by i) pairing of the virtual and physical worlds [48], ii) enabling data to be seamlessly transmitted between the physical and virtual worlds with two-way communication [49] and iii) enabling the virtual entity to exist simultaneously with the physical entity [50] is an integral part of building healthy SCs and Urban Metaverse-as-a-Services (UMaaSs) (elaborated in Section 3.4) augmented with real-time streaming data. SCs, filled with ubiquitous sensors (Figure 1), ease the detection of real urban environments and they stream this information simultaneously to build urban DTs for accurate topography, visualisation, simulation, anticipation, precise interpretation and predictions, and solving urban problems with innovative eco-friendly ways of urban planning benefiting the well-being of citizens.

DTs of physical worlds would be the base for developing ultra-realistic metaverse worlds. Readers are referred to our previous studies ([51], [52], [53]) for the examples of DTs developed by us. On one hand, these similar DTs – digitised copies/mirrors of SC domains – in highly synchronised environments are not only utilised to manage SC assets efficiently and effectively but also to help SC services to be integrated into the metaverse platforms easier to facilitate a more immersive experience leading to significantly increased quality of urban living. The interaction between DTs and the urban metaverse cyberspaces – UMaaSs – is conceptualised in Figure 4. On the other hand, the concept of the metaverse with its advancing immersive tools would not only enable the development of the realistic modelling of urban processes as they behave in their physical worlds, but also, would encourage and accelerate further community engagement by addressing user requirements better leading to more advanced models [3]. A metaverse, which is parallel to the physical world, needs mature and secure DTs technology in addition to parallel intelligence to enable it to evolve autonomously [54]. For instance, the project – Virtual London (ViLO) platform – (Figure 2) [55] integrates real-time weather information, that affects the visual aspect of the digital model. Regarding "Smart transportation", a specific emphasis was put on the visualisation of mobility data sets. ViLO can retrieve and visualise the location and data of bike-sharing docks, bus networks and tube lines, including the location of bus stops and tube stations and the real-time position of buses and trains. The realisation of the metaverse is highly correlated with the advancements in DTs [12], [56] that reflect the lively atmosphere of a real-time physical entity in which urban physical objects (e.g. roads, buildings) along with real-world real-time data (e.g. traffic flow) are digitised in a moulded environment [3]. Most of the cities have their multiple 3D models involving underground infrastructure used for planning and construction, and these models are categorised as "(high-fidelity virtual) SC physical worlds (twins)" and this should not be confused with "SC DTs". Highly realistic "SC DTs" (i.e. models) are composed of synchronised "(high-fidelity virtual) SC physical worlds (twins)" and related delay-sensitive "SC digital data twins" (Figure 4) allowing residents and other users to interact with the virtual SC ecosystem that is created similarly to the real SC ecosystem.

 doi:10.20944/preprints202402.0317.v1

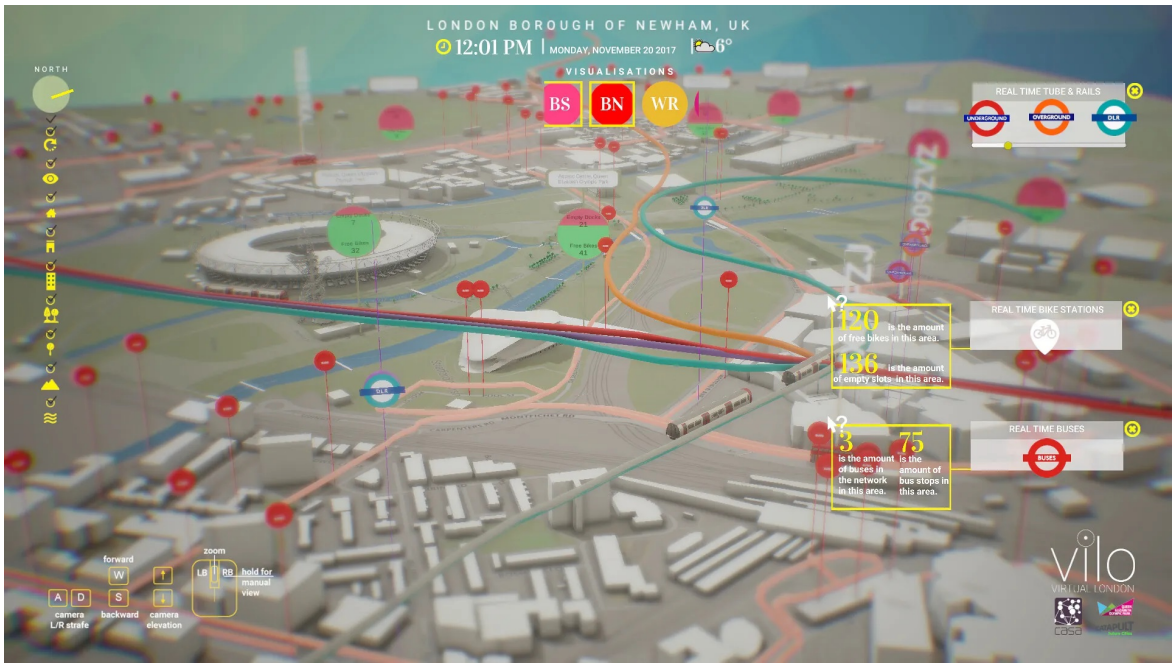

Figure 2. Simulation of reality through DTs: ViLO model showing live sensor data on infrastructure equipped with VR and AR [55]. 3D urban modelling and virtual urban static and mobile objects reflecting the streamlining of the real data of CPSs are blended and this scene is augmented with information/knowledge/wisdom from real-world activities for effective decision-making.

3.3. Urban metaverse ecosystem: MetaCyberCity

The urban metaverse ecosystem, the so-called MetaCyberCity is the interconnected network of decentralised blockchain worlds, i.e. UMaaSs, 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 3.4). The general infrastructure of the urban metaverse with the key enabling technologies is depicted in Figure 3. 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 [3]. 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" [3]. An urban metaverse can be defined as the expansion of DTs in the fields of people and society [54]. 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 [57]. 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.

 doi:10.20944/preprints202402.0317.v1

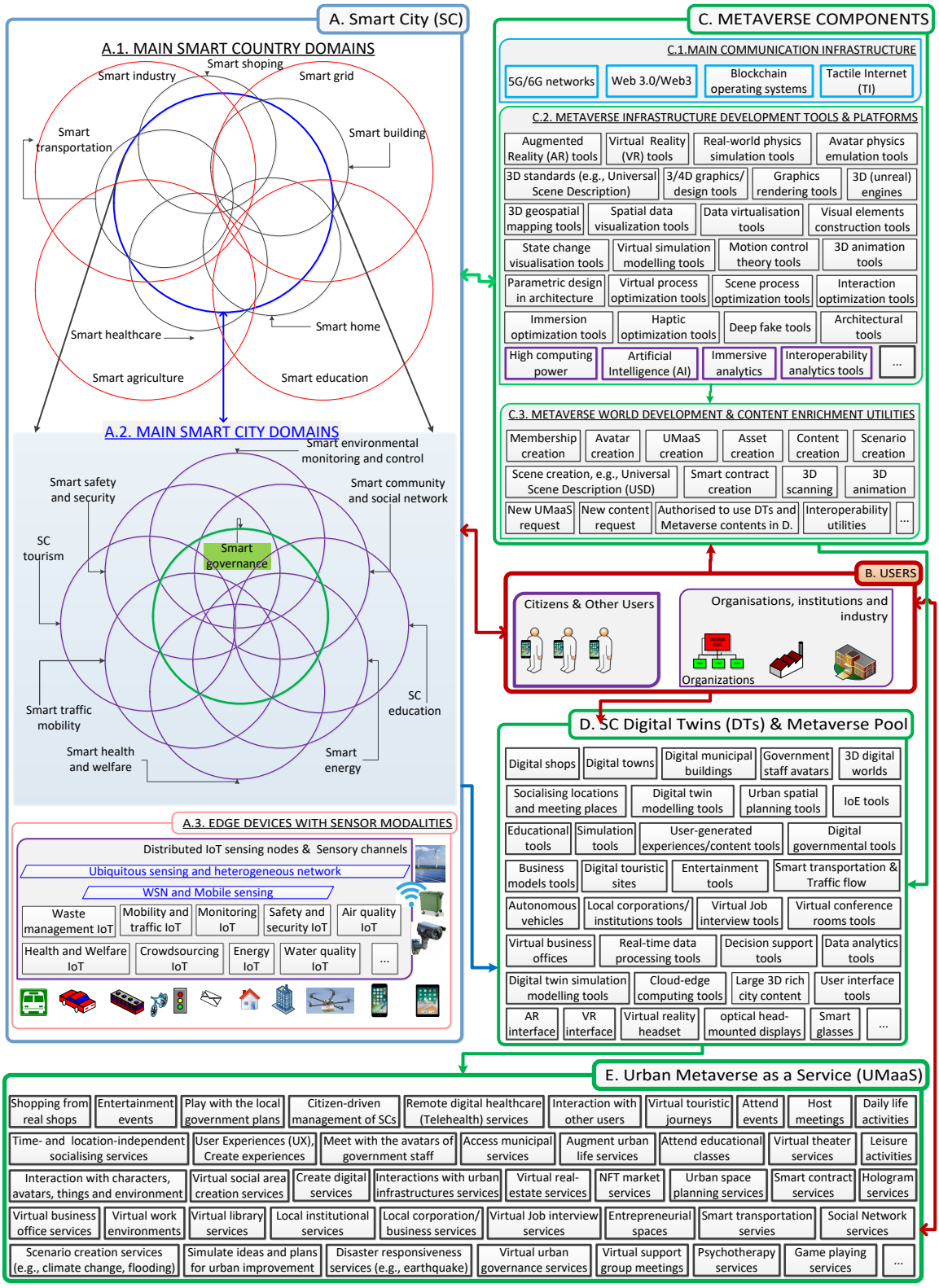

Figure 3. Architecture of a metaverse city: Main components and their interaction with each other [3].

