The Sixth International Conference on Blockchain Computing and Applications (BCCA 2024)
26–29 November, 2024 – Dubai, UAE

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

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*—In the upcoming years, it is anticipated that cybercrime activities will be widespread in this ecosystem, which has trillions of dollars in economic value. This report explores a Blockchain-Facilitated Federated Security-Preserving Deep Learning (BF-FSPDL) authentication and verification method using immersive metaverse devices. Blockchain technology and Federated Learning (FL) are merged not only to eliminate the requirement of a trusted third party for the verification of the authenticity of transactions and immersive actions, but also, to avoid Single Point of Failure (SPoF) and Generative Adversarial Networks (GAN) attacks by detecting the malicious nodes using the majority voting mechanism. The developed approaches in this research have been tested using Motion Capture Suits (MoCaps) in a co-simulation environment with the Proof of Work (PoW) consensus mechanism. The preliminary results prove the viability of employing the proposed approaches in realising the objectives presented in this report. The results suggest that the approaches can prevent impersonation, identity theft, and theft of credentials or avatars promptly before any transactions have been executed. The proposed system will be tested with a larger number of nodes involving the Proof of Stake (PoS) consensus mechanism using several other metaverse immersive devices as future work.**

***Index Terms*—Metaverse, Proof of Work (PoW), Proof of Stake (PoS), Urban Twins (UTs), cybercommunities, cybersecurity, cyberthreats, blockchain, Single Point of Failure (SPoF), Generative Adversarial Networks (GAN).**

I. Introduction

Numerous urban metaverse use cases have already been adopted by urban life to improve Quality of Life (QoL) by overcoming spatial and temporal constraints, and the trend suggests that this will accelerate exponentially in the years to come. Ensuring secure and reliable urban metaverse cyberspaces requires addressing two critical challenges, namely, cybersecurity and privacy protection. In the upcoming years, it is anticipated that cybercrime activities will be widespread in this ecosystem, which has trillions of dollars in economic value. The techniques under “Internet of Everything (IoE)” and Automation of Everything (AoE) [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 (Smart City (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 UTs.

The quality of resident experiences in the urban ecosystem is improved by the use of advanced infusion metaverse technologies (e.g., VR/AR headset, full haptic body suits, i.e. Motion Capture Suits (MoCaps)). The abilities of these devices can be instrumented to improve privacy and security when paired with additional technological innovations like Federated Learning (FL) and blockchain. In this paper, a blockchain-facilitated approach, which uses metaverse-immersive devices to generate Federated Security-Preserving Deep Learning (FSPDL) models, is designed. This design, by avoiding Single Point of Failure (SPoF) 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.

A. *URBAN METAVERSE & CYBERTHREATS*

Urban metaverse worlds/cyberspaces (i.e. Urban Metaverse-as-a-Services (UMaaSs)) – 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. More detailed information about urban metaverse cyberspaces can be reached in [9], [10], [11].

Cybersecurity threats against the metaverse as well as privacy concerns are analysed in [12], [13], [14], [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 cyberthreats that can be launched in urban cybercommunities are elaborated in [19] with possible countermeasures.

B. FEDERATED LEARNING & BLOCKCHAIN

FL, introduced by Google, has gained prominence as an effective solution for addressing data silos, enabling collaboration among multiple parties without sharing their data [20]. In FL, each entity trains its own data locally, and only the locally generated model itself is sent to the central server to aggregate all the models to form the final model for each entity to utilise. The concepts and applications of FL are analysed in [21]. From a technical standpoint, DL can be performed in a collaborative manner, where a parameter server is required to maintain the latest parameters available to all parties [22]. Although local data is not directly shared with FL, models trained on this data may also be spied on by malicious adversaries, semi-honest parties, or honest but curious parties, when local models are aggregated into a centre. Moreover, under the circumstance of knowing the local model, spies may adopt some attacks to restore the original data, which indirectly leads to information leakage [23].

