6^{th} *International Conference on Blockchain Computing and Applications (BCCA 2024)*
26–29 November, 2024 – Dubai, UAE

Urban Metaverse Cyberthreats and Countermeasures Against These Threats

1st Kaya Kuru
School of Engineering and Computing
University of Central Lancashire
Preston, UK
https://orcid.org/0000-0002-4279-4166

2nd Kaan Kuru
School of Engineering and Computing
University of Central Lancashire
Preston, UK
https://orcid.org/0009-0007-3900-1085

***Abstract*—Ensuring seamless connectivity, data accuracy, and user privacy are critical aspects that need further attention for the efficacy of urban metaverse cyberspaces with Urban Twins (UTs), particularly, from technical, legislative, and ethical standpoints. A large number of transactions and immersive experiences shall be managed safely in an automated manner in urban metaverse cyberspaces. Cybersecurity measures in urban cyberspaces encounter a unique set of challenges due to the immersive nature of these spaces. In this direction, this study analyses cyberthreats within urban metaverse cyberspaces and basic countermeasures against these threats.**

***Index Terms*—Metaverse, Urban Twins (UTs), Digital Twins (DTs), cybersecurity, cyberthreats, blockchain.**

I. Introduction

The approaches behind "Internet of Everything (IoE)" [1] combine people, organisations, processes, things, and data into a tangible, coherent framework known as Cyber-Physical Systems (CPSs). CPSs are employed to create Cyber-Physical Social Systems (CPSSs) that work together to create a smarter, more interconnected world [2]. The metaverse, an extension of CPSSs, has the potential to affect its users dramatically with its enriched sets of capabilities 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 with Urban Twins (UTs) or Digital Twins (DTs). Accurate digital replication of real-world fragments of urbanisation at various granularities can be achieved in the virtual plane through UTs [3]. Readers are referred to the previous studies ([4], [5], [6], [7], [8], [9], [10]) for the examples of DTs. In highly synchronized environments, similar DTs/UTs are used not only to govern urban assets effectively and efficiently, but also to make it easier for urban services to be incorporated into metaverse worlds, facilitating a more immersive experience that improves the standard of living in cities. 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. Using 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. Our research question in this research 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 to alleviate privacy concerns? All the assets can be lost if the private key, which is kept in the individual wallet, is lost or a mistakenly approved transaction cannot be taken back, where there is no central authority to intervene. Therefore, cybersecurity is more important in this platform on Web3 when compared to Web2. In this direction, in this paper, the possible cyberrisks, cyberthreats and privacy concerns in urban metaverse cyberspaces are revealed, and how these threats can be addressed with a series of countermeasures is analysed.

II. CYBERTHREATS AND COUNTERMEASURES

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. Vast amounts of data including movements, preferences, emotions and biometrics will be collected in the urban cybercommunities. This Big Data (BD) is subject to potential data breaches, unauthorised access, and misuse of sensitive information. New and effective approaches (e.g. [11]) 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 [12]. We need to get ready to deal with these hazards while we are embracing many promising potentials within this new type of urban ecosystem. The main threats that can be launched in urban cybercommunities are demonstrated in Fig. 1 along with the basic countermeasures. These cyberthreats are intertwined with one another and it is difficult to differentiate them with distinctive borders. Urban Metaverse-as-a-Services (UMaaSs) are the ubiquitous fragmented parallel urban environments, which make it possible to effectively customise certain urban metaverse services [13].