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 secure manner; smart contracts extend

 doi:10.20944/preprints202402.0317.v1

the capabilities of blockchain technology; they are executable codes that can convert into software 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 [38]. The key components of the metaverse in developing urban worlds are summarised in Figure 3 C.

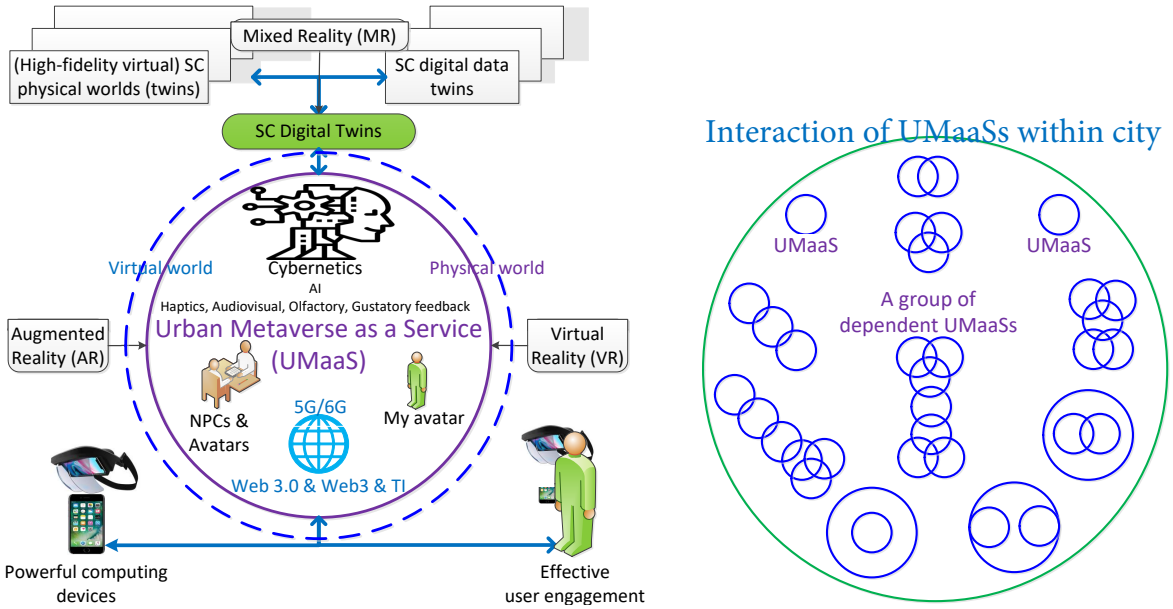

Figure 4. Left: Pivotal components of UMaaS. Blurring borders between virtual and physical worlds. Right: Various structural design models of UMaaSs: Jointed (dependent) and unconnected (independent) spaces (Figure 3E).

3.4. Urban Metaverse-as-a-Services (UMaaSs)

We explained the concept of UMaaS within urban metaverse worlds for the first time in our previous research [3]. 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 Figure 3E. 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 SC DTs. 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 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 (Figure 4 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

 doi:10.20944/preprints202402.0317.v1

multiagent nodes, can be governed by the principles of Decentralised Autonomous Organisation (DAO), by which they turn into member-owned organizations. 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 power to direct the policies of not only local and central governments but also other related organisation 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.

3.5. 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 [1] 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.

3.6. 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

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

 doi:10.20944/preprints202402.0317.v1

a set of rules defined for them representing their real-world characteristics by fulfilling the scene anticipation. Avatars can interact with NPCs concerning the rules defined for NPCs.

3.7. 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 [3]. 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.

3.8. 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 our previous research [3], [44], [52], [58]. 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 that is investigated in 3.2 with related metaverse content. The engines of the metaverse communication infrastructure on which metaverse applications can run seamlessly are placed in Figure 3 C.1. The foundational pillars of this infrastructure are 5G/6G networks, Web 3.0 / Web3, blockchain operating systems and Tactile Internet (TI).

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) [59].

 doi:10.20944/preprints202402.0317.v1

6G, not only promises to connect things with 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 [38] 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 [60] 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 [3]. 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 [61] 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 SC DTs (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 [54].

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 [62]. 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 [63]. 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 [64], 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 [65].

4. Cyberthreats and Basic Countermeasures for Urban Cyberspaces

Possible urban cyberrisks, cyberthreats, and privacy concerns are analysed in this section before exploring the proposed PPML authentication technique in Section 5. 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 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, unauthorized 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

 doi:10.20944/preprints202402.0317.v1

ecosystem. The main threats that can be launched in urban cybercommunities are demonstrated in Figure 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 before revealing the proposed approach in this study in Section 5. 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, optimizing 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 [66]. On one hand, promising Quantum Computing (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 [38].

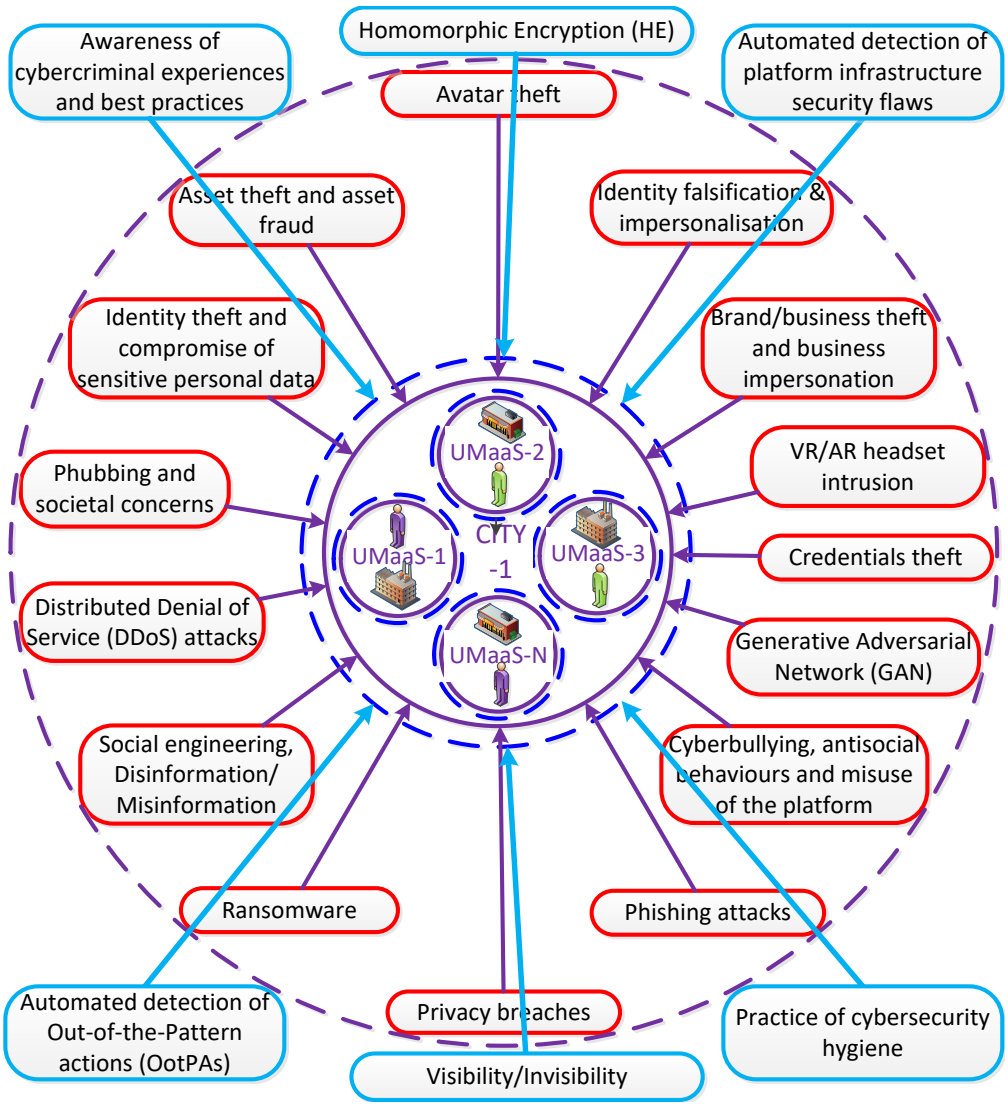

Figure 5. Cyberthreats against urban metaverse cyberspaces and basic countermeasures.

 doi:10.20944/preprints202402.0317.v1

4.1. Urban Metaverse Cyberthreats

4.1.1. 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 [67]. 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 (4.1.15)) 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 given by the government would mitigate these concerns, but this may not be an ideal option for residents concerning privacy regarding being tracked by the government.

