IEEE/ASME MESA 2024 – 20th Int. Conference on Mechatronic, Embedded Systems and Applications
02-04 September 2024, Genova-Italy

Blockchain-Enabled Privacy-Preserving Machine Learning Authentication With Immersive Devices for Urban Metaverse Cyberspaces

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*—Urban life has already embraced many urban metaverse use cases to increase the Quality of Life (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 Quality of Experiences (QoE) to readily evolve and mitigate the problems of urbanisation. Cybersecurity and privacy protection are the two crucial challenges in making secure and reliable urban metaverse 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 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. In this direction, this paper presents a blockchain-enabled method for immersive device-based Decentralized Privacy-Preserving Machine Learning (BE-DPPML) authentication and verification. It can be effectively instrumented against identity theft and impersonation, as well as against the theft of credentials, identities, or avatars.**

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

I. INTRODUCTION

Urban metaverse worlds/cyberspaces – an extension of residents and urban society, where the virtual and the physically real blend and are more organically integrated within the Cybercommunity of Wisdom (CoW) and where real-person resident avatars, government avatars, governmental entities, organisations, businesses, and avatars driven by Artificial Intelligence (i.e. AI bots or virtual users) can interact – would impact urban ways of living significantly on a global scale, with many practical implementations by democratising skills/assets within an urban ecosystem. The 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]. Accurate digital replication of real-world fragments of urbanisation (SC Digital Twins (DTs) (i.e., Urban Twins (UTs)) at various granularities can be achieved in the virtual plane through UTs [3]. Readers are referred to the previous studies [4], [5], [6], [7], [8] for the examples of DTs. In highly synchronized environments, similar DTs 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 Quality of Life (QoL) through improved Quality of Experiences (QoE). The success of urban metaverse communities, augmented with the CoW, depends on the quality of data-driven UTs, the seamless exchange of data between cyber and physical urban 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. The urban metaverse, an extension of CPSSs, has the potential to affect its residents 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 UTs. 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.

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. On one hand, incorporating 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 paired with

additional technological innovations like AI and blockchain. 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? In this direction, in this paper, a blockchain-based authentication approach, which uses metaverse-immersive devices to generate Privacy-Preserving Machine Learning (PPML) or Privacy-Preserving Deep Learning (PPDL) 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 targeted functional abilities of the immersive devices and the essential objectives of the urban metaverse cyberspaces.

II. Background and Literature Survey

A. Urban Metaverse Cyberspaces

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. The urban metaverse ecosystem is the interconnected network of blockchain-based decentralised cybercommunities, i.e. UMaaSs, and resident avatars can navigate from one cybercommunity to another with interoperable abilities and they can build their UMaaS worlds. Large numbers 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). Urban metaverse cyberspaces are composed of both centralised and decentralised architecture regarding the objectives of the cyberspaces, some of which are controlled by the local city governments and some of which (i..e., user-owned, user-centric) may be managed by their users or together with the local government. Blockchain, as a distributed database, provides unique data structures (i.e. crypto worlds) that were designed to make many people interact/transact with each other without thinking about privacy too much. On the other hand, Distributed Ledger Technology (DLT) aims to incorporate privacy into the transactions further. Blockchain, a type of DLT, is implemented as a decentralised Peer-to-Peer (P2P) network and stores a digital ledger in a distributed and secure manner; smart contracts extend 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 [9]. The key components of the metaverse in developing urban worlds (Urban Metaverse-as-a-Services (UMaaSs)) are summarised in [10] with a variety of metaverse cybercommunities. UMaaSs are the ubiquitous fragmented parallel urban environments, which make it possible to effectively customise certain urban metaverse services [10].

