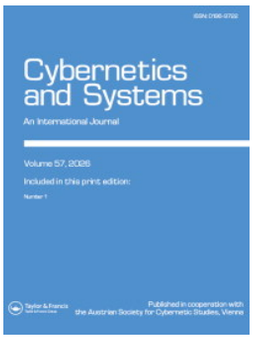

Taylor & Francis
Taylor & Francis Group

Cybernetics and Systems
An International Journal

ISSN: 0196-9722 (Print) 1087-6553 (Online) Journal homepage: www.tandfonline.com/journals/ucbs20

Avatar Authenticated Metaverse Environment with Improved Key Management and Information Flow Control with Obfuscation

Vijitha Sriramulu & Anandan Rajendran

To cite this article: Vijitha Sriramulu & Anandan Rajendran (29 Dec 2025): Avatar Authenticated Metaverse Environment with Improved Key Management and Information Flow Control with Obfuscation, Cybernetics and Systems, DOI: 10.1080/01969722.2025.2598613

To link to this article: https://doi.org/10.1080/01969722.2025.2598613

CYBERNETICS AND SYSTEMS: AN INTERNATIONAL JOURNAL
https://doi.org/10.1080/01969722.2025.2598613

Avatar Authenticated Metaverse Environment with Improved Key Management and Information Flow Control with Obfuscation

Vijitha Sriramulu and Anandan Rajendran

Department of Computer Science and Engineering, Vels Institute of Science, Technology & Advanced Studies, Velan Nagar, P.V. Vaithiyalingam Road, Pallavaram, Chennai 600 117, Tamil Nadu, India

ABSTRACT

The metaverse, a virtual world that simulates reality, is developing quickly and is about to become widely incorporated into human existence in a number of areas, including healthcare, education, and transportation. Utilizing the core principles of traditional classroom training, its online counterpart offers increased flexibility, accessibility, inclusivity, and cost-efficiency. Advancements in technology and educational tools automate data collection, enabling precise assessment of knowledge, tailored learning experiences, and targeted faculty interventions to accommodate diverse learner needs. The onset of global technological advancements accelerated the adoption of virtual learning solutions, prompting a significant transformation in teaching methods. This paper proposes a novel avatar-authenticated metaverse environment, leveraging cloud computing benefits and incorporating techniques such as Improved Key Management (IKM), Enhanced Information Flow Control (EIFC), with an obfuscation process. The EIFC method, coupled with obfuscation, introduces the Red Fox-Adapted Tuna Swarm Optimization algorithm (RFATSO) to optimally choose an improved Blowfish key from a series of sub-keys in the improved Blowfish algorithm. Experimental evaluation against established techniques showcases the effectiveness of the proposed approach in revolutionizing educational practices.

KEYWORDS

Blockchain; cloud computing; enhanced information flow control and avatar authentication; metaverse

Introduction

The rapid advancement and proliferation of cutting-edge technologies have ushered in the concept of the metaverse, viewed as the next evolutionary phase of the Internet (Sánchez-Adame et al. 2023). This metaverse is a virtual environment that mimics the real world and allows users to interact with others by manipulating virtual avatars through wearable technology such as VR or AR

CONTACT Vijitha Sriramulu vijisri.s27@gmail.com Department of Computer Science and Engineering, Vels Institute of Science, Technology & Advanced Studies, Velan Nagar, Velan Nagar, P.V. Vaithiyalingam Road, Pallavaram, Chennai 600 117, Tamil Nadu, India.

Supplemental data for this article can be accessed online at https://doi.org/10.1080/01969722.2025.2598613.

equipment. Coined by Neal Stephenson in his 1992 science fiction novel "Snow Crash" (Wang et al. 2023; Yang et al. 2022), the term "metaverse" blends "meta" (suggesting transcendence) with "universe," indicating a synthetic realm linked to reality, capable of replicating real-life scenarios (Xu et al. 2023). Developments in VR, AR, IoT, AI, and DT have transformed the metaverse from an abstract idea into a tangible reality, offering users immersive experiences that transcend temporal and spatial limitations (Truong and Le 2023).

The emergence of robust metaverse platforms has influenced various technological domains connected to the internet, facilitated by seamless and widespread access to computing resources (Joo-Eon 2021; Khowaja et al. 2023). It's important to note that the metaverse refers specifically to a computer-generated environment, distinct from metaphysical or spiritual realms, encompassing services like augmented reality, lifelogging, mirror worlds, and virtual worlds (Joshi and Pramod 2023). Notably, META, the parent company of Facebook, Instagram, and WhatsApp, is actively promoting the concept of the metaverse (Deveci et al. 2024). The term "Metaverse+" has also gained attraction, impacting fields such as the internet, education, finance, and industrial IoT (Deveci et al. 2024).

Integrating the metaverse into education, especially E-learning, presents a significant opportunity for transformation. It offers a shared virtual space where users interact through digital avatars, enhancing traditional online learning with immersive experiences. However, addressing challenges like privacy, digital equity, and technological readiness is crucial to ensure fair access and maximize the educational benefits of the metaverse (Ren et al. 2023). Blockchain technology, with its decentralized foundation and transparent operational ethos, presents a potential solution to these challenges (Zhang et al. 2023). Yet, employing blockchain for metaverse trust management remains an emerging research area (Le et al. 2023).

The transformative nature of blockchain, characterized by decentralization, transparency, immutability, and the elimination of intermediaries, has reshaped transactional and informational exchange paradigms (Wang et al. 2021). Decentralized systems, while advantageous, face security challenges, with malicious entities seeking to exploit vulnerabilities continually (Aldweesh 2023). To address these challenges, this research proposes establishing a novel avatar-authenticated metaverse environment by utilizing the benefits of cloud computing. Further, its efficacy is enhanced by employing advanced techniques such as IKM and EIFC with an obfuscation process. This initiative aims to enhance trust and security within the metaverse environment. The major contribution of this research is summarized as follows:

- Proposes an Improved Key Management (IKM) Process during the login stage, ensuring secure mutual authentication between users and

CSPs by utilizing an enhanced Blowfish key for data encryption, with a novel XOR-based encryption method involving an improved chaotic key derived from a modified cubic map.

- Proposing an Enhanced Information Flow Control (EIFC) mechanism utilizing an obfuscation process to strengthen the security of avatar-to-avatar interactions within a metaverse environment. The core innovation lies in the incorporation of a proxy for encrypting the avatar data using the improved Blowfish key (kb) via an obfuscation process, which enhances the overall cryptographic complexity.
- Introducing the Red Fox-Adapted Tuna Swarm Optimization (RFATSO) algorithm, which integrates the strengths of Tuna Swarm Optimization (TSO) and Red Fox Optimization (RFO) to achieve optimal sub-key selection in the Improved Blowfish algorithm. The enhancements focus on refining the search space during both the spiral foraging and parabolic foraging phases, resulting in improved convergence accuracy, robustness, and contributes to enhancing the efficiency and security.
- Implements an Improved Blowfish Algorithm where the function F is modified to enhance security properties. The improved key expansion and the utilization of an XOR-based key mixing process during data encryption significantly enhance the algorithm's resistance against cryptanalysis.

The research on developing a novel avatar-authenticated metaverse environment is structured into five sections, each focusing on different aspects of the study. Initially, the Literature Review section involves a thorough examination of existing approaches to metaverse-based applications. Subsequently, the Proposed Methodology of Metaverse Environment with Avatar Authentication Protocol section elaborates on the establishment of the avatar-authenticated metaverse environment, employing improved key management and information flow control with obfuscation processes. The experimental findings are then extensively discussed in the Results and Discussion section, while a brief conclusion summarizing the overall scope of the research is provided in the Conclusion section.

Literature Review

Oh et al. (2023) have developed a system facilitated secure content trading within the metaverse through blockchain technology. It guaranteed secure content handling and data integrity, leveraging smart contracts for trustworthy transactions. User experience was enhanced by searchable encryption, simplifying content discovery. Through performance analyses, the

system's security was evaluated, demonstrating its resilience in dynamic metaverse settings compared to comparable systems.

Kim et al. (2023) have suggested an authentication scheme for the metaverse utilized blockchain with verifiable credentials and decentralized identifiers. It addressed privacy issues by enabling safe identity verification without disclosing private information to service providers. The scheme withstood security attacks and preserved privacy through AVISPA simulation, BAN logic, and ROR model analyses. Researchers demonstrated its superior performance and efficiency compared to other schemes in the metaverse environment.

Awan et al. (2023) have introduced sought to enhance security within distributed systems, focusing on the Metaverse. In order to mitigate threats like Sybil attacks, it used a probabilistic trust model that gave system nodes weights based on their behavior and entity reputation. Blockchain integration created a solid basis of trust, and smart contracts lessened dishonest behavior and the need for middlemen. A decentralized dispute resolution framework promoted fairness. Implementing this approach in real-time blockchain outperformed existing methods, showcasing improved threat detection and adaptability.

Ryu et al. (2022) have developed a system model to ensure secure communication and transparent management of user identification in the metaverse, employing blockchain technology. To protect relationships among users and platforms, as well as between avatars, their suggested system model includes a mutual authentication approach utilizing biometric information and ECC. Security analysis using AVISPA, ROR model, and BAN logic validated the scheme's efficacy. Comparative analysis revealed that the suggested system has the ability to secure metaverse environments since it has broader security features and cheaper computation and transmission costs than existing schemes.

Xu et al. (2023) have presented a trustless architecture for a blockchain-enabled metaverse, aiming to streamline resource integration and allocation by combining hardware and software elements. Researchers presented an OTCE method relying on local trust assessment. Employing a hypergraph model, the system evaluated the trustworthiness of user groups using graph analytics. This empowered groups to establish security protocols autonomously, without interference from unrelated nodes. OTCEs supported expansive and adaptable application environments, maintaining robust security measures.

Zhang et al. (2022) have proposed an authentication protocol that offloads computational tasks from clients to servers, resulting in a substantial reduction in client workload and overall latency. Security analysis employing the ROR model and GNY logic affirmed the protocol's resilience.

Comparative experiments confirmed its low-latency advantage. The protocol was implemented in EIoT electricity transaction systems within a Metaverse context, demonstrating its efficacy in practical scenarios.

Gong et al. (2023) have proposed RSMS to uphold service reliability and security in the Metaverse without compromising performance. The two protocols that make up RSMS are a group authentication protocol for creating and maintaining safe service groups and a blockchain-based mutual authentication protocol for various Metaverse service resource nodes, confirming their dependability. Security analyses were undertaken, and the lightweight nature of RSMS was shown to positively influence Metaverse service throughput.

Seo and Park (2024) have developed an innovative approach merging blockchain and substitution cipher methods to enhance metaverse security. This method entailed creating rule tables for encryption and decryption, emphasizing resilience against security threats like brute-force attacks. Performance tests demonstrated quicker encryption and decryption compared to asymmetric key algorithms. Findings highlighted the effectiveness and efficiency of this approach for secure and efficient data handling in the metaverse.

Hassan et al. (2025) have established an improved privacy-preserving authentication method that protects against a variety of threats by utilizing blockchain, biohashing, elliptic curve cryptography, and a physically unclonable function. The developed framework has multiple stages, such as password change, avatar creation, and user and avatar authentication, and it is not dependent on a single central authority. To provide decentralization, interoperability, and privacy-preserving characteristics like user anonymity and untraceability, the created approach makes use of blockchain, ECC, biohashing, and PUF. The ProVerif, Scyther, and Burrows Abadi Needham (BAN) logic were used to evaluate the security of the created technique.

Belfqih and Abdellaoui (2025) have developed a decentralized authentication system that uses the IPFS data management framework and blockchain technology to provide safe, instantaneous communication between Internet of Things devices. The proposed protocol uses the elliptic curve cryptography, Ethereum blockchain, smart contracts, and ASCON encryption to ensure the secrecy, availability, and integrity of sensitive IoT data. The mutual authentication process employs asymmetric key pairs, public key registration on the blockchain, and the Diffie-Hellman key exchange algorithm to generate a shared secret that, when combined with a unique identifier, enables secure device verification. IPFS is also used for secure data storage, with the content identifier (CID) encrypted using ASCON and integrated into the blockchain for authentication and traceability.

Furthermore, the compiled research is concisely displayed in Table 1, offering a streamlined overview of their features and limitations to enhance comprehension.

Table 1. Characteristics and drawbacks of existing approaches to metaverse-based applications.

Author (citation)	Methodology	Characteristics	Drawbacks
Oh et al. (2023)	Safe content exchange with blockchain technology in the metaverse	The system made use of searchable encryption to successfully allow search functions, guard against unwanted access using content encryption, and stop unauthorized content exposure.	Though, this framework could have computational overhead associated with implementing searchable encryption, which might impact system performance, particularly in scenarios with large volumes of data or high user traffic.
Kim et al. (2023)	The metaverse's authentication system made use of blockchain technology with decentralized IDs and verifiable credentials.	By using secure authentication and a key agreement between the user and the service provider, this created a secure communication channel was created that protected against various threats.	This approach didn't consider the possible security issues that arose in the blockchain.
Awan et al. (2023)	MSBC-CTrust	The improvements in detecting threats and promptly addressing them validated the model's robustness and flexibility.	A limitation found in this framework was the potential scalability challenges associated with blockchain technology, particularly when managing trust for a large number of virtual entities within the dynamic and expansive environment of the Metaverse.
Ryu et al. (2022)	Mutual authentication scheme	This scheme incurred reduced communication and computation expenses and offered a broader array of security features compared to current schemes.	This model could be susceptible to biometric data inaccuracies.
Xu et al. (2023)	Trustless architecture for a blockchain-enabled metaverse	This architecture offered an effective means of coordinating hardware and software.	The proposed metaverse architecture would be effective through the construction of a demo metaverse.
Zhang et al. (2022)	LLAKEP	By altering the time-consuming crypto-graphic processes needed in the algorithms for both ends of communication, this protocol reduced the computational strain on devices with lower processing capacity.	This protocol would be efficient if it were designed to include low-latency AKE protocols tailored specifically for Metaverse scenarios.
Gong et al. (2023)	RSMS	The design considered the features of	Real-time monitoring and security evaluations of

(*continued*)

Table 1. Continued.

Author (citation)	Methodology	Characteristics	Drawbacks
		Metaverse services and the characteristics of entities within the Metaverse service system framework. Furthermore, simulation experiments and security analysis confirmed the effectiveness of the mechanism.	registered nurses were necessary to more quickly identify suspect RNs.
Seo and Park (2024)	SBAC	The approach employed a substitution cipher and demonstrated improved encryption and decryption performance when compared to conventional cryptographic algorithms, excelling in terms of both memory usage and elapsed times.	Some limitations of this approach included the time required for data splitting and the intricacy associated with employing multiple smart contracts for data storage.
Hassan et al. (2025)	PRIDA-ME	It provides strong interoperability across metaverse platforms.	Scalability remains a challenge, and reliance on distributed identity storage may cause synchronization delays.
Belfqih and Abdellaoui (2025)	ASCON	The protocol meets its goals, which makes it scalable and appropriate for safe Internet of Things applications.	The main limitation is the increased computational and storage overhead on IoT devices due to the complexity of blockchain, IPFS, and Ascon-based encryption protocols.