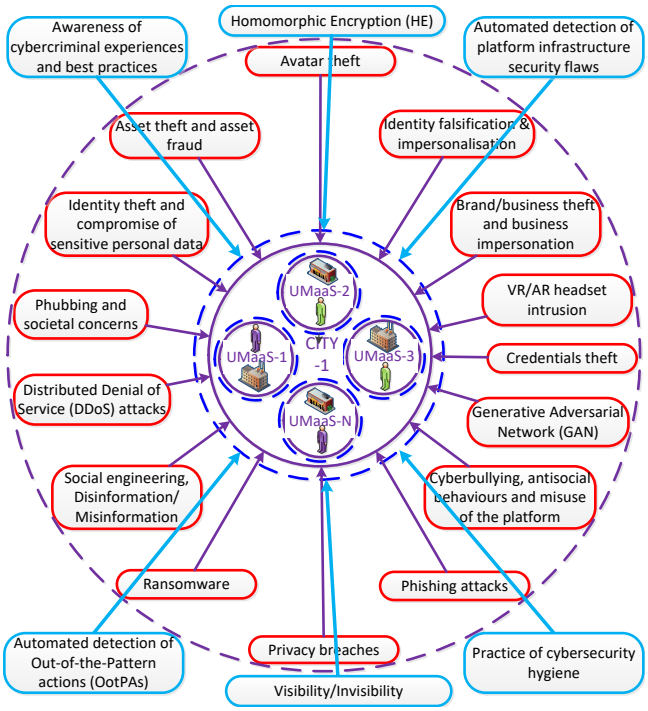

Fig. 1: Cyberthreats against Urban Metaverse-as-a-Services (UMaaSs) (red) and basic countermeasures (blue).

A. URBAN METAVERSE CYBERTHREATS

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, comprise five essential modules: audio and video synthesis display, voice generation, character generation, animation generation, and interaction using information and communication technology (ICT) (e.g. motion capture, computer graphics, ML, speech synthesis, and high-precision rendering) [14]. 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. Generative Adversarial Network (GAN) (Section II-A15)) 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 entities to cybercommunities using authentication tokens would mitigate these concerns, but this may not be an ideal option for residents concerning privacy regarding being tracked by the authority.

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 instrumented in the execution of various malicious actions. The metaverse environments can be destabilised by malicious software (i.e. Malware) that can stop us from reaching our environment, prevent us from transferring our 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. Malicious software attacks can target vulnerabilities in metaverse platforms, leading to unauthorised 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 II-A1). Stronger and more effective authentication approaches are being developed to protect users by avoiding any possible identity theft.

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 II-B2) and should not be sharing their private keys with others in cybercommunities to avoid every type of attack that is summarised in Fig. 1. The encryption approaches currently used in the blockchain seem safe to protect them against decryption approaches considering the current computing power. Nevertheless, it is noteworthy to emphasise that every encrypted code is vulnerable to decryption and we are witnessing the theft of huge amounts of assets (e.g. crypto money) in the metaverse worlds. Stolen credentials can be

used to make unauthorised purchases and to launder money through stolen metaverse accounts.

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. 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. [15] examine the security and privacy risks associated with a realistic digital clone (avatar) of an individual falling into the wrong hands. In his study, a network intrusion detection system, by protecting against cyberattacks, misuse, and negligence, and dynamic information flow tracking methods, by examining the user login flow details, are proposed to detect unauthorised access to the metaverse platforms to avoid avatar theft.

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 II-A3) 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 II-A15). Fake digital assets such as non-existent properties, services, and fraudulent cryptocurrencies can be traded with legitimate currency with promises of unrealistic returns. 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.

6) Brand/business theft and business impersonation: In urban metaverse worlds, companies and residents can build digital duplicates of their actual physical assets (e.g. physical stores). 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. Impersonated stores that mimic legitimate companies can be used to compromise user credentials along with financial damages. For instance, in order to sell counterfeit goods, cybercriminals can set up a phony online store that looks just like the real one. Customers may fall for these fake metaverse businesses and think they are purchasing authentic goods. Cybercriminals can use these digital businesses as a template to con other companies, organisations, and even governmental bodies.