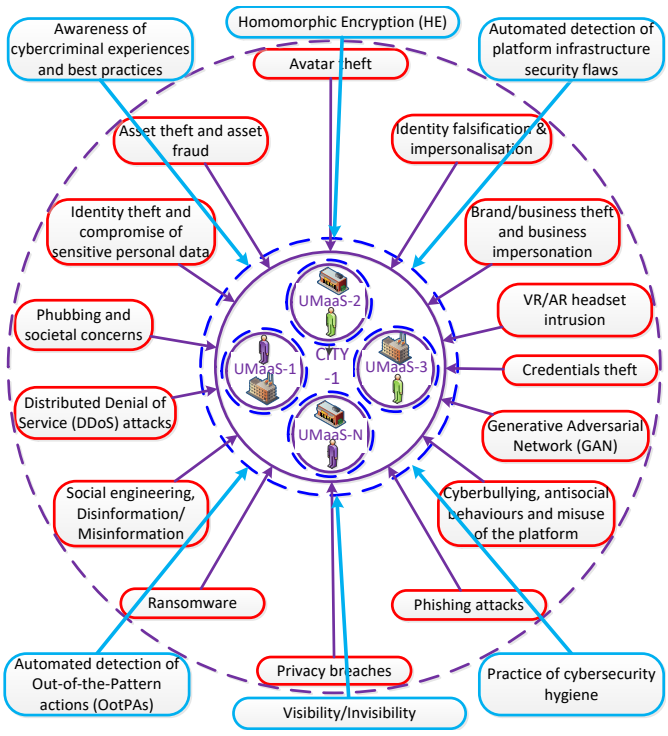

Fig. 1: Cyberthreats against Urban Metaverse-as-a-Services (UMaaSs) (red) and basic countermeasures (blue).

B. Cyberthreats To Metaverse Cyberspaces

Cybersecurity threats against the metaverse as well as privacy concerns are analysed in [11], [12], [13], [14]. 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 [15]. 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 [16]. New and effective approaches (e.g. [17]) 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 [18]. 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. These cyberthreats are elaborated in [19]. We need to get ready to deal with these hazards while we are embracing many promising potentials within this new type of Immersive urban ecosystem.

C. Countermeasures To Cyberthreats

The countermeasures (Fig. 1) against the aforementioned cyberthreats (Sections II-B) in the urban metaverse ecosystem are elaborated in [19]. Urban metaverse cyberspaces should facilitate the exchange of information in a trusted way through the metaverse ecosystem built on decentralised blockchain technologies. Blockchain, with its privacy-preserving mechanisms by verifying the training process securely, has been recently employed to enable the secure generation of SAI in a distributed manner. A blockchain FL (BlockFL) mechanism, enabling on-device ML without any centralised, training data or coordination by utilising a consensus mechanism is proposed in [20] 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. [21] aim to address the threat from GAN attacks pose to collaborative deep learning (CDL) and propose a model-preserving CDL framework, called MP-CLF, which can effectively resist the GAN attack. An adversary detection-deactivation method for metaverse-oriented CDL is proposed in [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 [23]. 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 [24].

Standard FL/CL model generation tools based on wearable devices can be provided by the main urban city, or the developers of the metaverse devices, to users to train their models in a standard way, through which messages can be communicated 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 (Fig. 1). 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. 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, without requiring the authentication of a third party, while immersing themselves with urban experiences and executing their transactions. Therefore, a blockchain-based approach, which is elaborated in the following subsection, is proposed in this research. The proposed authentication and verification approach, the so-called BE-DPPML, addresses those aforementioned concerns effectively and efficiently.

III. BLOCKCHAIN-ENABLED DECENTRALISED PRIVACY-PRESERVING MACHINE LEARNING (BE-DPPML) AUTHENTICATION AND VERIFICATION

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. Automated solutions with privacy-preserving mechanisms can mitigate the cyberthreats 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

[1]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.

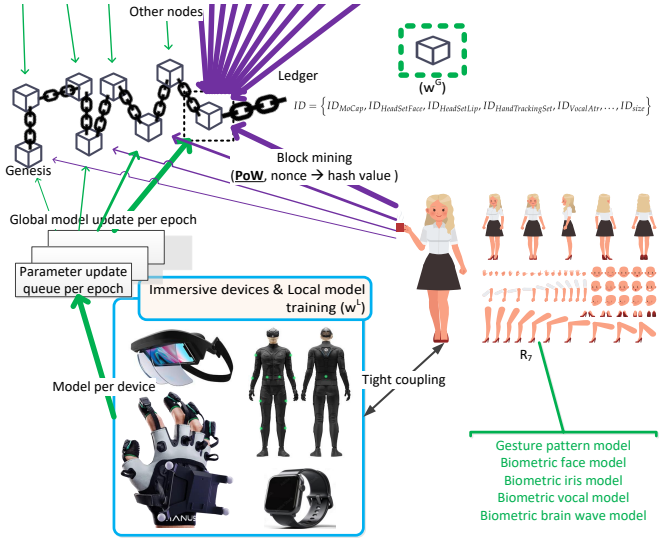

Fig. 2: User-based DPPML model generation using immersive metaverse devices. The next block which is being added to the distributed ledger has the most recent model update where as the last block has the final model itself.[1]