4.1.2. Identity theft and compromise of sensitive personal 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 the execution of various malicious actions. The metaverse environments can be compromised by malicious software (i.e. Malware) that can stop us from reaching our environment, prevent us from transferring our personal 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 unauthorized access, data breaches, or disruption of services. Every now and then, our highly sensitive personal data gets leaked and becomes compromised due to the ineffective implementation of cybersecurity measures in the online services/social media that we use. Compromised identity data can be moulded to create fake avatars that can mimic their counterparts to manipulate other users (Sections 4.1.1).

4.1.3. 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 4.2.2) and should not be sharing their private keys with others in cybercommunities to avoid every type of attack that is summarised in Figure 5. The encryption approaches currently used in the blockchain seem safe to protect them against decryption approaches considering the current computing power. Nevertheless,

 doi:10.20944/preprints202402.0317.v1

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. Stolen credentials can be used to make unauthorized purchases and to launder money through stolen metaverse accounts.

4.1.4. 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 user's real counterpart. Stolen avatars might be used for money laundering purposes with cryptocurrencies. Vladimirov et al. [68] 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.

4.1.5. 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 4.1.3) 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 4.1.15). 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.

4.1.6. 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.

 doi:10.20944/preprints202402.0317.v1

4.1.7. Cyberbullying, antisocial behaviours and 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 [69]. 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 [33]. 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 [70]. 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.

4.1.8. 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 environments 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 [3]. Moreover, it is well known that physical inactivity increases the risk of serious health conditions coronary heart disease, stroke, hypertension, and osteoporosis [71]. 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 [3].

4.1.9. Phishing attacks

In addition to the aforementioned phishing attacks mentioned in other subsections (Sections 4.1.1, 4.1.2), 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.

4.1.10. 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 [72]. Virtual products (as a part of an advertisement) or AI-driven avatars, with their seemingly authentic stories,

 doi:10.20944/preprints202402.0317.v1

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 4.1.1) such as the creation of realistic avatars (Sections 4.1.1 and 4.1.2) and businesses/stores (Section 4.1.6) 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 the urban metaverse spaces look like a realistic environment. Some checks and balances are required to validate the genuineness of actions and associated contents to be protected thoroughly.

4.1.11. 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. live concerts), while experiences are happening, are expected to increase in this ecosystem to exploit the situation by putting severe pressure.

4.1.12. 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 body-based 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 [73]. Owners of data are concerned with the risks of unauthorized usage of their sensitive data by various entities, including service providers [74] 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 [44]. Within this context, urban metaverse cyberspaces should be transparent with users about how they process the sensitive data of their users (Figure 6). 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 by the user concerning transparency. Residents should be able to leave the platforms as they wish without giving a reason.

 doi:10.20944/preprints202402.0317.v1

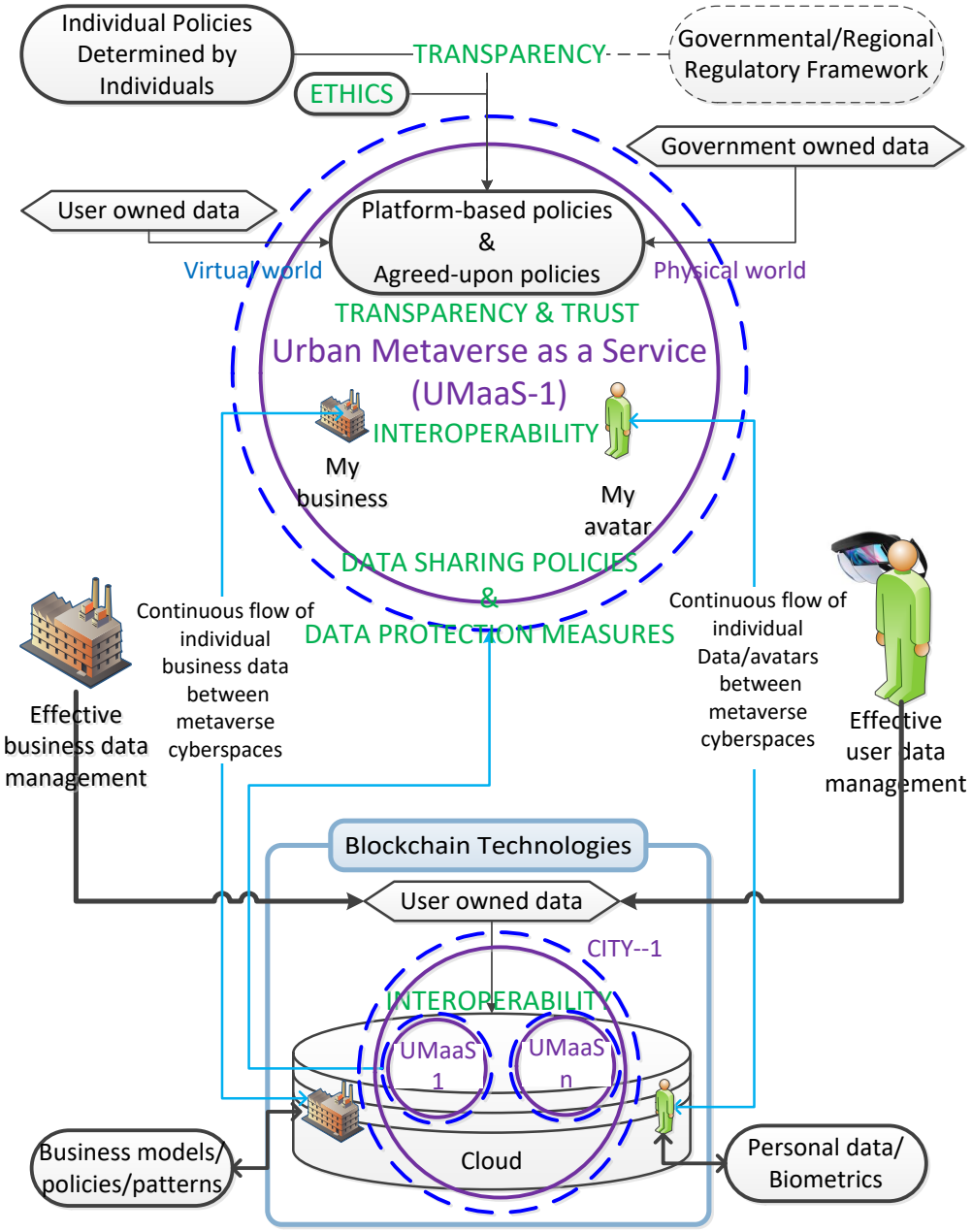

Figure 6. Interoperability and transparency umbrella of MetaCyberCity: Flow of individual data, businesses and avatars between metaverse cyberspaces on the encryption-based and fully decentralised blockchain architecture. Individuals, as owners of their data, are the main actors in managing and controlling their sensitive data with little or no governmental/regional restrictions/interventions.

The 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, Hand Tracking Toolkit (HTT), different types of Wearable Sensors (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. Unauthorized 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

 doi:10.20944/preprints202402.0317.v1

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 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 settings of immersive urban platforms as elaborated in Section 4.1.7.

4.1.13. 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 [37]. 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 [38]. 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 [40] 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 standardized metaverse security measures concerning the vulnerabilities and inconsistencies between a variety of interconnected devices and applications, which can impact users' experiences negatively.

4.1.14. 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 4.1.4). 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

 doi:10.20944/preprints202402.0317.v1

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.

4.1.15. Generative Adversarial Network (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 [22]. The GAN attack has shown that poorly protected local data is vulnerable to being learned by adversaries [24]. 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 [22]. 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.

4.2. Basic Countermeasures for Urban Cyberspaces

4.2.1. Agreed-upon standards, policies and ethics

As shown in Figure 6, the platform-based policies per specific cybercommunity, by considering its intended objectives and basic requirements, are moulded using i) individual policies determined by the users and businesses of cybercommunities regarding the rights of data sovereignty and ii) governmental or regional regulatory framework (e.g. General Data Protection Regulation (GDPR)). 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 interoperable ability of the metaverse. By keeping these essential metrics of the metaverse ecosystem in mind, which are instilled in the MetaCyberCity.

4.2.2. 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 the cybersecurity measures. Therefore, first and foremost, all users of any urban metaverse platform have to be trained using the tools instilled into the platform about how to practice cybersecurity hygiene to avoid everyday cyberattacks (Section 4.1) such as malware exposures or social engineering specific. 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 (Figure 6) and advanced automated AI tools to detect instant

 doi:10.20944/preprints202402.0317.v1

attacks. For instance, strong metaverse credentials, with multiple-factor authentication (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 (Figure 5) augmented in this environment as elaborated in Section 4.1. 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) (Figure 4) 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 other 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.