7) Misuse of the platform, antisocial behaviours, and cyberbullying: An immersive urban metaverse ecosystem would be the perfect world for antisocial behaviours like fraud, sexual assault, and cyberbullying [16]. A violation happens roughly every seven minutes in the virtual reality game VRChat [17]. With more application areas added, it is anticipated that criminal activity will rise as the metaverse grows. These crimes will have an impact on the mental and emotional health of victims in the virtual world, just as they do on victims in the real world [18]. When it comes to data sovereignty, these crimes might be carried out by avatars using false identities and might not be traceable. To allay these worries, avatars can be registered with tokens in cybercommunities. This allows for the tracking of inappropriate behaviours and accordingly, users are held accountable for their adversary actions such as cancelling tokens. Furthermore, the metaverse software allows for the enforcement of physical avatar rules. For example, Meta introduced boundary limits for Horizon Worlds, which will allow users to manage their virtual reality experience. For instance, the default setting for non-friends will be approximately four feet apart between an individual avatar and others; however, an avatar can now modify their individual boundary from the settings. Moreover, the users can be exposed to racism. 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.

8) Phubbing and societal concerns: Phubbing is the act of rejecting or ignoring the company of a person in favour of a mobile phone or a cyber environment. Given the immersive nature of the urban metaverse ecosystem, it is highly likely that the degree of phubbing in our actual social settings will rise. From the perspective of a cyberdystopia, the replacement of real, intimate, close relationships in urban settings by virtual experiences through avatars may have unanticipated negative effects and give rise to new kinds of psychological issues for people, such as feelings of social exclusion, loneliness, and social segregation. This is because, despite their immersive services, metaverse worlds are insufficient to provide real closeness, and this needs to be examined by related disciplines [13]. Moreover, physical inactivity is known to raise the risk of several serious illnesses, including osteoporosis, hypertension, coronary heart disease, and stroke [19]. In order to prevent the previously mentioned health issues, physical activity should be encouraged in metaverse worlds as the widespread use of these worlds may lead to physical inactivity [13].

9) Phishing attacks: In addition to the aforementioned phishing attacks mentioned in other subsections (Sections II-A1, II-A2), cybercriminals might create fake metaverse platforms 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 believe

that they are interacting with legitimate cybercommunities.

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 relationship between the mind, brain, and body is examined in the Matrix trilogy, with particular attention to how this relationship is altered when it is revealed that the world is an illusion [20]. Virtual products (as a part of an advertisement) or AI-driven avatars, with their seemingly authentic stories, can be injected into the urban metaverse cyberspace as they are a part of the real environment to influence us one way or the other. Residents might be targeted for money laundering purposes. Social engineering attacks can be more convincing compared to web2, as cyber attackers can deceive users in a variety of effective approaches, particularly, using identity falsification and impersonation scams (Section II-A1) such as the creation of realistic avatars (Sections II-A1 and II-A2) and businesses/stores (Section II-A6) by exploiting the trust of others. They 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.

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

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. An analysis of 25 Smart Cities (SCs) with major concerns revealed a lack of information on privacy policies or even privacy protection [21]. Data owners worry about the possibility that different parties, involving service suppliers, may use their sensitive information without authorisation [22] on the cloud/fog platforms. We learned from the court cases and compensations that the technology giants governing social media had sold sensitive data without the authorisation of their users, which is a breach of privacy and security. The development of cybercommunities with data collection from highly distributed UTs makes it imperative to address the issue of how to prevent sensitive data from being read by unauthorised parties [2]. Within this context, urban metaverse cyberspaces should be transparent with users about how they process the sensitive data of their users. Data sharing should be implemented using a consent-based approach where no personal data can be shared with third parties. Empowering users in the metaverse requires granular privacy controls and the ability to control what data is shared. Residents should be able to withdraw their pre-given consents and their collected data must be deleted urgently if demanded by them. Users must be informed of the policies of the platform about what types of data can be deleted if requested concerning transparency. Residents should be able to leave the platforms as they wish without giving a reason.

The more the avatar resembles the user with advancing technologies, the more personal data such as physiological and behavioural signatures as well as the environmental space can be compromised with the sensory data transformation using immersive devices (e.g. VR/AR headset, MoCaps, haptics gloves, 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 owners using private keys (i.e. cryptographic password or personal digital signature) securely within this token economy. Unauthorised access to user behaviour tracking that leads to emotion recognition for specific types of inputs could lead to serious privacy violations. For instance, users can be targeted by advertisements and they can be tracked with individual trajectory content management techniques, which can harm them mentally and financially. The invasion of physical privacy is the other concern. An avatar can be attacked 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 II-A7.