composed of i) biographic identification data such as name, surname, date of birth, and ii) biometric identification data as biological characteristics (DNA, facial features, height, fingerprints, iris features, vein features, and palm features) and behavioural/gesture patterns (facial expressions, movement patterns (gait), lip motion, emotion expression or reactions to interactions using physiological responses, voice pitch patterns/prints, and speech patterns). Automated Emotion Recognition (AER) and Automated Behaviour Recognition (ABR) technologies can detect humans' emotional/behavioural states in real-time using facial expressions, voice attributes, text, body movements, and neurological signals and have a broad range of applications across many sectors [25]. 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 [26] for interested readers. The way of building DL gesture models should consider these privacy and ethical concerns as well as the regulatory framework. 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 [27] 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

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

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

from other users. Within this context, immersive metaverse 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. The capabilities of these devices can be instrumented to improve privacy and security when combined with other technologies such as blockchain and SAI. 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

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

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

extracting the patterns from users' gesture cues, which leads to patterns distinguishing us from the rest of the world. These patterns, as well as the aforementioned distinctive individual signatures, can be utilised effectively for authentication purposes via a diverse range of metaverse technologies (e.g. VR/AR headsets, MoCaps, haptics gloves, and HTT), different types of many other Wearable Sensors (WSs)), which are improving with larger sets of options and a diverse range of attributes [28], [29]. 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 [30].

The urban metaverse cyberspaces and associated entities are distributed on the decentralised public and private ledgers. 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 II. 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 [31]. In this vein, a DPPML scheme, based on transparency and personal consent, 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 are 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 Fig. 2. 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 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, $S = \{F_1, F_2, \ldots, F_{epoch}\}$. Local weights ($w^L$) and global weights ($w^G$) are synchronously updated after every epoch iteration to generate particular vocal or gesture models, M_{ID}, per immersive device, ID, as displayed in Eq. 1.

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

Residents, R, perform the PoW operations with a block generation rate of λ and whoever is successful in reaching a hash key, by finding a nonce that is smaller than the target value based on the difficulty of PoW, places the 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 (Fig. 2), 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.

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

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 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 to avoid any possible data leakage,

Data: System input:
$M_{ID_{MoCap}} = \{R_{1_{(M_{ID_{MoCap}})}}, R_{2_{(M_{ID_{MoCap}})}}, R_{3_{(M_{ID_{MoCap}})}}, \ldots, R_{size_{(M_{ID_{MoCap}})}}\}$
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. $|w^G - w^{G-1}| \leq \epsilon$);
        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 *($F \in S$)* **do**
                ModelVal = $R_{me_{(M_{ID_{MoCap}})}} <--$ $F = \{A_1, A_2, \ldots, A_{size}\}$;
                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

Algorithm 3: Proof of identity using blockchain-based DPPML pre-trained models with immersive devices where $ID = ID_{MoCap}$.

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.