Research Gap

A review of recent works related to metaverse security highlights notable progress in blockchain-based authentication and privacy mechanisms, yet also reveals critical gaps that the proposed approach aims to address. For instance, leveraging searchable encryption (Oh et al. 2023) for secure content trading which enhances privacy but incurs significant computational overhead when scaled to high-volume environments. In contrast, the proposed method maintains low overhead by optimizing cryptographic efficiency through the Improved Blowfish algorithm and RFATSO-based key selection. Similarly, while the verifiable credentials and decentralized identifiers are employed for secure communication (Kim et al. 2023), their framework does not account for the inherent vulnerabilities in blockchain infrastructure itself. On the contrary, the proposed model mitigates such risks by incorporating obfuscation layers and improved information flow control (EIFC) to ensure layered

security, beyond blockchain reliance. The MSBC-CTrust model (Awan et al. 2023) focuses on threat detection but faces scalability issues due to the resource-intensive nature of blockchain in large-scale metaverse ecosystems. A low-cost mutual authentication scheme (Ryu et al. 2022) that relies on biometric inputs introduces vulnerability due to potential inaccuracies. In contrast, the proposed approach augments biometric data with an improved chaotic key and XOR-based encryption, enhancing both robustness and accuracy. Further, existing architectures in Xu et al. (2023) and Zhang et al. (2022) stress efficient hardware-software coordination and reduced cryptographic load. While beneficial, these approaches fall short in delivering end-to-end security within the avatar-to-avatar interaction model that is central to the metaverse. The proposed model fills this gap by introducing an obfuscation-based EIFC mechanism specifically tailored for secure interactions among avatars. In terms of protocol-level enhancements, solutions such as RSMS (Gong et al. 2023) and SBAC (Seo and Park 2024) offer tailored designs and improved encryption speed, but either lack real-time entity monitoring or involve overhead due to multi-contract execution. Additionally, approaches like PRIDA-ME (Hassan et al. 2025) and ASCON (Belfqih and Abdellaoui 2025) address interoperability and IoT-level security but struggle with synchronization and storage overheads. In contrast, the proposed protocol, however, is designed with scalability, using lightweight cryptographic operations and an optimization algorithm (RFATSO) that ensures efficient key generation even in high-demand scenarios. Overall, the proposed framework not only advances theoretical understanding through algorithmic innovation but also ensures cryptographic efficiency, and making it more suitable for deployment in metaverse environments than the existing solutions.

Proposed Methodology of Metaverse Environment with Avatar Authentication Protocol

Education is the process through which individuals acquire knowledge, skills, values, beliefs, and habits through various forms of learning. It plays a crucial role in personal development, societal progress, and economic prosperity by empowering individuals to navigate the complexities of the modern world and contribute meaningfully to their communities and societies. E-learning, facilitated by electronic technologies such as the internet and digital devices, aims to enhance access, flexibility, and effectiveness of learning experiences by delivering educational practices, tools, and resources through digital platforms.

The metaverse, a collective virtual shared space, has seen a rise in interest and development driven by advancements in VR, AR, AI, blockchain technology, and connectivity. This emergence presents significant

implications for education, offering transformative opportunities to enhance teaching and learning experiences. However, it also poses challenges related to security, privacy, digital literacy, and equitable access that must be addressed to realize its full potential in education.

Researchers are exploring transformative approaches to E-learning *via* the metaverse, one of which is avatar-based interaction. Avatar-based interaction allows users to engage in virtual environments represented by digital avatars, enhancing the learning experience with a sense of presence, identity, and interaction within the virtual space. Educators can leverage avatars to create dynamic and engaging E-learning environments tailored to the diverse needs and preferences of learners in the digital age.

The ongoing evolution of the metaverse environment drives continuous improvement in avatar-based interaction, enhancing usability, functionality, and security. Developers work to optimize avatar authentication processes, improve avatar customization options, and enhance communication features to provide users with a seamless and enjoyable experience. This research aims to harness the potential of avatar-based interaction to revolutionize E-learning and create transformative educational experiences within the metaverse. Figure 1 depicts a visual representation of E-learning facilitated through a metaverse environment.

Overview of Avatar-Authenticated Metaverse Environment

The proposed avatar-authenticated metaverse environment comprises four entities: blockchain, user, certificate authority, and service provider.

- **Blockchain**- The proposed avatar-authenticated metaverse environment makes use of a public blockchain, known for its decentralized structure. With this configuration, there is no need for a central authority because every node can join the network on its own. This makes it possible for everyone to view and add to the ledger. To reach a consensus on a single record of transactions, proof-based consensus techniques like proof of stake and proof of work are employed. The blockchain functions under the presumption of a reliable consensus mechanism and only maintains authentication-related data, especially DID documents.
- **User**- In order to get VCs, users create DIDs on the blockchain and give them to the CA along with their personal information. They then register with CSPs for access to the metaverse using minimal information. Interaction within the virtual environment involves avatars, with users employing DIDs, VCs, and public keys for secure authentication. This ensures secure interactions without revealing additional personal information. DIDs are unique identifiers created by users themselves,

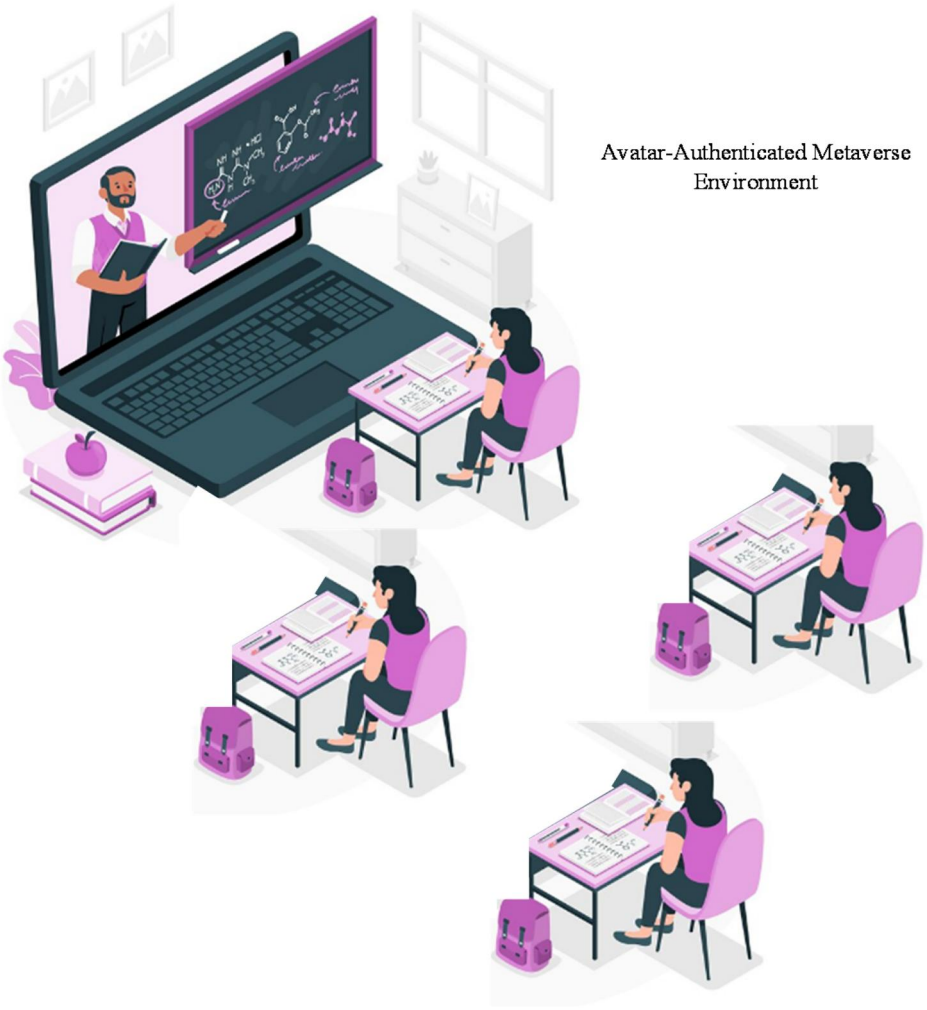

Figure 1. A scenario of E-learning conducted *via* a metaverse environment.

offering an alternative to centralized authentication authorities. VCs enable people to store and distribute identity information without depending on centralized systems by representing and validating their identities and permissions digitally.

- **Certificate Authority**- CA is a trustworthy organization in charge of setting up and distributing system parameters. Before granting a credential, it verifies the user's personal information and DID, confirming facts such as age and occupation. These credential values undergo authentication among users/avatars within the metaverse environment.
- **Cloud Service Provider**- Users utilize DIDs to register for CSP services, with CSPs verifying user identities upon access. Furthermore, throughout the avatar authentication phase, CSPs oversee the exchange of request and response messages within their specific virtual environments.

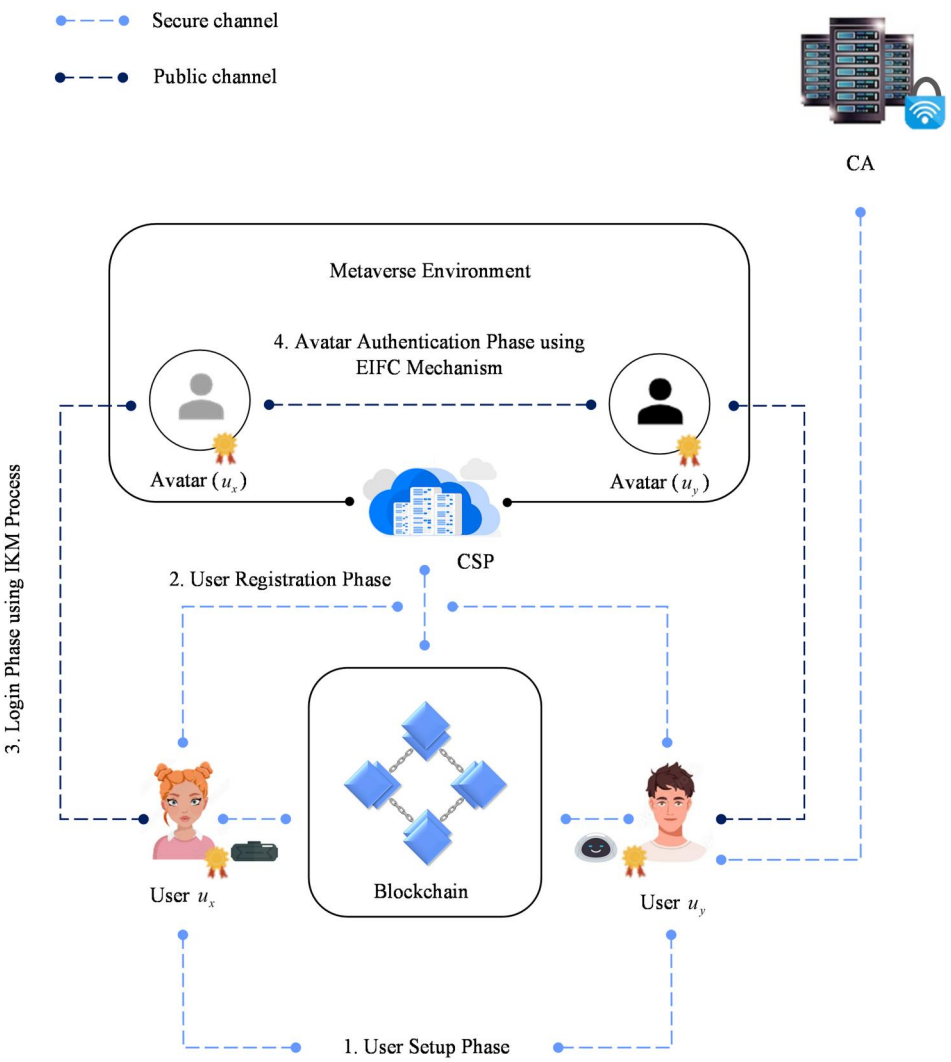

Figure 2. Procedural flow in avatar-authenticated metaverse environment.

The methodology proposed herein adopts a systematic approach delineated into four phases, as outlined below. Additionally, the visual depiction of the processes executed within these phases is portrayed in Figure 2.

i. **User setup phase**- The user creates a DID during this phase, and the CA verifies the user's private data by providing a verifiable credential.
ii. **User registration phase**- Following the user setup phase, the user signs up with the CSP utilizing their DID in the user registration phase. Before making the user's avatar in the virtual world, the CSP first verifies the validity of the user's DID.
iii. **Login phase utilizing IKM process**- After the registration of user into the E-learning space within the metaverse, the user attempts to connect with

the CSP, both parties verify each other's identity by employing an IKM process. They create a secure communication channel through the session key they decide upon after successfully verifying each other's legitimacy.

iv. **Avatar authentication phase employing EIFC with an obfuscation process**- The user engages with other avatars in the metaverse environment. The user provides VCs with the necessary personal information needed for the avatar authentication process in order to ensure safe avatar-to-avatar interactions. An obfuscation method and an EIFC mechanism are used to authenticate avatar-avatar interactions. Additionally, a novel optimization algorithm known as the RFATSO algorithm is implemented to optimally choose an improved Blowfish key from a series of sub-keys in the improved Blowfish algorithm.

Before executing the mentioned phases, CA engages in initializing system parameters, a process aimed at securely configuring and disseminating cryptographic keys, certificates, and other security-related parameters to ensure the system's secure operation. By initializing these parameters through a CA, organizations can guarantee the secure conduct of cryptographic operations and establish trust in communication between entities. The parameters initialized by the CA include the following steps:

- System Parameter Setup- Initially, CA establishes the system parameters. This involves generating large prime numbers (i, j), specifying an additive group g^A, defining an elliptic curve c_i over f_i, determining a generator G for the curve, and selecting appropriate one-way hash functions H. Additionally, the CA generates a secret key Sc_{CA}^k and computes a corresponding public key Pu_{CA}^k.
- Parameter Sharing- Subsequently, the CA shares the system parameters, denoted as $P = \left\{i, j, g^A, c_i, G, Pu_{CA}^k, h(.)\right\}$, with the network.

This process ensures that cryptographic operations are conducted securely and fosters trust among network entities.

User Setup Phase

The user creates their decentralized identification during the user setup step, and CA provides VC to validate the user's personal data. This stage is conducted *via* a secure connection. The detailed steps explained below with corresponding illustration (Figure 3) ensure that the user's personal details are confirmed and maintained with integrity.

