Peer-to-Peer Networking and Applications (2025) 18:210
https://doi.org/10.1007/s12083-025-02020-w

Blockchain-based decentralized identifier in metaverse environment for secure and privacy-preserving authentication with improved key management and cryptosystem

Vijitha S[1] · **Anandan R**[1]

Received: 5 April 2024 / Accepted: 13 May 2025

Abstract
The metaverse is gaining popularity because it offers a virtual environment with social interactions that are similar to those in the real world. Because of this heightened attention, protecting privacy and security is becoming more and more crucial. Users can create a variety of avatars in the metaverse, which presents internal security issues if misused and leads to deceptive or dangerous behavior. Metaverse in e-learning platforms becomes an interesting aspect in the current scenario. However, users trying access to the metaverse are exposed to a number of external security threats because they interact with service providers through open channels. To overcome this issue, a novel privacy-preserving and secure authentication protocol using Improved Light Weight key management-based CryptoSystem (ILWKM-CS) is proposed. The proposed ILWKM-CS scheme for privacy-preserving and secure authentication comprises four distinct phases: User setup, User Registration, Login, and Avatar authentication. In the User setup phase, individuals establish their Decentralized Identifiers (DID), and a verifiable credential is issued by the central authority as evidence of the personal data of the user. The next step is user registration, where users create an avatar in the virtual space and register using their DID. Using the ILWKM system, the user and the service provider authenticate each other during the login phase. Lastly, avatars interact with other avatars within the virtual environment and authentication is ensured between them using the MECC technique in the Avatar authentication phase. Moreover, the optimal key is generated to encrypt the message via the proposed hybrid optimization TSAOO algorithm.

Keywords Metaverse · ILWKM · MECC · TSAOO algorithm · And Avatars

1 Introduction

The concept of the"Metaverse"was first used in"Snow Crash,"a work of science fiction written by Neal Stephenson in 1992. It combines the prefix"meta,"which denotes the “virtual” and “transcendent”, with"universe,"symbolizing space and world [1]. Within a Metaverse, people can utilize smart devices, such as earphones and goggles to explore various virtual realms and engage in a multitude of remote and virtual activities, including travel, education, and commerce, all by taking on the persona of avatars [2, 3]. Similar to this, a Metaverse platform is a completely immersive 3D virtual reality environment where users can communicate with one another, conduct business, and take part in cultural events by taking on the roles of avatars. Metaverse environments offer a higher level of immersion compared to current online settings and are anticipated to witness widespread adoption [4, 5]. Numerous platforms, like Roblox, Minecraft, and Fortnite have surfaced as metaverse environments have grown in popularity, providing virtual reality experiences made possible by avatars. Furthermore, a variety of devices like HTC VIVE and Oculus Quest, harnessing XR, VR, and AR technologies, are integrated into metaverse platforms to deliver lifelike services, utilizing physical user data such as gaze and motion information [6, 7].

Although metaverse environments provide a number of enticing features, there are a number of important issues that must be resolved. Within these environments, user-platform server communication takes place through public channels, which leaves them vulnerable to potential security risks like

✉ Vijitha S
vijithas.se@vistas.ac.in

Anandan R
anandan.se@vistas.ac.in

[1] Department of Computer Science and Engineering, Vels Institute of Science, Technology & Advanced Studies, Velan Nagar, P.V. Vaithiyalingam Road, Pallavaram, Chennai, 600117 Tamil Nadu, India

Published online: 12 June 2025

message manipulation, communication interference, and security breaches such as impersonation and MITM attacks [8, 9]. Additionally, in order to access their particular services, users need to complete the process of registration with each platform server. This can be burdensome for users, as they must repeatedly supply personal information like personal data, passwords, and usernames every time they sign up with a new platform server [10, 11]. Furthermore, each platform server's security procedures determine the confidentiality and authenticity of user data, especially passwords and IDs. However, it is permissible for bad actors to make false avatars in order to trick people in virtual environments. However, avatars cannot verify the authenticity of other avatars, posing significant risks such as identity exposure, theft, and fraudulent activities related to virtual assets during avatar interactions [12, 13].

In order to resolve these problems, users and platform servers must develop secure communication channels. Avatar authentication is crucial for ensuring the security of avatar interactions, particularly during activities like trading and chatting within virtual spaces [12]. Additionally, a private and transparent approach to user-identifying data management is needed. Model inversion assaults are a phenomenon whereby recent techniques demonstrate the capacity to retrieve and recreate information obtained from pre-trained model weights [6, 9]. This kind of sensitive information exposure, along with the category or outcome (prognosis) that goes along with it, presents a serious risk to the field of privacy-preserving machine learning. This information can be potentially misused by malicious individuals to cause real-world harm or to craft powerful adversarial attacks [5]. Hence, the development of privacy-preserving machine learning models is imperative, not only to address data leakage but also to safeguard against these risks [9]. This research suggests a new privacy-preserving and secure authentication protocol using the ILWKM-CS scheme. The major contribution of this work is as follows:

- Proposing ILWKM approach for encrypting the data in the login phase, in which the user's message is encrypted with the secret key that is acquired from MECC and the service providers' message is encrypted by using a session key which is created by a modified chaotic map.
- Proposing MECC in the phase of Avatar authentication, in which the avatar can interact with other avatars by encrypting the message through a private key. Moreover, the TSAOO method is contributed to generate the optimal key, which encrypts the avatars' message in the Avatar authentication phase.

The remaining structure of this manuscript is organized as follows: Sect. 2 reviews the body of research on secure authentication protocols and privacy protection. The proposed work is described in Sect. 3. The assessment of various measures is demonstrated in Sect. 4 and the proposed work is summarized in Sect. 5.

2 Literature review

In 2023, Myeonghyun Kim et al. [13] has introduced a novel authentication system that leverages blockchain technology, verifiable credentials and decentralized identifiers to facilitate secure identity verification and authentication for users in the metaverse. This creative method solves privacy issues with the handling of personal information by guaranteeing that users can authenticate themselves without disclosing private information to service providers. Through thorough security assessments that include BAN logic, the ROR model, and AVISPA simulation it has been demonstrated that the suggested system is resistant to malevolent security attacks and protects privacy.

In 2022, Jongseok Ryu et al. [14] has created a system model aiming to achieve both secure communication and the transparent management of user identification data within metaverse environments, employing blockchain technology for these objectives. Furthermore, they implemented a mutual authentication method that ensures safe interactions between avatars by establishing secured channels of communication among users and platform servers using biometric information and ECC. This study carried out a comprehensive investigation, incorporating BAN logic, ROR model, AVISPA, and informal security assessments, to verify the integrity of this mutual authentication technique.

In 2023, Minghui Xu et al. [15] has introduced an innovative trustless framework for a blockchain-powered metaverse, with the primary goal of enhancing resource integration and allocation efficiency through the consolidation of both hardware and software elements. They present an OTCE technique based on localized trust assessment in order to achieve their design objectives. In this approach, the metaverse is represented by a hypergraph, with discrete hyperedges connecting different user groups with well defined relationships. The usage of graph analytics techniques can then be used to determine the degree of trust for each user group. Each group can independently develop its own security plan as needed by utilizing these trust values, free from interference from unrelated nodes.

In 2022, Kedi Yang et al. [16] had suggested a dual-factor authentication framework that integrates chameleon signatures with biometric-based authentication. Their method tackles two major issues: impersonation in the real world and disguise in the virtual world. The author offers a chameleon collision signature technique as a solution to the problem of virtual identity verification. They create an identity model which incorporates the chameleon key and the player's biometric template in order to verify the avatar's

real-world identity. In order to ensure that the avatar's virtual and physical identities are consistent, they have also created two decentralized protocols for authentication based on the avatar's identity model. A security study has been conducted to demonstrate how well this authentication approach preserves the reliability and traceability of the avatar's identity.

In 2023, Vu Tuan Truong and Long Bao Le [17] have introduced MetaCIDS, a groundbreaking CID framework that utilizes metaverse devices to collectively safeguard the metaverse environment. An FL system that combines a supervised classifier with attention approaches and unsupervised autoencoders within the MetaCIDS framework allows Metaverse users to train a CID model with their local network data. Using network flows produced by tracking local network traffic, the blockchain network simultaneously makes it easier to train a machine learning algorithm for intrusion detection. Users can then receive metaverse tokens by reporting validated intrusion notifications to the blockchain. Security analysis shows that MetaCIDS successfully identifies zero-day attacks and that the training process is impervious to data manipulation, SPoF, and up to 33% of hostile nodes.

In 2023, Sunder Ali Khowaja et al. [18] has introduced a novel approach called GASCNN tailored for medical image processing, which exhibited robustness against both data and class leakage attacks. In the first step, mappings of features from residual networks were used to create synthetic medical images using GANs. After that, they secured the model weights using spike learning techniques and transformed ResNet into an SNN using a transformation methodology. Rebuilding model weights became much more difficult as a result of this encryption procedure, which involved converting spatial domain data into the temporal axis.

In 2023, Hung Duy Le et al. [19] has introduced MetaCrowd, a framework for ML crowdsourcing based on blockchain technology to address the issues mentioned and ensure that ML becomes accessible to all metaverse users and service providers. Unlike traditional crowdsourcing systems that depend on centralized authorities, MetaCrowd operates in a decentralized and automated manner by leveraging blockchain-based technology and smart contracts. This decentralized strategy successfully allays worries about trust and single points of failure.

In 2023, Yongjun Ren et al. [20] has introduced an innovative cross-chain transaction scheme known as HCNCT, which builds upon an enhanced hash timelock mechanism. This strategy includes a notary system, in which a team of notaries actively monitors and takes part in cross-chain transactions. It successfully resolves the problem that arises with conventional hash timelock techniques when malevolent users try to jam the transaction route by generating a large number of timed-out transactions. Moreover, the inclusion of verifiable secret sharing within the notary group serves to address the centralization issue commonly linked to notary mechanisms. Additionally, the author provided a comprehensive explanation of the cross-chain transaction, key processing, and transaction verification procedures within the system. They have also developed a mechanism for evaluating user credibility, effectively reducing the incidence of malicious user defaults.

In 2024, Jungwon Seo, & Sooyong Park, [21] has framed the SBAC approach against probable security attacks. To fully assess the efficacy associated with the recommended technique, a number of exact performance trials were conducted. The results showed that the suggested approach performed faster at encrypting data than asymmetric key techniques. Furthermore, the suggested approach outperformed the symmetric and asymmetric key methods in terms of decryption speed. The outcomes of the performance evaluations and security analysis demonstrated the usefulness and effectiveness of the recommended strategy, establishing it as a viable option for quickly and securely handling data in the metaverse setting.

2.1 Problem statement

The problem statement for an authentication scheme in a metaverse environment (as per Table 1) revolves around the need to securely verify the identities of users as they interact and transact within the immersive digital world of the metaverse [19]. In this complex and multifaceted environment, where individuals may engage in various activities, from social interactions to financial transactions, there is a crucial requirement to establish trust and protect user data and assets [14]. The challenge lies in designing an authentication system that not only ensures robust security but also accommodates the unique characteristics of the metaverse, such as the seamless transition between physical and virtual spaces, diverse user avatars, and a potentially vast and dynamic user base [13, 16]. Furthermore, striking the right balance between user convenience and security is a critical aspect of the problem, as overly burdensome authentication processes can hinder the user experience, while weak security measures can lead to fraud and privacy breaches [15, 17]. Therefore, the problem statement must address the development of an authentication scheme that is tailored to the metaverse environment, ensuring both the safety of user interactions and a smooth, user-friendly experience [18, 20].