4.2.3. Automated 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 (Figure 7). 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 (Figure 6). 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 has, shall be measured regarding the resilience to the potential metaverse cyberthreats (Section 4.1) 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 using automated decentralised privacy-preserving CL models, by considering the privacy of residents, to avoid any interruptions in real time.

 doi:10.20944/preprints202402.0317.v1

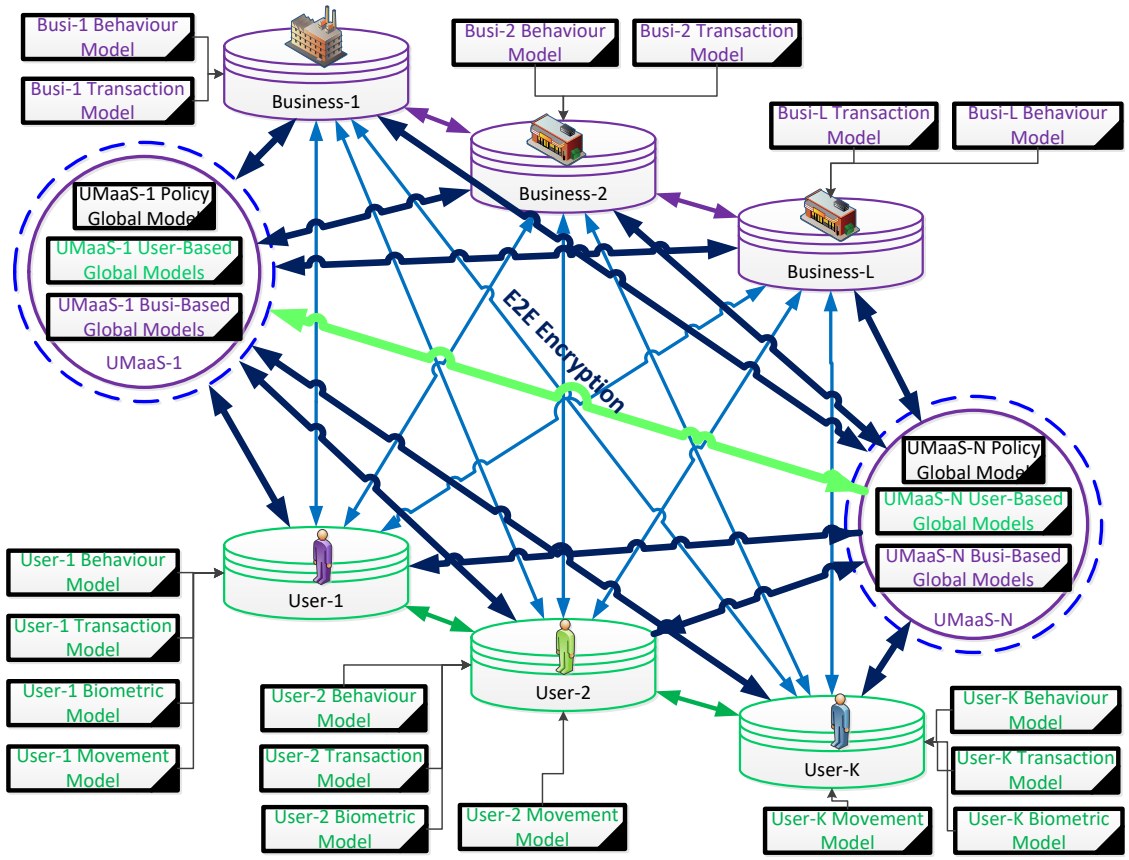

Figure 7. Decentralised End-to-End (E2E) privacy-preserving CDL architecture: UMaaS-, Business-, and user-based local and global models. All users, businesses, and granular UMaaSs as urban cybercommunity entities can communicate with one another whenever needed to run local automated allowed queries on local models and to contribute to the construction of targeted global models of UMaaSs.

4.2.4. Automated detection of Out-of-the-Pattern actions (OotPAs)

P2P/E2E interactions between entities are illustrated in Figure 7 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 fit the real-world decent life norms or automated detection of 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, 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 (Figure 6). 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

 doi:10.20944/preprints202402.0317.v1

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 Figure 8, automated platform-, user- and/or business-focused cybersecurity ML models can be generated by utilising SAI, primarily CDL to both detect OotPAs leading to the detection of cyberattacks and address those attacks in real time using the automated cybersecurity measures (Figure 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 Figure 7. 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) .

4.2.5. 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 4.2.2) 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.

4.2.6. Visibility verses invisibility & Anonymity

Invisibility, feeling the immersive nature of the cybercommunities without being seen, 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. It is noteworthy to emphasise that 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.

 doi:10.20944/preprints202402.0317.v1

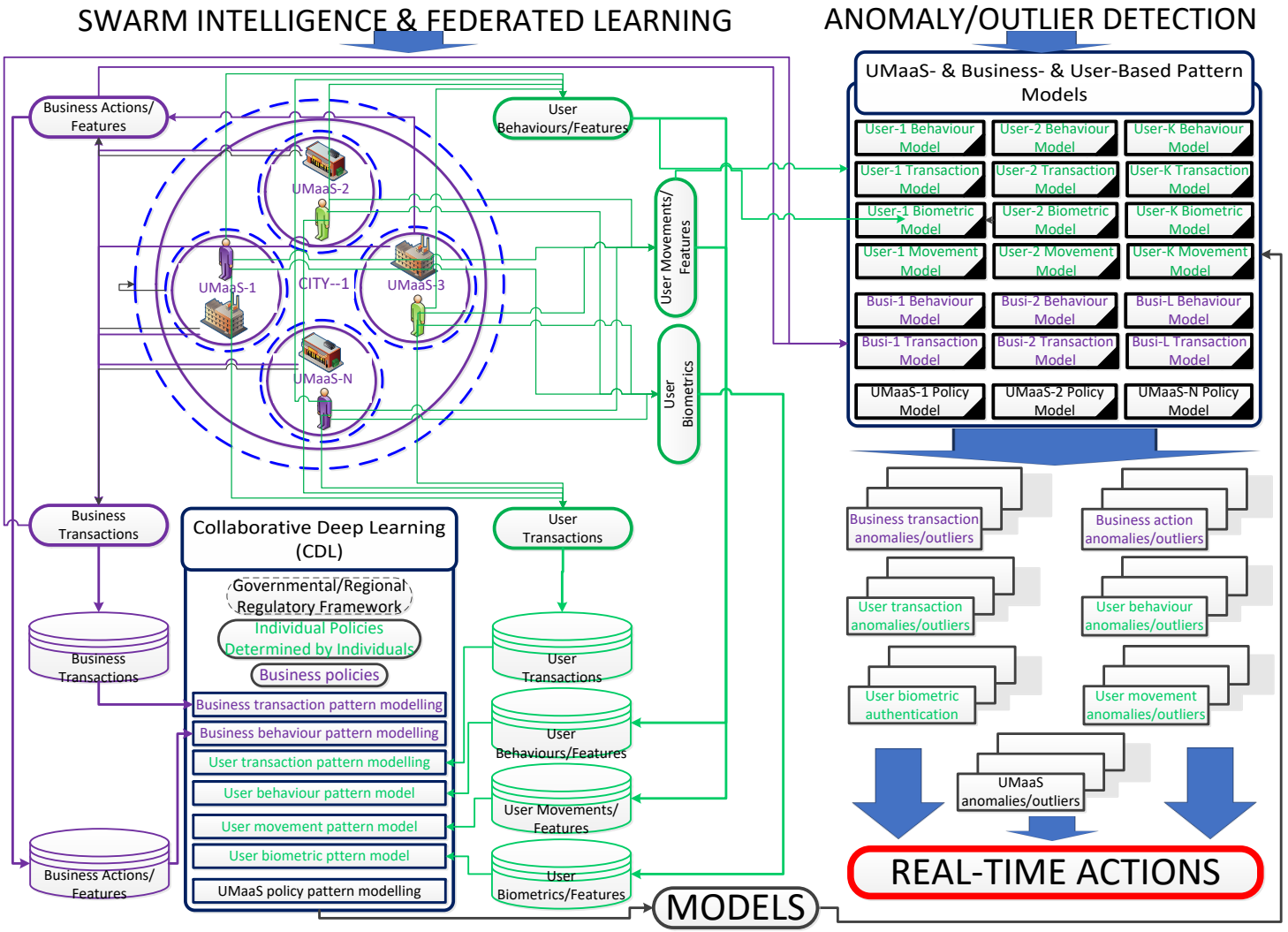

Figure 8. MetaCyberCity: UMaaS- & Business- & User-Based AI learning and modelling; Human-out-of-the loop real-time anomaly detection to take real-time actions.

 doi:10.20944/preprints202402.0317.v1

4.2.7. 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's, both in terms of memory consumption and processing time [75]. 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 the data from unauthorised access and user's privacy. 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 needs to be computed by multiple entities. Another privacy preservation technique, which has captured a wide range of attention, is differential privacy that was developed in [76], 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.

5. Blockchain-Based Decentralised Privacy-Preserving Machine Learning (DPPML) Authentication and Verification Approach

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 perspective in Figure 8. Automated solutions with privacy-preserving mechanisms can mitigate the cyberthreats (Section 4.1) 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

 doi:10.20944/preprints202402.0317.v1

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 [77]. 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 [78] for interested readers. The way of building DL gesture models should consider these privacy and ethical concerns as well as the regulatory framework (Figure 6). 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 reinforcement learning, which can improve the realism of individuals in regard to avatars [79] 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 4.1.14. 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 Section 1. 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 headset, MoCaps, haptics gloves, and HTT), 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 [80].

The urban metaverse cyberspaces and associated entities are distributed on the decentralised public and private ledgers (Figure 7). 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 (Figure 6), 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. 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 Figure 9. The pseudo codes of model training with a MoCap device are presented on blockchain in Algorithms 1 and 2. More specifically, Algorithm 1 shows the local training of the model with epochs fed by the particular online instant features acquired from the

 doi:10.20944/preprints202402.0317.v1

device, which is worn by one of the active nodes on the blockchain whereas Algorithm 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. Algorithm 1 is run by each node individually at the edges locally whereas Algorithm 2 is run on blockchain by all the active nodes where current nodes can leave and new nodes can join at any time. From a 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, $S = \left\{F_1, F_2, \ldots, F_{epoch}\right\}$. 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.

$$ID = \left\{ID_{MoCap}, ID_{HeadSetFace}, ID_{HeadSetLip}, ID_{HandTrackingSet}, ID_{VocalAtr}, \ldots, ID_{size}\right\} \tag{1}$$

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 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 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 (Figure 9), 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 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 parameter 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, with the required timestamp history where models, generated using false parameters, cannot result in authenticating the

 doi:10.20944/preprints202402.0317.v1

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 (Figure 7) 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.