Step 1: The user, u_x initiates the process by providing a unique identifier (id_x), a password (pw_x), and biometric information (i_x^{bio}). Subsequently, u_x chooses

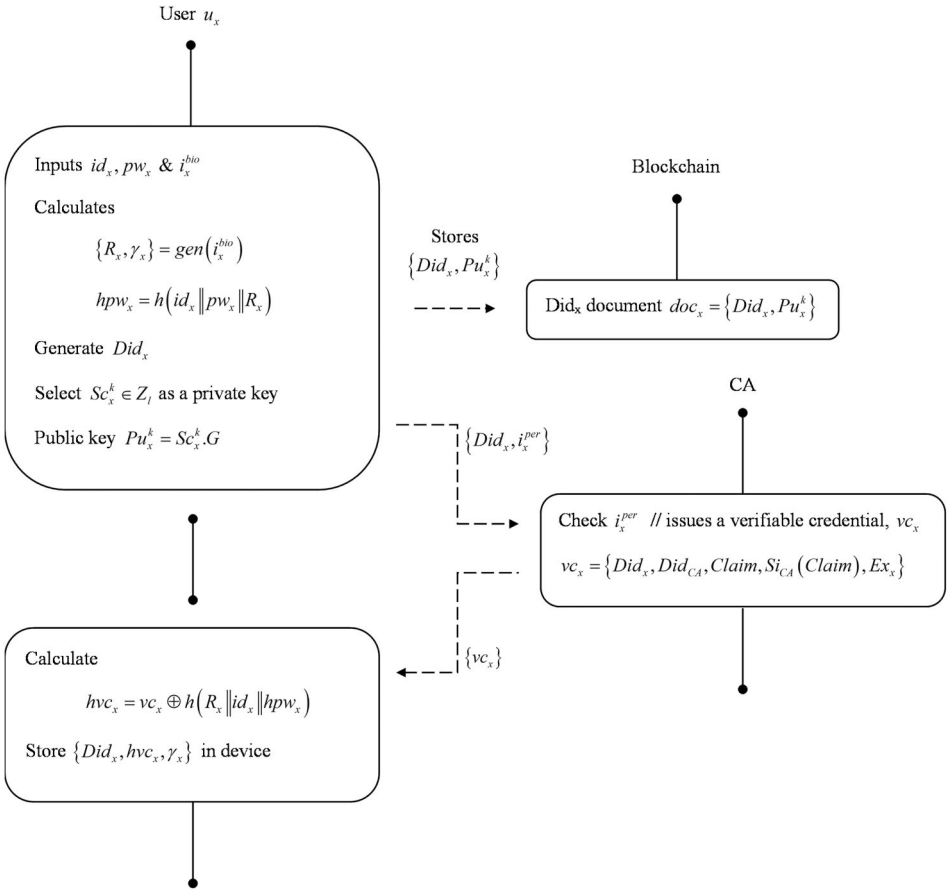

Figure 3. Functioning of the user setup phase.

an arbitrary number $Sc_x^k \in Z_l$ as a private key, then the User, u_x processes $gen(i_x^{bio}) = \{R_x, \gamma_x\}, hpw_x = h(id_x \| pw_x \| R_x), Pu_x^k = Sc_x^k.G$. Following this, u_x creates their own Did_x, which points to the location of the user's (u_x) decentralized identifier document, $doc_x = \{Did_x, Pu_x^k\}$ on the blockchain.

Step 2: u_x requests the CA to issue a credential by transmitting Did_x along with personal information (i_x^{per}). The CA verifies u_x's personal information and validates Did_x. Upon verification, the CA issues a vc_x denoted as $\{Did_x, Did_{CA}, Claim, Si_{CA}(Claim), Ex_x\}$, attesting to u_x's personal details such as occupation and age. Subsequently, the CA forwards vc_x to u_x. After confirming the validity of vc_x, u_x computes $hvc_x = vc_x \oplus h(R_x \| id_x \| hpw_x)$. u_x then stores $\{Did_x, hvc_x, \gamma_x\}$ on the device.

User Registration Phase

The user uses their decentralized identity to register with CSP within the user registration step. The user's avatar is generated in virtual space once CSP verifies the legitimacy of the user's decentralized identification. A

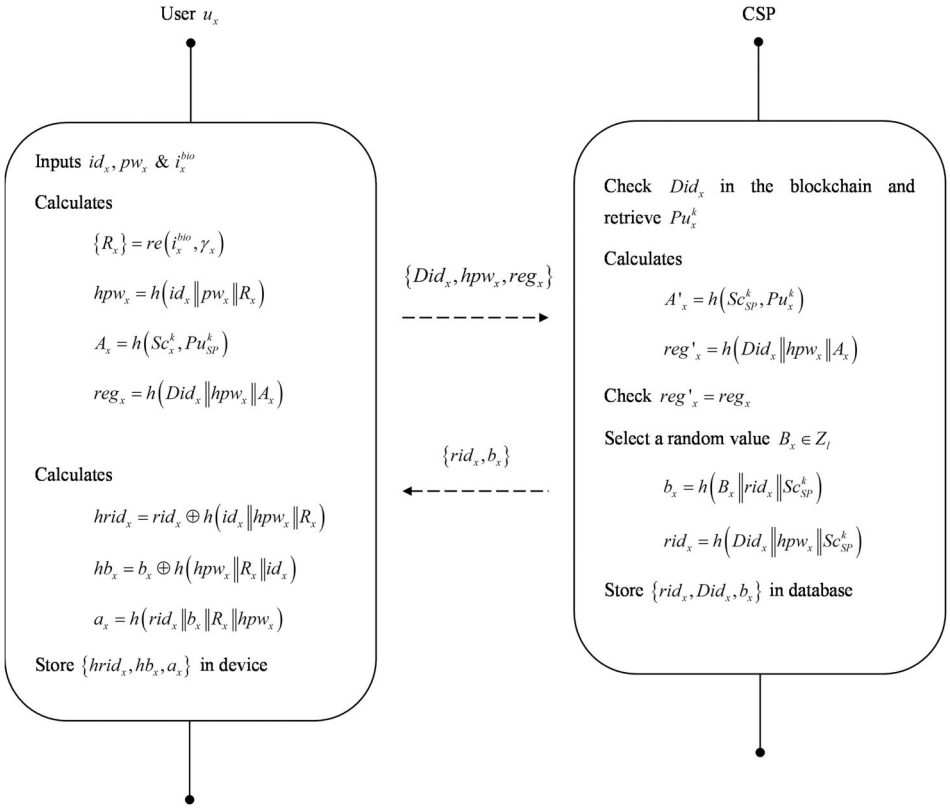

Figure 4. Functioning of the user registration phase.

secure channel is used for the entire operation. The detailed steps explained below with corresponding illustration (Figure 4) ensure the secure registration of the user and the subsequent generation of their avatar.

Step 1: The user u_x initiates the process by providing their identity (id_x), password (pw_x), and biometric information (i_x^{bio}). From this, u_x computes $\{R_x\} = rep(i_x^{bio}, \gamma_x)$, $hpw_x = h(id_x \| pw_x \| R_x)$ and $A_x = h(Sc_x^k, Pu_{CSP}^k)$, and finally computes $reg_x = h(Did_x \| hpw_x \| A_x)$. u_x then sends $\{Did_x, hpw_x, reg_x\}$ to the cloud service provider (CSP).

Step 2: CSP verifies the validity of the decentralized identifier (Did_x) and retrieves the corresponding public key (Pu_x^k) from the blockchain. If valid, CSP computes $A'_x = h(Sc_{CSP}^k, Pu_x^k)$, $reg'_x = h(Did_x \| hpw_x \| A_x)$, and verifies if reg_x matches reg'_x. If the comparison is correct, CSP chooses a random value $B_x \in Z_l$ and evaluates $b_x = h(B_x \| rid_x \| Sc_{CSP}^k)$ and $rid_x = h(Did_x \| hpw_x \| Sc_{CSP}^k)$. CSP then sends $\{rid_x, b_x\}$ to u_x and stores $\{rid_x, Did_x, b_x\}$ securely in a database.

Step 3: User, u_x computes $hrid_x = rid_x \oplus h(id_x \| hpw_x \| R_x)$ and $hb_x = b_x \oplus h(hpw_x \| R_x \| id_x)$. u_x also computes $a_x = h(rid_x \| b_x \| R_x \| hpw_x)$, and stores $\{hrid_x, hb_x, a_x\}$ in user's (u_x) XR devices.

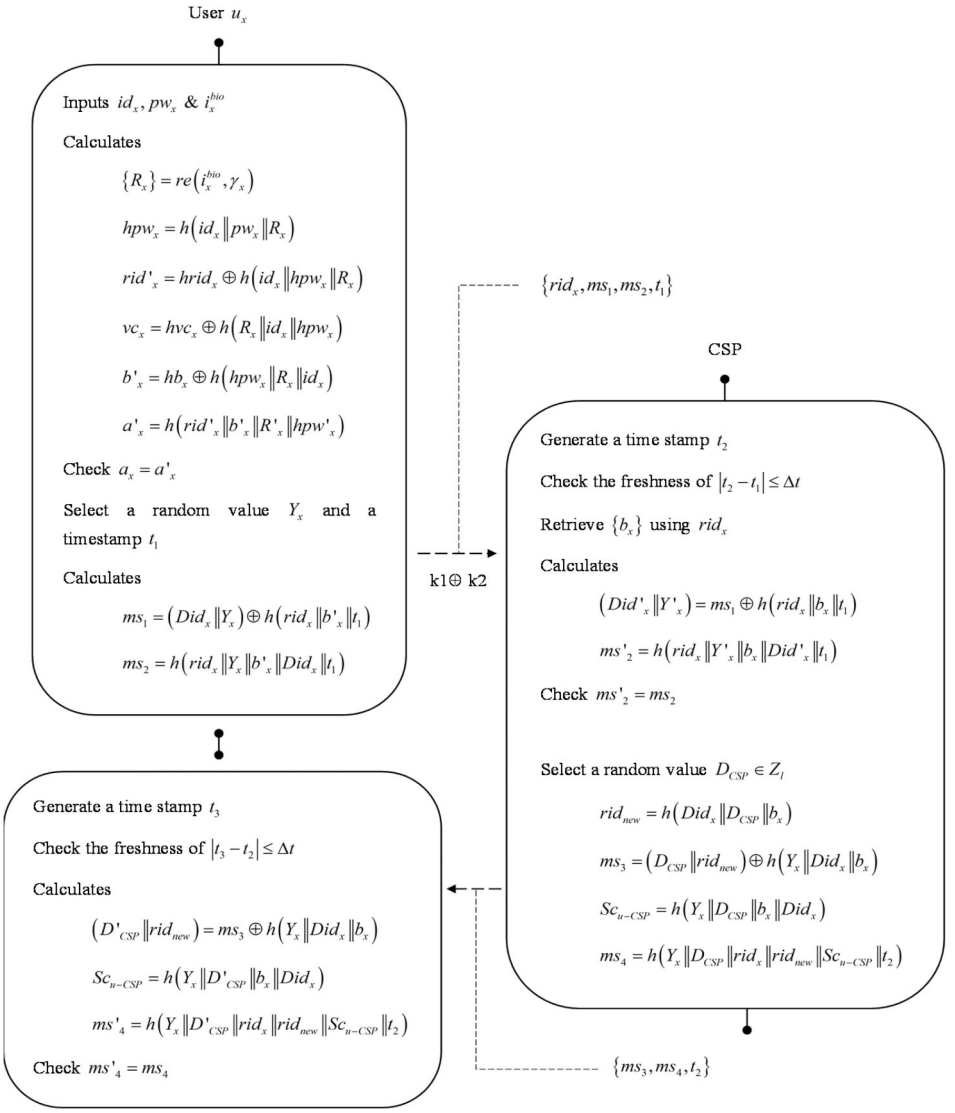

Figure 5. Functioning of login phase.

Login Phase

When user u_x tries to access CSP, both parties engage in mutual authentication. After mutual authentication is successful and a session key is established, u_x and CSPs communicate securely using this session key. To facilitate this, an IKM process is proposed in this phase, which is efficient than the existing key management process (Matthew, Muhammed, and Varadarajan 2019). The login phase is seen in Figure 5, and the specific procedures involved are described below.

Step 1: User u_x initiates the login process by entering their identity (id_x), password (pw_x), and biometric information (i_x^{bio}). u_x then computes various

parameters, including $\{R_x\} = rep(i_x^{bio}, \gamma_x)$, $hpw_x = h(id_x \| pw_x \| R_x)$, and $rid'_x = hrid_x \oplus h(id_x \| hpw_x \| R_x)$. u_x also computes other values such as $vc_x = hvc_x \oplus h(R_x \| id_x \| hpw_x)$, $b'_x = hb_x \oplus h(hpw_x \| R_x \| id_x)$, $a'_x = h(rid'_x \| b'_x \| R'_x \| hpw'_x)$, and the condition $a_x = a'_x$ is also checked. If the equation holds true, u_x selects a random value (Y_x) and a current timestamp (t_1), and evaluates $ms_1 = (Did_x \| Y_x) \oplus h(rid_x \| b'_x \| t_1)$ and $ms_2 = h(rid_x \| Y_x \| b'_x \| Did_x \| t_1)$. Subsequently, u_x sends $\{rid_x, ms_1, ms_2, t_1\}$ to CSP.

Step 2: CSP, upon receiving the message from u_x, generates a current timestamp (t_2) and verifies its freshness. CSP retrieves the value $\{b_x\}$ from the database using rid_x and calculates values such as $(Did'_x \| Y'_x) = ms_1 \oplus h(rid_x \| b_x \| t_1)$ and $ms'_2 = h(rid_x \| Y'_x \| b_x \| Did'_x \| t_1)$. CSP then checks the validity of $ms'_2 = ms_2$, selects a random value $D_{CSP} \in Z_l$, and computes new values including $rid_{new} = h(Did_x \| D_{CSP} \| b_x)$, $ms_3 = (D_{CSP} \| rid_{new}) \oplus h(Y_x \| Did_x \| b_x)$, $Sc_{u-CSP} = h(Y_x \| D_{CSP} \| b_x \| Did_x)$ and $ms_4 = h(Y_x \| D_{CSP} \| rid_x \| rid_{new} \| Sc_{u-CSP} \| t_2)$, in addition, CSP forwards $\{ms_3, ms_4, t_2\}$ to u_x.

Step 3: Upon receiving the messages from CSP, u_x verifies the freshness of t_3 and computes additional values such as $(D'_{CSP} \| rid_{new}) = ms_3 \oplus h(Y_x \| Did_x \| b_x)$, $Sc_{u-CSP} = h(Y_x \| D'_{CSP} \| b_x \| Did_x)$ and $ms'_4 = h(Y_x \| D'_{CSP} \| rid_x \| rid_{new} \| Sc_{u-CSP} \| t_2)$. u_x then check the validity of $ms'_4 = ms_4$, calculates $hrid'_x = rid_{new} \oplus h(id_x \| hpw_x \| R_x)$, and update $hrid_x$ accordingly.

Improved Key Management Process. In this research, an Improved Key Management (IKM) process is introduced to enhance the mutual authentication process during the login phase between users and CSP. To guarantee safe access to CSP services, the user and CSP must mutually authenticate. Upon successful mutual authentication and agreement on a session key, a secure communication channel is established between the user u_x and the CSP. The procedural steps followed in this process are as follows.

1. The user u_x's data is encrypted at the user's end using an initial round key (k1), generated by an Improved Blowfish algorithm. This key, k1, is retained by the user u_x.
2. The encrypted data is then transmitted to a proxy.
3. Within the proxy, the encrypted data undergoes further encryption using another key, denoted as k2, which is derived from an Improved Chaotic map. The improved chaotic key k2 is obtained from the expression, which is shown in Eq. (1) where $(sX_m(1 - X_m))$ denotes logistic map and $\left(\frac{se^{X_m}.(1-e^{X_m})}{e^{X_m}}\right)$ represents the modified cubic map (Tewfik, Nacira, and Amina 2022) in which s is a positive and it ranges between 0 to 4.

$$X_{m+1} = \frac{\left[\left[(sX_m(1-X_m)) + \left(\frac{se^{X_m}.(1-e^{X_m})}{e^{X_m}}\right)\right] \bmod_1\right]}{2} \tag{1}$$

4. Subsequently, key k2 is transmitted back to the user u_x.
5. At the user u_x's end, keys k1 and k2 are utilized in an XOR encryption process.
6. Then, the CSP requests data of the user u_x from the proxy.
7. Upon the CSP's request for the user u_x's data, the proxy responds by transmitting the user u_x's re-encrypted data to the CSP.
8. To decrypt the user u_x's data, the CSP requests the user u_x to provide the XOR-encrypted key.
9. Upon receiving this request, the user u_x promptly sends the XOR-encrypted key to the CSP.
10. It enables the CSP to retrieve the user u_x's data.