3 An outline of privacy-preserving and secure authentication using ILWKM-CS scheme in e-learning platform

3.1 System model

The metaverse can make better eLearning by providing more customized, immersive and interactive ways to

Table 1 Features and Challenges of Previous Studies

Author [Citation]	Methodology	Features	Challenges
Myeonghyun Kim et al. [13]	Secure Authentication scheme	The costs of computation and communication were significantly reduced	There are several obstacles in investigating authentication procedures for ensuring a safe and dependable metaverse environment, mostly because of the potential security threats within the blockchain
Jongseok Ryu et al. [14]	ECC	The suggested method offers a wider range of security features at lower computation and communication costs	It becomes less scalable when dealing with a large user base
Minghui Xu et al. [15]	OTCE	It enables large and flexible application environments, also known as"sandboxes,"while providing strong security assurances	It can be difficult to strike a balance between the demand for low-latency interactions and security
Kedi Yang et al. [16]	Two-factor authentication	Time consumption was reduced	It can be difficult to ensure both cost and accessibility for a large user base
Vu Tuan Truong And Long Bao Le [17]	MetaCIDS	Accuracy, Recall and Precision were maximized	The IDS model's performance has to be improved
Sunder Ali Khowaja et al. [18]	GASCNN	A higher F1 score was obtained	One drawback to be mindful of is that the GAN requires retraining if data associated with a particular application is changed
Hung Duy Le et al. [19]	MetaCrowd	It was cost-efficient	Failures in authentication or the assignment of machine-learning tasks can negatively impact the user experience, as real-time interactions are crucial
Yongjun Ren et al. [20]	HCNCT	The time needed to finish was reduced	Need to enhance the efficiency of the model
Jungwon Seo, & Sooyong Park, [21]	AES	It accomplished better memory consumption and elapsed time	Exploring data compression approaches is difficult for proficient blockchain storage

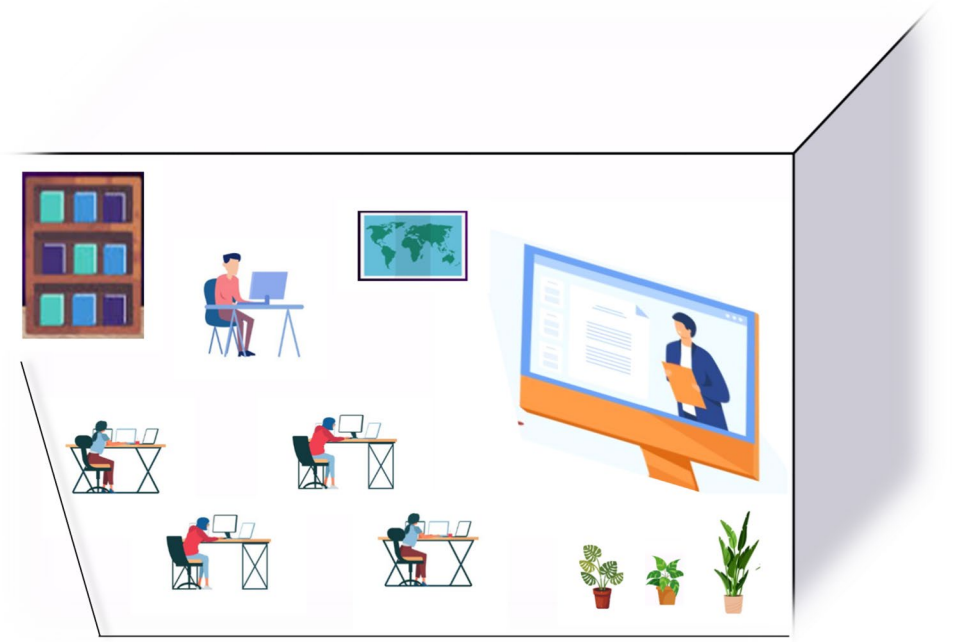

Fig. 1 Metaverse in eLearning environment

learn. The major impact of the metaverse on eLearning is enhanced immersive learning experiences and improved interactivity and accessibility. People can move into a virtual world in the metaverse and have the potential to interact with other people within the virtual space. This makes learning more memorable and fun. Moreover, the users can access their virtual learning platform from anywhere through an internet connection. This allows people who live in remote areas or people with disabilities can get an education. More specifically, a virtual classroom-based use case is used in this work. Learning is more immersive and hands-on in virtual classrooms in the metaverse than in extant online classrooms. Users take part in real-time discussions, can interact with other users and can attend virtual lectures in virtual classrooms. However, when using the blockchain-based DID and VCS. An increasing number of users and transactions leads to congestion and delays in DID verification. Also, handling the network partitioning and downtime leads to inconsistent data and service disruptions. To address this issue, a secure and privacy-preserving authentication is proposed. This offers an engaging and dynamic learning experience. Figure 1 illustrates the metaverse in the eLearning environment. The process of authentication followed under the scenario is illustrated in Fig. 2.

As illustrated in Fig. 2, a Decentralized identifier (DID) in the metaverse platform for privacy-preserving and secure authentication approach involves four steps: User, Certificate authority C_A, Blockchain and Service provider S_P. The elucidation of each entity is given below:

User: Users generate DIDs in the blockchain and send them in C_A, together with personal data for verifiable credentials. The user then registers with S_P in order to participate in the Metaverse platform. Minimal information is transmitted during registration with S_P, and no additional personal data is shared. Users within a virtual environment can communicate with one another and share information by using the generated avatars. The use of public keys, DID, and verifiable credentials provides secure communication among avatars is achieved through.

Certificate authority C_A: C_A functions as a highly trustworthy entity responsible for initializing and disseminating system parameters. Users provide it with their DIDs and personal information, and it verifies both. Subsequently, C_A issues credentials to users, giving proof of their personal details such as age and occupation. Authentication of credential values is essential for interactions among avatars or users in the metaverse platform.

Blockchain: The authentication scheme employs a public blockchain that is a fully decentralized framework where any node can enter a blockchain without a trusted authority. Every member of the blockchain has the ability to read the ledger and contribute transactions. To ensure consensus on a single source of truth, the public blockchain makes use of evidence-based consensus algorithms like as proof of work (PoW) and proof of stake (PoS). Only information pertaining to authentication, specifically DID papers, is stored on the blockchain in this system. The assumption is made that the blockchain's consensus process operates correctly and reliably in the proposed scheme.

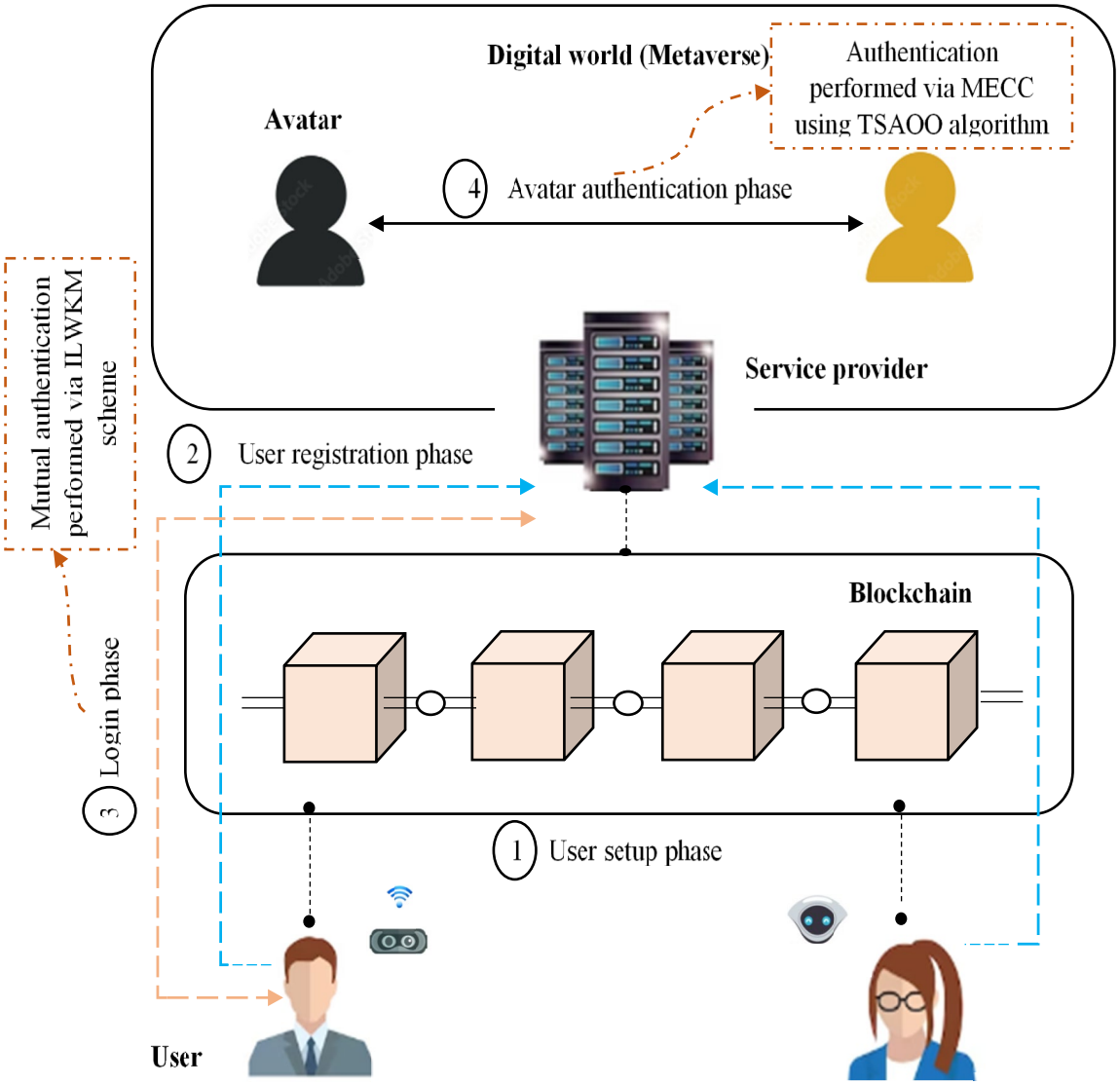

Fig. 2 Proposed system model

Service provider: S_P offer services that let users do a variety of things in virtual environments, such as gaming, learning, and medical care. Users register with S_P using DIDs, and S_P verifies user identity when access is attempted. Additionally, during the avatar authentication phase, S_P manages the forwarding of requests as well as response messages within its virtual space.

The proposed privacy-preserving and secure authentication using the ILWKM-CS scheme is comprised of four phases: User setup phase, User registration phase, Login phase and Avatar authentication phase. The flow of the suggested process is elucidated as follows:

User setup phase: During this phase, the user creates their DID. Further, C_A issues a verifiable credential to the user, serving as proof of the personal data of the users.
User registration phase: The user proceeds to register S_P using their DID. Then SP validates the user's DID, after which the avatar of the user is created within the virtual platform.
Login phase: When the user tries to access the S_P, the mutual authentication is used by both S_P and the user. When mutual authentication is completed successfully using the ILWKM mechanism, a session key is agreed upon, creating a secure channel of communication between the user and S_P.

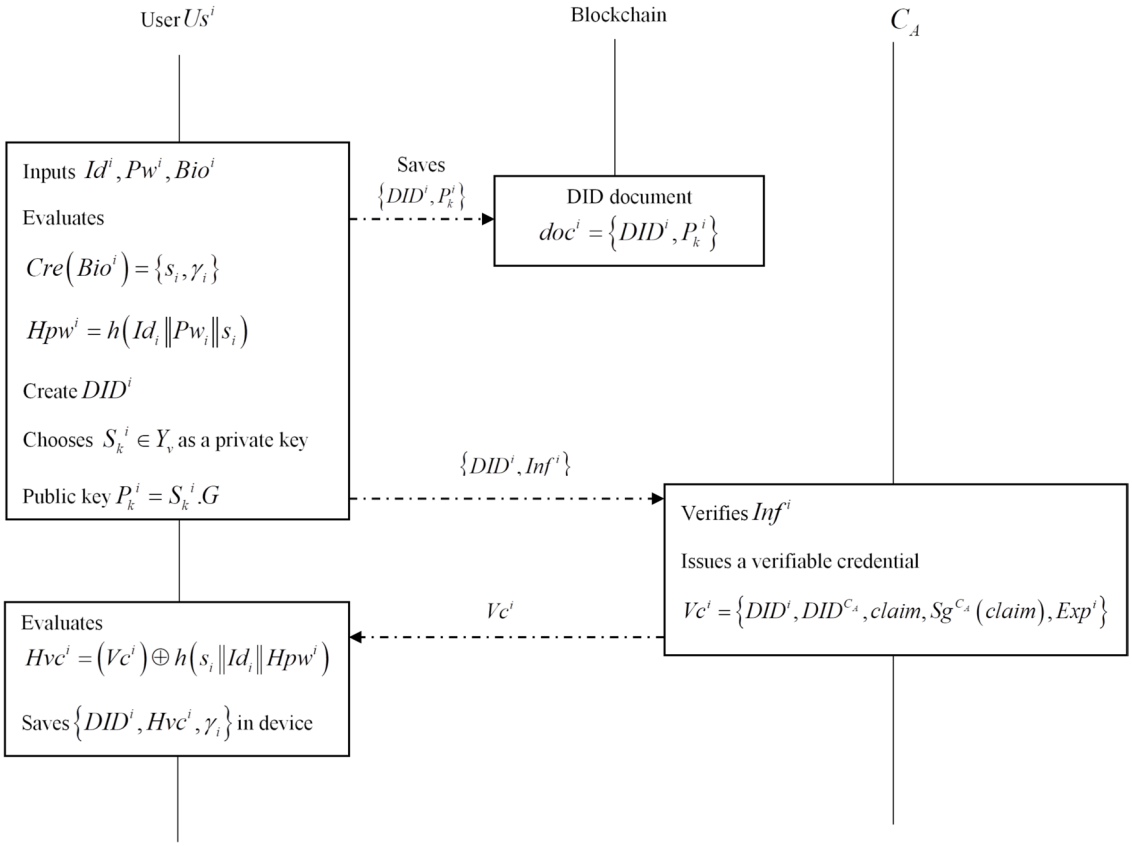

Fig. 3 Process of user setup phase

Avatar authentication phase: Within the virtual environment, the user engages with other avatars. To ensure secure interactions between avatars, the user presents verifiable credentials, demonstrating the necessary personal information for the avatar authentication process.