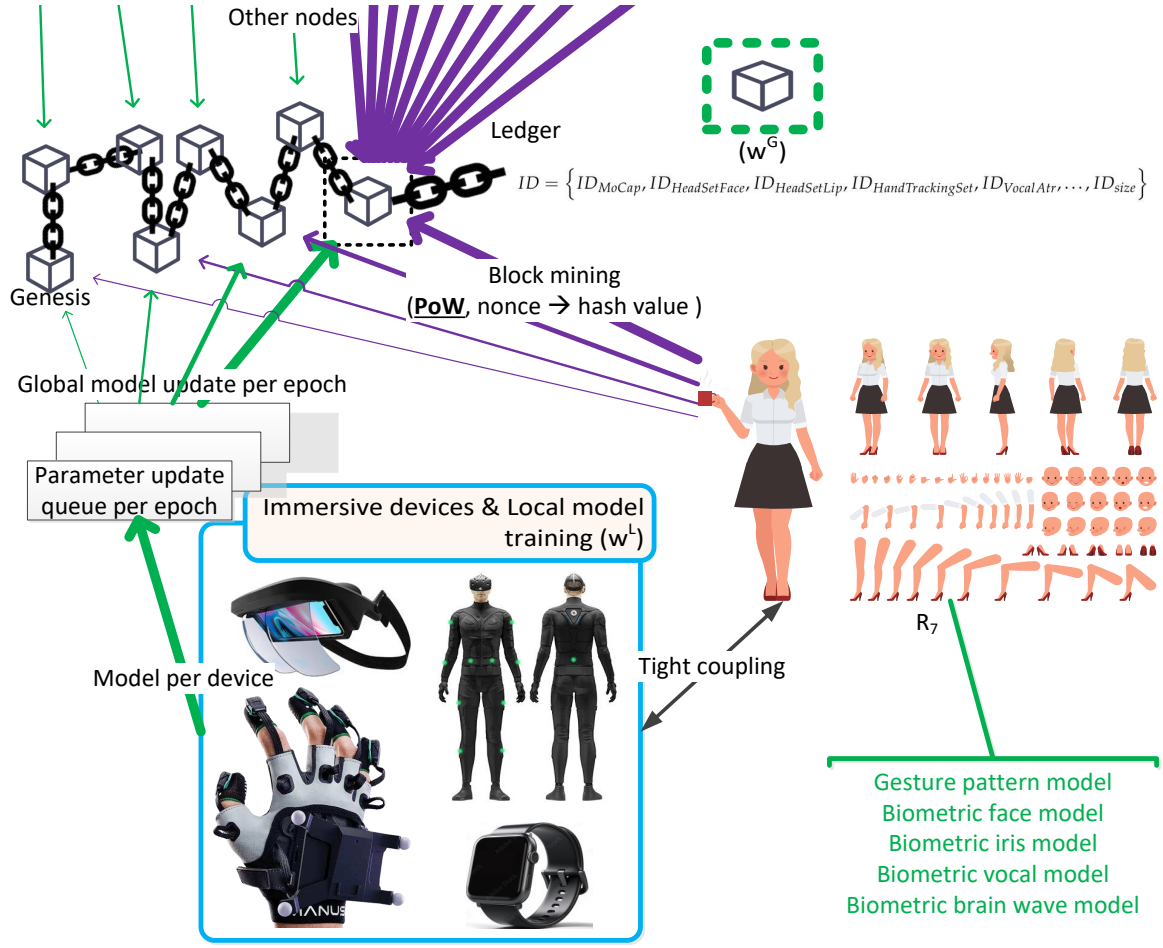

Figure 9. User-based DPPML model generation using immersive metaverse devices. The next block which is being added to the distributed ledger has the most recent model update where as the last block has the final model itself.[2]

 doi:10.20944/preprints202402.0317.v1

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

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

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 Algorithm 3, 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. 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 single point failure 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 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

[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.

 doi:10.20944/preprints202402.0317.v1

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 (Figure 10). 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.

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
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 based on 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 body of 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;
                Blockchain(ID_MoCap).ledger += Blockchain(ID_MoCap).newblock;
                => Delete the updated parameters from queue;
                UpdateQueue.first.Delete;
            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
```

 doi:10.20944/preprints202402.0317.v1

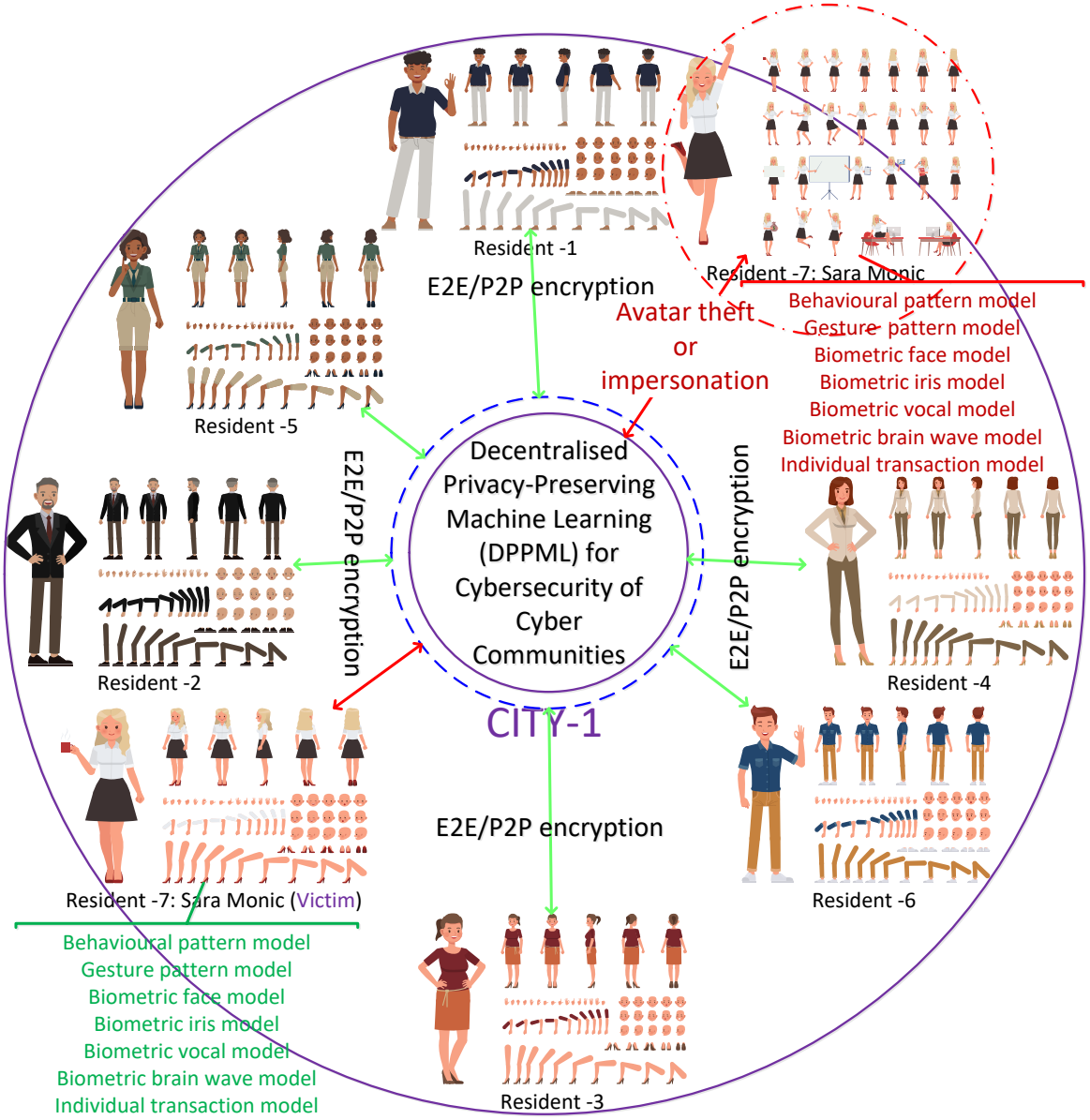

Figure 10. Detection of avatar theft (Section 4.1.4) and identity impersonation (Section 4.1.1). Quarantine of a harmful user to avoid possible cyberattacks.

 doi:10.20944/preprints202402.0317.v1

Algorithm 3: 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
```

6. Challenges

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

- 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 responsibility and accountability?

 doi:10.20944/preprints202402.0317.v1

- 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, 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 within the EU, but data sharing and user profiling are extremely difficult in decentralised urban metaverse worlds by processing individual-specific data scattered all around the world. 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).
- QC, with easy-to-decrypt abilities, can help hackers in cracking blockchain-based hash keys,reaching our wallets, and sensitive data.
- Only the governmentally 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.
- 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.
- 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.
- Gesture signatures can be changed depending on the diverse range of metaverse immersive technologies (e.g. VR/AR headsets, MoCaps, haptics gloves, hand tracking toolkit (HTT), different types of Wearable Sensors (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

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

 doi:10.20944/preprints202402.0317.v1

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.