This mutual authentication process between the user and the CSP significantly enhances the security of the login phase. By employing cryptographic techniques and utilizing proxy intermediaries, the IKM process establishes a robust framework for ensuring the authentication and trust between users and CSPs in cloud environments. The security of the login procedure is reinforced by the IKM process's smooth operation, which also highlights how well it protects user data and provides safe channels of communication between users and CSPs. Furthermore, the event is illustrated graphically in Figure 6 to aid with comprehension.

Avatar Authentication Phase

In the virtual environment, a user's u_x interaction with other avatars u_y requires secure authentication. To ensure the authenticity of the interactions between avatars, the user provides authenticated credentials to verify personal information. In this research, an enhanced information flow control mechanism with an obfuscation process is utilized during the avatar authentication phase to guarantee secure authentication. Furthermore, a novel optimization algorithm called the RFATSO algorithm is introduced to choose the optimal key from a series of sub-keys in the improved Blowfish algorithm within this phase. Figure 7 illustrates the avatar authentication phase, with the detailed steps outlined below.

Step 1: u_x initiates the interaction by sending a request containing their decentralized identifier (Did_x) to u_y. Upon receiving the request, u_y retrieves the public key $\{Pu_x^k\}$ associated with Did_x, generates a random value (N_y), and timestamps the interaction (t_4). Subsequently, u_y calculates values including $n_y = N_y.G$, $au_1 = N_y.Pu_y^k$, $ms_5 = vc_y.h(Did_x \| Did_y \| au_1 \| t_4)$,

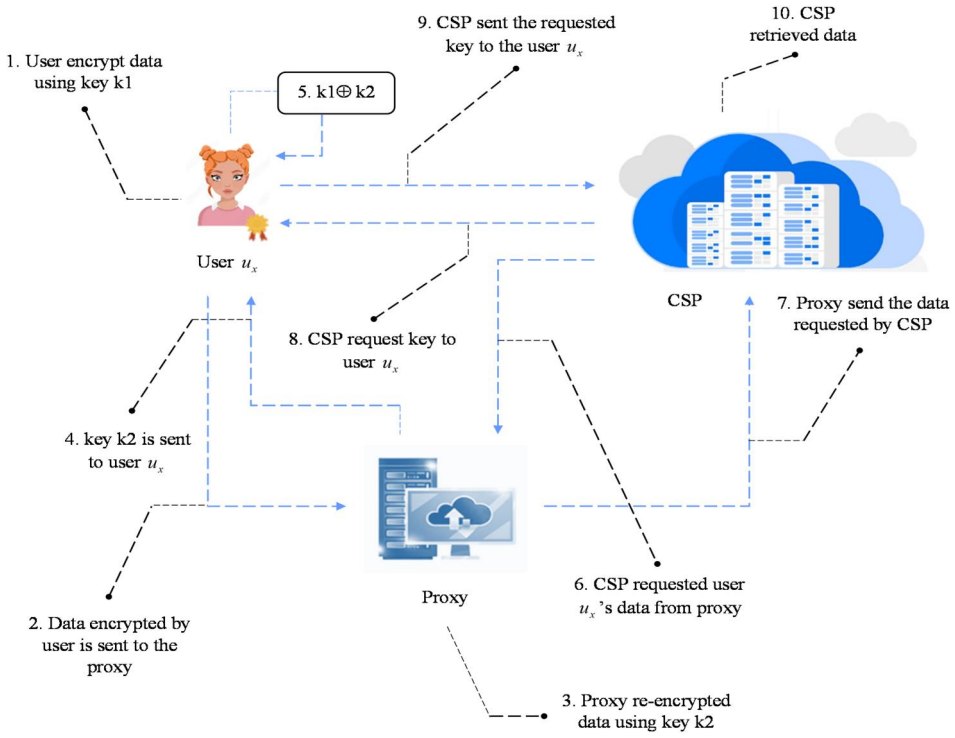

Figure 6. A scenario of an interaction between user and CSP.

and $ms_6 = .h(vc_y \| Did_y \| au_1 \| t_4)$. u_y then sends $\{Did_y, ms_5, ms_6, n_y, t_4\}$ back to u_x.

Step 2: Upon receiving the message $\{Did_y, ms_5, ms_6, n_y, t_4\}$, u_x verifies the validity of the timestamp t_4 and retrieves the public key $\{Pu_y^k\}$ associated with Did_y from the blockchain. u_x proceeds to compute values including $au_1' = n_y.Sc_x^k$, $vc_y = ms_5.h(Did_x \| Did_y \| au_1' \| t_4)$, $ms_6' = .h(vc_y \| Did_y \| au_1' \| t_4)$ and verifies the authenticity of the received message by checking equation equal or not ($ms_6' = ms_6$) and signature ($Si_{CA}(Claim)$) of the vc_y. Following this, u_x generates a random value (q_x) and computes $Q_x = q_x.G$, $au_2 = q_x.Pu_y^k$, $ms_7 = vc_x.h(Did_x \| Did_y \| au_2 \| t_5)$, $Sc_{xy}^k = h(au_1 \| au_2)$, and $ms_8 = h(vc_x \| Did_x \| au_2 \| h(au_1 \| au_2) \| t_5)$. u_x then sends $\{ms_7, ms_8, q_x, t_5\}$ to u_y.

Step 3: Upon receiving the message $\{ms_7, ms_8, q_x, t_5\}$, u_y verifies the freshness of the timestamp t_5 and computes $au_2' = q_x.Pu_y^k$, $vc_x = ms_7.h(Did_x \| Did_y \| au_2' \| t_5)$, and $ms_8' = h(vc_x \| Did_x \| au_2' \| h(au_1 \| au_2') \| t_5)$. Finally, u_y ensures that if the computed values match with the received ones i.e., $ms_8' = ms_8$ and verifies the signature $Si_{CA}(Claim)$ of vc_x.

Enhanced Information Flow Control Mechanism Using Obfuscation Process. Information flow control is an essential aspect of computer security, which

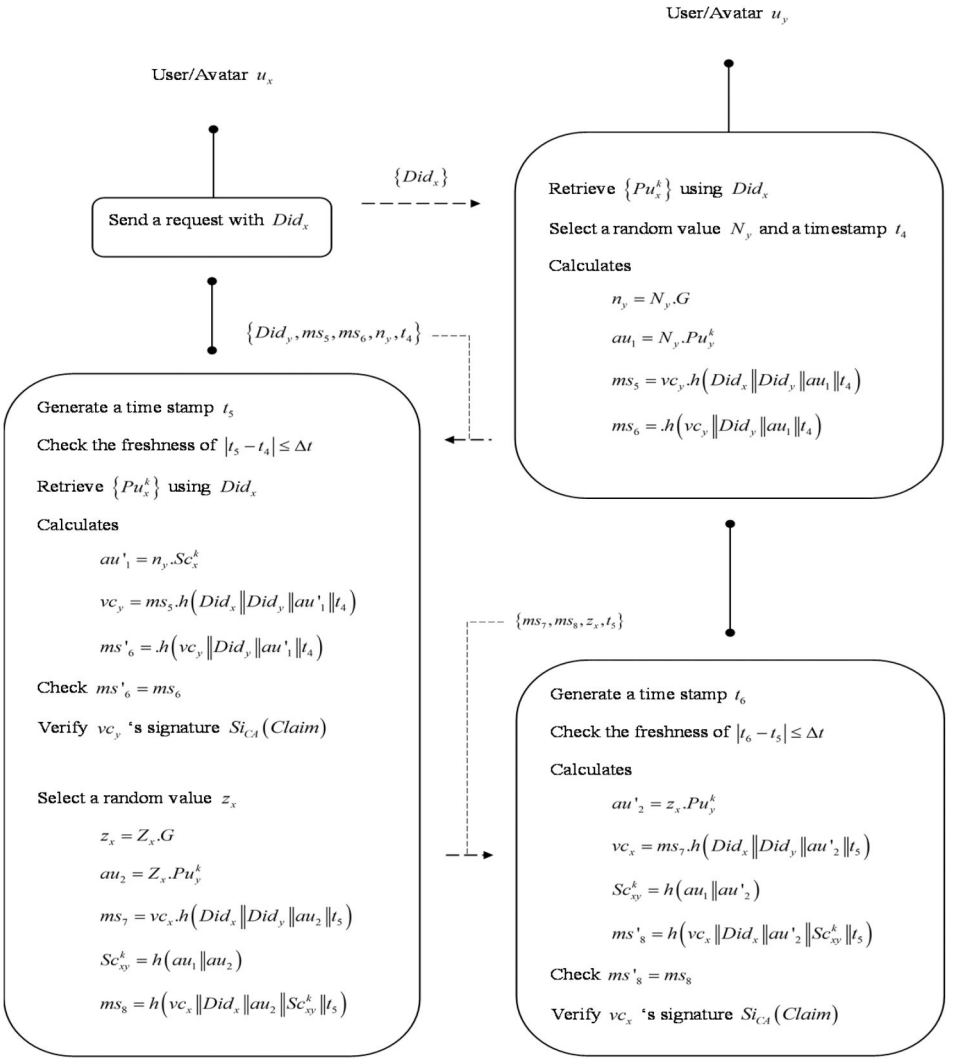

Figure 7. Functioning of the avatar authentication phase.

aims to regulate how information moves within a system to prevent unauthorized or unintended data disclosures (Zhang et al. 2021). It enforces policies that restrict access, modification, and transmission of information, ensuring data security.

The research employs a novel Enhanced Information Flow Control (EIFC) mechanism with an obfuscation process to enhance the security of avatar-to-avatar interactions in a metaverse environment. The key procedural steps followed in this mechanism are listed below, and these steps are visually illustrated in Figure 8.

1. In this environment, each user/avatar receives a VC issued by a CA to verify the source of user data.

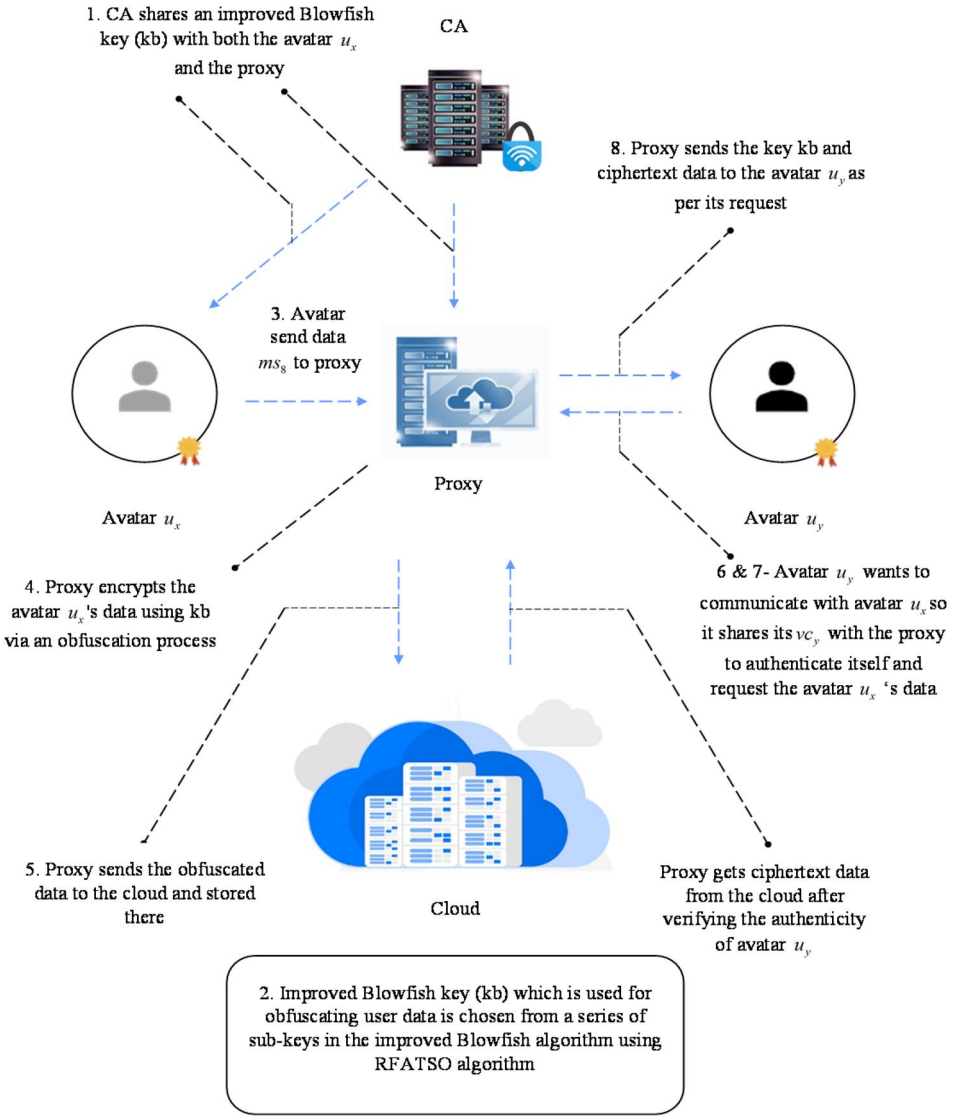

Figure 8. A scenario of avatar-to-avatar interaction.

2. Initially, the CA shares an optimal key i.e., an improved Blowfish key (kb) with both the user (avatar) u_x and the proxy. This key (kb) is optimally chosen from a series of sub-keys in the improved Blowfish algorithm using RFATSO algorithm.
3. When the avatar u_x with vc_x initiates interaction with other avatars, it sends data ms_8 to the proxy for encryption.
4. The proxy encrypts the avatar u_x's data using the improved Blowfish key (kb) via an obfuscation process.
5. The obfuscated data (ciphertext) is then sent to the cloud and stored there.

6. If another user (avatar) u_y wants to communicate with avatar u_x, it shares its vc_y with the proxy to authenticate itself.
7. The avatar u_y then requests the proxy to retrieve the data of the avatar u_x stored in the cloud.
8. After verifying the authenticity of the avatar u_y through its vc_y, the proxy sends the ciphertext data stored in the cloud along with the improved Blowfish key (kb) to the avatar u_y.

By employing an EIFC mechanism with an obfuscation process, the system enhances the security of avatar-to-avatar interactions. One key advantage lies in the issuance of VC by a CA, which verifies the authenticity of user data sources, thus preventing unauthorized access. Additionally, the utilization of an improved Blowfish key (kb) optimally chosen through the RFATSO algorithm, enhances encryption efficiency and resilience against potential attacks. The obfuscation process further improves data protection by obscuring sensitive information, reducing the risk of interception or exploitation. Moreover, storing ciphertext data in the cloud ensures data persistence and accessibility while maintaining confidentiality (Li et al. 2021). By integrating these components, the system establishes a trusted environment for avatar interactions, supporting a secure and trustworthy metaverse environment conducive to immersive and collaborative experiences.