3.2 Initialization phase

The system variables are initialized first by C_A. For initialization, C_A creates huge prime numbers u,v, a generator G, an additive group A_G, an elliptic curve E_{C_u} over Q_u, a secret key $S_k^{C_A}$ and one-way hash functions H_f as well as it evaluates a public key $P_k^{C_A}$. Following this, C_A issues the parameters of the system as $Pmt = \{u, v, A_G, E_{C_u}, G, P_k^{C_A}, h_f(.)\}$ to the network.

3.3 User setup

The user starts the procedure by creating their own DID. Following this, C_A generates a verifiable credential for the user, serving as proof of the user's Inf^i. Over a secure link, this entire process takes place. Figure 3 shows the procedure for the user setup phase.

The steps to be involved in the user setup phase are as follows:

Step 1: User Us^i (i^{th} user) provides a password S_k^j, a unique Id^j and biometric data Bio^i. Further, Us^i choose an arbitrary number $S_k^i \in Y_v$ as a private key as well as evaluate $P_k^i = S_k^i.G, Hpw^i = h(Id_i \| Pw_i \| s_i)$, and $Cre(Bio^i) = \{s_i, \gamma_i\}$. Subsequently, Us^i creates Us^i's own DID^i, which represents the position of DID document as $doc^i = \{DID^i, P_k^i\}$ on the blockchain.

Step 2: Us^i demands C_A to generate a credential by providing DID^i along with personal information Inf^i. C_A validates a Us^i's Inf^i and DID^i as well as provides a verifiable credential $Vc^i = \{DID^i, DID^{C_A}, claim, Sg^{C_A}(claim), Exp^i\}$, which assures for Us^i's Inf^i including, age, occupation, and so on. Further, C_A transmits Vc^i to Us^i. Once Vc^i confirms, Us^i evaluates $Hvc^i = (Vc^i) \oplus h(s_i \| Id_i \| Hpw^i)$ as well as saves $\{DID^i, Hvc^i, \gamma_i\}$ in the equipment.

3.4 User registration phase

The user Us^i registers with S_P utilizing the user's DID.S_P validates the legitimacy of the user's DID and subsequently

generates the avatar of a user in a virtual platform. The user registration process is depicted in Fig. 4, and the entire phase is carried out via a secure channel. The following are the steps to participate in the user registering phase:

Step 1: User Us^i (i^{th} user) provides a password Pw_i, a unique Id^i and traces biometric information Bio^i. Further, Us^i evaluates $Hpw^i = h(Id_i \| Pw_i \| s_i), \{s_i\} = Rep(Bio^i, \gamma_i)$, $b^i = h(S_k^i, P_k^{S_P})$, $Reg^i = h(DID^i \| Hpw^i \| b^i)$ and transmits $\{DID^i, Hpw^i, Reg_i\}$ to S_P.

Step 2: S_P validates the validity of DID^i as well as extracts P_k^i from the blockchain. If it is justified, S_P evaluates $Reg^{i\prime} \stackrel{?}{=} h(DID^i \| Hpw^i \| b^i)$, $b^i = h(S_k^{S_P}.P_k^i)$ and checks $Reg^i = Reg^{i\prime}$. If it is valid, S_P chooses an arbitrary nonce $d_i \in Y_v$ as well as evaluate $Rid^i = h(DID^i \| Hpw^i \| S_k^{S_P})$, $J_i = h(d_i \| Rid^i \| S_k^{S_P})$. Following this, S_P delivers $\{Rid^i, J_i\}$ to Us^i and saves in the database securely as $\{Rid^i, DID^i, J_i\}$.

Step 3: Us^i evaluates $HRid^i = Rid^i \oplus h(Id_i \| Hpw_i \| s_i)$, $L_i = h(Rid^i \| J_i \| s_i \| Hpw_i)$, $HJ_i = J_i \oplus h(Hpw_i \| s_i \| Id_i)$ as well as saves $\{HRid^i, HJ_i, L_i\}$.

3.5 Login phase

During the user's Us^i attempt to access the S_P, a mutual authentication protocol takes place among the S_P and user. Secure communication between the user and S_P, the system is guaranteed after mutual authentication is successful and a session key is established. The login phase is depicted in Fig. 5, wherein, Us^i sends the message to S_P that can be encrypted using the public key and private key ($\chi \varphi_k$) of the MECC approach. Further, S_P decrypts it and transmits another encrypted message to Us^i. The message is encrypted by using a session key Ses_K that can be generated by a modified chaotic map in the ILWKM scheme. The elucidation of ILWKM is given below and the description of the MECC approach is given in the next section. The steps to be involved in the login phase are as follows:

Step 1: User Us^i inputs Id_i, Pw_i and Bio^i. Further, Us^i evaluates $\{s_i\} = Rep(Bio^i, \gamma_i)$, $Rid^{i\prime} = HRid^i \oplus h(Id_i \| Hpw_i \| s_i)$, $Hpw_i = h(Id_i \| Pw_i \| s_i)$, $J_i' = HJ_i \oplus h(Hpw_i \| s_i \| Id_i)$, $Vc^i = Hvc^i \oplus h(s_i \| Id_i \| Hpw^i), L_i\prime = h(Rid^i \| J_i\prime \| s_i \| Hpw_i)$

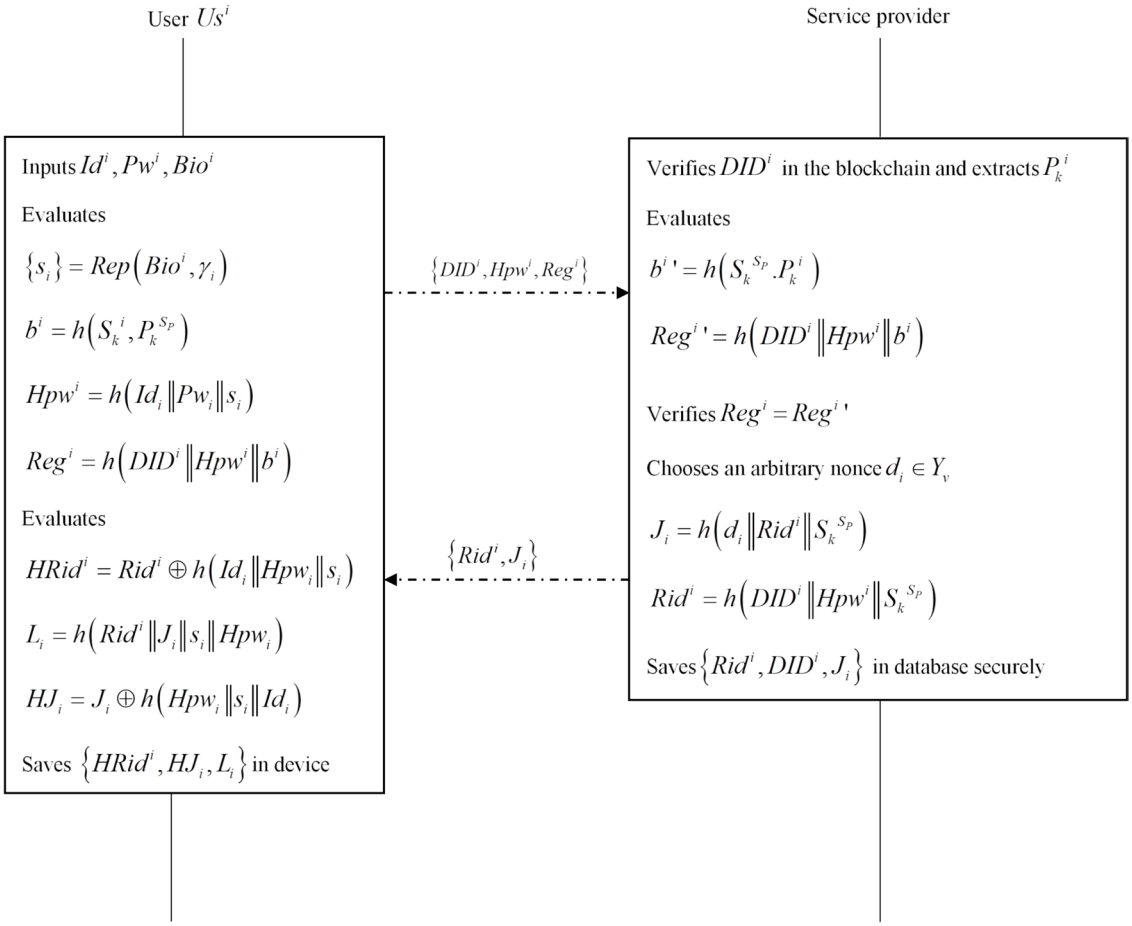

Fig. 4 Process of the phase of user registration

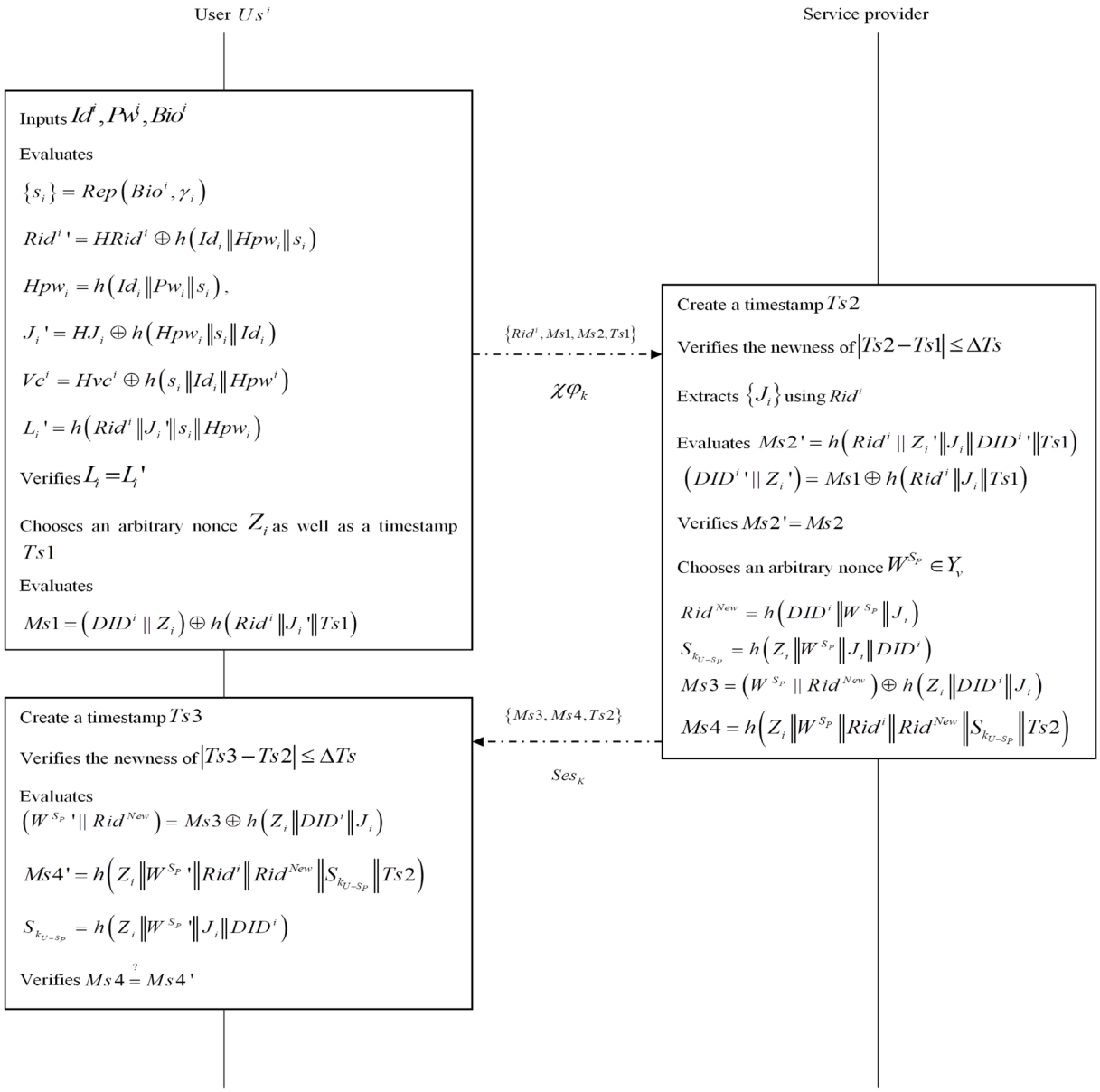

Fig. 5 Proposed scheme of Login phase

as well as verifies $L_i = L_i\prime$. If it is valid, Us^i chooses an arbitrary nonce Z_i with a present timestamp $Ts1$ and evaluate $Ms1 = (DID^i \| Z_i) \oplus h\left(Rid^i \| J_i' \| Ts1\right)$, $Ms2 = h(Rid^i \| Z_i \| J_i\prime \| DID^i \| Ts1)$. Following this, Us^i transmits $\{Rid^i, Ms1, Ms2, Ts1\}$, along with $\chi\varphi_k$ to S_P.