Privacy-Preserving Machine Learning (PPML) or more specifically, Privacy-Preserving Deep Learning (PPDL) schemes have been developed and employed to further preserve sensible data and privacy while performing FL. Multiple distributed encrypted data points can be uploaded by their owners to a central server, collected by the platform, or processed data models using specific agreed-upon transparent DL training models, which are then later aggregated to establish the global model without sharing the data itself. The Homomorphic Encryption (HE) scheme allows data to be processed without needing to decrypt it. SEALion, CryptoNet [24], and CryptoDL are the early implementation examples (trained networks) of the PPDL scheme via encrypted outputs using HE. A PPDL system in which many learning participants perform NN-based DL over a combined dataset of all, without revealing the participants' local data to a central server is presented in [25] using asynchronous stochastic gradient descent, in combination with HE. An FL-enabled network data analytics function architecture with partial HE to secure ML model sharing with privacy-preserving mechanisms is proposed in [26]. A full HE scheme to the standard DNN, ResNet-20, is applied in [27] to implement PPML. A universal multi-modal vertical FL framework is proposed in [20] to effectively acquire cross-domain semantic features on homomorphic-encrypted data. FL mechanism is introduced into the deep learning of medical models in Internet of Things (IoT)-based healthcare system in [23] in which cryptographic primitives, including masks and HE, are applied for further protecting local models, so as to prevent the adversary from inferring private medical data by various attacks such as model reconstruction attack or model inversion attack or model inference attacks. Considering a specific application of Human Activity Recognition (HAR) across a variety of different devices from multiple individual users, the vertical FL scheme is developed to integrate shareable features from heterogeneous data across different devices into a full feature space, while the horizontal FL scheme is developed to effectively aggregate the encrypted local models among multiple individual users to achieve a high-quality global HAR model in [28], in which a computationally efficient scheme resembling HE is then improved and applied to support the parameter aggregation without giving access to it, which enables heterogeneous data sharing with privacy protection across different personal devices and multiple users in building a more precise personalised HAR model.

Urban metaverse cyberspaces should facilitate the exchange of information in a trusted way through the metaverse ecosystem built on decentralised blockchain technologies. Various studies, by merging blockchain technologies and FL, aims to address the shortcomings of FL such as Generative Adversarial Networks (GAN) attacks and SPoF. Blockchain, with its privacy-preserving mechanisms by verifying the training process securely, has been recently employed to enable the secure generation of FL 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 [29] 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) – a decentralized consensus 160-bit secure hash generation mechanism (SHA-1) – 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. [30] aim to address the threat from GAN attacks pose to collaborative deep learning and propose a model-preserving FL framework, called MP-CLF, which can effectively resist the GAN attack. An adversary detection-deactivation method for metaverse-oriented FL is proposed in [31] 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 [22].

A privacy-preserving two-party distributed algorithm of back-propagation which allows a neural network to be trained without requiring either party to reveal the individual data to the other is presented in [32].

Standard FL 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. However, in addition to the inefficiency of homomorphic-based encryption, the authenticity of local or global models cannot be guaranteed without the authentication of a trusted third party. But, every third party within the urban metaverse ecosystem is untrusted, concerning privacy in particular, considering semi-honest parties or honest but curious parties. Moreover, the locally or globally pre-trained gesture models can be replaced by cybercriminals with their recently trained models instantly, particularly when the credentials of a user are hijacked. 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-facilitated approach, which is elaborated in Section II, is proposed in this research. The proposed authentication and verification approach, the so-called BF-FSPDL, addresses those aforementioned concerns.