Improved Blowfish Algorithm. Blowfish is a symmetric block cipher algorithm that encrypts data in 64-bit blocks. It operates using a Feistel network and consists of two main parts: key expansion and data encryption (Parihar and Kulshrestha 2016). The conventional Blowfish algorithm is susceptible to certain cryptanalytic attacks, particularly when dealing with weak keys. So, in this research, an improved Blowfish algorithm is proposed by improving function F, which leads this algorithm to the development of more advanced block ciphers with improved security properties. This improved Blowfish algorithm is utilized in EIFC for obfuscating data (Manikandasaran, Arockiam, and Malarchelvi 2019) through the RFATSO algorithm for choosing an optimal key from a series of sub-keys.

Key Expansion:

- The key expansion process breaks down a key of up to 448 bits into sub-key arrays totaling 4168 bytes.
- This algorithm uses a large number of sub-keys:
  - The z-array consists of 18, 32-bit sub-keys: z1, z2, … , z18.
  - Four 32-bit S-boxes, each consisting of 256 entries: S1,0, S1,1, … , S1,255; S2,0, S2,1, … , S2,255; S3,0, S3,1, … , S3,255; S4,0, S4,1, … , S4,255.

- Steps to generate sub-keys:
  - Initialize the z-array and S-boxes with a fixed string derived from the hexadecimal digits of pi.
  - XOR each 32-bit segment of the key with successive sub-keys (z1, z2, … , possibly up to z14) until the entire z-array has been XORed with key bits.

Data Encryption:

- Blowfish operates on a 16-round Feistel network during encryption.
- Each round involves key-dependent permutation and data-dependent substitution, with operations like XORs or additions on 32-bit words.
- Four indexed array data lookup tables are created for each round.
- Improved function F:
  - Divide the 64-bit data element E into two 32-bit halves: EL and ER.
  - The process carried out in improved function F is shown below.

For each of the 16 rounds:

EL = EL ⊕ zi
ER = F(EL) ⊕ ER
Swap EL and ER

After the 16 rounds, undo the last swap:

Swap EL and ER
ER = ER ⊕ z17
EL = EL ⊕ z18

Recombine EL and ER.

Decryption:

- Decryption follows the same process as encryption, but with z1, z2, … , z18 used in reverse order.
- The improved function F (Quilala, Sison, and Medina 2018) is as follows (Figure 9), where ≪ - left shift operation and ≫ - right shift operation:

$$F = ((((S1[a] \oplus S4[d]) \gg) + (S2[b] \ll) \gg) \oplus (S3[c] \ll) \bmod 232) \quad (2)$$

Red Fox-Adapted Tuna Swarm Optimization Algorithm. The RFATSO algorithm is a novel swarm-based metaheuristic optimization algorithm proposed through modification to the conventional TSO algorithm (Xie et al. 2021) using the RFO algorithm (Połap and Woźniak 2021). Inspired by the foraging behaviors of tuna, such as spiral and parabolic foraging schemes, TSO seeks to emulate the intelligent hunting techniques of these marine predators. The RFATSO algorithm adapts these natural foraging behaviors

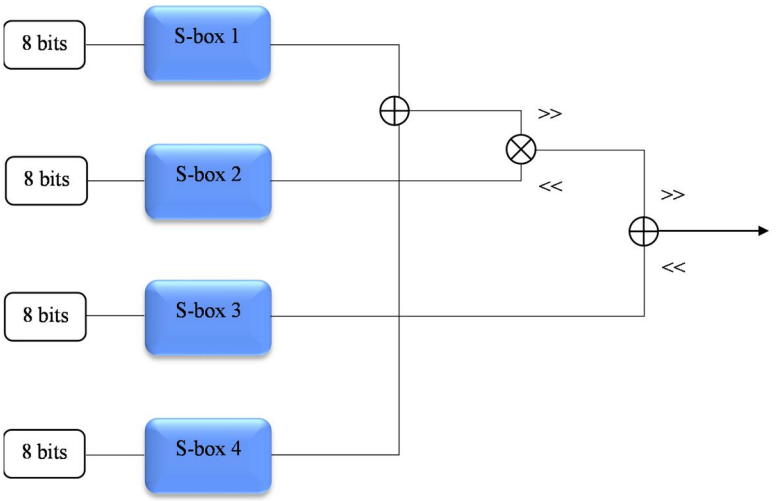

Figure 9. Improved function F.

into an optimization algorithm and enhances its efficiency in selecting an optimal key, known as the improved Blowfish key (kb), by incorporating modifications introduced by the RFO algorithm. Specifically, the RFATSO algorithm selects an optimal key from a series of sub-keys in the improved Blowfish algorithm, which is used to obfuscate the data of the avatar. Additionally, the algorithm is utilized in the EFIC mechanism during the avatar authentication phase for data obfuscation. By mimicking the collective intelligence and cooperative hunting methods of tuna, the RFATSO algorithm aims to efficiently search for optimal solutions in complex optimization problems. Assume that the sub-keys in the improved Blowfish algorithm as tunas.

Objective Function & Solution Encoding

Objective Function: The objective function aims to minimize the correlation between the original message and the decrypted message using the optimal key. Mathematically, the objective function can be defined as:

$$F_{Obj} = \min(Correlation \quad between \quad Original \quad message \quad and \quad Decrypted \quad message) \tag{3}$$

Solution Encoding: The solution encoding in the RFATSO algorithm represents the selection of an improved Blowfish key from a series of sub-keys in the improved Blowfish algorithm. Each solution in the population corresponds to a potential key configuration.

The section below shows the proposed algorithm's mathematical framework in an elaborated manner, providing a detailed explanation of its workings.

Initialization:

RFATSO algorithm initiates the optimization process by creating initial populations randomly and uniformly within the defined search space (Eq. (4)). This stage sets the foundation for subsequent iterations where the algorithm will evolve and refine these initial solutions to find optimal outcomes.

$$V_O^{in} = rd.(U_b - L_b) + L_b, O = 1, 2, ..., p \tag{4}$$

In Eq. (4), the nth initial individual is represented as V_n^{in}, is generated within the search space boundaries defined by U_b (upper boundary) and L_b (lower boundary). The algorithm involves p tuna populations, each initialized using a uniformly distributed random vector rd ranging from 0 to 1.

Spiral Foraging:

It is a predatory scheme observed in certain marine species, such as tuna, when hunting schooling fish like sardines and herring. When the prey detects predators, they form dense formations and constantly change direction to evade capture. In response, the tuna group adopts a tight spiral formation to chase and capture the prey. While individual fish within the school may lack a strong sense of direction, they adjust their swimming direction based on the movements of nearby fish, gradually forming a cohesive group with a shared goal of hunting. Additionally, the tuna exchange information with neighboring individuals, with each fish following the lead of the one before it, facilitating information sharing and coordination within the school. This scheme allows the tuna to effectively hunt and capture their prey in a coordinated manner. Mathematically, the spiral foraging scheme is described using formulas that model the movement and coordination of the tuna school as they pursue their prey.

$$V_O^{ITE+1} = \begin{cases} C_{w_1}.\left(V_{best}^{ITE} + \eta.\left|V_{best}^{ITE} - V_O^{ITE}\right|\right) + C_{w_2}.V_O^{ITE}, O = 1 \\ C_{w_1}.\left(V_{best}^{ITE} + \eta.\left|V_{best}^{ITE} - V_O^{ITE}\right|\right) + C_{w_2}.V_{O-1}^{ITE}, O = 1, 2, ..., p \end{cases} \tag{5}$$

$$C_{w_1} = I + (1 - I).\frac{ITE}{ITE_{\max}} \tag{6}$$

$$C_{w_2} = (1 - I) - (1 - I).\frac{ITE}{ITE_{\max}} \tag{7}$$

$$\eta = e^{S\beta}.\cos(2\pi S) \tag{8}$$

$$\beta = e^{3\cos(((ITE_{\max}+1/ITE)-1)\pi)} \tag{9}$$

In which each individual V_O^{ITE+1} in the next iteration $ITE + 1$ is determined based on the current best individual V_O^{ITE} and the previous individual. The movement is influenced by weight coefficients C_{w_1} and C_{w_2}, which

determine the tendency of individuals to move toward the best individual and the previous one. Additionally, a constant η controls the extent to which individuals follow the best and previous ones in the initial phase. The iteration number ITE is tracked, with a maximum number of iterations denoted by $ITE_{\max}$. Finally, a random number S between 0 and 1 is used to introduce randomness into the movement process.

The scheme of spiral foraging, where tuna move in a spiral around a target, is effective for exploiting the search space around the target. However, blindly following the optimal individual can be ineffective if it fails to find the target. To address this, a random coordinate in the search space is generated as a reference point for the spiral search. This allows each individual to explore a wider area, enhancing the algorithm's global exploration ability. In summary, by introducing random coordinates as reference points, the RFATSO algorithm improves its ability to explore diverse areas of the search space beyond just focusing on the current optimal solution.

$$V_O^{ITE+1} = \begin{cases} C_{w_1}.\left(V_{rd}^{ITE} + \eta.\left|V_{rd}^{ITE} - V_O^{ITE}\right|\right) + C_{w_2}.V_O^{ITE}, O = 1 \\ C_{w_1}.\left(V_{rd}^{ITE} + \eta.\left|V_{rd}^{ITE} - V_O^{ITE}\right|\right) + C_{w_2}.V_{O-1}^{ITE}, O = 1, 2, ..., p \end{cases} \tag{10}$$

Here, the random reference points in the search space are represented by V_{rd}^{ITE}.

Initially, the algorithm emphasizes global exploration, so random individuals are used as reference points. As iterations progress, the algorithm shifts toward local exploitation by transitioning the reference points from random individuals to optimal individuals. This approach aligns with the typical behavior of metaheuristic algorithms, which start with extensive global exploration before focusing on precise local exploitation. In summary, RFATSO dynamically adjusts the reference points of spiral foraging to balance between global exploration and local exploitation as the iteration progresses.

$$V_O^{ITE+1} = \begin{cases} C_{w_1}.\left(V_{rd}^{ITE} + \eta.\left|V_{rd}^{ITE} - V_O^{ITE}\right|\right) + C_{w_2}.V_O^{ITE}, O = 1, if \quad rd < \dfrac{ITE}{ITE_{\max}} \\ C_{w_1}.\left(V_{rd}^{ITE} + \eta.\left|V_{rd}^{ITE} - V_O^{ITE}\right|\right) + C_{w_2}.V_{O-1}^{ITE}, O = 1, 2, ..., p, if \quad rd < \dfrac{ITE}{ITE_{\max}} \\ C_{w_1}.\left(V_{best}^{ITE} + \eta.\left|V_{best}^{ITE} - V_O^{ITE}\right|\right) + C_{w_2}.V_O^{ITE}, O = 1, if \quad rd \geq \dfrac{ITE}{ITE_{\max}} \\ C_{w_1}.\left(V_{best}^{ITE} + \eta.\left|V_{best}^{ITE} - V_O^{ITE}\right|\right) + C_{w_2}.V_{O-1}^{ITE}, O = 1, 2, ..., p, if \quad rd \geq \dfrac{ITE}{ITE_{\max}} \end{cases} \tag{11}$$

Parabolic Foraging:

In addition to spiral formation, tunas utilize a cooperative feeding scheme called parabolic foraging. In this approach, tunas form a parabolic shape around a reference point, which is the food they are hunting. Simultaneously, they search the area around themselves for food. Both schemes, spiral and parabolic foraging, are executed concurrently with an equal probability of 50% for each. The mathematical model representing this dual approach is described by Eq. (12) Where J represents a randomly generated number with a value of either 1 or −1.

$$V_O^{ITE+1} = \begin{cases} V_{best}^{ITE} + rd.\left(V_{best}^{ITE} - V_O^{ITE}\right) + J.K^2.\left(V_{best}^{ITE} - V_O^{ITE}\right), & if \quad rd < 0.5 \\ J.K^2.V_O^{ITE}, & if \quad rd \geq 0.5 \end{cases} \tag{12}$$

$$K = \left(1 - \frac{ITE}{ITE_{\max}}\right)^{\left(\frac{ITE}{ITE_{\max}}\right)} \tag{13}$$

To enhance the RFATSO algorithm's capability, Eq. (12) representing the mathematical model of tuna's parabolic foraging scheme is combined and simplified, resulting in Eq. (15). Additionally, a condition from the RFO algorithm (Eq. (17)) is substituted into Eq. (15), leading to a simplified form expressed in Eq. (23) and it replaces Eq. (12). This process aims to update the representation of the combined schemes and conditions within the RFATSO algorithm, potentially improving its performance and effectiveness in optimizing solutions.

$$2V_O^{ITE+1} = V_{best}^{ITE} + rdV_{best}^{ITE} - rdV_O^{ITE} + J.K^2V_{best}^{ITE} - J.K^2V_O^{ITE} + J.K^2V_O^{ITE} \tag{14}$$

$$2V_O^{ITE+1} = V_{best}^{ITE} + rdV_{best}^{ITE} - rdV_O^{ITE} + J.K^2V_{best}^{ITE} \tag{15}$$

$$Fox_{n-1}^{new} = \delta R_{Fox}.\sin(\vartheta_1) + \delta R_{Fox}.\sin(\vartheta_2) + \cdots + \delta R_{Fox}.\sin(\vartheta_{n-1}) + Fox_{n-1}^{actual} \tag{16}$$

$$Fox_{n-1}^{actual} = \left[Fox_{n-1}^{new} - \delta R_{Fox}.\sin(\vartheta_1) - \delta R_{Fox}.\sin(\vartheta_2) - \cdots - \delta R_{Fox}.\sin(\vartheta_{n-1})\right] \tag{17}$$

Substitution of a condition from the RFO algorithm into Eq. (15) is shown below where $V_O^{ITE} = Fox_{n-1}^{actual}$, $V_O^{ITE+1} = Fox_{n-1}^{new}$ & $R_{Fox} = R_{Tuna}$.

$$2V_O^{ITE+1} = V_{best}^{ITE} + rdV_{best}^{ITE} - rd\left[V_O^{ITE+1} - \delta R_{Tuna}.\sin(\vartheta_1) - \delta R_{Tuna}.\sin(\vartheta_2) - \cdots - \delta R_{Tuna}.\sin(\vartheta_{n-1})\right] + J.K^2V_{best}^{ITE} \tag{18}$$

$$2V_O^{ITE+1} = V_{best}^{ITE} + rdV_{best}^{ITE} + J.K^2V_{best}^{ITE} - rdV_O^{ITE+1} + rd\delta R_{Tuna}.\sin(\vartheta_1) + rd\delta R_{Tuna}.\sin(\vartheta_2) + \cdots + rd\delta R_{Tuna}.\sin(\vartheta_{n-1}) \tag{19}$$

$$2V_O^{ITE+1} = V_{best}^{ITE}(1 + rd + J.K^2) - rdV_O^{ITE+1} + rd\delta R_{Tuna}.\sin(\vartheta_1) + rd\delta R_{Tuna}.\sin(\vartheta_2) + \cdots + rd\delta R_{Tuna}.\sin(\vartheta_{n-1}) \tag{20}$$

$$2V_O^{ITE+1} + rdV_O^{ITE+1} = V_{best}^{ITE}(1 + rd + J.K^2) + rd\delta R_{Tuna}.\sin(\vartheta_1) + rd\delta R_{Tuna}.\sin(\vartheta_2) + \cdots + rd\delta R_{Tuna}.\sin(\vartheta_{n-1}) \tag{21}$$

$$V_O^{ITE+1}(2+rd) = V_{best}^{ITE}(1+rd+J.K^2) + rd\delta R_{Tuna}.\sin(\vartheta_1) + rd\delta R_{Tuna}.\sin(\vartheta_2) + \cdots + rd\delta R_{Tuna}.\sin(\vartheta_{n-1}) \tag{22}$$

$$V_O^{ITE+1} = \frac{\begin{bmatrix} V_{best}^{ITE}(1+rd+J.K^2) + rd\delta R_{Tuna}.\sin(\vartheta_1) \\ + rd\delta R_{Tuna}.\sin(\vartheta_2) + \cdots + rd\delta R_{Tuna}.\sin(\vartheta_{n-1}) \end{bmatrix}}{[2+rd]} \tag{23}$$

Tuna engage in cooperative hunting using two different foraging schemes to locate their prey. In the optimization process of RFATSO, the population is initially generated randomly within the search space. In each iteration, individuals randomly select one of the two foraging schemes or choose to regenerate their position in the search space based on a probability parameter, *PP*. The specific value of *PP* will be determined during parameter setting simulation experiments. Throughout the optimization process, all individuals in the population of RFATSO are continuously updated and evaluated until a termination condition is met. Finally, the optimal individual and its corresponding objective value are returned. Algorithm 1 shows the pseudo-code.