Step 2: S_P creates a present timestamp $Ts2$ and verify the newness of the timestamp. Further, S_P extracts $\{J_i\}$ from the database through Rid^i as well as evaluate $Ms2\prime = h(Rid^i \| Z_i\prime \| J_i \| DID^i\prime \| Ts1)$, $(DID^i\prime \| Z_i) = Ms1 \oplus h(Rid^i \| J_i \| Ts1)$. Then S_P validates the $Ms2\prime \stackrel{?}{=} Ms2$ and chooses an arbitrary nonce $W^{S_P} \in Y_v$ as well as evaluates $Rid^{New} = h(DID^i \| W^{S_P} \| J_i)$, $S_{k_{U-S_P}} = h(Z_i \| W^{S_P} \| J_i \| DID^i)$, $Ms3 = \left(W^{S_P} \| Rid^{New}\right) \oplus h\left(Z_i \| DID^i \| J_i\right)$, $Ms4 = h(Z_i \| W^{S_P} \| Rid^i \| Rid^{New} \| S_{k_{U-S_P}} \| Ts2)$. Following this, S_P sends $\{Ms3, Ms4, Ts2\}$ along with Ses_K to Us^i.

Step 3: Once the message received, Us^i decrypts the message using Ses_K and validate the newness of $Ts2$ as well as evaluates $\left(W^{S_P'} \| Rid^{New}\right) = Ms3 \oplus h\left(Z_i \| DID^i \| J_i\right)$, $Ms4\prime = h(Z_i \,||\, W^{S_P'} \,||\, Rid^i \,||\, Rid^{New} \,||\, S_{k_{U-S_P}} \,||\, Ts2)$, $S_{k_{U-S_P}} = h(Z_i \,||\, W^{S_P'} \,||\, J_i \,||\, DID^i)$. Further, Us^i validates the validity of $Ms4 \stackrel{?}{=} Ms4\prime$, and evaluates $HRid^{i\prime} = Rid^{New} \oplus h\left(Id_i \| Hpw_i \| s_i\right)$ as well as updates $HRid^i$ with $HRid^{i\prime}$.

3.5.1 ILWKM scheme for authentication between Us^i and S_P

Improved Light Weight Key Management [22] is the design of cryptographic key management systems that employ two phases in key management including establishing a symmetric encryption key and session key creation. Compared to the authentication schemes, the ILWKM minimizes the time required for key generation for fast authentication. It is highly scalable and handles a large number of user interactions. Combining the DID with the lightweight cryptography that user data remains secure while maintaining privacy and control. Here, the symmetric encryption is considered to be the MECC key to encrypt the message sent from Us^i to S_P.

Following message encryption, it will use the Modified Chaotic Map to calculate its own session key Ses_K, as shown in Eq. (1). Here, $\beta = 0.3$.

$$x_{n+1} = [Logistic(Quadratic(Cubic)x_n)] + [\sinh(\beta x) + \sinh^{-1}(\beta x)] \quad (1)$$

Thus, the modified chaotic map generated key is represented as Ses_K. Further, this session key Ses_K will generate the master key Ms_K and it is used to encrypt the parameters of encryption.

3.6 Avatar authentication phase

Within the virtual space, the user Us^i has the capability to interact with other avatars, represented as Us^j. To ensure secure interactions between avatars, the user is required to provide verifiable credentials that serve as proof of their Inf^i. This initiates the avatar authentication phase, as depicted in Fig. 6. Us^j Sends a message to Us^i by encrypting the message using the MECC approach. Then, Us^i decrypts the data with φ_k and again sends the message to Us^j by encrypting the message with the optimal key, generated via the TSAOO algorithm. The steps to be involved in the Avatar authentication phase are as follows:

Step 1: Us^i transmits a request with DID^i to Us^j. Following this request, Us^j extracts $\{P_k^i\}$ through DID^i and chooses an arbitrary nonce n^j with a present timestamp $Ts4$. Further, Us^j evaluates $N^j = n^j.G$, $Ms5 = (Vc^j).h(DID^i \| DID^j \| Aut^1 \| Ts4)$, $Aut^1 = n^j.P_k^j$,$Ms6 = h(Vc^j \| DID^j \| Aut^1 \| Ts4)$ as well as transmits $\{DID^j, Ms5, Ms6, N^j, Ts4\}$ to Us^i by encrypting the message using the MECC approach.

Step 2: Following the message accept $\{DID^j, Ms5, Ms6, N^j, Ts4\}$, Us^i decrypts the message and verify the validity of $Ts4$ and extracts $\{P_k^i\}$ from the blockchain through DID^j. Further, Us^i evaluates $Aut^{1\prime} = N^j.S_k^i$, $Ms6\prime = h(Vc^j \| DID^j \| Aut^{1\prime} \| Ts4)$, $(Vc^j) \stackrel{?}{=} Ms5.h(DID^i \| DID^j \| Aut^{1\prime} \| Ts4)$ and checks $Ms6 \stackrel{?}{=} Ms6\prime$ as well as the signature of Vc^j as $Sg^{C_A}(claim)$. Subsequently, Us^i chooses an arbitrary nonce d_i and evaluates $D_i = d_i.G, Aut^2 = d_i.P_k^j$, $Ms8 = h(Vc_i \| DID^i \| Aut^2 \| h(Aut^1 \| Aut^2 \| Ts5))$, $Ms7 = (Vc_i).h(DID^i \| DID^j \| Aut^2 \| Ts5)$ as well as Us^i sends $\{Ms7, Ms8, D_i, Ts5\}$ along with the optimal key $\wp^*$ to Us^j.

Step 3: After receiving the message $\{Ms7, Ms8, D_i, Ts5\}$, Us^i decrypts the data using $\wp^*$ and verify the newness of $Ts5$ as well as evaluates $(Vc_i) = Ms7.h(DID^i \| DID^j \| Aut^{2\prime} \| Ts5)$, $Aut^{2\prime} = D_i.S_k^j$, $Ms8\prime = h(Vc_i \| DID^i \| Aut^{2\prime} \| h(Aut^1 \| Aut^{2\prime} \| Ts4))$. Eventually, Us^i verifies that $Ms8 \stackrel{?}{=} Ms8\prime$ is valid and checks Vc_i's signature as $Sg^{C_A}(claim)$.

3.6.1 MECC for encryption

Modified Elliptic Curve Cryptography (MECC) is a variant of Elliptic Curve Cryptography (ECC) [23], which is a public-key cryptography strategy. This adopts elliptic curves from mathematics for safeguarding communication. This offers the equivalent rate of security measures like extant public-key cryptography strategies. The main difference is offering security with tiny key sizes. Thereby, this ensures that ECC is specifically significant in resource-constrained platforms. Each user in ECC has a pair of cryptographic keys including a private key φ_k and public key χ_k. The private key is kept secret, while the public key is shared openly. Along with these keys, a secret key

$$\lambda_k$$

is adopted. Initially, χ_k is created using Eq. (2) and encrypted it. Subsequently, generate φ_k on the server side and decrypts the message. Further, create

$$\lambda_k$$

as in Eq. (3) and point on the curve pc. Finally,

$$\lambda_k$$

is summed up with the encryption and subtracted as the decryption.

$$\chi_k = \varphi_k \times pc \quad (2)$$

$$\lambda_k = \chi_k + pc + \varphi_k \quad (3)$$

The generated secret key evaluation is improved for efficient encryption as in Eq. (4).

$$\lambda_k^{Imp} = \frac{\chi_k^{\,2} + \varphi_k^{\,2} + pc}{(2\chi_k) \times pc} \quad (4)$$

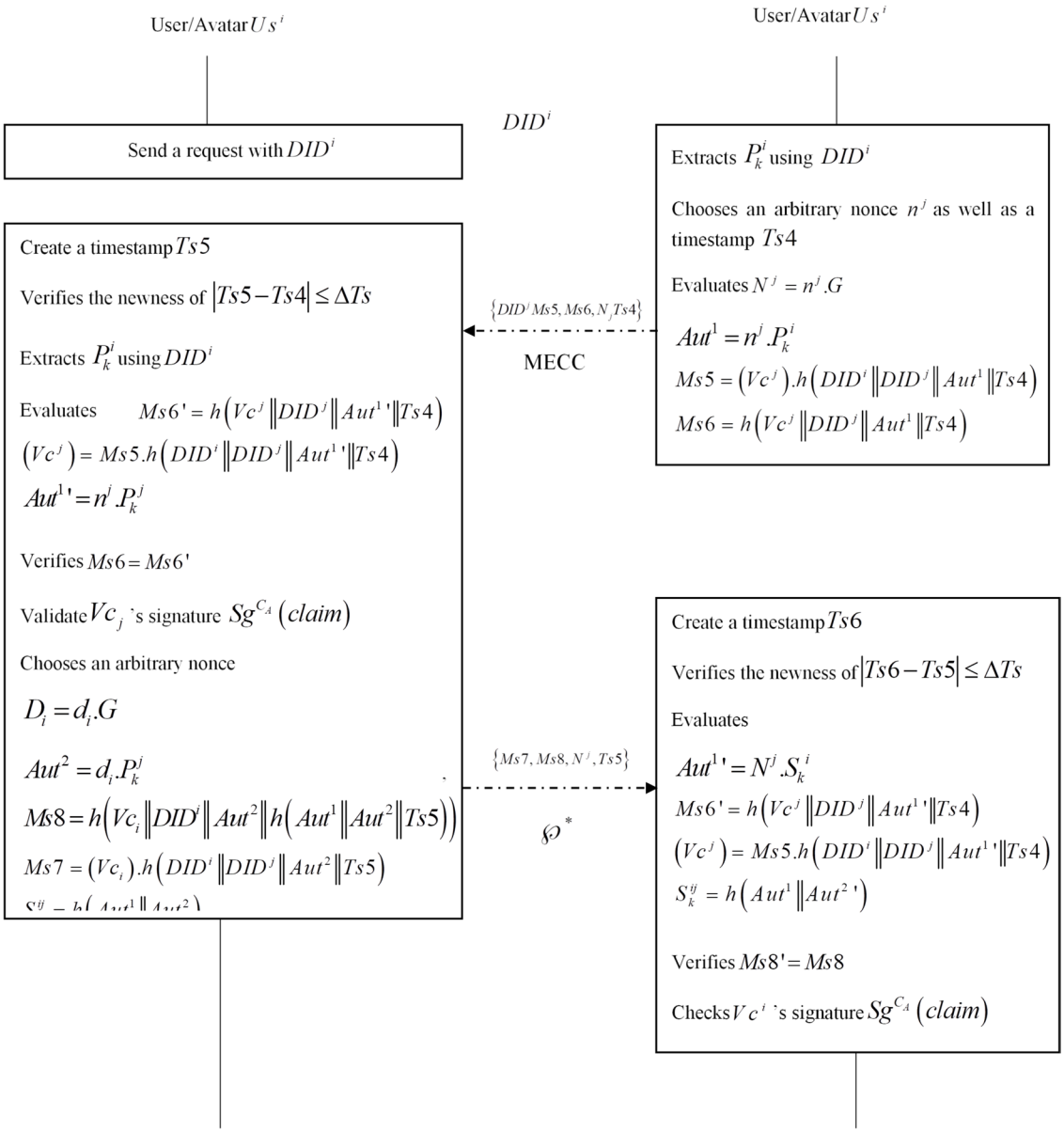

Fig. 6 Proposed scheme of Avatar authentication phase

Encryption The original data is sent towards the affine *pc* in the encryption phase. The information is then encrypted, using two ciphertexts C_T^1 and C_T^2 that are specified in Eqs. (5) and (6).

$$C_T^1 = \lambda_k + (W \times pc) \tag{5}$$

$$C_T^2 = \lambda_k + (O^{Msg} + (W \times \chi_k)) \tag{6}$$

where, O^{Msg} denotes message, and W denotes arbitrary number generated between 1 to $n-1$. Thus, the encrypted information is securely sent to the cloud server.