- 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 inputing more data instances with high-quality attributes.
- Transaction throughput, transaction confirmation delay, and block capacity are the three key challenges in moulding AI and blockchain technologies in an effective way [81]
- 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 [81].

7. Lessons Learned

The lessons learned during this research can be summarised as follows:

- The urban metaverse ecosystem is evolving rapidly and national, regional, and global regulatory framework is 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 this 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.
- Governmental polices 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.
- As users create and share large amounts 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: [82]) 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 the oneself against data leakages and from unauthorised access. The use of biometric identities will increase in the future for establishing better authentication systems, particularly on public ledgers.
- 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.
- 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.

 doi:10.20944/preprints202402.0317.v1

- 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.
- 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.
- Collective global legislative framework is essential to provide residents with trustworthy cyber worlds by preventing the 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 swarm AI should be based on laws and regulatory framework in the sense of protecting users' privacy and anonymity.
- The infrastructure of urban cyberspaces should be tested before accommodating experiences with 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.
- 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 assets of users and businesses, which, in turn, will boost the investments in metaverse cybersecurity solutions.
- Urban metaverse cyberspaces need to ensure that every resident can access to the cybercommunity, regardless of their social position, income or technical skills and they are protected against cybercriminals.
- In urban metaverse cyberspaces, residents should decide how their data would be managed and processed through the individual policies where residents are the owner of their data that is 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.
- 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 [83]. The fuse of QC with an exponentially increasing computation power and 6G technologies is expected to provide the residents with highly powerful computing and comminations 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 [3].
- 6G, expected by 2030 [38], as a key pillar in developing metaverse technologies, would significantly enhance seamless genuine immersive experiences [47], [84] 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 [3].
- 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 as when compared to Web2.

 doi:10.20944/preprints202402.0317.v1

8. Discussion

Today, and every day, worldwide, one million more people are born-into or move-into a city [85]. The global population is expected to double by 2050 [86] and more than 68% of the population will be living in an urban environment by 2050 [87] with a population of 5 billion [88]. 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 [3] 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 [3]) 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 [3]. 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 platforms, devices, and hyper-realistic MetaHumans [3]. 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 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 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 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

 doi:10.20944/preprints202402.0317.v1

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 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 4.2.7). 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) (Figure 4) 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 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 to 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?

9. 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 massive immersive human-machine interactions, will be providing cities with new ways for the digital transition; it will respond to urbanisation with more intelligent services through the exploration and exploitation of the metaverse

 doi:10.20944/preprints202402.0317.v1

concept by mirroring the high-fidelity life of urban societies [3], pawing 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 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. 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. In this research, a blockchain-based DPPML authentication and verification approach that utilises the behavioural/gesture signature (i.e. digital body footprint) obtained from immersive metaverse wearable devices is designed to extend the privacy and security of residents in metaverse urban cyberspaces with blockchain technologies. This approach can be instrumented effectively against 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. To the best of our knowledge, this research is the first one in the literature that utilised the body's cyber signature in extending the protection of residents in cyber worlds with blockchain technologies. The secure and reliable urban metaverse cyberspaces, supported by similar approaches, will be constructing ecosystems of trust among all the entities within the urban metaverse ecosystem. We will be focusing on applying the proposed approach in real-world applications, with a couple of immersive devices as a future objective.

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).

Author Contributions: The authors contributed equally to this work.

Funding: This research received no external funding.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

 doi:10.20944/preprints202402.0317.v1

ABR	Automated Behaviour Recognition
AER	Automated Emotion Recognition
AoE	Automation of Everything
AI	Artificial Intelligence (AI)
BD	Big Data
BP	Business Profiling
CA	Content Awareness
CCPA	California Consumer Privacy Act
CDL	Collaborative Deep Learning
CL	Collaborative Learning
CPSs	Cyber-Physical Systems
CPSS	Cyber–Physical–Social Systems
CoBs	Classification of Businesses
CP	Content Profiling
CoUs	Classification of Users
DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
DAO	Decentralised Autonomous Organisation
DNN	eep Neural Network
DTs	Digital Twins
E2E	End-to-End
FL	Federated Learning
GMaaS	Global Model as a Service
GAN	Generative Adversarial Network
GDPR	General Data Protection Regulation
HAR	Human Activity Recognition
HD	high-definition
HE	Homomorphic Encryption
HTT	Hand Tracking Toolkit
ICT	Information Communication Technology
IMS	Identity Management Systems
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
NFTs	Non-Fungible Tokens
NGOs	Non-Governmental Organisations
QC	Quantum Computing
QoE	Quality of Experiences
QoL	Quality of Life
PoS	Proof-of-Stake
PoW	Proof-of-Work
P2P	Peer-to-Peer
PP	Platform Profiling
PPML	Privacy-Preserving Machine Learning
PPDL	Privacy-Preserving Deep Learning
OotPEs	Out-of-the-Pattern Events

SA	Situational Awareness
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
ViLO	Virtual London
WRSs	Wearable Resistive Sensors
WSs	Wearable Sensors

References

1. Stephenson, N. *Snow Crash*, 1 ed.; Bantam Books: New York, USA, 1992.
2. TheNexus. A Summary of "Snow Crash" by Neal Stephenson (1992), 2023.
3. Kuru, K. MetaOmniCity: Toward Immersive Urban Metaverse Cyberspaces Using Smart City Digital Twins. *IEEE Access* **2023**, *11*, 43844–43868. doi:10.1109/ACCESS.2023.3272890.
4. Park, S.M.; Kim, Y.G. A Metaverse: Taxonomy, Components, Applications, and Open Challenges. *IEEE Access* **2022**, *10*, 4209–4251. doi:10.1109/ACCESS.2021.3140175.
5. Al-Ghaili, A.M.; Kasim, H.; Al-Hada, N.M.; Hassan, Z.B.; Othman, M.; Tharik, J.H.; Kasmani, R.M.; Shayea, I. A Review of Metaverse's Definitions, Architecture, Applications, Challenges, Issues, Solutions, and Future Trends. *IEEE Access* **2022**, *10*, 125835–125866. doi:10.1109/ACCESS.2022.3225638.
6. Ritterbusch, G.D.; Teichmann, M.R. Defining the Metaverse: A Systematic Literature Review. *IEEE Access* **2023**, *11*, 12368–12377. doi:10.1109/ACCESS.2023.3241809.
7. Huynh-The, T.; Pham, Q.V.; Pham, X.Q.; Nguyen, T.T.; Han, Z.; Kim, D.S. Artificial intelligence for the metaverse: A survey. *Eng. Appl. Artif. Intell.* **2023**, *117*, 105581. doi:https://doi.org/10.1016/j.engappai.2022.105581.
8. Yang, Q.; Zhao, Y.; Huang, H.; Xiong, Z.; Kang, J.; Zheng, Z. Fusing Blockchain and AI With Metaverse: A Survey. *IEEE Open Journal of the Computer Society* **2022**, *3*, 122–136. doi:10.1109/OJCS.2022.3188249.
9. Maksymyuk, T.; Gazda, J.; Bugár, G.; Gazda, V.; Liyanage, M.; Dohler, M. Blockchain-Empowered Service Management for the Decentralized Metaverse of Things. *IEEE Access* **2022**, *10*, 99025–99037. doi:10.1109/ACCESS.2022.3205739.
10. Zhao, Y.; Jiang, J.; Chen, Y.; Liu, R.; Yang, Y.; Xue, X.; Chen, S. Metaverse: Perspectives from graphics, interactions and visualization. *Visual Informatics* **2022**, *6*, 56–67. doi:https://doi.org/10.1016/j.visinf.2022.03.002.
11. Lv, Z.; Xie, S.; Li, Y.; Shamim Hossain, M.; El Saddik, A. Building the Metaverse by Digital Twins at All Scales, State, Relation. *Virtual Reality & Intelligent Hardware* **2022**, *4*, 459–470. doi:https://doi.org/10.1016/j.vrih.2022.06.005.
12. Aloqaily, M.; Bouachir, O.; Karray, F.; Ridhawi, I.A.; Saddik, A.E. Integrating Digital Twin and Advanced Intelligent Technologies to Realize the Metaverse. *IEEE Consumer Electronics Magazine* **2022**, pp. 1–8. doi:10.1109/MCE.2022.3212570.
13. Kusuma, A.T.; Supangkat, S.H. Metaverse Fundamental Technologies for Smart City: A Literature Review. 2022 International Conference on ICT for Smart Society (ICISS), 2022, pp. 1–7. doi:10.1109/ICISS55894.2022.9915079.
14. Musamih, A.; Dirir, A.; Yaqoob, I.; Salah, K.; Jayaraman, R.; Puthal, D. NFTs in Smart Cities: Vision, Applications, and Challenges. *IEEE Consumer Electronics Magazine* **2022**, pp. 1–14. doi:10.1109/MCE.2022.3217660.
15. Bansal, G.; Rajgopal, K.; Chamola, V.; Xiong, Z.; Niyato, D. Healthcare in Metaverse: A Survey on Current Metaverse Applications in Healthcare. *IEEE Access* **2022**, *10*, 119914–119946. doi:10.1109/ACCESS.2022.3219845.