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. How smart wearables can be used to implement advanced multiverse worlds is analysed in [23]. One of the key elements of the metaverse is wearable hardware, which has the potential to introduce new risks. These devices, which store resident biometric data, could become prime targets for attacks as the use of VR/AR headsets grows. These headsets could provide hackers with an easily accessible point of entry. GPS services on which immersive devices rely can be easily spoofed and GPS signals can be lost promptly due to DoS attacks, which causes severe prolonged signal outages. The 6G ecosystem is anticipated to have a large number of connected devices and network tenants, which makes it highly vulnerable to DDoS attacks [24], [25]. The three primary cybersecurity concerns in urban cybercommunities are DoS attacks, avatar theft, and privacy breaches, particularly for wearable metaverse immersive devices. Immersive services can be disrupted due to a lack of standardised security measures concerning the vulnerabilities and inconsistencies between a variety of interconnected devices and applications, which can impact users' experiences negatively. Ensuring real socialising and preventing privacy intrusions without lowering Quality of Experience (QoE) is paramount. The introduction of blockchain in urban use cases aims to address these concerns. In [26], a blockchain-based framework for DTs was presented to guarantee transaction security when data is streamed between virtual and physical entities. In the coming years, more and more urban metaverse use cases are anticipated to prompt the development of comparable security frameworks.

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 II-A4). Furthermore, vital signs (e.g. heart and respiratory rates) can be detected through smart devices and AR/VR sets. Cyberattackers are inclined to exploit the vulnerabilities in VR/AR devices to steal the aforementioned sensitive personal information or to partially take control of these devices with several intrusion activities such as content placement. How we are responding to the placed items in the virtual environment can make us the target of advertisements. The privacy of users will be violated substantially when a hacker gains access to a user's VR/AR headset, sharing your life with you and seeing every part of your life. Users of VR headsets immersed in the virtual environment are in a vulnerable position, and they can be physically harmed by the manipulation of their perception and they can be directed in the wrong direction, leading to physical damage or life-threatening actions. Moreover, they, particularly children, can be mentally harmed by inappropriate content out of the context placed in virtual environments through wearable immersive devices.

15) Generative Adversarial Network (GAN): The GAN attack has demonstrated that inadequately safeguarded local data is susceptible to being discovered by adversaries [27]. In collaborative deep learning (CDL), malicious participants in the urban metaverse cybercommunity can use downloaded parameters improperly to build a GAN that will allow them to obtain other people's private information illegally, or they can upload misleading parameters that will degrade the model's performance [28]. 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. In order to mitigate the threat that GAN attacks pose to CDL, Chen et al. [27] proposed a framework, MP-CLF, for model-preserving CDL and an adversary detection-deactivation method for metaverse-oriented CDL was proposed in [28].

B. COUNTERMEASURES FOR URBAN CYBERSPACES

1) Agreed-upon standards, policies and ethics: 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 regulations (e.g. USA California Consumer Privacy Act (CCPA), China Cyber Security Law and General Principles of Civil Law, and EU 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 interoperable metaverse ecosystem.

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 cyberrisks, should be mitigated. In this direction, everybody has to prepare themselves for the advantages and disadvantages of the technology by equipping themselves with some level of understanding about metaverse immersive experiences regarding the use of this developing technology before engaging in this ecosystem. The human factor is the main concern in cybersecurity measures. Therefore, first and foremost, all users of any urban metaverse platform have to be trained using the tools instilled into the platform about how to practice cybersecurity hygiene to avoid everyday cyberattacks (Section II-A) such as malware exposures or social engineering. Even the best systems can not be protected without practising cybersecurity hygiene properly.