The above encryption of two cipher texts needs to be improved for proficient data encryption which can be defined in Eq. (7) and Eq. (8).

$$C_{T_{Imp}}^1 = ((W \times pc) + 2\lambda_k^{Imp}) + ((\chi_k^2 + \varphi_k^2) \times pc) \tag{7}$$

$$C_{T_{Imp}}^{2} = O^{Msg} + \left\{ \left[\varphi_k + \left(W\left(\chi_k{}^{2} \right) \right) + \lambda_k{}^{Imp} + W\left(\varphi_k{}^{2} + pc \right) \right] + C_{T_{Imp}}^{1} \times \lambda_k{}^{Imp} \right\} \tag{8}$$

Decryption In the decryption phase, the receiver securely downloads encrypted data and decrypts using the MECC strategy. Mathematically, the decryption function is computed as in Eq. (9).

$$O^{Msg} = \left(\left(\left(C_T^2 - \varphi_k \right) \times C_T^1 \right) - \lambda_k \right) \tag{9}$$

This decryption computation form is improved for an efficient decryption process that can be defined as in Eq. (10).

$$O_{Imp}^{Msg} = C_{T_{Imp}}^{2} - \left\{ \left[\left(W\left(\chi_k{}^{2} \right) + \varphi_k \right) + W\left(\varphi_k{}^{2} + pc \right) + \lambda_k{}^{Imp} \right] + C_{T_{Imp}}^{1} \times \lambda_k{}^{Imp} \right\} \tag{10}$$

3.6.2 Hybrid optimization TSAOO algorithm for optimal key generation

In the avatar authentication phase, the user Us^i has the capability to interact with other avatars Us^j. For authentication purposes, the user sends the message to other avatars by encrypting the message $\{Ms7, Ms8, D_i, Ts5\}$ with the optimal key. The optimal key is generated by employing a hybrid optimization TSAOO algorithm. The hybrid optimization TSAOO algorithm is the combination of two optimization strategies to reduce the computational time of the optimal key generation process. The hybrid optimization TSAOO algorithm involves two strategies like TSO [24] algorithm and the OO [25] algorithm. By inspiring the osprey's hunting as well as carrying fish strategy, the OO algorithm is used for optimal key generation. However, the speed and convergence are slow to optimize the key. To address this, the TSO algorithm is incorporated by inspiring the tuna swarm's foraging behaviour. Thus, the incorporated form of the hybrid optimization algorithm is termed as TSAOO algorithm.

Solution encoding and objective function The solution of the TSAOO algorithm is the arbitrarily created keys $\wp_i$, where $i = 1,2,...,n$. Among these keys, the best key $\wp^*$ is chosen using the TSAOO algorithm. The objective function applies to the TSAOO algorithm is defined as in Eq. (11)

Obj fun = Correlation between encryption data & original data (11)

Mathematical modelling

Initialization—proposed phase: In order to generate efficient solutions inside problem-solving domains, the proposed TSAOO operates as a population-based strategy approach that leverages the communal search skills of its members. This is accomplished by a methodical process. Each osprey in this structure, acting as an individual of the TSAOO populace, gives the problem variables values according to where it is located in the search domain. Consequently, every key function as a possible solution to the issue is represented mathematically as a vector. These keys can be thought of as the total TSAOO population, as described in Eq. (12). Equation (13) states that the osprey locations within the searching space are first randomly initialized at the beginning of TSAOO.

$$O = \begin{bmatrix} O_1 \\ \vdots \\ O_i \\ \vdots \\ O_d \end{bmatrix}_{d \times m} = \begin{bmatrix} o_{1,1} & \cdots & o_{1,j} & \cdots & o_{1,m} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ o_{i,1} & \cdots & o_{i,j} & \cdots & o_{i,m} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ o_{d,1} & \cdots & o_{d,j} & \cdots & o_{d,m} \end{bmatrix}_{d \times m} \tag{12}$$

$$o_{i,j} = r_{i,j}.(ub_j - lb_j) + lb_j \tag{13}$$

where, $i = 1,2,...,d$, $j = 1,2,...,m$, the population matrix of the location of the key is indicated as O, the ospreys count is represented as d, the arbitrary value within the interval [0, 1] is denoted as $r_{i,j}$, $o_{i,j}$ indicates i^{th} osprey in j^{th} dimension, O_i indicates i^{th} osprey, the count of problem variables is denoted as m, ub_j indicates highest limit, and lb_j indicates least limit of j^{th} variable. The problem's fitness function is established through the utilization of a vector, as articulated in Eq. (14).

$$Ftn = \begin{bmatrix} Ftn_1 \\ \vdots \\ Ftn_i \\ \vdots \\ Ftn_d \end{bmatrix}_{d \times 1} = \begin{bmatrix} Ftn(O_1) \\ \vdots \\ Ftn(O_i) \\ \vdots \\ Ftn(O_d) \end{bmatrix}_{d \times 1} \tag{14}$$

Exploration phase – proposed phase: Ospreys, serving as keys, demonstrate adept hunting skills with keen eyesight, enabling them to accurately locate underwater fish. They launch a hunting attack underwater after determining the fish's location. TSAOO's first population update phase is designed to mimic this natural osprey behavior. The osprey's placement inside the searching region is significantly altered by mimicking its approach to fish, which enhances TSAOO's exploration abilities to identify ideal locations and avoid local optima. Like underwater prey, each key in the TSAOO design takes into account the existence of other keys in searching areas with higher objective function values. This creates a plan that encourages successful exploration and exploitation. Similar to submerged prey, each key in the TSAOO design considers the locations of other keys with higher objective function values in the search space. For every key, a collection of fish is established using Eq. (15).

$$P_i = \{O_k | k \in \{1,2,...,d\} \wedge O_k < O_i\} \cup \{O_{best}\} \tag{15}$$

where, P_i denotes a set of fish's positions and O_{best} denotes the best candidate solution. The osprey utilizes a stochastic approach to pinpoint the fish's location and commences an attack. A reconsidered location is calculated using Eq. (16), which simulates the osprey's approach to the fish. According to Eq. (17), this updated location surpasses the prior osprey position if it increases the objective function value. Here, $I_{i,j}$ denotes an arbitrary number and Cf_i indicates the chosen fish for i^{th} osprey.

$$o^{p1}_{i,j,Osprey} = r_{i,j}.(Cf_i - I_{i,j}.o_{i,j}) + o_{i,j} \tag{16}$$

$$o^{p1}_{i,j} = \begin{cases} o^{p1}_{i,j}, lb_j \le o^{p1}_{i,j} \le ub_j \\ lb_j, o^{p1}_{i,j} < lb_j \\ ub_j, o^{p1}_{i,j} > ub_j \end{cases} \tag{17}$$

The optimal location is improved using Eq. (16). For this, the TSO algorithm is adopted by inspiring the food-searching behaviour of the Tuna swarm. The mathematical form of the food-searching strategy of Tuna is defined in Eq. (18).

$$O^{t+1}_i = \begin{cases} O^t_{best} + rand.(O^t_{best} - O^t_i) + J.p^2.(O^t_{best} - O^t_i), if\ rand < 0.5 \\ J.p^2.O^t_i, if\ rand \ge 0.5 \end{cases} \tag{18}$$

Adding two conditions of Eq. (18), we get as in Eq. (19–22).

$$2O^{t+1}_i = O^t_{best} + rand.(O^t_{best} - O^t_i) + J.p^2.(O^t_{best} - O^t_i) + J.p^2.O^t_i \tag{19}$$

$$2O^{t+1}_i = O^t_{best} + rand.O^t_{best} - rand.O^t_i + J.p^2.O^t_{best} - J.p^2.O^t_i + J.p^2.O^t_i \tag{20}$$

$$2O^{t+1}_i = O^t_{best} + rand.O^t_{best} - rand.O^t_i + J.p^2.O^t_{best} \tag{21}$$

$$O^t_i = \frac{2O^{t+1}_i - O^t_{best} - rand.O^t_{best} - J.p^2.O^t_{best}}{[-rand]} \tag{22}$$

Apply the value of O^t_i in $o_{i,j}$ as in Eq. (16), we get a developed formulation as per Eq. (23–27),

$$o^{p1}_{i,j,Osprey} = \left[\frac{2O^{t+1}_i - O^t_{best} - rand.O^t_{best} - J.p^2.O^t_{best}}{[-rand]}\right] + r_{i,j}.\left(Cf_i - I_{i,j}.\left[\frac{2O^{t+1}_i - O^t_{best} - rand.O^t_{best} - J.p^2.O^t_{best}}{[-rand]}\right]\right) \tag{23}$$

$$o^{p1}_{i,j,Osprey} = \frac{-2O^{t+1}_i}{rand} + r_{i,j}.Cf + \frac{O^t_{best}}{rand} + \frac{rand.O^t_{best}}{rand} + \frac{J.p^2.O^t_{best}}{rand} + r_{i,j}.I_{i,j}.\frac{2O^{t+1}_i}{rand} - \frac{r_{i,j}.I_{i,j}.O^t_{best}}{rand} - \frac{r_{i,j}.I_{i,j}.rand.O^t_{best}}{rand} - \frac{r_{i,j}.I_{i,j}.J.p^2.O^t_{best}}{rand} \tag{24}$$

$$\left[o^{p1}_{i,j,Osprey} + \frac{2O^{t+1}_i}{rand} - r_{i,j}.I_{i,j}.\frac{2O^{t+1}_i}{rand}\right] = \frac{O^t_{best}}{rand} + \frac{rand.O^t_{best}}{rand} + \frac{J.p^2.O^t_{best}}{rand} + r_{i,j}.Cf - \frac{r_{i,j}.I_{i,j}.O^t_{best}}{rand} - \frac{r_{i,j}.I_{i,j}.J.p^2.O^t_{best}}{rand} - \frac{r_{i,j}.I_{i,j}.rand.O^t_{best}}{rand} \tag{25}$$

$$o^{p1}_{i,j,Osprey}\left[1 + \frac{2}{rand} - r_{i,j}.I_{i,j}.\frac{2}{rand}\right] = \frac{O^t_{best}}{rand}\left[\begin{matrix} rand + J.p^2 + 1 + r_{i,j}.Cf - r_{i,j}.I_{i,j} \\ -r_{i,j}.I_{i,j}.rand - r_{i,j}.I_{i,j}.J.p^2 \end{matrix}\right] \tag{26}$$

$$o^{p1}_{i,j,Osprey} = \frac{\frac{O^t_{best}}{rand}\left[1 + rand + J.p^2 + + r_{i,j}.Cf - r_{i,j}.I_{ij} - r_{i,j}.I_{i,j}.rand - r_{i,j}.I_{i,j}.J.p^2\right]}{\left[1 + \frac{2}{rand} - r_{i,j}.I_{i,j}.\frac{2}{rand}\right]} \tag{27}$$

Therefore, Eq. (16) is replaced by Eq. (27). Additionally, it assesses the fitness of the previous coati, as specified in Eq. (28). Here, Ftn^{Ph1}_i denotes the value of the objective function and O^{Ph1}_i denotes the new position of osprey based on the first phase.

$$O_i = \begin{cases} O^{Ph1}_i, & Ftn^{Ph1}_i < Ftn_i \\ O_i, & else \end{cases} \tag{28}$$

Exploitation phase: The osprey moves the successfully captured fish to a safe location so it can be eaten. The second phase mimics this natural osprey behavior while upgrading the population in TSAOO. Subtle changes are made to the osprey's position inside the search arena by mimicking the process of shifting the fish towards a favorable location. This process increases TSAOO's ability to take advantage of local search opportunities, promoting convergence toward better solutions close to those that have previously been found. The TSAOO method, which simulates osprey behavior, starts by calculating a new random position for every individual in the population, which is an"appropriate location for fish utilization,"using Eqs. (29) and (30). Here, t denotes iteration counter, $t = 1,2,...,L$, L denotes overall number of iterations, $j = 1,2,...,m$,$i = 1,2,...,d$, and $r_{i,j}$ denotes random number in the interval [0, 1].

$$o_{i,j}^{p2} = \frac{lb_j + r_{i,j}.(ub_j - lb_j)}{t} + o_{i,j} \tag{29}$$

$$o_{i,j}^{p2} = \begin{cases} o_{i,j}^{p2}, lb_j \le o_{i,j}^{p2} \le ub_j \\ lb_j, o_{i,j}^{p2} < lb_j \\ ub_j, o_{i,j}^{p2} > ub_j \end{cases} \tag{30}$$

Following this, the present location of the respective osprey is exceeded only when the improvements occur in the evaluated location within the objective function, as described in Eq. (31).

$$O_i = \begin{cases} O_i^{Ph2}, Ftn_i^{Ph2} < Ftn_i \\ O_i, else \end{cases} \tag{31}$$

Figure 7 illustrates the flowchart of the suggested hybrid TSAOO algorithm.