Algorithm 1. Pseudocode of RFATSO

Input maximum iteration $ITE_{\max}$ and size of population p of the RFATSO algorithm
Initialize tunas' population randomly
Allocate free parameters $I \quad and \quad PP$
while $ITE < ITE_{\max}$
    Evaluate tunas' objective value
    Update V_{best}^{ITE}
    for (each tuna) do
        Update $C_{w_1}, C_{w_2} \quad and \quad K$
        if $(rd < PP)$ then
            Update the position V_O^{ITE+1} using Eq. (4)
        else if $(rd \geq PP)$ then
            if $(rd < 0.5)$ then
                if $\left(\frac{ITE}{ITE_{\max}} < rd\right)$ then
                    Update the position V_O^{ITE+1} using Eq. (10)
                else if $\left(\frac{ITE}{ITE_{\max}} \geq rd\right)$ then
                    Update the position V_O^{ITE+1} using Eq. (5)
            else if $(rd \geq 0.5)$ then
                Update the position V_O^{ITE+1} using Eq. (23)
    end for
        $ITE = ITE + 1$
end while
Return the best solution V_{best} and the best objective value $F_{Obj}(V_{best})$

Results and Discussion

Simulation Procedure

The proposed Avatar-Authenticated Metaverse Environment was simulated using PYTHON, with the Python version specified as "Python 3.7." Additionally, the simulation utilized an "Intel(R) Core (TM) i5-1035G1 CPU @ 1.00 GHz 1.19 GHz" processor and had "20.0 GB" of installed RAM.

Simulation Configuration

In a metaverse environment where users access virtual services hosted by a service provider (SP) through wearable devices such as VR and AR, mutual authentication techniques originally developed for IoT environments can be effectively applied. In this setting, a Certificate Authority (CA) receives the user's Decentralized Identifier (DID) and personal information, both of which require verification. Upon successful validation, the CA issues a digital credential to the user, certifying their identity. Initially, the user registers with the SP using their DID. When the user later attempts to access metaverse services, the SP verifies the user's identity using the previously issued credential and the associated DID. The user generates their own DID and corresponding private key, and this DID is published on a blockchain network, which is used solely to store DID documents, having no personal or biometric data is stored on-chain, ensuring privacy. The authentication process begins with the user submitting a unique identifier, password, and biometric information. The user also selects an arbitrary number to serve as their private key and transmits their DID along with their personal information to the CA to request a credential. The CA then verifies the user's identity and validates the submitted DID before issuing the credential.

Performance Analysis

The evaluation encompassed both the Improved Blowfish and traditional encryption methodologies, emphasizing key factors such as encryption and decryption times, latency, and Key Sensitivity. It also examined various attack types, including CCA, SCA, CPA, KPA, EDA, KCA, and FIA. Additionally, the Improved Blowfish scheme underwent a comparative analysis with state-of-the-art encryption techniques like ECC (Ryu et al. 2022), ASCON (Belfqih and Abdellaoui 2025), AES (Seo and Park 2024), and ASB (Kim et al. 2023). Furthermore, a comprehensive assessment contrasted the Improved Blowfish scheme with established encryption approaches such as Blowfish, Elgamal, AES, RSA, Fernet, and MECC (Sriramulu 2025).

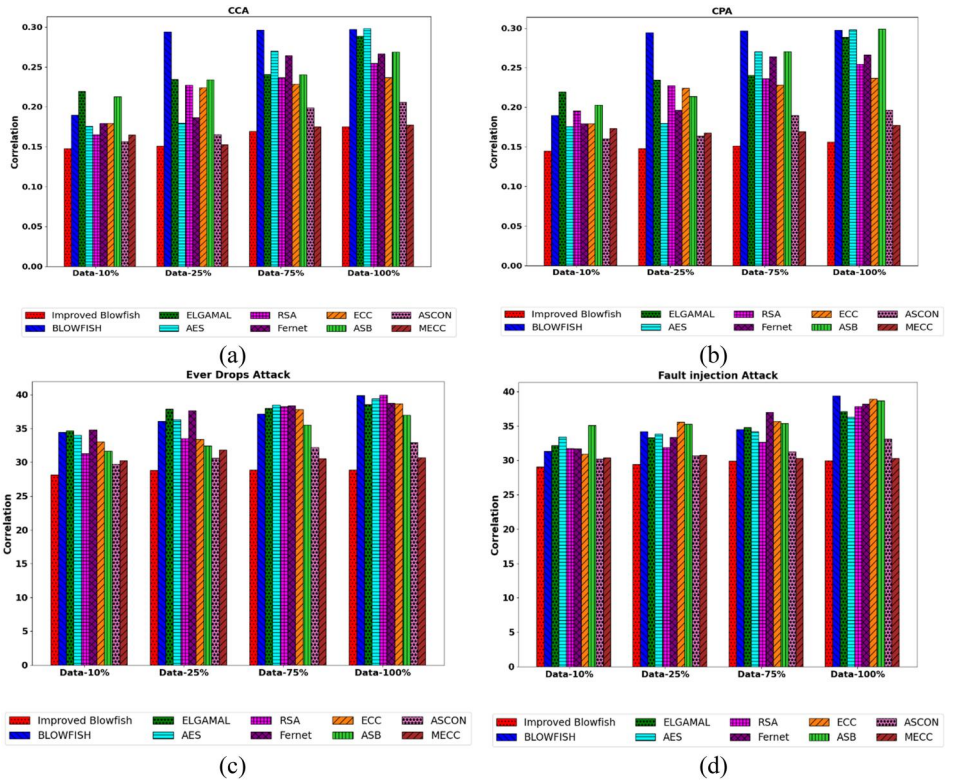

Figure 10. Attack analysis on improved blowfish and conventional methods (a) CCA, (b) CPA, (c) EDA, and (d) FIA.

Simultaneously, convergence analysis was conducted for both the RFATSO and conventional approaches, including SSOA, ACO, PSO, TSO, and RFO.

Attack Analysis

In the evaluation of the Improved Blowfish authentication model for avatar-authenticated metaverse environments, a comprehensive analysis was conducted, contrasting its resilience against a range of conventional encryption methods, including Blowfish, Elgamal, ASCON (Belfqih and Abdellaoui 2025), AES (Seo and Park 2024), AES, RSA, Fernet, ECC (Ryu et al. 2022), ASB (Kim et al. 2023), and MECC (Sriramulu 2025). This analysis is depicted in both Figures 10 and 11, providing a visual representation of the comparison. Specifically, the Improved Blowfish model is scrutinized under various attack models such as CCA, CPA, EDA, FIA, KCA, KPA and SCA. Moreover, the analysis encompassed a study of the model's performance across different levels of data variation, ranging from 10% to 100%. Moreover, it is imperative that the model achieves lower attack ratings to ensure efficacious authentication performance. CCA is a cryptographic exploit where an adversary endeavors to obtain the

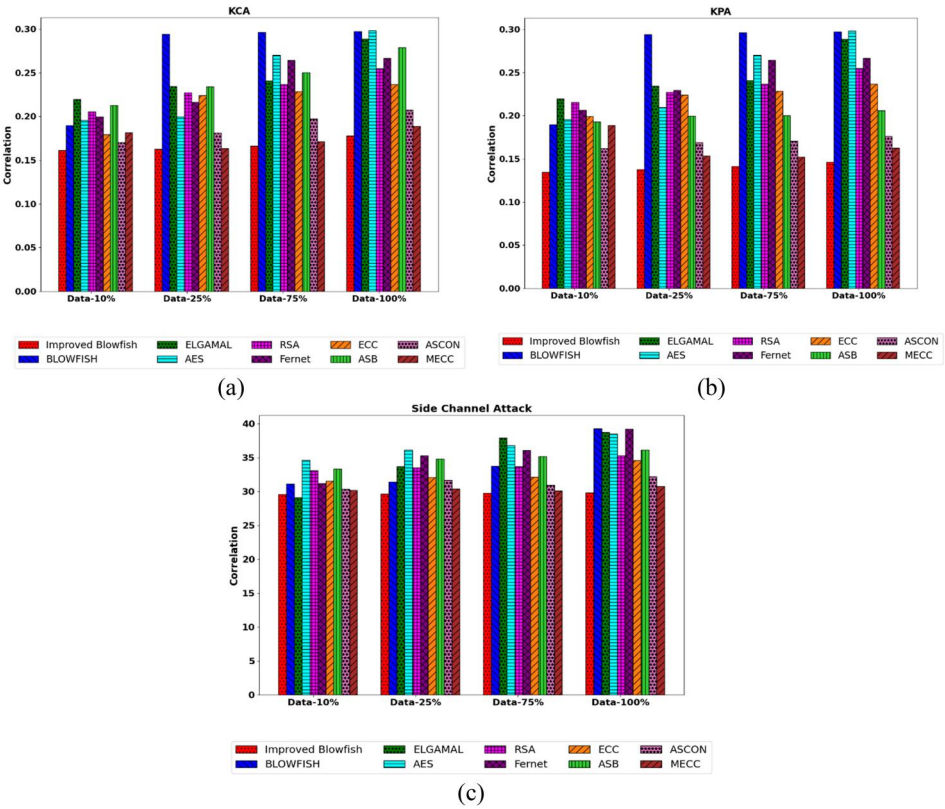

Figure 11. Attack analysis on improved blowfish and conventional methods (a) KCA, (b) KPA, and (c) SCA.

decryption of selected ciphertexts, aiming to reveal details about the secret key or decrypt further ciphertexts. In this context, the Improved Blowfish approach exhibits a CCA attack rate of 0.147 at a data variation of 10%, meanwhile, other methods such as Blowfish, Elgamal, ASCON (Belfqih and Abdellaoui 2025), AES (Seo and Park 2024), AES, RSA, Fernet, ECC (Ryu et al. 2022), ASB (Kim et al. 2023), and MECC (Sriramulu 2025) recorded the highest CCA attack ratings. An adversary can obtain the encryption of certain plaintexts by a cryptographic attack known as a CPA, which gives them knowledge about the encryption scheme and possibly the secret key. For data variation at 100%, the Improved Blowfish approach demonstrated the minimal CPA rate of 0.156. Conversely, traditional methods exhibited higher CPA ratings: Blowfish = 0.297, Elgamal = 0.288, ASCON (Belfqih and Abdellaoui 2025) = 0.241, AES (Seo and Park 2024) = 0.211, AES = 0.298, RSA = 0.254, Fernet = 0.266, ECC (Ryu et al. 2022) = 0.236, ASB (Kim et al. 2023) = 0.298, and MECC (Sriramulu 2025) = 0.177.

Unauthorized communication interception allows adversaries to monitor or listen in on information sent between parties without the required authorization. This is known as an EDA attack. Mainly, the Improved

Blowfish method showcased its superiority by achieving the least EDA rate of 28.792 when subjected to a data variation of 25%. This highlights its robustness in mitigating unauthorized interception of communication. Additionally, compared to conventional strategies, which yielded higher EDA ratings, the Improved Blowfish approach demonstrates its efficacy in enhancing security measures. An adversary purposefully introduces mistakes or flaws into a system in order to jeopardize its confidentiality, availability, or integrity. This type of attack is known as an FIA attack. During the evaluation of Figure 10, it became evident that the Improved Blowfish scheme displayed diminishing FIA ratings with decreasing data variation. Notably, the Improved Blowfish approach consistently generated the least FIA ratings compared to conventional methods. Specifically, the FIA ratings for the Improved Blowfish approach are 29.058, 29.433, 29.919, and 29.980, respectively.

Continuing the examination of the attack analysis, it's noteworthy to observe that the performance of both the Improved Blowfish scheme and conventional methods across different attack scenarios is depicted in Figure 11. The KCA and KPA are cryptographic exploits aimed at compromising encryption systems. In a KCA attack, adversaries exploit correlations between specific aspects of the cryptographic key and observable data to deduce or compromise the key. Conversely, in a KPA attack, adversaries possess samples of both the plaintext and its corresponding encrypted form, aiming to deduce the encryption key or uncover patterns in the encryption algorithm. At a data variation of 75%, the Improved Blowfish method demonstrated superior performance with the lowest KCA and KPA scores of 0.166 and 0.141, respectively. In comparison, other methods, including Blowfish, Elgamal, ASCON (Belfqih and Abdellaoui 2025), AES (Seo and Park 2024), AES, RSA, Fernet, ECC (Ryu et al. 2022), ASB (Kim et al. 2023), and MECC (Sriramulu 2025) demonstrated significantly higher KCA ratings. An SCA is a kind of attack that uses inadvertent information breaches, including power usage or electromagnetic emissions, to deduce sensitive data or cryptographic keys. Especially at a data variation of 100%, the SCA attack value of the Improved Blowfish scheme is recorded at 29.843, whereas conventional methods like Blowfish, Elgamal, ASCON (Belfqih and Abdellaoui 2025), AES (Seo and Park 2024), AES, RSA, Fernet, ECC (Ryu et al. 2022), ASB (Kim et al. 2023), and MECC (Sriramulu 2025) displays higher SCA ratings of 39.285, 38.753, 32.54, 38.519, 38.519, 35.293, 39.234, 34.563, 36.131 and 30.795, respectively. The results of the analysis revealed that the Improved Blowfish authentication model consistently achieved lower attack ratings compared to conventional methods across all evaluated attack scenarios and levels of data variation. This improvement is primarily attributed to the implementation of an IKM

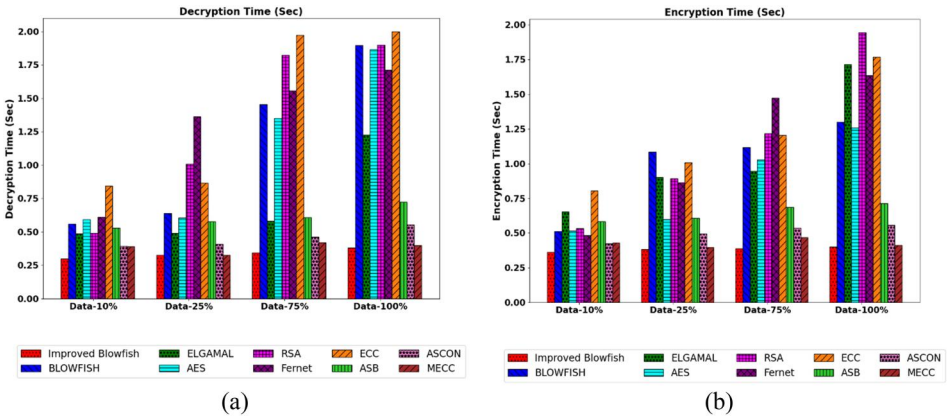

Figure 12. Validation on improved blowfish and conventional strategies (a) decryption time and (b) encryption time.