Urban metaverse cyberspaces look like our real environment, a kind of DT of it. First, we should be thinking of incorporating similar cybersecurity measures that are implemented in our real environment along with the ones in Web2 into this real and virtual blended ecosystem and, accordingly, urban metaverse cyberspaces should be protected in a similar way by their main managing bodies (i.e. city governors) with policies in place and advanced automated AI tools to detect instant 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 augmented in this environment as elaborated in Section II-A. 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 honest but curious and semi-honest parties. In this sense, the main urban entity and its cybercommunity entities (i.e. UMaaSs) should be addressing the concerns of its residents appropriately, privacy concerns in particular, to provide proper cybersecurity hygiene. 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 where the platform-based generated data is in the hands of the good to be processed by advanced AI tools to serve noble ends.

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. 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. 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 cybercommunities have, shall be measured regarding the resilience to the potential metaverse cyberthreats (Section II-A) before embarking on these cybercommunities. 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 on 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 metaverse worlds, particularly in managing structured and unstructured data and storing and disseminating it. More explicitly, AIOps provides event correlation capabilities by analysing real-time data and can determine deviations from typical patterns that might point to system anomalies. AI can be used effectively to predict attacks in the metaverse urban cyberspaces. ML-based trained models can help detect attacks directly to the infrastructure of the platform and defend the system from these attacks by improving its defence mechanisms with real-time effective solutions in an automated manner. Platform-based activities, interactions and experiences can be monitored in real-time using automated decentralised privacy-preserving CL models to avoid any interruptions.

4) Automated detection of Out-of-the-Pattern actions (OoPAs): P2P/E2E interactions between entities are evident within the distributed urban ecosystem with multiple experiences. In addition to the interactions with other residents, users interact with urban businesses (e.g. via AI-driven avatars) within immersive urban 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, and AI-generated avatars/bots can be classified with a scale of categorisation (e.g. ranging from very bad to very good) for various criteria (e.g. trust, use of language, behaviours) based on their pre-

observed, pre-noted actions and the feedback obtained from the other residents and businesses in the same cybercommunity. 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. Any user should face punishment if acting against the policies of the platform virtually or legally based on the severity of the actions. They, based on their actions, can be categorised as "red", "orange", "yellow", or "green" regarding their risk profiles based on the aforementioned criteria, but always by prioritising privacy and respecting data sovereignty. Entities, with repeated, extreme adverse actions, can be tagged with colours on a red gradient to make other virtual businesses and residents vigilant against these entities. Entities can be banned from entering cybercommunities where their actions are getting severe. However, all these approaches, which are dependent on human responsible actions, are not sufficient to provide residents with completely instant, automated, and secure protection within this newly developing urban metaverse ecosystem, considering the large number of transactions and actions, which need to be authenticated and verified immediately. CDL can help detect OotPAs to alleviate cyberthreats. Automated platform-, user- and/or business-focused cybersecurity ML models can be generated by utilising CDL to both detect OotPAs leading to the disclosure of cyberattacks and address those attacks in real-time using the automated cybersecurity measures. Nevertheless, these approaches have their shortcomings in providing the required level of privacy, authentication and verification mechanisms.

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 II-B2) within the urban metaverse cybercommunity. Cybercommunities and their 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 cybercommunities swiftly.

6) Visibility versus invisibility & Anonymity: Invisibility, feeling the immersive nature of the cybercommunities without being seen, and anonymity, situations where an individual's identity is unknown to other users using an anonymous avatar during the immersive interaction, are two sensitive subjects, which should be investigated in detail with respect to the objectives and requirements of specific cybercommunities and the rights of other users within the same cybercommunity. 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.