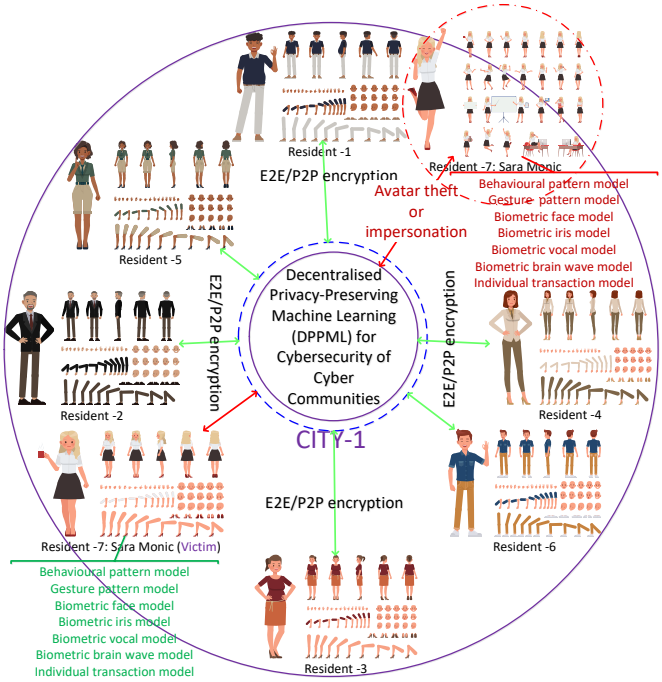

Fig. 3: Detection of avatar theft and identity impersonation. Quarantine of a harmful user to avoid possible cyberattacks.

The above operations are repeated for all ID using different blockchain forms.

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 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 any of the attribute sets in the sample array. Each entity knows nothing about the trained data and its providers' identity while using the global ML models in an automated manner with the entity parameters to get a targeted classified outcome needed. The global model construction and use of this model should ensure that there is no adversarial entity collaborating with the process, which can be avoided using effective E2E/P2P encryption mechanisms (Fig. 3). 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.

IV. 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]. These cyber worlds will be a target for cybercriminals to exploit as their economic value increases with newly created 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. *

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. 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. 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. Our research question was if we can turn the abilities of immersive metaverse devices into the residents' advantage in providing their security and avoiding a breach of privacy. In a broader perspective, if it is possible to build a trustworthy, urban metaverse cybercommunity, without requiring a centralised government to protect our privacy or a third party to mediate between entities, e.g. for a transaction. This research designs a novel blockchain-enabled DPPML (BE-DPPML) authentication and verification approach, based on physics-based characters of individuals (i.e. body cyber footprint/identity – e.g. facial expressions, movement patterns (gait), lip motion, emotional expression or reactions to experiences using physiological responses, voice pitch patterns/prints, and speech patterns [33]) 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. As a future work, the signatures obtained from a couple of sensors will be fused for a more advanced gesture model [34] and the proposed system is aimed to be integrated into metaverse cyberspaces.

V. LIMITATIONS OF THE RESEARCH

The particular BE-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 using 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). The proposed authentication approach in this research requires the collaboration and cooperation of users in metaverse cyberspaces to mine the blocks and verify their authenticity as block miners. Users can be encouraged to take part in block mining activities by earning particular cryptocurrencies allocated to metaverse cyberspaces.

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, "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.

[5] 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.

[6] 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.

[7] 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.

[8] K. Kuru, "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] 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.

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

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

[12] M. Pooyandeh, K.-J. Han, and I. Sohn, "Cybersecurity in the ai-based metaverse: A survey," *Applied Sciences*, vol. 12, no. 24, 2022.

[13] Y. Huang, Y. J. Li, and Z. Cai, "Security and privacy in metaverse: A comprehensive survey," *Big Data Mining and Analytics*, vol. 6, no. 2, pp. 234–247, 2023.

[14] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2022.

[15] K. Kuru and K. Kuru, "Urban metaverse cyberthreats and countermeasures to mitigate them," in *Proceedings of IEEE Sixth International Conference on Blockchain Computing and Applications (BCCA 2024)*, 2024.

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

[17] ——, "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.

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

[19] K. Kuru and K. Kuru, "Urban metaverse cyberthreats and countermeasures against these threats," in *Sixth International Conference on Blockchain Computing and Applications (BCCA 2024)*, 2024, pp. 1–8.

[20] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Blockchained on-device federated learning," *IEEE Communications Letters*, vol. 24, no. 6, pp. 1279–1283, 2020.

[21] 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.

[22] 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.

[23] L. Lyu, Y. Li, K. Nandakumar, J. Yu, and X. Ma, "How to democratise and protect ai: Fair and differentially private decentralised deep learning," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1003–1017, 2022.

[24] T. Chen and S. Zhong, "Privacy-preserving backpropagation neural network learning," *IEEE Transactions on Neural Networks*, vol. 20, no. 10, pp. 1554–1564, 2009.

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

[26] A. McStay, "Emotional ai, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy," *Big Data & Society*, vol. 7, no. 1, p. 2053951720904386, 2020.