16. Almarzouqi, A.; Aburayya, A.; Salloum, S.A. Prediction of User's Intention to Use Metaverse System in Medical Education: A Hybrid SEM-ML Learning Approach. *IEEE Access* **2022**, *10*, 43421–43434. doi:10.1109/ACCESS.2022.3169285.
17. Chengoden, R.; Victor, N.; Huynh-The, T.; Yenduri, G.; Jhaveri, R.H.; Alazab, M.; Bhattacharya, S.; Hegde, P.; Maddikunta, P.K.R.; Gadekallu, T.R. Metaverse for Healthcare: A Survey on Potential Applications, Challenges and Future Directions. *IEEE Access* **2023**, *11*, 12765–12795. doi:10.1109/ACCESS.2023.3241628.
18. Wang, M.; Yu, H.; Bell, Z.; Chu, X. Constructing an Edu-Metaverse Ecosystem: A New and Innovative Framework. *IEEE Transactions on Learning Technologies* **2022**, *15*, 685–696. doi:10.1109/TLT.2022.3210828.
19. Suanpang, P.; Niamsorn, C.; Pothipassa, P.; Chunhapataragul, T.; Netwong, T.; Jermsittiparsert, K. Extensible Metaverse Implication for a Smart Tourism City. *Sustainability* **2022**, *14*. doi:10.3390/su142114027.
20. Gong, M.; Zhang, Y.; Gao, Y.; Qin, A.K.; Wu, Y.; Wang, S.; Zhang, Y. A Multi-Modal Vertical Federated Learning Framework Based on Homomorphic Encryption. *IEEE Transactions on Information Forensics and Security* **2024**, *19*, 1826–1839. doi:10.1109/TIFS.2023.3340994.
21. Yang, Q.; Liu, Y.; Chen, T.; Tong, Y. Federated Machine Learning: Concept and Applications. *ACM Trans. Intell. Syst. Technol.* **2019**, *10*. doi:10.1145/3298981.
22. Li, P.; Zhang, Z.; Al-Sumaiti, A.S.; Werghi, N.; Yeun, C.Y. A Robust Adversary Detection-Deactivation Method for Metaverse-oriented Collaborative Deep Learning. *IEEE Sensors Journal* **2023**, pp. 1–1. doi:10.1109/JSEN.2023.3325771.
23. Hitaj, B.; Ateniese, G.; Perez-Cruz, F. Deep Models Under the GAN: Information Leakage from Collaborative Deep Learning. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security; Association for Computing Machinery: New York, NY, USA, 2017; CCS '17, p. 603–618. doi:10.1145/3133956.3134012.
24. Chen, Z.; Wu, J.; Fu, A.; Su, M.; Deng, R.H. MP-CLF: An effective Model-Preserving Collaborative deep Learning Framework for mitigating data leakage under the GAN. *Knowledge-Based Systems* **2023**, *270*, 110527. doi:https://doi.org/10.1016/j.knosys.2023.110527.
25. Lyu, L.; Li, Y.; Nandakumar, K.; Yu, J.; Ma, X. How to Democratise and Protect AI: Fair and Differentially Private Decentralised Deep Learning. *IEEE Transactions on Dependable and Secure Computing* **2022**, *19*, 1003–1017. doi:10.1109/TDSC.2020.3006287.
26. Kuru, K. Management of geo-distributed intelligence: Deep Insight as a Service (DINSaaS) on Forged Cloud Platforms (FCP). *Journal of Parallel and Distributed Computing* **2021**, *149*, 103–118. doi:https://doi.org/10.1016/j.jpdc.2020.11.009.
27. Zhang, L.; Xu, J.; Vijayakumar, P.; Sharma, P.K.; Ghosh, U. Homomorphic Encryption-Based Privacy-Preserving Federated Learning in IoT-Enabled Healthcare System. *IEEE Transactions on Network Science and Engineering* **2023**, *10*, 2864–2880. doi:10.1109/TNSE.2022.3185327.
28. Bos, J.W.; Lauter, K.; Loftus, J.; Naehrig, M. Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme. Cryptography and Coding; Stam, M., Ed.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2013; pp. 45–64.
29. Phong, L.T.; Aono, Y.; Hayashi, T.; Wang, L.; Moriai, S. Privacy-Preserving Deep Learning via Additively Homomorphic Encryption. *IEEE Transactions on Information Forensics and Security* **2018**, *13*, 1333–1345. doi:10.1109/TIFS.2017.2787987.
30. Zhou, C.; Ansari, N. Securing Federated Learning Enabled NWDAF Architecture With Partial Homomorphic Encryption. *IEEE Networking Letters* **2023**, *5*, 299–303. doi:10.1109/LNET.2023.3294497.
31. Lee, J.W.; Kang, H.; Lee, Y.; Choi, W.; Eom, J.; Deryabin, M.; Lee, E.; Lee, J.; Yoo, D.; Kim, Y.S.; No, J.S. Privacy-Preserving Machine Learning With Fully Homomorphic Encryption for Deep Neural Network. *IEEE Access* **2022**, *10*, 30039–30054. doi:10.1109/ACCESS.2022.3159694.
32. Zhou, X.; Liang, W.; Ma, J.; Yan, Z.; Wang, K.I.K. 2D Federated Learning for Personalized Human Activity Recognition in Cyber-Physical-Social Systems. *IEEE Transactions on Network Science and Engineering* **2022**, *9*, 3934–3944. doi:10.1109/TNSE.2022.3144699.
33. Huq, N.; Reyes, R.; Lin, P.; Swimmer, M. Cybersecurity Threats Against the Internet of Experiences. *Trend Micro Research* **2022**.
34. Pooyandeh, M.; Han, K.J.; Sohn, I. Cybersecurity in the AI-Based Metaverse: A Survey. *Applied Sciences* **2022**, *12*. doi:10.3390/app122412993.

35. Huang, Y.; Li, Y.J.; Cai, Z. Security and Privacy in Metaverse: A Comprehensive Survey. *Big Data Mining and Analytics* **2023**, *6*, 234–247. doi:10.26599/BDMA.2022.9020047.
36. Wang, Y.; Su, Z.; Zhang, N.; Xing, R.; Liu, D.; Luan, T.H.; Shen, X. A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials* **2022**, pp. 1–1. doi:10.1109/COMST.2022.3202047.
37. Rostami, S.; Maier, M. The Metaverse and Beyond: Implementing Advanced Multiverse Realms With Smart Wearables. *IEEE Access* **2022**, *10*, 110796–110806. doi:10.1109/ACCESS.2022.3215736.
38. Kalla, A.; De Alwis, C.; Gur, G.; Gochhayat, S.P.; Liyanage, M.; Porambage, P. Emerging Directions for Blockchainized 6G. *IEEE Consumer Electronics Magazine* **2022**, pp. 1–1. doi:10.1109/MCE.2022.3164530.
39. Ryu, J.; Son, S.; Lee, J.; Park, Y.; Park, Y. Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain. *IEEE Access* **2022**, *10*, 98944–98958. doi:10.1109/ACCESS.2022.3206457.
40. Hemdan, E.E.D.; Mahmoud, A.S.A., BlockTwins: A Blockchain-Based Digital Twins Framework. In *Blockchain Applications in IoT Ecosystem*; Choudhury, T.; Khanna, A.; Toe, T.T.; Khurana, M.; Gia Nhu, N., Eds.; Springer International Publishing: Cham, 2021; pp. 177–186. doi:10.1007/978-3-030-65691-1_12.
41. Kwabena, O.A.; Qin, Z.; Zhuang, T.; Qin, Z. MSCryptoNet: Multi-Scheme Privacy-Preserving Deep Learning in Cloud Computing. *IEEE Access* **2019**, *7*, 29344–29354. doi:10.1109/ACCESS.2019.2901219.
42. Kim, H.; Park, J.; Bennis, M.; Kim, S.L. Blockchained On-Device Federated Learning. *IEEE Communications Letters* **2020**, *24*, 1279–1283. doi:10.1109/LCOMM.2019.2921755.
43. Chen, T.; Zhong, S. Privacy-Preserving Backpropagation Neural Network Learning. *IEEE Transactions on Neural Networks* **2009**, *20*, 1554–1564. doi:10.1109/TNN.2009.2026902.
44. Kuru, K.; Ansell, D. TCitySmartF: A Comprehensive Systematic Framework for Transforming Cities Into Smart Cities. *IEEE Access* **2020**, *8*, 18615–18644. doi:10.1109/ACCESS.2020.2967777.
45. Kuru, K.; Yetgin, H. Transformation to Advanced Mechatronics Systems Within New Industrial Revolution: A Novel Framework in Automation of Everything (AoE). *IEEE Access* **2019**, *7*, 41395–41415. doi:10.1109/ACCESS.2019.2907809.
46. Harrison, C.; Eckman, B.; Hamilton, R.; Hartswick, P.; Kalagnanam, J.; Paraszczak, J.; Williams, P. Foundations for Smarter Cities. *IBM Journal of Research and Development* **2010**, *54*, 1–16. doi:10.1147/JRD.2010.2048257.
47. Tang, F.; Chen, X.; Zhao, M.; Kato, N. The Roadmap of Communication and Networking in 6G for the Metaverse. *IEEE Wireless Communications* **2022**, pp. 1–15. doi:10.1109/MWC.019.2100721.
48. White, G.; Zink, A.; Codecá, L.; Clarke, S. A digital twin smart city for citizen feedback. *Cities* **2021**, *110*, 103064. doi:https://doi.org/10.1016/j.cities.2020.103064.
49. El Saddik, A. Digital Twins: The Convergence of Multimedia Technologies. *IEEE MultiMedia* **2018**, *25*, 87–92. doi:10.1109/MMUL.2018.023121167.
50. Laamarti, F.; Badawi, H.F.; Ding, Y.; Arafsha, F.; Hafidh, B.; Saddik, A.E. An ISO/IEEE 11073 Standardized Digital Twin Framework for Health and Well-Being in Smart Cities. *IEEE Access* **2020**, *8*, 105950–105961. doi:10.1109/ACCESS.2020.2999871.
51. Kuru, K. 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* **2021**, *2*, 448–469. doi:10.1109/OJITS.2021.3132725.
52. Kuru, K.; Khan, W. A Framework for the Synergistic Integration of Fully Autonomous Ground Vehicles With Smart City. *IEEE Access* **2021**, *9*, 923–948. doi:10.1109/ACCESS.2020.3046999.
53. Kuru, K.; Worthington, S.; Ansell, D.; Pinder, J.M.; Sujit, A.; Jon Watkinson, B.; Vinning, K.; Moore, L.; Gilbert, C.; Jones, D.; others. AITL-WING-HITL: Telemanipulation of autonomous drones using digital twins of aerial traffic interfaced with WING. *IEEE Access* **2023**, *11*.
54. Lv, Z.; Qiao, L.; Li, Y.; Yuan, Y.; Wang, F.Y. BlockNet: Beyond reliable spatial Digital Twins to Parallel Metaverse. *Patterns* **2022**, *3*, 100468. doi:https://doi.org/10.1016/j.patter.2022.100468.
55. Hudson-Smith, A.; Signorelli, V. Digital Innovation for Data Visualisations in Participatory Urban Planning, 2022.
56. Wu, Y.; Zhang, K.; Zhang, Y. Digital Twin Networks: A Survey. *IEEE Internet of Things Journal* **2021**, *8*, 13789–13804. doi:10.1109/JIOT.2021.3079510.
57. Arslan, M. Metaverse'in Akıllı Kent Hizmetlerine Etkisi. *Akademik Araştırmalar ve Çalışmalar Dergisi (AKAD)* **2022**, *14*, 292 – 303. doi:10.20990/kilisiibfakademik.1146016.