C. IMMERSIVE DEVICES AND BODY SIGNATURE

Authentication of residents and verifying their true identities without a third party or a central authority is imperative in developing private and secure urban metaverse cybercommunities. Regular identity checks are crucial to both address fake avatars or avatars that have been stolen via unauthorised access to user credentials and avoid their imminent adverse consequences – such as breach of privacy and loss of assets. Individual data that can be used for authentication is composed of i) biographic identification data such as name, surname, date of birth, and ii) biometric identification data as biological characteristics (DNA, facial features, height, fingerprints, iris features, vein features, and palm features) and behavioural/gesture patterns (facial expressions, movement patterns (gait), lip motion, emotion expression or reactions to interactions using physiological responses, voice pitch patterns/prints, and speech patterns). Automated Emotion Recognition (AER) and Automated Behaviour Recognition (ABR) technologies can detect humans' emotional/behavioural states in real time using facial expressions, voice attributes, text, body movements, and neurological signals and have a broad range of applications across many sectors [33]. 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 [34] for interested readers. The way of building DL gesture models should consider these privacy and ethical concerns as well as the regulatory framework. Humans, 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 regarding avatars [35] as well. Every action or transaction during the immersive interaction of individuals can be copied into the metaverse ecosystem. These consecutive actions or transactions generate particular patterns, in other words, a cyber identity of individuals, that differentiates them from other users. Within this context, 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 FL. The actions of residents can be profiled through their bodies, coupled with advanced multiple sensory technologies that are based on a variety of body signatures, while interacting with the metaverse ecosystem, particularly by using VR headsets and full haptic body suits, i.e. MoCaps, equipped with multi-sensory abilities enabling tactile sensation. Users immerse themselves with full-body haptic suits including finger and full-body tracking sets, by which every motion can be replicated in virtual worlds and the real world with a bidirectional haptic interaction (e.g. touch, and handshake in a virtual environment). A sequence of these motions can build our unique body features by extracting the patterns from users' gesture cues, which leads to patterns distinguishing us from the rest of the world. These patterns, i.e. the 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 Hand Tracking Toolkit (HTT)), different types of many other Wearable Sensors (WSs)), which are improving with larger sets of options and a diverse range of attributes. For instance, Wearable Resistive Sensors (WRSs) that could directly characterise joint movements are one of the most promising technologies for hand gesture recognition due to their easy integration, low cost, and simple signal acquisition [36].

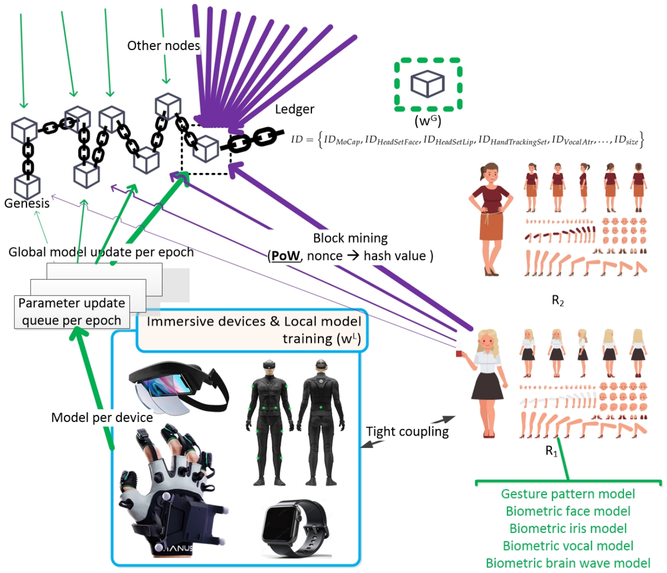
Other nodes
Ledger
(w^G)
$ID = \{ID_{MoCap}, ID_{HeadSetFace}, ID_{HeadSetLip}, ID_{HandTrackingSet}, ID_{VocalAtr}, \dots, ID_{size}\}$
Genesis
Global model update per epoch
Block mining
(PoW, nonce → hash value)
Parameter update
queue per epoch
Immersive devices & Local model
training (w^L)
Model per device
Tight coupling
R$_2$
R$_1$
Gesture pattern model
Biometric face model
Biometric iris model
Biometric vocal model
Biometric brain wave model

Fig. 1: User-based FSPDL model generation with immersive devices.[1]

II. Methodology

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 FL as expressed earlier in Section I-B. The FSPDL scheme, based on transparency and personal consent, is developed using the cyber gesture signature with wearable immersive devices to protect users' privacy and security 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 languages using tightly coupled immersive wearable metaverse devices as visualised in Fig. 1. 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 block 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. It is imperative to employ a technique to determine if adding the candidate blocks to the chain is appropriate or not. Only trustworthy blocks with updates are allowed to continue forward with the subsequent consensual block thanks to the distributed validation mechanism, i.e., the voting scheme in Alg.3 by avoiding GAN attacks and SPoF. To put it another way, Alg.3, enabling other nodes to reject altered data rapidly using hashes (i.e., signatures of data), combines the voting results with the corresponding local models and stores them in the successive consensual block if the voting consensus is higher than the predetermined threshold value (e.g. 50%) (i.e., $VotingPercentage > VotingThreshold$) based on the accumulated votes as shown in Alg.2. From a more technical standpoint, the gesture feature set for particular attributes, $F = \{A_1, A_2, \dots, A_{size}\}$, of resident entities, $R = \{R_1, R_2, \dots, R_{size}\}$, need to be trained per individual with an epoch sample size, $S = \{F_1, F_2, \dots, F_{epoch}\}$. 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

```
Data: System input: $ID_{MoCap}$.IP & $ID_{MoCap}$.Port & $meR$.ID
Data: Instant input: $F = \{A_1, A_2, \dots, A_{size}\}$ &
      $S = \{F_1, F_2, \dots, F_{epoch}\}$
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,
  $F = \{A_1, A_2, \dots, A_{size}\}$;
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
          $S = \{F_1, F_2, \dots, F_{epoch}\}$;
        [$\alpha_{iteration}, w_{iteration}$] = 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 $=\{ID_{MoCap}, ID_{HeadSetFace}, ID_{HeadSetLip}, ID_{HandTrackingSet}, \dots, ID_{size}\}$.

[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.

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

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

where malicious devices connected to illegitimate models are not included.

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

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

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

Residents in the cybercommunities, 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. 1), 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 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. In order for users in metaverse cyberspaces to mine blocks and confirm each other's