4 Results and discussion

4.1 Simulation procedure

The simulation for the suggested Secure and Privacy-Preserving Authentication Scheme in a Metaverse Environment was conducted using PYTHON, particularly in version "3.7." The computational framework used an "Intel(R) Core(TM) i5-1035G1 CPU @ 1.00 GHz 1.19 GHz" processor, and the system was equipped with a "20.0 GB RAM."

4.2 Performance analysis

The evaluation covered both the MECC and traditional encryption techniques, emphasizing many crucial elements: latency, encryption and decryption time, and key sensitivity. Additionally, the analysis covered a number of attack types, such as KPA, CCA, EDA, FIA, KCA, SCA, and CPA. Additionally, the MECC scheme was subjected to a comparative analysis with state-of-the-art encryption methods like AES [21] and MA-ECC [14]. A comprehensive evaluation was also conducted, contrasting the MECC scheme with established encryption approaches such as ECC, RSA, Blowfish, Fernet, and Elgamal.

4.3 Attack analysis

Figures 8 and 9 illustrate the analysis of attacks on both the MECC and traditional encryption techniques within the context of the Secure and Privacy-Preserving Authentication scheme. Additionally, a comparative examination is conducted between the MECC scheme and various models, including ECC, RSA, Blowfish, Fernet, Elgamal, AES [21], and MA-ECC [14]. The assessment encompasses a thorough analysis of the MECC and existing methods concerning CCA, CPA, KPA, SCA, EDA, FIA, and KCA with data variations modified to 10%, 25%, 75%, and 100%. The primary goal is to mitigate the attack ratings of the models, ensuring enhanced security and effective preservation of privacy in the authentication scheme. The term"CCA"describes a cryptographic assault in which an adversary aims to decrypt selected ciphertexts in order to learn the private key or decrypt more ciphertexts. Specifically, with a data variation of 25%, the MECC method achieved the lowest CCA attack rate at 0.163, whereas the conventional strategies obtained greater CCA attack ratings, notably, ECC = 0.293, RSA = 0.270, Blowfish = 0.262, Fernet = 0.242, Elgamal = 0.262, AES [21] = 0.216 and MA-ECC [14] = 0.227, respectively. A cryptographic attack known as a CPA occurs when an adversary manages to decrypt selected plaintexts in order to learn more about the method of encryption or find the secret key. In this regard, the MECC scheme's measured CPA attack value is noticeably lower, dipping below 0.17. Traditional approaches, on the other hand, continuously display greater CPA attack values, surpassing 0.19.

Unauthorized communication interception that enables an adversary to hear or observe the information being shared between parties is known as an EDA attack. Moreover, the EDA attack rate for the MECC approach ranges from 31.836 to 31.468. This is notably lower compared to ECC, RSA, Blowfish, Fernet, Elgamal, AES [21], and MA-ECC [14], respectively. When an adversary purposefully adds mistakes or defects into a system that threaten its security, accessibility, or confidentiality, this is known as an FIA attack. For example, considering the 10% data variation, the MECC method achieved an FIA attack rate of 30.480, surpassing the performance of existing encryption methods such as ECC (5.513), RSA (35.297), Blowfish (34.238), Fernet (35.191), Elgamal (32.706), AES [21] (36.971), and MA-ECC [14] (32.097), respectively.

Commencing the analysis of the attack, our focus shifts to the intricacies of the MECC's methodology and the pivotal points of compromise. This examination is pivotal in comprehending how the adversary gained access and the specific tactics employed. As detailed in Fig. 9, we will navigate through these details to shed light on the specific tactics and strategies employed. A cryptographic attack known as the KCA attack uses correlations between specific features of the encrypted key and identifiable information to infer or compromise the key. For the data variation = 100%, the MECC generated the KCA attack score of 0.189, whereas the ECC is 0.195, RSA is 0.296, Blowfish is 0.288, Fernet is 0.197, Elgamal is 0.241, AES [21] is 0.293 and MA-ECC [14] is 0.260, respectively. A KPA is a type of cryptographic attack in which the attacker has samples of the plaintext and its encrypted version to figure out the encryption key

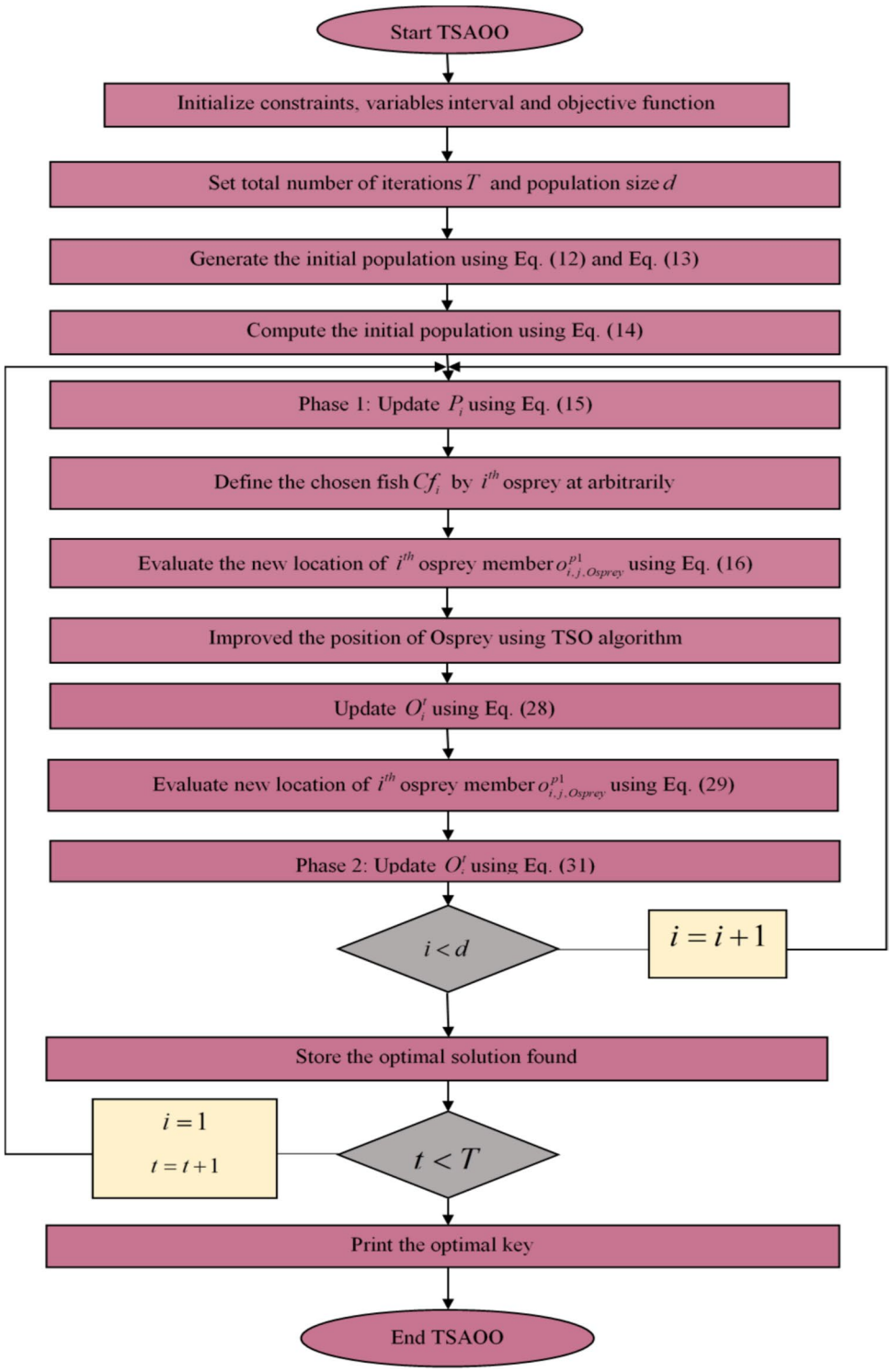

Fig. 7 Flowchart of suggested hybrid optimization TSAOO algorithm

or identify algorithmic trends. At a 75% data variation, the KPA attack value in the MECC scheme is notably lower compared to ECC, RSA, Blowfish, Fernet, ElGamal, AES [21], and MA-ECC [14], respectively. An SCA attack uses inadvertent information leakage, such as power usage or electromagnetic emissions, to deduce sensitive data or cryptographic keys. The MECC scheme attained the minimum SCA attack rate of 30.467 with a 75% data variation. Therefore, the suggested MECC scheme offer better resistance to attacks over the traditional schemes, which can be attributed to the can be attributed to the integration of the Improved Lightweight Key Management-based Crypto

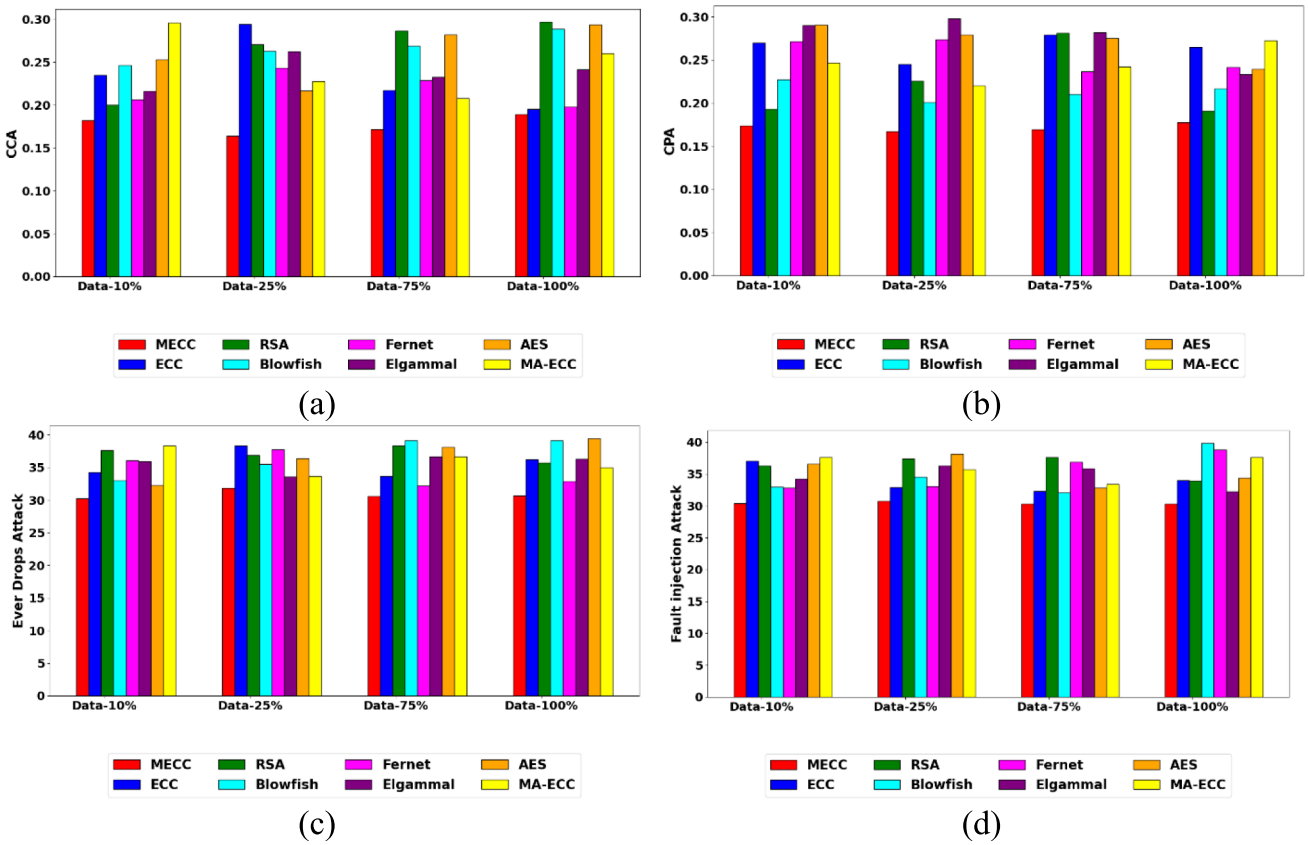

Fig. 8 Attack analysis on MECC and existing encryption schemes **a**) CCA **b**) CPA **c**) EDA and **d**) FIA

System and the hybrid TSAOO algorithm based generation of optimal key enhances the security while maintaining efficiency. The MECC methodology ensures secure communication by implementing robust authentication and key generation processes between the user and the service provider. The method demonstrates resilience against a variety of security attacks through the incorporation of an ILWKM-based login phase and optimal key generation is achieved using a hybrid optimization strategy.