Process during the login phase and the incorporation of EIFC throughout the authentication phase. Additionally, the adoption of a Hybrid Optimization Algorithm for key generation significantly enhances the robustness and efficiency of security measures. These advancements solidify the superiority of the Improved Blowfish approach in defending against potential threats and ensuring enhanced security within the metaverse environment.

Analysis on Encryption and Decryption Time

Encryption time refers to the duration required to convert plaintext into ciphertext using cryptographic algorithms, while decryption time denotes the duration needed to reverse this process, transforming ciphertext back into plaintext within a cryptographic system. Figure 12a and 12b provide a detailed examination of the decryption and encryption time for both the Improved Blowfish method and conventional strategies, offering valuable insights into their performance within the Avatar-Authenticated Metaverse Environment. A critical aspect of an efficacious authentication approach is the ability to minimize both encryption and decryption time. Particularly, at a data variation of 75%, the Improved Blowfish approach demonstrated the shortest decryption time of 0.346 s, outperforming conventional methods including Blowfish, Elgamal, ASCON (Belfqih and Abdellaoui 2025), AES (Seo and Park 2024), AES, RSA, Fernet, ECC (Ryu et al. 2022), ASB (Kim et al. 2023), and MECC (Sriramulu 2025). This highlights the efficiency of the Improved Blowfish method in decrypting data within the Avatar-Authenticated Metaverse Environment. Additionally, the Improved Blowfish method demonstrated the most efficient encryption time at 0.362 s at a data variation of 10%. Conversely, conventional methods such as

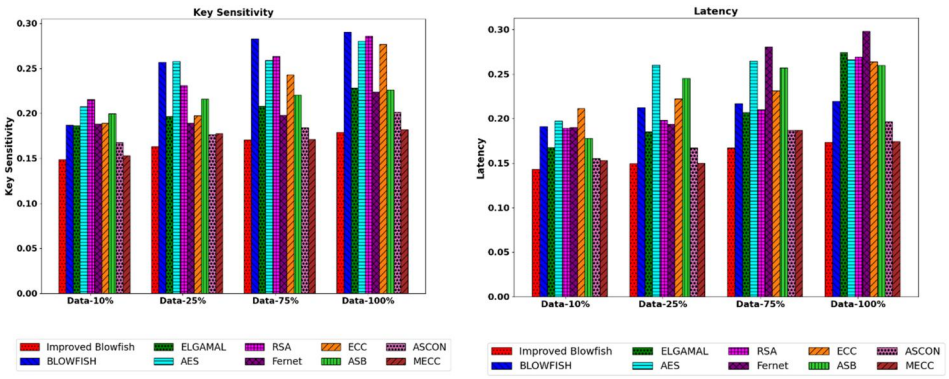

Figure 13. Validation on improved blowfish and conventional methods (a) key sensitivity and (b) latency.

Blowfish (0.514 s), Elgamal (0.655 s), ASCON (Belfqih and Abdellaoui 2025) (0.352 s), AES (Seo and Park 2024) (0.517 s), AES (0.517 s), RSA (0.532 s), Fernet (0.484 s), ECC (Ryu et al. 2022) (0.803 s), ASB (Kim et al. 2023) (0.582 s), and MECC (Sriramulu 2025) (0.430 s) recorded comparatively longer encryption times. Therefore, the analysis of encryption and decryption times in the Avatar-Authenticated Metaverse Environment underscores the superiority of the Improved Blowfish approach over conventional methods. This enhancement is primarily attributed to the EIFC throughout the authentication phase and the utilization of a Hybrid Optimization Algorithm for key generation. These enhancements collectively contribute to reduced encryption and decryption times, thus enhancing the efficiency and performance of the encryption process in the metaverse environment.

Analysis on Key Sensitivity and Latency

Key sensitivity in authentication signifies the degree to which cryptographic keys are vulnerable to compromise, underscoring the need for stringent key management practices to safeguard against security breaches. Figure 13a illustrates the comparison of key sensitivity analysis between the Improved Blowfish method and conventional approaches for the Avatar-Authenticated Metaverse Environment. Minimizing key sensitivity ratings is essential for establishing an effective authentication protocol in metaverse environments. In particular, the Improved Blowfish model achieved a lower key sensitivity rate of 0.178 (data variation = 100%), while conventional strategies (Blowfish, Elgamal, ASCON (Belfqih and Abdellaoui 2025), AES (Seo and Park 2024), AES, RSA, Fernet, ASB (Kim et al. 2023), and MECC (Sriramulu 2025)) scored higher key sensitivity ratings, ranging from 0.182 to 0.290. Latency in an authentication scheme refers to the time delay from initiation to completion of the authentication process, essential for ensuring

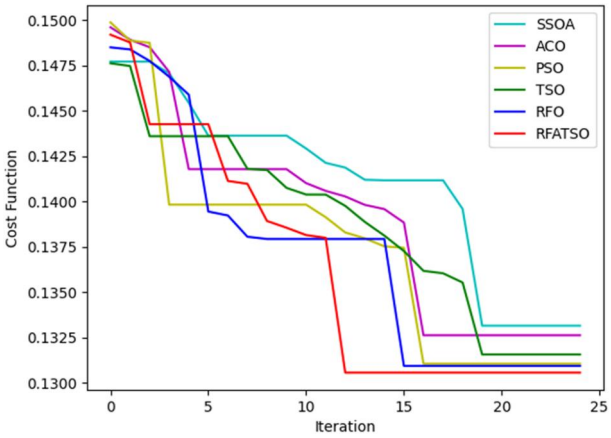

Figure 14. Convergence analysis on RFATSO and conventional methods.

swift and efficient access to resources while verifying user identity or access credentials. Figure 13b explains the latency analysis conducted on both Improved Blowfish and conventional methodologies for the Avatar-Authenticated Metaverse Environment. At a data variation of 75%, the Improved Blowfish scheme achieves a latency of 0.167. Despite this, Blowfish, Elgamal, ASCON (Belfqih and Abdellaoui 2025), AES (Seo and Park 2024), AES, RSA, Fernet, ECC (Ryu et al. 2022), ASB (Kim et al. 2023), and MECC (Sriramulu 2025) recorded the lowest latency ratings of 0.216, 0.207, 0.175, 0.264, 0.210, 0.280, 0.231, 0.257 and 0.187, respectively. This superiority is evident in the consistently low levels of both key sensitivity and latency observed in the Improved Blowfish scheme, highlighting its effectiveness in enhancing security and performance compared to traditional approaches.

Convergence Analysis

The convergence analysis of the RFATSO method is compared with that of SSOA, ACO, PSO, TSO and RFO for Avatar-Authenticated Metaverse Environment, as illustrated in Figure 14. Furthermore, the analysis extends to different numbers of iterations. In the initial (0th) iteration, all algorithms exhibited higher cost ratings. However, as the iterations progressed, the cost ratings decreased. Nonetheless, the RFATSO scheme consistently achieved lower cost values compared to conventional methodologies. At the 25th iteration, the RFATSO scheme notably attained the lowest cost rate of 0.1305, whereas SSOA, ACO, PSO, TSO, and RFO registered higher cost ratings, with values of 0.1346, 0.1337, 0.1319, 0.1326, and 0.1314, respectively. Overall, these findings highlight the efficacy of the RFATSO approach in enhancing authentication protocols and optimizing cost functions within the metaverse environment.

Performance Analysis of the Improved Blowfish over Traditional Methods by Key Variation

The performance analysis presented in Figure 15 highlights the effectiveness of the Improved Blowfish algorithm over traditional encryption methods, including Blowfish, ElGamal, ASCON, AES, RSA, Fernet, ECC, and ASB by varying key sizes (16, 32, 64, and 128 bits) and evaluating against several attack vectors and performance metrics. Across all measures, the Improved Blowfish consistently shows lower correlation rates, indicating higher resistance to cryptanalytic attacks. In the case of Chosen Ciphertext Attack (CCA), the proposed model shows the lowest correlation of 0.125 at key size 128, significantly outperforming Blowfish 0.148 and RSA 0.187. For Chosen Plaintext Attack (CPA), Improved Blowfish achieves a correlation of 0.125, while AES and ElGamal reach higher values of 0.146 and 0.184 respectively. Under Known Ciphertext Attack (KCA), the Improved Blowfish again performs best with a correlation rate of 0.125 at 128 key size bits, compared to ECC 0.187. Regarding KPA, the proposed algorithm delivers a strong performance with a rate of 0.121, much lower than ASCON (0.127) and Fernet (0.223). In EDA, Improved Blowfish maintains an optimal value of 0.120, whereas RSA and ElGamal show variability with values of 0.128 and 0.135. For FIA, the model resists data tampering effectively with a correlation rate of 0.152, while traditional Blowfish and ASB register 0.165 and 0.235 respectively. In terms of Side-Channel Attack (SCA), the proposed approach demonstrates minimal vulnerability, achieving a correlation rate of 0.121 at key size 128. Finally, for key sensitivity, the Improved Blowfish algorithm exhibits strong performance with a rate of 0.123, indicating stable encryption behavior, while conventional algorithms like RSA and ECC lag behind at 0.129 and 0.196. Overall, the findings confirm that the Improved Blowfish algorithm offers a robust and consistent cryptographic solution across multiple security metrics and varying key lengths.

The analysis of encryption and decryption time at 16-bit key variation presented in Table 2 shows that the Improved Blowfish algorithm achieves the fastest performance, with both encryption and decryption times at just 0.003 s, significantly outperforming all other methods. Traditional Blowfish shows the slowest times, with 0.685 s for encryption and 1.509 s for decryption, making it inefficient for time-sensitive applications. ElGamal and ECC exhibit moderate performance, with encryption times of 0.016 and 0.013 s respectively. AES and RSA show relatively higher encryption times of 0.193 and 0.134 s, with decryption times of 0.103 and 0.056 s. Fernet, while slightly faster, still lags behind the proposed method with 0.149 s of encryption time. ASCON and ASB also perform better than conventional algorithms, with encryption times of 0.051 and 0.099 s, but are still noticeably

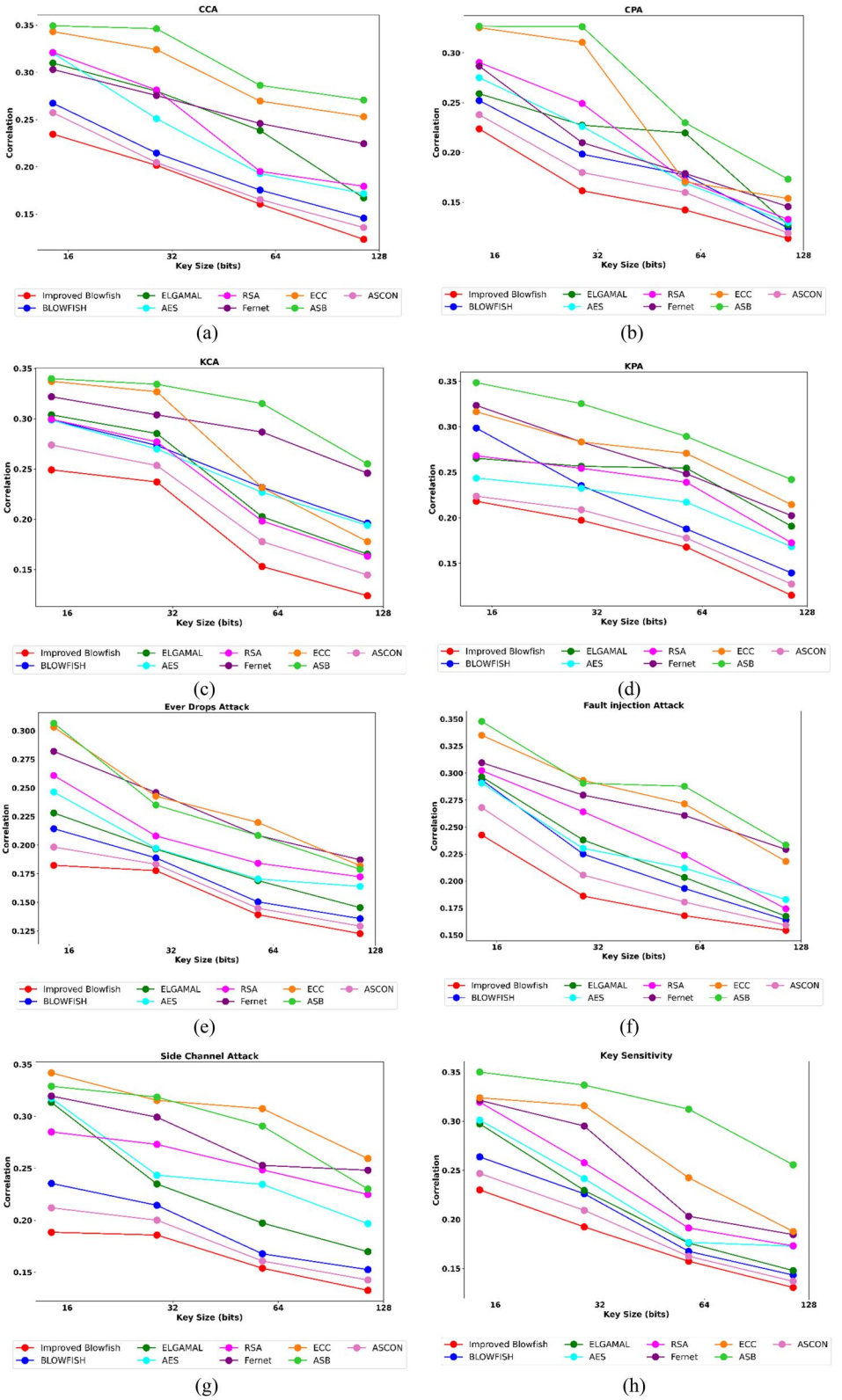

Figure 15. Performance analysis of the improved blowfish algorithm over conventional models by varying the key sizes (a) CCA, (b) CPA, (c) KCA, (d) KPA, (e) EDA, (f) FIA, (g) SCA, and (h) key sensitivity.

Table 2. Analysis of encryption and decryption time at 16-bit key variation.

Methods	Encryption time	Decryption time
Improved Blowfish	0.003	0.003
BLOWFISH	0.685	1.509
ELGAMAL	0.016	0.051
AES	0.193	0.103
RSA	0.134	0.056
FERNET	0.149	0.042
ECC	0.013	0.049
ASB	0.099	0.049
ASCON	0.051	0.022

slower than Improved Blowfish. Overall, the proposed model demonstrates superior efficiency, making it ideal for resource-constrained environments.