7) Homomorphic Encryption (HE): It allows for the execution of intricate queries and calculations on encrypted data by multiple entities while maintaining the confidentiality of the data and its encryption [29]. If the owner of the data wishes to visualise the processed result, they can use the private key to decrypt it if it is still encrypted. In practice, however, there is a significant computational cost associated with exchanging and computing sensitive data without the need to decrypt it. The computational complexity of the ciphertext operation is significantly higher than that of the plaintext operation [30]. Partially HE, somewhat HE, and fully HE are the three different forms of HE. In comparison to the other two HEs, Fully HE has the greatest computational overhead and allows for infinite addition and multiplication of ciphertexts. Despite its complexity and computational overhead, Fully HE is used by many large corporations, including Microsoft, for sensitive data that needs to be processed by multiple parties. Above all, it makes it possible to train encryption structures based on homomorphism in order to construct larger learning models or CDL models. HE aims to shield the data from unauthorised access and user privacy by preventing the recovery of the original data. In the future, ML-as-a-Service (MLaaS) techniques that leverage HE-like approaches to process encrypted data will receive special attention, especially for applications requiring a high degree of privacy preservation on data that must be computed by multiple entities and is stored in public domains. Differential privacy, a different method of maintaining privacy that has drawn a lot of interest, was created in [31]. Nevertheless, as more noise is introduced into the data to boost privacy and security, the model's accuracy declines in this approach.

III. Discussion and Conclusion

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 devices. 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 [32]. We visualise that residents will be spending a greater portion of their daily life in urban immersive 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 their economic value increases with newly created assets. 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. 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. The urban metaverse industry must work together in a fruitful collaboration to create robust security frameworks for wearable immersive metaverse devices such as VR/AR devices or MoCaps, cyberspaces, and applications. 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. There is a research gap in revealing potential cyberthreats in urban metaverse worlds and addressing these threats. In this respect, while the urban-based metaverse worlds are developing, this research analyses cyberthreats and basic cybersecurity measures against those cyberthreats comprehensively within the urban metaverse ecosystem.

REFERENCES

[1] K. Kuru and H. Yetgin, "Transformation to advanced mechatronics systems within new industrial revolution: A novel framework in automation of everything (aoe)," *IEEE Access*, vol. 7, pp. 41 395–41 415, 2019.

[2] K. Kuru and D. Ansell, "Tcitysmartf: A comprehensive systematic framework for transforming cities into smart cities," *IEEE Access*, vol. 8, pp. 18 615–18 644, 2020.

[3] F. Tang, X. Chen, M. Zhao, and N. Kato, "The roadmap of communication and networking in 6g for the metaverse," *IEEE Wireless Communications*, pp. 1–15, 2022.

[4] K. Kuru and W. Khan, "A framework for the synergistic integration of fully autonomous ground vehicles with smart city," *IEEE Access*, vol. 9, pp. 923–948, 2021.

[5] K. Kuru, S. Worthington, D. Ansell, J. M. Pinder, A. Sujit, B. Jon Watkinson, K. Vinning, L. Moore, C. Gilbert, D. Jones *et al.*, "Aitl-wing-hitl: Telemanipulation of autonomous drones using digital twins of aerial traffic interfaced with wing," *IEEE Access*, vol. 11, 2023.

[6] K. Kuru, J. M. Pinder, B. J. Watkinson, D. Ansell, K. Vinning, L. Moore, C. Gilbert, A. Sujit, and D. Jones, "Toward mid-air collision-free trajectory for autonomous and pilot-controlled unmanned aerial vehicles," *IEEE Access*, vol. 11, pp. 100 323–100 342, 2023.

[7] K. Kuru, "Conceptualisation of human-on-the-loop haptic teleoperation with fully autonomous self-driving vehicles in the urban environment," *IEEE Open J. Intell. Transp. Syst.*, vol. 2, pp. 448–69, 2021.

[8] ——, "Planning the future of smart cities with swarms of fully autonomous unmanned aerial vehicles using a novel framework," *IEEE Access*, vol. 9, pp. 6571–6595, 2021.

[9] ——, "Technical report: Analysis of intervention modes in human-in-the-loop (hitl) teleoperation with autonomous ground vehicle systems," *Central Lancashire online Knowledge*, 2022.

[10] ——, "Technical report: Analysis of intervention modes in human-in-the-loop (hitl) teleoperation with autonomous unmanned aerial systems," *Central Lancashire online Knowledge*, 2024.

[11] ——, "Management of geo-distributed intelligence: Deep insight as a service (dinsaas) on forged cloud platforms (fcp)," *Journal of Parallel and Distributed Computing*, vol. 149, pp. 103–118, 2021.