[27] X. B. Peng, P. Abbeel, S. Levine, and M. van de Panne, "Deepmimic: Example-guided deep reinforcement learning of physics-based character skills," *ACM Trans. Graph.*, vol. 37, no. 4, jul 2018.

[28] K. Kuru, "Use of wearable miniaturised medical devices with artificial intelligence (ai) in enhancing physical medicine," in *Proceedings of World Congress on Physical Medicine & Rehabilitation & International Congress on Psychology & Behavioral Sciences*, vol. 1, 2024.

[29] K. Kuru, O. Erogul, and C. Xavier, "Autonomous low power monitoring sensors," *Sensors*, vol. 21, 2021.

[30] S. Duan, F. Zhao, H. Yang, J. Hong, Q. Shi, W. Lei, and J. Wu, "A pathway into metaverse: Gesture recognition enabled by wearable resistive sensors," *Advanced Sensor Research*, vol. 2, no. 8, p. 2200054, 2023.

[31] 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.

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

[33] W. Khan and K. Kuru, "An intelligent system for spoken term detection that uses belief combination," *IEEE Intelligent Systems*, vol. 32, no. 1, p. 70–79, Jan. 2017.

[34] K. Kuru, "Sensors and sensor fusion for decision making in autonomous driving and vehicles," 2023.

[35] K. Kuru, D. Ansell, M. Jones, B. J. Watkinson, N. Caswell, P. Leather, A. Lancaster, P. Sugden, E. Briggs, C. Davies, T. C. Oh, K. Bennett, and C. De Goede, "Intelligent autonomous treatment of bedwetting using non-invasive wearable advanced mechatronics systems and mems sensors: Intelligent autonomous bladder monitoring to treat ne," *Medical & Biological Engineering & Computing*, vol. 58, no. 5, p. 943–65, 2020.

[36] K. Kuru *et al.*, "Iotfauav: Intelligent remote monitoring of livestock in large farms using autonomous uninhabited aerial vehicles," *Computers and Electronics in Agriculture*, 2023.

[37] K. Kuru, D. Ansell, B. Jon Watkinson, D. Jones, A. Sujit, J. M. Pinder, and C. L. Tinker-Mill, "Intelligent automated, rapid and safe landmine

and unexploded ordnance (uxo) detection using multiple sensor modalities mounted on autonomous drones," *IEEE Transactions on Geoscience and Remote Sensing*, 2023.

[38] K. Kuru, A. Sujit, D. Ansell, J. M. Pinder, B. Jon Watkinson, D. Jones, R. Hamila, and C. Tinker-Mill, "Iintelligent, automated, rapid, and safe landmine, improvised explosive device and unexploded ordnance detection using maggy," *IEEE Access*, 2024.

[39] K. Kuru and K. Kuru, "Blockchain-enabled privacy-preserving machine learning authentication with immersive devices for urban metaverse cyberspaces," in *IEEE/ASME MESA 2024 – 20th Int. Conference on Mechatronic, Embedded Systems and Applications*, 2024.

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

[41] ——, "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.

[42] K. Kuru, D. Ansell, D. Jones, B. Watkinson, J. M. Pinder, J. A. Hill, E. Muzzall, C. Tinker-Mill, K. Stevens, and A. Gardner, "Intelligent airborne monitoring of livestock using autonomous uninhabited aerial vehicles," in *The 11th European Conference on Precision Livestock Farming*, 2024.

[43] K. Kuru, "Use of autonomous uninhabited aerial vehicles safely within mixed air traffic," in *Proceedings of Global Conference on Electronics, Communications and Networks (GCECN2024)*, 2023.

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

[45] ——, "Telemanipulation of autonomous drones using digital twins of aerial traffic," *IEEE Dataport*, 2024.

[46] ——, *A Novel Hybrid Clustering Approach for Unsupervised Grouping of Similar Objects*. Springer International Publishing, 2014, p. 642–653.

[47] ——, "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.

[48] ——, "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.

[49] ——, "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.

[50] 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.

[51] K. Kuru, B. J. Watkinson, D. Ansell, D. Hughes, M. Jones, N. Caswell, P. Leather, K. Bennett, P. Sugden, C. Davies, and C. DeGoede, "Smart wearable device for nocturnal enuresis," in *2023 IEEE EMBS Special Topic Conference on Data Science and Engineering in Healthcare, Medicine and Biology*, 2023, pp. 95–96.