Statistical Study on Key Sensitivity

The detailed statistical analysis aims to rigorously evaluate the effectiveness of different approaches, with a focus on minimizing key sensitivity across various metrics. The goal is to ensure highly precise outcomes through a meticulous evaluation process. This thorough examination involves scrutinizing key statistical metrics, including "Best, Minimum, Worst, Maximum, and Standard Deviation." By assessing these fundamental statistical measures, the analysis provides a comprehensive understanding of the models' performance in estimating the Avatar-Authenticated Metaverse Environment. Table 3 provides a detailed statistical analysis comparing various aspects of the Improved Blowfish method with those of Blowfish, Elgamal, AES, RSA, Fernet, ASB (Kim et al. 2023), ASCON (Belfqih and Abdellaoui 2025), AES (Seo and Park 2024), and MECC (Sriramulu 2025) in the context of the avatar-authenticated metaverse environment. This analysis encompasses key sensitivity measures, offering valuable insights into the comparative performance of each approach. Considering the best statistical metric, the key sensitivity of the Improved Blowfish scheme is recorded at 0.179. However, conventional schemes obtained the highest key sensitivity ratings, with values such as Blowfish = 0.290, Elgamal = 0.228, ASCON (Belfqih and Abdellaoui 2025)= 0.201, AES (Seo and Park 2024)= 0.280, AES = 0.280, RSA = 0.286, Fernet = 0.224, ECC (Ryu et al. 2022)= 0.277, ASB (Kim et al. 2023)= 0.226, and MECC (Sriramulu 2025)= 0.182, respectively. Additionally, for the mean statistical metric, the Improved Blowfish scheme achieved the lowest sensitivity rate of 0.165, whilst Blowfish, Elgamal, ASCON (Belfqih and Abdellaoui 2025), AES (Seo and Park 2024), AES, RSA, Fernet, ECC (Ryu et al. 2022), ASB (Kim et al. 2023), and MECC (Sriramulu 2025) registered higher key sensitivity ratings.

Table 3. Statistical assessment on key sensitivity.

Statistical metrics	Best	Mean	Standard deviation	Worst	Median
Improved Blowfish	0.179	0.165	0.011	0.149	0.167
Blowfish	0.290	0.254	0.041	0.187	0.270
Elgamal	0.228	0.205	0.015	0.186	0.202
AES	0.280	0.251	0.027	0.208	0.259
RSA	0.286	0.249	0.027	0.216	0.247
Fernet	0.224	0.200	0.014	0.188	0.194
ECC (Ryu et al. 2022)	0.277	0.227	0.035	0.189	0.220
ASB (Kim et al. 2023)	0.226	0.216	0.010	0.199	0.218
ASCON (Belfqih and Abdellaoui 2025)	0.182	0.180	0.012	0.168	0.201
MECC (Sriramulu 2025)	0.182	0.171	0.011	0.153	0.174

Conclusion

This research presented a comprehensive and secure avatar-authenticated metaverse environment tailored to enhance e-learning platforms by leveraging cloud computing. The proposed framework introduces several key innovations that collectively strengthen authentication, data privacy, and communication integrity. First, an Improved Key Management process was introduced during the login phase, ensuring mutual authentication between users and CSPs. This was achieved through an improved Blowfish key-based encryption, incorporating a novel XOR-based encryption mechanism that utilizes a chaotic key generated from a modified cubic map, thereby significantly increasing resistance to unauthorized access. Second, an Enhanced Information Flow Control mechanism was proposed, incorporating an obfuscation process to safeguard avatar-to-avatar interactions within the metaverse. The innovation lies in the use of a proxy-based encryption scheme, where avatar data is encrypted using the improved Blowfish key (kb) *via* obfuscation, effectively elevating the complexity and confidentiality of information flow. Third, the RFATSO algorithm was introduced, which synergizes the exploration strengths of TSO and RFO. This hybrid optimization technique enhanced the selection of optimal sub-keys during the encryption process by refining the search space in both spiral foraging and parabolic foraging phases, thereby improving convergence accuracy, robustness, and overall security efficiency. The framework is designed for lightweight implementation, making it suitable for resource-constrained metaverse devices such as VR/AR wearables and IoT-enabled systems. Especially at a data variation of 100%, the SCA attack value of the Improved Blowfish scheme is recorded at 29.843, whereas conventional methods like Blowfish, Elgamal, AES, RSA, Fernet, ECC, ASB, and MECC displays higher SCA ratings of 39.285, 38.753, 38.519, 35.293, 39.234, 34.563, 36.131, and 30.795, respectively. Moreover, the system's use of decentralized identifiers (DIDs) and credential-based authentication ensures secure, privacy-preserving user access in dynamic virtual environments. These combined strengths confirm the approach's real-world viability and highlight its

potential for scalable and secure deployment in next-generation metaverse platforms. Furthermore, future research will focus on implementing the proposed approach in a real-time metaverse environment.

Nomenclature

ASB	Authentication Scheme using Blockchain
AES	Advanced Encryption Standard
IKM	Improved Key Management
EIFC	Enhanced Information Flow Control
RFATSO	Red Fox-Adapted Tuna Swarm Optimization algorithm
VR	Virtual Reality
AR	Augmented Reality
IoT	Internet of Things
AI	Artificial Intelligence
DT	Digital Twins
CSP	Cloud Service Provider
ROR	real-or-random model
AVISPA	Automated Validation of Internet Security Protocols and Applications
BAN	Burrows–Abadi–Nikoogadam
ECC	Elliptic Curve Cryptography
OTCE	On-Demand Trusted Computing Environment
RSMS	Reliable and Secure Metaverse Service
GNY	Gong–Needham–Yahalom
EIoT	Energy Internet of Things
AKE	Authenticated Key Exchange
RN	Resource Node
SBAC	Substitution Cipher Access Control
LLAKEP	Low-Latency Authentication and Key Exchange Protocol
MECC	Modified Elliptic Curve Cryptography
DID	Decentralized Identifier
VC	Verifiable credential
CA	Certificate Authority
TSO	Tuna Swarm Optimization
RFO	Red Fox Optimization
RSA	Rivest–Shamir–Adleman

Acknowledgments

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.

Authors Contributions

CRediT: **Vijitha S**: Conceptualization, Methodology, Resources; **Anandan R**: Validation, Visualization.

Disclosure Statement

No potential conflict of interest was reported by the authors.

Funding

This research did not receive any specific funding.

Data Availability Statement

No new data were generated or analyzed in support of this research.

References

Aldweesh, A. 2023. "Enhancing Metaverse Security with Block Chain Authentication: Methods and Analysis." *Computer Integrated Manufacturing Systems* 29: 1–13.

Awan, K. A., I. U. Din, A. Almogren, and B. Seo-Kim. 2023. "Blockchain-Based Trust Management for Virtual Entities in the Metaverse: A Model for Avatar and Virtual Organization Interactions." *IEEE Access* 11: 136370–136394. https://doi.org/10.1109/ACCESS.2023.3337806.

Belfqih, H., and A. Abdellaoui. 2025. "Decentralized Blockchain-Based Authentication and Interplanetary File System-Based Data Management Protocol for Internet of Things Using Ascon." *Journal of Cybersecurity and Privacy* 5 (2): 16. https://doi.org/10.3390/jcp5020016.

Deveci, M., D. Pamucar, I. Gokasar, L. Martinez, M. Köppen, and W. Pedrycz. 2024. "Accelerating the Integration of the Metaverse into Urban Transportation Using Fuzzy Trigonometric Based Decision Making." *Engineering Applications of Artificial Intelligence* 127 (Part A): 107242. https://doi.org/10.1016/j.engappai.2023.107242.

Gong, Y., X. Chang, J. Mišić, V. B. Mišić, and Y. Yao. 2023. "RSMS: Towards Reliable and Secure Metaverse Service, Provision." 73: 17430–17442.

Hassan, U., Mehmood, Y. Abbas, W. Iqbal, A. Chehri, and J. Iqbal. 2025. "PRIDA-ME: A Privacy-Preserving, Interoperable and Decentralized Authentication Scheme for Metaverse Environment." *IEEE Open Journal of the Communications Society* 6: 493–515. https://doi.org/10.1109/OJCOMS.2024.3523518.

Joo-Eon, J. 2021. "The Effects of User Experience-Based Design Innovativeness on User-Metaverse Platform Channel Relationships in South Korea." *Journal of Distribution Science* 19 (11): 81–90.

Joshi, S., and P. J. Pramod. 2023. "A Collaborative Metaverse Based A-La-Carte Framework for Tertiary Education (CO-MATE)." *Heliyon* 9 (2): e13424. https://doi.org/10.1016/j.heliyon.2023.e13424.

Khowaja, S. A., K. Dahri, M. A. Jarwar, and I. H. Lee. 2023. "Spike Learning Based Privacy Preservation of Internet of Medical Things in Metaverse." *IEEE Journal of Biomedical and Health Informatics* 29: 8224–8232.

Kim, M., J. Oh, S. Son, Y. Park, J. Kim, and Y. Park. 2023. "Secure and Privacy-Preserving Authentication Scheme Using Decentralized Identifier in Metaverse Environment." *Electronics* 12 (19): 4073. https://doi.org/10.3390/electronics12194073.

Le, H. D., V. T. Truong, D. N. M. Hoang, and L. B. Le. 2023. "MetaCrowd: Blockchain-Empowered Metaverse via Decentralized Machine Learning Crowdsourcing." https://doi.org/10.1109/WCNC57260.2024.10570920

Li, W., J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya. 2021. "Blockchain-Based Trust Management in Cloud Computing Systems: A Taxonomy, Review and Future Directions." *Journal of Cloud Computing* 10 (1): 2021. https://doi.org/10.1186/s13677-021-00247-5.

Manikandasaran, S. S., L. Arockiam, and P. D. S. K. Malarchelvi. 2019. "MONcrypt: A Technique to Ensure the Confidentiality of Outsourced Data in Cloud Storage." *International Journal of Information and Computer Security* 11 (1): 1. https://doi.org/10.1504/IJICS.2019.096846.

Matthew, K. M., A. Q. Muhammed, and V. Varadarajan. 2019. "An Improved Key Management Scheme in Cloud Storage." *International Journal of Advanced Intelligence Paradigms* 14 (3/4): 197–203.

Oh, J., M. Kim, Y. Park, and Y. Park. 2023. "A Secure Content Trading for Cross-Platform in the Metaverse With Blockchain and Searchable Encryption." *IEEE Access*11: 120680–120693. https://doi.org/10.1109/ACCESS.2023.3328232.

Parihar, V., and A. Kulshrestha. 2016. "Blowfish Algorithm: A Detailed Study." *International Journal For Technological Research In Engineering* 3 (9): 2347–4718.

Połap, D., and M. Woźniak. 2021. "Red Fox Optimization Algorithm." *Expert Systems with Applications* 166: 114107. https://doi.org/10.1016/j.eswa.2020.114107.

Quilala, T. F. G., A. M. Sison, and R. P. Medina. 2018. "Modified Blowfish Algorithm." *Indonesian Journal of Electrical Engineering and Computer Science* 12 (1): 38–45. https://doi.org/10.11591/ijeecs.v12.i1.pp38-45.

Ren, Y., Z. Lv, N. N. Xiong, and J. Wang. 2023. "HCNCT: A Cross-Chain Interaction Scheme for the Blockchain-Based Metaverse." *ACM Transactions on Multimedia Computing Communications and Applications* 20 (7), 1–23.

Ryu, J., S. Son, J. Lee, Y. Park, and Y. Park. 2022. "Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain." *IEEE Access* 10: 98944–98958. https://doi.org/10.1109/ACCESS.2022.3206457.

Sánchez-Adame, L. M., G. Monroy-Rodríguez, S. Mendoza, D. Decouchant, and A. P. Mateos-Papis. 2023. "Framework for Ethically Designed Microtransactions in the Metaverse." *IEEE Access* 11: 140687–140700. https://doi.org/10.1109/ACCESS.2023.3341057.

Seo, J., and S. Park. 2024. "SBAC: Substitution Cipher Access Control Based on Blockchain for Protecting Personal Data in Metaverse." *Future Generation Computer Systems* 151: 85–97. https://doi.org/10.1016/j.future.2023.09.022.

Sriramulu, V. 2025. "Blockchain Based Decentralized Identifier in Metaverse Environment for Secure and Privacy-Preserving Authentication with Improved Key Management and Cryptosystem." In Communication. https://doi.org/10.1007/s12083-025-02020-w

Tewfik, B., D. Nacira, and Y. Amina. 2022. "Some Improved Chaotic Maps Applied to image encryption." Paper presented at 1st International Conference on Engineering, Natural and Social Sciences, Konya, Turkey, December 20–23.

Truong, V. T., and L. B. Le. 2023. "MetaCIDS: Privacy-Preserving Collaborative Intrusion Detection for Metaverse Based on Blockchain and Online Federated Learning." *IEEE Open Journal of the Computer Society* 4: 253–266. https://doi.org/10.1109/OJCS.2023.3312299.

Wang, H., H. Li, A. Smahi, F. Zhao, Y. Yao, C. C. Chan, S. Wang, W. Yang, and S. Y. R. Li. 2023. "MIS: A Multi-Identifier Management and Resolution System Based on Consortium Blockchain in Metaverse." arXiv Preprint arXiv 2301.03529. https://doi.org/10.1145/3597641

Wang, M., C. Xu, X. Chen, L. Zhong, Z. Wu, and D. O. Wu. 2021. "BC-Mobile Device Cloud: A Blockchain-Based Decentralized Truthful Framework for Mobile Device Cloud." *IEEE Transactions on Industrial Informatics* 17 (2): 1208–1219. https://doi.org/10.1109/TII.2020.2983209.

Xie, L., T. Han, H. Zhou, Z. R. Zhang, B. Han, and A. Tang. 2021. "Tuna Swarm Optimization: A Novel Swarm-Based Metaheuristic Algorithm for Global Optimization." *Computational Intelligence and Neuroscience* 2021 (1): 9210050. https://doi.org/10.1155/2021/9210050.

Xu, M., Y. Guo, Q. Hu, Z. Xiong, D. Yu, and X. Cheng. 2023. "A Trustless Architecture of Blockchain-Enabled Metaverse." *High-Confidence Computing* 3 (1): 100088. https://doi.org/10.1016/j.hcc.2022.100088.

Yang, K., Z. Zhang, Y. Tian, and J. Ma. 2022. "A Secure Authentication Framework to Guarantee the Traceability of Avatars in Metaverse." Cryptography and Security arXiv: 2209.08893v3 [csCR] 6. https://doi.org/10.1109/TIFS.2023.3288689

Zhang, Q., Z. Xiong, J. Zhu, S. Gao, and W. Yang. 2023. "A Privacy-Preserving Auction Mechanism for Learning Model as an NFT in Blockchain-Driven Metaverse." *ACM Transactions on Multimedia Computing Communications and Applications* 20(7), 1–24.

Zhang, X., X. Huang, H. Yin, J. Huang, S. Chai, B. Xing, X. Wu, and L. Zhao. 2022. "Llakep: A Low-Latency Authentication and Key Exchange Protocol for Energy Internet of Things in the Metaverse Era." *Mathematics* 10 (14): 2545. https://doi.org/10.3390/math10142545.

Zhang, Z., Z. Yang, X. Du, W. Li, X. Chen, and L. Sun. 2021. "Tenant-Led Ciphertext Information Flow Control for Cloud Virtual Machines." *IEEE Access* 9: 15156–15169. https://doi.org/10.1109/ACCESS.2021.3051061.