4.4 Decryption and encryption time analysis

In a cryptographic system, encryption time is the amount of time needed to change plaintext into ciphertext, and decryption time is the amount of time needed to reverse the process and change ciphertext back to plaintext. Figure 10 elucidates the comparative analysis, wherein the MECC scheme is contrasted with ECC, RSA, Blowfish, Fernet, Elgamal, AES [21], and MA-ECC [14] concerning encryption and decryption times for the Secure and Privacy-Preserving Authentication scheme. Achieving effective security and privacy-preserving authentication requires the model to exhibit minimal encryption and decryption periods. Moreover, at a 25% data variation, the MECC approach demonstrated an exceptionally low encryption time of 0.397 s, in contrast to ECC, RSA, Blowfish, Fernet, ElGamal, AES [21] and MA-ECC [14] all registered longer encryption times. Simultaneously, at a 10% data variation, the MECC scheme achieved a minimal decryption time of 0.391 s, contrasting with ECC (0.915 s), RSA (1.067 s), Blowfish (1.573 s), Fernet (1.591 s), Elgamal (1.685 s), AES [21] (1.089 s), and MA-ECC [14] (1.082 s), all of which reported longer decryption durations. The outcomes of our efficiency and safety feature evaluation show that the MECC methodology outperforms conventional techniques in terms of encryption and decryption durations. Furthermore, it effectively satisfies a higher number of privacy needs than current techniques. As a result, the MECC scheme is a strong option that may provide users with a safe service in the metaverse environment.

4.5 Analysis of key sensitivity and latency

The crucial necessity of protecting and preserving the secrecy of cryptographic keys in order to guarantee safe and dependable authentication procedures is known as"key sensitivity"in authentication. The analysis of key sensitivity is conducted for both the MECC and traditional methodologies (ECC, RSA, Blowfish, Fernet, Elgamal, AES

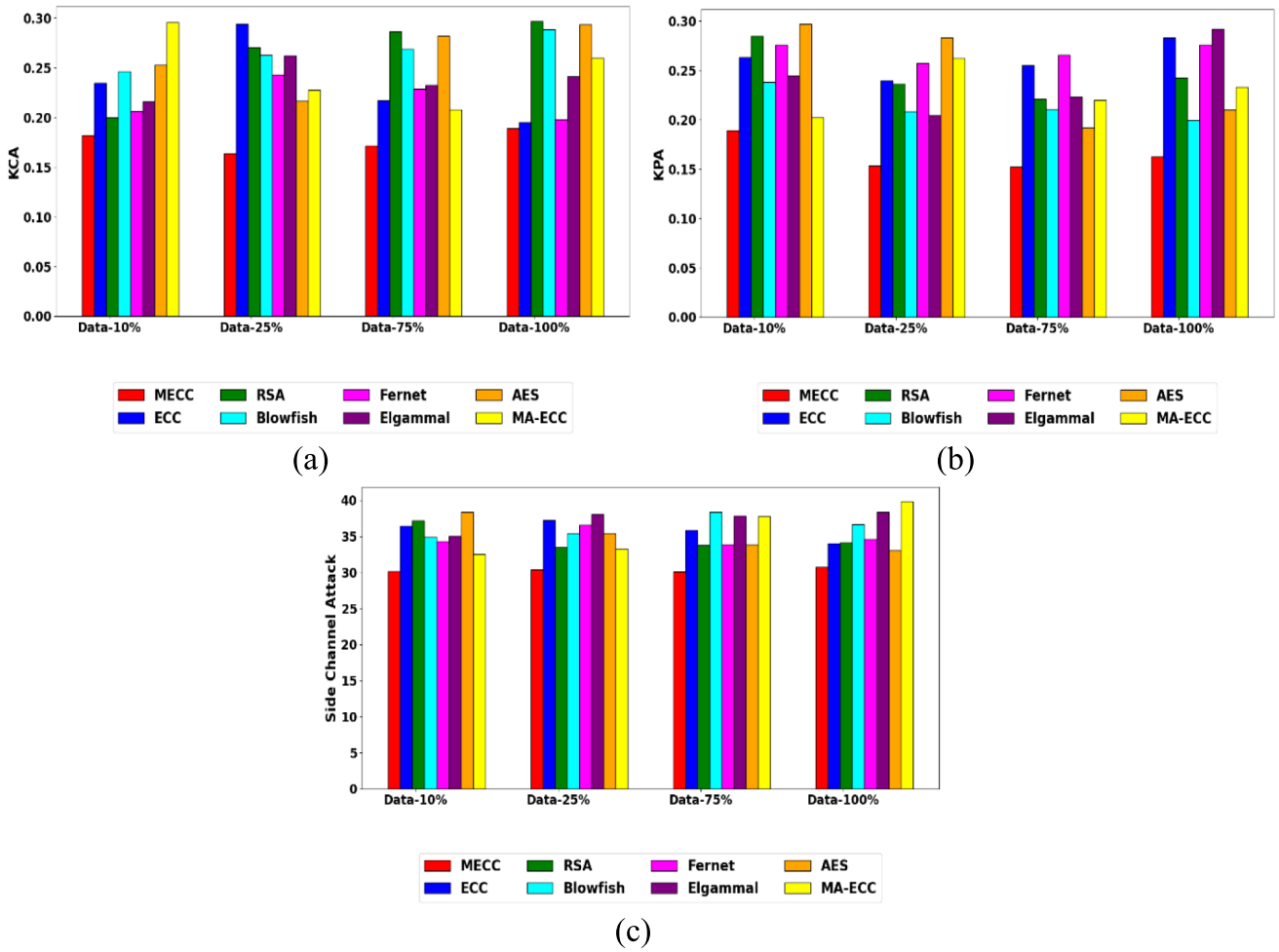

Fig. 9 Attack analysis on MECC and traditional encryption schemes **a**) KCA **b**) KPA and **c**) SCA

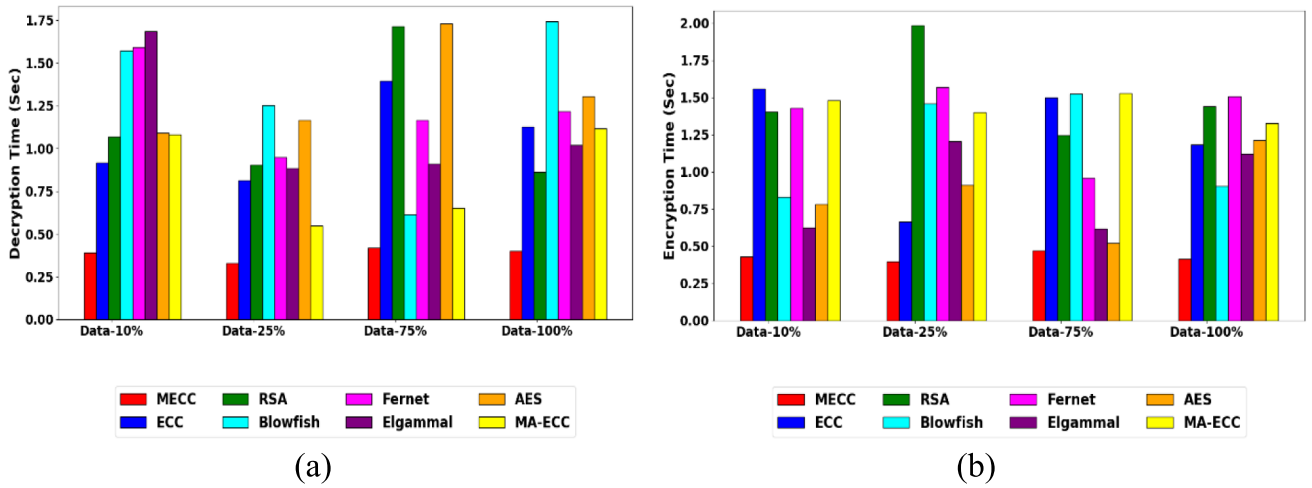

Fig. 10 Assessment of MECC and traditional encryption schemes **a**) Decryption Time and **b**) Encryption Time

[21], and MA-ECC [14]) in the context of the Secure and Privacy-Preserving Authentication scheme, as illustrated in Fig. 11(a). Here, the key sensitivity value must be minimized to ensure the effective performance of the model. In general, with a 10% data variation, the MECC method achieved a key sensitivity of 0.152. In contrast, ECC, RSA, Blowfish, Fernet, Elgamal, AES [21], and MA-ECC [14] recorded higher key sensitivities, scoring 0.264, 0.274, 0.209, 0.191, 0.233, 0.212, and 0.206, respectively.

Latency in authentication refers to the delay or time lapse between the initiation of an authentication request and the verification or response, impacting the speed and responsiveness of the authentication process. Figure 11(b) provides an overview of the latency analysis comparing the MECC method with conventional methodologies. Minimizing latency values is crucial for ensuring higher security and privacy in the authentication scheme. At a data variation of 100%, ECC displayed the highest latency value at 0.293, followed by RSA at 0.278, and MA-ECC [14] at 0.262. Conversely, the MECC scheme showcased the lowest latency rate, registering a value of 0.174. The results of the study of key sensitivity and latency show that the MECC method works better than well-known schemes, showing higher effectiveness in both ratings.

4.6 Convergence analysis

Monitoring the iterative reduction of errors to verify that an algorithm is moving closer to an accurate or ideal solution is known as the convergence evaluation of error rates. Figure 12 provides an overview of the convergence evaluation for both the TSAOO and traditional methods in the Secure and Privacy-Preserving Authentication scheme. A comparison study is also carried out using models like SSOA, SMO, BOA, TSO, and OOA. Obtaining minimal ratings on cost with quicker convergence is necessary to ensure effective model performance. All algorithms showed high error levels in the first (0 th) iteration. Nonetheless, the cost rate steadily dropped as the iterations went on. Surprisingly, from the 12 th to the 25 th iteration, our TSAOO strategy achieved minimal cost ratings. In a comprehensive assessment, our TSAOO approach demonstrated exceptional performance by achieving the lowest cost rate of 0.153 at the 25 th iteration. This surpassed conventional methods, notably outperforming SSOA (0.164), SMO (0.156), BOA (0.171), TSO (0.154), and OOA (0.155), respectively. Therefore, the TSAOO technique, developed on the foundation of ILWKM and a hybrid optimization method, demonstrates substantially lower costs in comparison to traditional methods.

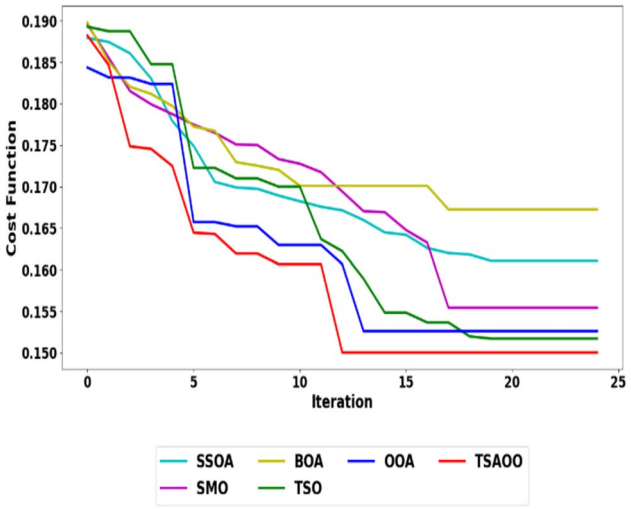

Fig. 12 Convergence evaluation on TSAOO and conventional methods

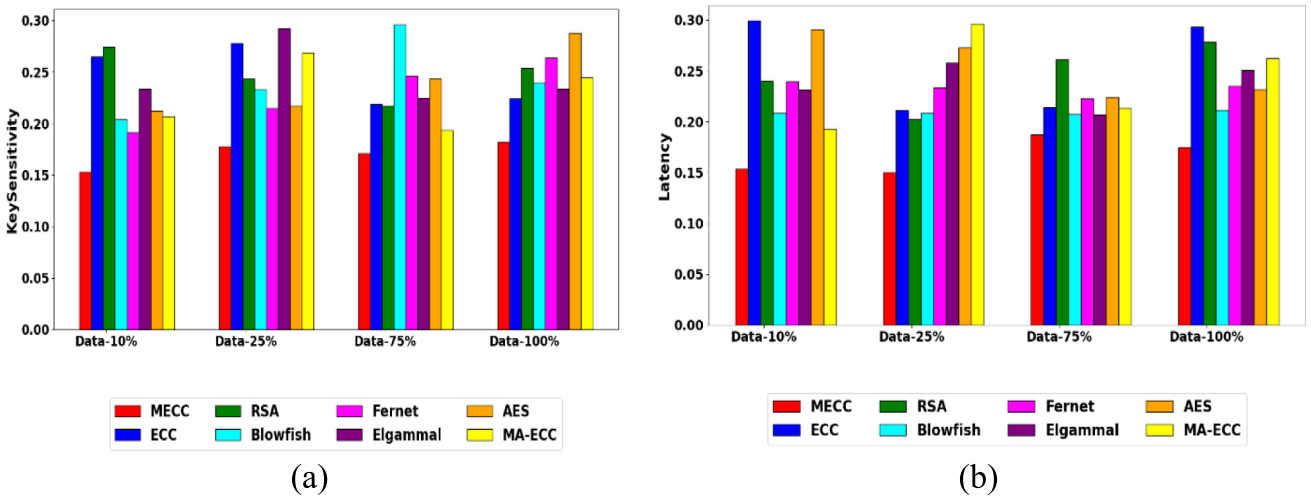

Fig. 11 Assessment on MECC and traditional encryption strategies **a**) Key Sensitivity and **b**) Latency