[52] K. Kuru, "Technical report: Big data - concepts, infrastructure, analytics, challenges and solutions," 2024.

[53] K. Kuru, D. Ansell, D. Hughes, B. J. Watkinson, F. Gaudenzi, M. Jones, D. Lunardi, N. Caswell, A. R. Montiel, P. Leather, D. Irving, K. Bennett, C. McKenzie, P. Sugden, C. Davies, and C. Degoede, "Treatment of nocturnal enuresis using miniaturised smart mechatronics with artificial intelligence," *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 12, pp. 204–214, 2024.

[54] K. Kuru, M. Niranjan, and Y. Tunca, "Establishment of a diagnostic decision support system in genetic dysmorphology," in *2012 11th International Conference on Machine Learning and Applications*, vol. 2, 2012, pp. 164–169.

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

[58] ——, "Urban metaverse cyberthreats and countermeasures against these threats," in *Proceedings of IEEE Sixth International Conference on Blockchain Computing and Applications (BCCA 2024)*, 2024.

[59] K. Kuru, M. Niranjan, Y. Tunca, E. Osvank, and T. Azim, "Biomedical visual data analysis to build an intelligent diagnostic decision support system in medical genetics," *Artificial Intelligence in Medicine*, vol. 62, no. 2, p. 105–118, Oct. 2014.

[60] K. Kuru and W. Khan, "Novel hybrid object-based non-parametric clustering approach for grouping similar objects in specific visual domains," *Appl. Soft Comput.*, vol. 62, pp. 667–701, Jan. 2018.

[61] K. Kuru, S. Clough, D. Ansell, J. McCarthy, and S. McGovern, "Wildetect: An intelligent platform to perform airborne wildlife census automatically in the marine ecosystem using an ensemble of learning techniques and computer vision," *Expert Systems with Applications*, vol. 231, p. 120574, Nov. 2023.

[62] ——, "Intelligent airborne monitoring of irregularly shaped man-made marine objects using statistical machine learning techniques," *Ecological Informatics*, vol. 78, p. 102285, Dec. 2023.

[63] K. Kuru, "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.

[64] N. Caswell, K. Kuru, D. Ansell, M. J. Jones, B. J. Watkinson, P. Leather, A. Lancaster, P. Sugden, E. Briggs, C. Davies, C. Oh, K. Bennett, and C. DeGoede, "Patient engagement in medical device design: Refining the essential attributes of a wearable, pre-void, ultrasound alarm for nocturnal enuresis," *Pharmaceutical Medicine*, vol. 34, no. 1, p. 39–48, Jan. 2020.

[65] K. Kuru, D. Ansell, M. Jones, C. De Goede, and P. Leather, "Feasibility study of intelligent autonomous determination of the bladder voiding need to treat bedwetting using ultrasound and smartphone ml techniques: Intelligent autonomous treatment of bedwetting," *Medical & Biological Engineering & Computing*, vol. 57, no. 5, p. 1079–1097, Dec. 2018.

[66] K. Kuru, S. Girgin, K. Arda, and U. Bozlar, "A novel report generation approach for medical applications: The sisds methodology and its applications," *International Journal of Medical Informatics*, vol. 82, no. 5, p. 435–447, May 2013.

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

[68] K. Kuru and S. Girgin, *A Bilinear Interpolation Based Approach for Optimizing Hematoxylin and Eosin Stained Microscopical Images*. Springer Berlin Heidelberg, 2011, p. 168–178.

[69] K. Kuru, "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.

[70] K. Kuru, A. Sujit, D. Ansell, J. M. Pinder, D. Jones, B. Watkinson, R. Hamila, and C. L. Tinker-Mill, "Non-invasive detection of landmines, unexploded ordnances and improvised explosive devices using bespoke unmanned aerial vehicles," *Proceedings of EEE International Conference on Electrical and Computer Engineering Researches (ICECER'24)*, 2024.

[71] K. Kuru, "Technical report: Towards state and situation awareness for driverless vehicles using deep neural networks," *Central Lancashire online Knowledge*, 2024.

[72] ——, "Technical report: Human-in-the-loop telemanipulation platform for automation-in-the-loop unmanned aerial systems," *Central Lancashire online Knowledge*, 2024.