```
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 4: Proof of identity using blockchain-facilitated FSPDL pre-trained models with immersive devices where $ID = ID_{MoCap}$.

legitimacy as block miners, the authentication method that this research proposes requires their cooperation. Users can be incentivized to participate in block mining activities by earning specific cryptocurrencies allotted to metaverse cyberspaces. 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 UMaaSs. 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. 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. The original user data is retained with the data owner as in FL 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, which aims to preserve both the data's sovereignty – and privacy, to a certain extent. Updated gradients may reveal individual private or actual information when associated with data attributes and structures. Therefore, encryption mechanisms provide further privacy protection even though the updated gradients or communicated packets have been anonymised. The above operations are repeated for all ID using different blockchain forms.

Global gesture models, which are verified by other residents in UMaaSs and employ a PoW consensus mechanism, are deployed to be used for authentication mechanisms as proof, which has been implemented in Algorithm 4, 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 SPoF regarding the training in a central server as in FL 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, $S = \{F_1, F_2, \ldots, F_k\}$.

TABLE I: Parameters in Bi-LSTM-RNN [37].

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

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 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 person.

III. EXPERIMENTAL SETTINGS

The experiment was designed to test a cybercommunity environment with 30 independent nodes in a co-simulated environment. 2 users with MoCaps, indicating 2 nodes (Node-A and Node-B) were incorporated into the co-simulation. Miners were rewarded with 20 cybercommunity crypto coins for each mined block. 2 powerful laptops (processor: 13th Gen Intel(R) Core(TM) i9-13950HX, 2.20 GHz; RAM: 32 GB; cores: 24) were used by Node-A and Node-B and 1 workstation (processor: Intel Xeon Platinum 8280; RAM: 2.70 GHz; RAM: 128 GB; cores: 28; boosted: NVIDIA RTX 8000) server was employed to simulate the remaining 28 nodes in the co-simulated environment. Each simulated node was assigned to one of the cores of the workstation as an individual device. The nodes first trained their local models and then the global models as explained in Section II. The process ended when the gesture models of Node-A and Node-B converged to a solution where the gesture training accuracies were over 0.95. The gesture models for other simulated nodes were not trained for mined blocks while they were mining. The training was conducted using Bidirectional Long Short-Term Memory Recurrent Neural Networks (Bi-LSTM-RNN) with the parameters presented in Table I.

IV. RESULTS

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

V. DISCUSSION AND CONCLUSION

The metaverse cybercommunities, using decentralised data structures on private and public ledgers and interoperability architecture, may not be managed by a single entity, which makes it more difficult to track down and stop attackers. Adverse events need to be detected in real time proactively to avoid dire circumstances such as losing individual data, NFTs, virtual real estate, cryptocurrency, or a breach of privacy on the blockchain in which traceability of transactions and actions is difficult to follow, due to the nature of the blockchain ecosystem with a high level of data sovereignty and privacy. Our research question was if we can turn the abilities of immersive metaverse devices into the residents' advantage in providing their security and avoiding a breach of privacy. In a broader perspective, if it is possible to build a trustworthy, urban metaverse cybercommunity, without requiring a centralised authority/government to protect our privacy or a third party to mediate between entities, e.g. for a transaction. FL provides the opportunity to protect user privacy and data sovereignty while leveraging the combined intelligence of several dispersed nodes. However, FL, requiring a third trusted body, suffers from GAN attacks and SPoF concerning the central aggregator server, which not only may put the entire process of thorough learning at risk, but also, may jeopardise the timely and trustworthy authentication and verification. This research designs a novel blockchain-facilitated FSPDL (BF-FSPDL) 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) obtained from immersive metaverse wearable devices (e.g. VR/AR headset, MoCaps, haptics gloves, HTT). In this way, cyber signature models (Section I-C), with a diverse range of attributes, can be built step by step, verified by other residents and placed in blockchain ledgers to be deployed whenever needed to verify the authenticity of the residents/avatars even if all the credentials are in the hands of cybercriminals.