58. Kuru, K. Planning the Future of Smart Cities With Swarms of Fully Autonomous Unmanned Aerial Vehicles Using a Novel Framework. *IEEE Access* **2021**, *9*, 6571–6595. doi:10.1109/ACCESS.2020.3049094.
59. Pérez, G.O.; Ebrahimzadeh, A.; Maier, M.; Hernández, J.A.; López, D.L.; Veiga, M.F. Decentralized Coordination of Converged Tactile Internet and MEC Services in H-CRAN Fiber Wireless Networks. *Journal of Lightwave Technology* **2020**, *38*, 4935–4947. doi:10.1109/JLT.2020.2998001.
60. Chang, L.; Zhang, Z.; Li, P.; Xi, S.; Guo, W.; Shen, Y.; Xiong, Z.; Kang, J.; Niyato, D.; Wu, X.Q.Y. 6G-Enabled Edge AI for Metaverse:Challenges, Methods,and Future Research Directions. *Journal of Communications and Information Networks* **2022**, *7*, 107. doi:j.issn.2096-1081.2022.02.01.
61. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Communications Surveys Tutorials* **2019**, *21*, 2794–2830. doi:10.1109/COMST.2019.2899617.
62. Xu, X.; Cizmeci, B.; Schuwerk, C.; Steinbach, E. Model-Mediated Teleoperation: Toward Stable and Transparent Teleoperation Systems. *IEEE Access* **2016**, *4*, 425–449. doi:10.1109/ACCESS.2016.2517926.
63. Ebrahimzadeh, A.; Maier, M. Delay-Constrained Teleoperation Task Scheduling and Assignment for Human+Machine Hybrid Activities Over FiWi Enhanced Networks. *IEEE Transactions on Network and Service Management* **2019**, *16*, 1840–1854. doi:10.1109/TNSM.2019.2937020.
64. Wang, D.; Ohnishi, K.; Xu, W. Novel Emerging Sensing, Actuation, and Control Techniques for Haptic Interaction and Teleoperation. *IEEE Transactions on Industrial Electronics* **2020**, *67*, 624–626. doi:10.1109/TIE.2019.2927784.
65. IEEE. P1918.1 - Tactile Internet: Application Scenarios, Definitions and Terminology, Architecture, Functions, and Technical Assumptions, 2018.
66. S. Punla, C.; C. Farro, R. Are we there yet?: An analysis of the competencies of BEED graduates of BPSU-DC. *International Multidisciplinary Research Journal* **2022**, *4*, 50–59.
67. Cui, L.; Liu, J. Virtual Human: A Comprehensive Survey on Academic and Applications. *IEEE Access* **2023**, *11*, 123830–123845. doi:10.1109/ACCESS.2023.3329573.
68. Vladimirov, I.; Nenova, M.; Nikolova, D.; Terneva, Z. Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse: A Survey. 2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST), 2022, pp. 1–4. doi:10.1109/ICEST55168.2022.9828791.
69. Frenkel, S.; Browning, K. The Metaverse's Dark Side: Here Come Harassment and Assaults, 2021.
70. Sharma, V. Introducing a personal boundary for horizon worlds and venues, 2022.
71. Wiederhold, B.K. Metaverse Games: Game Changer for Healthcare? *Cyberpsychology, Behavior, and Social Networking* **2022**, *25*, 267–269, [https://doi.org/10.1089/cyber.2022.29246.editorial]. PMID: 35549346, doi:10.1089/cyber.2022.29246.editorial.
72. TheWachowskis. The Relationship Between Body, Brain, and Mind, 2023.
73. Eckhoff, D.; Wagner, I. Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions. *IEEE Communications Surveys Tutorials* **2018**, *20*, 489–516. doi:10.1109/COMST.2017.2748998.
74. Yau, S.S.; An, H.G.; Buduru, A.B. An Approach to Data Confidentiality Protection in Cloud Environments. *International Journal of Web Services Research* **2012**, *9*, 67–83. doi:10.4018/jwsr.20120701041.
75. Podschwadt, R.; Takabi, D.; Hu, P.; Rafiei, M.H.; Cai, Z. A Survey of Deep Learning Architectures for Privacy-Preserving Machine Learning With Fully Homomorphic Encryption. *IEEE Access* **2022**, *10*, 117477–117500. doi:10.1109/ACCESS.2022.3219049.
76. Dwork, C.; McSherry, F.; Nissim, K.; Smith, A. Calibrating Noise to Sensitivity in Private Data Analysis. Theory of Cryptography; Halevi, S.; Rabin, T., Eds.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2006; pp. 265–284.
77. Latif, S.; Ali, H.S.; Usama, M.; Rana, R.; Schuller, B.; Qadir, J. AI-Based Emotion Recognition: Promise, Peril, and Prescriptions for Prosocial Path, 2022, [arXiv:cs.HC/2211.07290].
78. McStay, A. Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy. *Big Data & Society* **2020**, *7*, 2053951720904386, [https://doi.org/10.1177/2053951720904386]. doi:10.1177/2053951720904386.
79. Peng, X.B.; Abbeel, P.; Levine, S.; van de Panne, M. DeepMimic: Example-Guided Deep Reinforcement Learning of Physics-Based Character Skills. *ACM Trans. Graph.* **2018**, *37*. doi:10.1145/3197517.3201311.

80. Duan, S.; Zhao, F.; Yang, H.; Hong, J.; Shi, Q.; Lei, W.; Wu, J. A Pathway into Metaverse: Gesture Recognition Enabled by Wearable Resistive Sensors. *Advanced Sensor Research* **2023**, *2*, 2200054, [https://onlinelibrary.wiley.com/doi/pdf/10.1002/adsr.202200054]. doi:https://doi.org/10.1002/adsr.202200054.
81. Zhang, Z.; Song, X.; Liu, L.; Yin, J.; Wang, Y.; Lan, D. 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.
82. Falchuk, B.; Loeb, S.; Neff, R. The Social Metaverse: Battle for Privacy. *IEEE Technology and Society Magazine* **2018**, *37*, 52–61. doi:10.1109/MTS.2018.2826060.
83. Huang, Y.; Zhu, Y.; Qiao, X.; Su, X.; Dustdar, S.; Zhang, P. Toward Holographic Video Communications: A Promising AI-Driven Solution. *IEEE Communications Magazine* **2022**, *60*, 82–88. doi:10.1109/MCOM.001.220021.
84. Chowdhury, M.Z.; Shahjalal, M.; Ahmed, S.; Jang, Y.M. 6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions. *IEEE Open Journal of the Communications Society* **2020**, *1*, 957–975. doi:10.1109/OJCOMS.2020.3010270.
85. Wilson, P. State of smart cities in UK and beyond. *IET Smart Cities* **2019**, *1*, 19–22. doi:10.1049/iet-smc.2019.0024.
86. Sun, Y.; Song, H.; Jara, A.J.; Bie, R. Internet of Things and Big Data Analytics for Smart and Connected Communities. *IEEE Access* **2016**, *4*, 766–773. doi:10.1109/ACCESS.2016.2529723.
87. Kiestra, P. Safe Cities Index 2019: Urban security and resilience in an interconnected world, 2019.
88. Neirotti, P.; Marco, A.D.; Cagliano, A.C.; Mangano, G.; Scorrano, F. Current trends in Smart City initiatives: Some stylised facts. *Cities* **2014**, *38*, 25 – 36. doi:https://doi.org/10.1016/j.cities.2013.12.010.