[12] ——, "Trustfsdv: Framework for building and maintaining trust in self-driving vehicles," *IEEE Access*, vol. 10, pp. 82 814–82 833, 2022.

[13] ——, "Metaomnicity: Toward immersive urban metaverse cyberspaces using smart city digital twins," *IEEE Access*, vol. 11, pp. 43 844–68, 2023.

[14] L. Cui and J. Liu, "Virtual human: A comprehensive survey on academic and applications," *IEEE Access*, vol. 11, pp. 123 830–123 845, 2023.

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

[16] K. Kuru and K. Kuru, "Blockchain-based decentralised privacy-preserving machine learning authentication and verification with immersive devices in the urban metaverse ecosystem," *Preprints*, 2024.

[17] S. Frenkel and K. Browning, "The metaverse's dark side: Here come harassment and assaults," 2021.

[18] N. Huq, R. Reyes, P. Lin, and M. Swimmer, "Cybersecurity threats against the internet of experiences," *Trend Micro Research*, 2022.

[19] B. K. Wiederhold, "Metaverse games: Game changer for healthcare?" *Cyberpsychology, Behavior, and Social Networking*, vol. 25, no. 5, pp. 267–269, 2022, pMID: 35549346.

[20] TheWachowskis, "The relationship between body, brain, and mind," 2023.

[21] D. Eckhoff and I. Wagner, "Privacy in the smart city—applications, technologies, challenges, and solutions," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 489–516, Firstquarter 2018.

[22] S. S. Yau, H. G. An, and A. B. Buduru, "An approach to data confidentiality protection in cloud environments," *International Journal of Web Services Research*, vol. 9, no. 3, pp. 67–83, 2012.

[23] S. Rostami and M. Maier, "The metaverse and beyond: Implementing advanced multiverse realms with smart wearables," *IEEE Access*, vol. 10, pp. 110 796–110 806, 2022.

[24] A. Kalla, C. De Alwis, G. Gur, S. P. Gochhayat, M. Liyanage, and P. Porambage, "Emerging directions for blockchainized 6g," *IEEE Consumer Electronics Magazine*, pp. 1–1, 2022.

[25] K. Kuru, D. Ansell, W. Khan, and H. Yetgin, "Analysis and optimization of unmanned aerial vehicle swarms in logistics: An intelligent delivery platform," *IEEE Access*, vol. 7, pp. 15 804–15 831, 2019.

[26] E. E.-D. Hemdan and A. S. A. Mahmoud, *BlockTwins: A Blockchain-Based Digital Twins Framework*. Springer, 2021, p. 177–186.

[27] Z. Chen, J. Wu, A. Fu, M. Su, and R. H. Deng, "Mp-clf: An effective model-preserving collaborative deep learning framework for mitigating data leakage under the gan," *Knowledge-Based Systems*, vol. 270, p. 110527, 2023.

[28] P. Li, Z. Zhang, A. S. Al-Sumaiti, N. Werghi, and C. Y. Yeun, "A robust adversary detection-deactivation method for metaverse-oriented collaborative deep learning," *IEEE Sensors Journal*, pp. 1–1, 2023.

[29] K. Kuru, "Technical report: Big data-concepts, infrastructure, analytics, challenges and solutions," *Central Lancashire online Knowledge*, 2024.

[30] R. Podschwadt, D. Takabi, P. Hu, M. H. Rafiei, and Z. Cai, "A survey of deep learning architectures for privacy-preserving machine learning with fully homomorphic encryption," *IEEE Access*, vol. 10, pp. 117 477–500, 2022.

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

[32] K. Kuru, "Technical report: Essential development components of the urban metaverse ecosystem," *University of Central Lancashire*, 2024.

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

[34] ——, "Human-in-the-loop telemanipulation schemes for autonomous unmanned aerial systems," in *2024 4th Interdisciplinary Conference on Electrics and Computer (INTCEC)*, 2024, pp. 1–6.