4.7 Statistical assessment of key sensitivity

Each approach undergoes a thorough statistical evaluation, including a thorough examination of important statistical characteristics like"Mean, Standard Deviation, Median, Best, and Worst,"to guarantee accurate results". Table 2 provides a statistical evaluation comparing the MECC approach with ECC, RSA, Blowfish, Fernet, Elgamal, AES [21], and MA-ECC [14] in terms of key sensitivity. In the analysis of the median statistical metric, the MECC model achieved the lowest key sensitivity rate at 0.174, though the ECC is 0.244, RSA is 0.249, Blowfish is 0.236, Fernet is 0.231, Elgamal is 0.234, AES [21] is 0.231 and MA-ECC [14] is 0.226, respectively. Furthermore, considering the worst-case statistical metric, the MECC approach achieved the lowest key sensitivity value at 0.194, even though the ECC, RSA, Blowfish, Fernet, Elgamal, AES [21] and MA-ECC [14] gained higher key sensitivity ratings.

5 Practical implication

The proposed authentication scheme minimizes disruptions for users interacting with the metaverse by performing authentication only during the initial login phase, while subsequent server interactions are handled similarly. This approach significantly reduces the need for re-authentication during an active session, ensuring a seamless user experience. Additionally, the authentication and verification processes are lightweight, meaning that the system does not impose significant delays on user interactions. The simplicity of the authentication steps is creating a DID, registering a VCS, and logging into the metaverse, which makes the process intuitive and easy for users to follow. Furthermore, the use of blockchain-based DIDs and VCS enhances security and trust, addressing key concerns related to identity verification. Also, this authentication should occur quickly enough to avoid disruption to the user's experience, particularly during avatar interactions in virtual environments. Additionally, as the users engage in social interactions and share personal information within metaverse spaces, the protocol ensures privacy by leveraging DIDs and verifiable credentials. This enables users to control their sharing of data, fostering a secure and trusted virtual environment where personal details remain confidential. The system is also designed to efficiently handle large-scale user interactions, ensuring scalability and a smooth experience.

Table 2 Statistical Evaluation of Key Sensitivity

Methods	Best	Median	Standard Deviation	Worst	Mean
MECC	18.20%	17.40%	1.10%	15.30%	17.10%
ECC	27.80%	24.40%	2.60%	21.90%	24.60%
RSA	27.40%	24.90%	2.10%	21.70%	24.70%
Blowfish	29.60%	23.60%	3.30%	20.40%	24.30%
Fernet	26.40%	23.10%	2.80%	19.10%	22.90%
Elgamal	29.20%	23.40%	2.70%	22.50%	24.60%
AES [21]	28.80%	23.10%	3.00%	21.20%	24.00%
MA-ECC [14]	26.90%	22.60%	3.00%	19.40%	22.90%

6 Conclusion

A novel privacy-preserving and secure authentication protocol using Improved Light Weight key management-based CryptoSystem (ILWKM-CS) was proposed. The proposed ILWKM-CS scheme for privacy-preserving and secure authentication comprises four distinct phases: User setup, User Registration, Login, and Avatar authentication. In the User setup phase, individuals established their Decentralized Identifiers (DID), and a verifiable credential was issued by the central authority as evidence of the personal data of the user. The next step is user registration, where users create an avatar in the virtual platform and register using their DID. Using the ILWKM technique, the service provider and the user are to mutually authenticate at the login step. Lastly, avatars interact with other avatars within the virtual environment and authentication occurs between them using the MECC technique in the Avatar authentication phase. Moreover, the optimal key was generated to encrypt the message via the proposed hybrid optimization TSAOO algorithm. In general, with a 10% data variation, the MECC method achieved a key sensitivity of 0.152. In contrast, ECC, RSA, Blowfish, Fernet, Elgamal, AES, and MA-ECC recorded higher key sensitivities, scoring 0.264, 0.274, 0.209, 0.191, 0.233, 0.212, and 0.206, respectively. However, the utilization of the TSAOO algorithm for generating the optimal encryption key may introduce additional computational overhead. While this algorithm is designed to improve the key generation process, its complexity could lead to slight delays in key generation. Also, the deployment of the MECC in the avatar authentication phase may be computationally expensive, particularly in resource-constrained environments. In future, an advanced technique will be employed to overcome these issues and enhance the performance of the model. The proposed approach will be extended by the implementation of signature-based schemes to evaluate its performance and security in more depth. Furthermore, we aim to deploy this research in a real-world metaverse environment in the future to assess the performance of the ILWKM-CS protocol in complex virtual settings. This will enable us to evaluate the effectiveness, security, and scalability within the interactive digital environment.

Authors contributions Vijitha S conceived the presented idea and designed the analysis. Also, he carried out the experiment and wrote the manuscript with support from Anandan R. All authors discussed the results and contributed to the final manuscript. All authors read and approved the final manuscript.

Funding This research did not receive any specific Funding.

Data availability No datasets were generated or analysed during the current study.

Declarations

Ethics approval Not Applicable.

Conflict of interest The authors declare no competing interests.

Consent to publish Not Applicable.

References

1. Zhang X, Huang X, Yin H, Huang J, Chai S, Xing B, ... Zhao L (2022) Llakep: A low-latency authentication and key exchange protocol for energy internet of things in the metaverse era. Mathematics 10(14):2545
2. Ahsani V, Rahimi A, Letafati M, Khalaj BH (2023) Unlocking metaverse-as-a-service the three pillars to watch: Privacy and security, edge computing, and blockchain. *arXiv preprint arXiv preprint* arXiv:2301.01221
3. Wang H, Li H, Smahi A, Zhao F, Yao Y, Chan CC, ... Li SYR (2023) MIS: A multi-identifier management and resolution system based on consortium blockchain in metaverse. *arXiv preprint* arXiv:2301.03529
4. Wang M, Xu C, Chen X, Zhong L, Wu Z, Wu DO (2020) BC-mobile device cloud: A blockchain-based decentralized truthful framework for mobile device cloud. IEEE Trans Industr Inf 17(2):1208–1219
5. Nguyen CT, Hoang DT, Nguyen DN, Xiao Y, Niyato D, Dutkiewicz E (2023) Metashard: A novel sharding blockchain platform for metaverse applications. IEEE Transactions on Mobile Computing
6. Zhang Q, Xiong Z, Zhu J, Gao S, Yang W (2024) A Privacy-preserving Auction Mechanism for Learning Model as an NFT in Blockchain-Driven Metaverse. ACM Trans Multimed Comput Commun Appl 20(7):1–24
7. Aldweesh A (2023) Enhancing Metaverse Security with Block Chain Authentication: Methods and Analysis. Comput Integr Manuf Syst 29(10):1–13
8. Ghantous N, Fakhri C (2022) Empowering metaverse through machine learning and blockchain technology: A study on machine learning, blockchain, and their combination to enhance metaverse. ScienceOpen Preprints
9. Mourtzis D, Angelopoulos J, Panopoulos N (2023) Blockchain integration in the era of industrial metaverse. Appl Sci 13(3):1353
10. Truong V, Le LB (2023) MetaCIDS: A metaverse collaborative intrusion detection system based on blockchain and federated learning. Authorea Preprints
11. Gadekallu TR, Wang W, Yenduri G, Ranaweera P, Pham QV, da Costa DB, Liyanage M (2023) Blockchain for the metaverse: A review. Futur Gener Comput Syst 143:401–419
12. Zhong H, Huang C, Zhang X, Pan M (2023) Metaverse CAN: Embracing Continuous, Active, and Non-intrusive Biometric Authentication. IEEE Network
13. Kim M, Oh J, Son S, Park Y, Kim J, Park Y (2023) Secure and privacy-preserving authentication scheme using decentralized identifier in metaverse environment. Electronics 12(19):4073
14. Ryu J, Son S, Lee J, Park Y, Park Y (2022) Design of secure mutual authentication scheme for metaverse environments using blockchain. Ieee Access 10:98944–98958
15. Xu M, Guo Y, Hu Q, Xiong Z, Yu D, Cheng X (2023) A trustless architecture of blockchain-enabled metaverse. High-confidence computing 3(1):100088
16. Yang K, Zhang Z, Youliang T, Ma J (2023) A secure authentication framework to guarantee the traceability of avatars in metaverse. IEEE Trans Inf Forensics Secur 18:3817–3832
17. Truong VT, Le LB (2023) MetaCIDS: Privacy-preserving collaborative intrusion detection for metaverse based on blockchain and online federated learning. IEEE Open Journal of the Computer Society
18. Khowaja SA, Dahri K, Jarwar MA, Lee IH (2023) Spike learning based privacy preservation of Internet of Medical Things in Metaverse. IEEE Journal of Biomedical and Health Informatics
19. Le HD, Truong VT, Hoang DN, Nguyen TV, Le LB (2024) MetaCrowd: Blockchain-Empowered Metaverse via Decentralized Machine Learning Crowdsourcing. In *2024 IEEE Wireless Communications and Networking Conference (WCNC)* (pp 1–6). IEEE
20. Ren Y, Lv Z, Xiong NN, Wang J (2024) HCNCT: A cross-chain interaction scheme for the blockchain-based metaverse. ACM Trans Multimed Comput Commun Appl 20(7):1–23
21. Seo J, Park S (2024) SBAC: Substitution cipher access control based on blockchain for protecting personal data in metaverse. Futur Gener Comput Syst 151:85–97
22. Khashan OA, Ahmad R, Khafajah NM (2021) An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. Ad Hoc Netw 115:102448
23. Vengala DVK, Kavitha D, Kumar AS (2023) Three factor authentication system with modified ECC based secured data transfer: untrusted cloud environment. Complex & Intelligent Systems 9(3):2915–2928
24. Xie L, Han T, Zhou H, Zhang ZR, Han B, Tang A (2021) Tuna swarm optimization: a novel swarm-based metaheuristic algorithm for global optimization. Comput Intell Neurosci 2021(1):9210050
25. Dehghani M, Trojovský P (2023) Osprey optimization algorithm: A new bio-inspired metaheuristic algorithm for solving engineering optimization problems. Frontiers in Mechanical Engineering 8:1126450

Mrs.Vijitha Sriramulu an Assistant Professor in the Department of Computer Science and Engineering at Vel's Institute of Science Technology and Advanced Studies (VISTAS), Chennai, Tamil Nadu, India. She has about 8 years of Teaching Experience from various Institutions. She has published articles in various International Journals, Books, Book Chapters, Multiple patents, Funded Projects and presented papers at various National and International conferences in the field of Computer Science and Engineering and also served as Journal Reviewer. Her areas of research include Computer Networks, Artificial Intelligence, Machine Learning, Networks, Block Chain Technology, Deep Learning and IoT.

Dr. R. Anandan completed his Post-Doctoral Degree in CSE from North America currently working as Professor and Head, Department of Computer Science and Engineering, School of Engineering and Director – Innovation and Incubation, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India. He has vast experience in corporate and all levels of Academic in Computer Science and Engineering his knowledge of interests not limited to Artificial intelligence Soft Computing, Machine Learning, High Performance Computing, Big data Analytics, Image Processing, 3D printing and knowledge Engineering. He has published more than 135 research papers in various International Journals such in Scopus, SCI and referred journal. He has presented 90 papers at various International Conferences. He received many National and International awards.He authored and Edited 27 booksand published 30 Chapters in leading publications. He filed 18 patents of his research work and three patents are granted. He produced 11 PhD candidates under his eminent guidance. He is also associated as Editor in Wiley, World Scientific Press, Springer and Nova Publishers. He also received four research grants from Government of India and three from non-governmental organization.