This research mainly focuses on mitigating the cyberthreats of “credentials theft” , “identity falsification & impersonation”, “Identity theft”, and “Avatar theft”. The preliminary results prove the viability of employing the proposed approaches in realising the objectives in this report. More explicitly, the results suggest that the approaches can prevent impersonation, identity theft, and theft of credentials or avatars promptly before any transactions have been executed. The proposed system will be tested with a larger number of nodes involving Proof of Stake (PoS) consensus mechanism using several other metaverse immersive devices.

VI. Limitations

A limited number of nodes (i.e., 30) were included in the experiments due to the limited computing resources and the computational difficulties of PoW. A network of devices must expend considerable computing power to perform the PoW consensus mechanism in the blockchain. Large amounts of energy are needed for PoW at scale as more miners/nodes join the network with expanding computing resources. The use of PoS consensus mechanism can compensate for such shortcomings. Therefore, we would like to test our system using this mechanism with several other metaverse immersive devices in our future studies and compare the results obtained from the implementations of PoW and PoS with a larger number of nodes in our further papers.

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] 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.

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

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

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

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

[14] 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.

[15] 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.

[16] K. Kuru, "Technical report: Big data - concepts, infrastructure, analytics, challenges and solutions," 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] M. Gong, Y. Zhang, Y. Gao, A. K. Qin, Y. Wu, S. Wang, and Y. Zhang, "A multi-modal vertical federated learning framework based on homomorphic encryption," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1826–1839, 2024.

[21] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, jan 2019.

[22] 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.

[23] L. Zhang, J. Xu, P. Vijayakumar, P. K. Sharma, and U. Ghosh, "Homomorphic encryption-based privacy-preserving federated learning in iot-enabled healthcare system," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2864–2880, 2023.

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

[25] L. T. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, "Privacy-preserving deep learning via additively homomorphic encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1333–1345, 2018.

[26] C. Zhou and N. Ansari, "Securing federated learning enabled nwdaf architecture with partial homomorphic encryption," *IEEE Networking Letters*, vol. 5, no. 4, pp. 299–303, 2023.

[27] J.-W. Lee, H. Kang, Y. Lee, W. Choi, J. Eom, M. Deryabin, E. Lee, J. Lee, D. Yoo, Y.-S. Kim, and J.-S. No, "Privacy-preserving machine learning with fully homomorphic encryption for deep neural network," *IEEE Access*, vol. 10, pp. 30 039–30 054, 2022.

[28] X. Zhou, W. Liang, J. Ma, Z. Yan, and K. I.-K. Wang, "2d federated learning for personalized human activity recognition in cyber-physical-social systems," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 6, pp. 3934–3944, 2022.

[29] 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.

[30] 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.

[31] 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.

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

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

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

[39] ——, "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.

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

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

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

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

[44] ——, "Sensors and sensor fusion for decision making in autonomous driving and vehicles," 2023.

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

[46] ——, "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.

[47] ——, "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.

[48] ——, "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.

[49] 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.

[50] K. Kuru, "Blockchain-enabled decentralized, secure and reliable voting through biometric identification using metaverse immersive devices and deep learning," 2025.

[51] ——, "Swarms of autonomous drones in logistics within smart city: Opportunities, challenges and future directions," 2025.

[52] ——, "6g in developing high-fidelity immersive digital twins," 2025.

[53] ——, "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.

[54] ——, "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.

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

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

[57] 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.

[58] ——, "Urban metaverse cyberthreats and countermeasures against these threats," in *2024 6th International Conference on Blockchain Computing and Applications (BCCA)*, 2024, pp. 228–235.

[59] ——, "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.

[60] ——, "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.

[61] 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.

[62] ——, "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.

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