[35] ——, "Technical report: Analysis of intervention modes in human-in-the-loop (hitl) teleoperation with autonomous unmanned aerial systems," *Central Lancashire online Knowledge*, 2024.
[36] ——, "Use of autonomous uninhabited aerial vehicles safely within mixed air traffic," in *Proceedings of Global Conference on Electronics, Communications and Networks (GCECN2024)*, 2023.
[37] ——, "Technical report: Analysis of intervention modes in human-in-the-loop (hitl) teleoperation with autonomous ground vehicle systems," *Central Lancashire online Knowledge*, 2022.
[38] ——, "Sensors and sensor fusion for decision making in autonomous driving and vehicles," 2023.
[39] ——, *A Novel Hybrid Clustering Approach for Unsupervised Grouping of Similar Objects*. Springer International Publishing, 2014, p. 642–653.
[40] ——, "Optimization and enhancement of h&e stained microscopical images by applying bilinear interpolation method on lab color mode," *Theoretical Biology and Medical Modelling*, vol. 11, no. 1, 2014.
[41] ——, "Definition of multi-objective deep reinforcement learning reward functions for self-driving vehicles in the urban environment," *IEEE Trans. Veh. Technol.*, vol. 11, pp. 1–12, Mar. 2024.
[42] ——, "Management of geo-distributed intelligence: Deep insight as a service (DINSaaS) on forged cloud platforms (FCP)," *Journal of Parallel and Distributed Computing*, vol. 149, pp. 103–118, Mar. 2021.
[43] ——, "Technical report: Big data - concepts, infrastructure, analytics, challenges and solutions," 2024.
[44] ——, "Blockchain-enabled decentralized, secure and reliable voting through biometric identification using metaverse immersive devices and deep learning," 2025.
[45] ——, "Swarms of autonomous drones in logistics within smart city: Opportunities, challenges and future directions," 2025.
[46] ——, "6g in developing high-fidelity immersive digital twins," 2025.
[47] ——, "Joint cognition of remote autonomous robotics agent swarms in collaborative decision-making & remote human-robot teaming," *Proceedings of The Premium Global Conclave and Expo on Robotics & Automation (AUTOROBO, EXPO2024)*, 2024.
[48] ——, "Use of wearable miniaturised medical devices with artificial intelligence (ai) in enhancing physical medicine," *Proceedings of Enhancing Physical Medicine. In: World Congress on Physical Medicine and Rehabilitation*, 2024.
[49] ——, "Technical report: Towards state and situation awareness for driverless vehicles using deep neural networks," *Central Lancashire online Knowledge*, 2024.
[50] ——, "Technical report: Human-in-the-loop telemanipulation platform for automation-in-the-loop unmanned aerial systems," *Central Lancashire online Knowledge*, 2024.
[51] K. Kuru and K. Kuru, "Urban metaverse cyberspaces & blockchain-enabled privacy-preserving machine learning authentication with immersive devices," in *2024 6th International Conference on Blockchain Computing and Applications (BCCA)*, 2024, pp. 734–741.
[52] ——, "Urban metaverse cyberthreats and countermeasures against these threats," in *2024 6th International Conference on Blockchain Computing and Applications (BCCA)*, 2024, pp. 228–235.
[53] ——, "Umetabe-dppml: Urban metaverse & blockchain-enabled decentralised privacy-preserving machine learning verification and authentication with metaverse immersive devices," *Internet of Things and Cyber-Physical Systems*, vol. 5, 2025.
[54] ——, "Blockchain-enabled privacy-preserving machine learning authentication with immersive devices for urban metaverse cyberspaces," in *2024 20th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications (MESA)*, 2024, pp. 1–8.
[55] J. Lowe and K. Kuru, "Design & development of a smart blind system using fuzzy logic," in *2024 20th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications (MESA)*, 2024, pp. 1–8.
[56] ——, "Development of machine intelligence for self-driving vehicles through video capturing," in *2024 20th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications (MESA)*, 2024, pp. 1–8.
[57] K. Kuru, O. Erogul, and C. Xavier, "Autonomous low power monitoring sensors," *Sensors*, vol. 21, 2021.