future internet

MDPI

Article

Blockchain-Enabled Secure and Interoperable Authentication Scheme for Metaverse Environments

Sonali Patwe * and Sunil B. Mane

Department of Computer Science and Engineering, COEP Technological University, Pune 411005, India
* Correspondence: ssp21.comp@coeptech.ac.in

Abstract: The metaverse, which amalgamates physical and virtual realms for diverse social activities, has been the focus of extensive application development by organizations, research institutes, and companies. However, these applications are often isolated, employing distinct authentication methods across platforms. Achieving interoperable authentication is crucial for when avatars traverse different metaverses to mitigate security concerns like impersonation, mutual authentication, replay, and server spoofing. To address these issues, we propose a blockchain-enabled secure and interoperable authentication scheme. This mechanism uniquely identifies users in the physical world as well as avatars, facilitating seamless navigation across verses. Our proposal is substantiated through informal security analyses, employing automated verification of internet security protocols and applications (AVISPA), the real-or-random (ROR) model, and Burrows–Abadi–Needham (BAN) logic and showcasing effectiveness against a broad spectrum of security threats. Comparative assessments against similar schemes demonstrate our solution's superiority in terms of communication costs, computation costs, and security features. Consequently, our blockchain-enabled, interoperable, and secure authentication scheme stands as a robust solution for ensuring security in metaverse environments.

Keywords: authentication; metaverse; blockchain; interoperability; decentralized identity; security

Citation: Patwe, S.; Mane, S.B. Blockchain-Enabled Secure and Interoperable Authentication Scheme for Metaverse Environments. *Future Internet* **2024**, *16*, 166. https://doi.org/10.3390/fi16050166

Academic Editor: Qiang Qu

Received: 31 January 2024
Revised: 25 April 2024
Accepted: 8 May 2024
Published: 11 May 2024

1. Introduction

The metaverse is rapidly evolving, with users witnessing continuous advancements and transformations with each passing day. This dynamic and ever-changing technology reflects ongoing developments, innovations, and adaptations that shape the metaverse into a more intricate and sophisticated digital realm. The term metaverse is a fusion of the words "meta" (meaning beyond) and "verse" (meaning world). The concept encompasses a novel category of internet applications and social structures extending beyond the physical world. Metaverse technology seamlessly integrates the physical and virtual worlds that traditionally exist independently. Coined in 1992 by Neal Stephenson in his science fiction book "Snow Crash," the term describes a virtual environment running parallel to the physical world that is facilitating work and communication through digital avatars [1].

The metaverse constructs a virtual world that replicates or enhances the physical world, providing a space where users can create or consume content, collaborate, engage in trade, or socialize. It aims to create a highly immersive environment that harmoniously blends virtual and physical existences. Metaverse applications leverage a combination of technologies, including the Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (ML), 5G/6G, Web 3.0, 3D Design, Mixed Reality (MR), Virtual Reality (VR), and Augmented Reality (AR). Through these technologies, the metaverse overcomes the limitations of the physical world, empowering meta-persons to perform tasks that would be otherwise impossible in reality [2,3].

Avatars are the virtual representations of physical users in the physical world. They mirror real-world features, gestures, and behaviors of users. Avatars possess virtual identities, allowing them to be recognized by devices and other avatars within the metaverse.

Within the metaverse, users generate virtual avatars as digital representations of themselves, enabling access to various services. However, the current metaverse allows users to create avatars without real-world identity verification, opening possibilities for malicious activities such as identity theft, impersonation, replay, server spoofing, replay-virtual-asset fraud, stalking, and privacy threats. Users also exchange information with third parties, but unmapped identities pose challenges. For dealing with unmapped identities, maintaining consistency between virtual and physical identities is crucial. A robust authentication scheme is essential to ensure user safety, especially given the lack of direct means for users to verify avatar identities [3,4].

The existing metaverse platforms rely on passwords, making them vulnerable, and providing extensive personal information to service providers poses privacy risks. Moreover, these platforms provide avatar authentication in silos although it is centralized in nature. The authentication mechanism in one platform is completely different from that in another platform. So, there is a need for interoperable identity mechanisms. If an avatar wants to traverse from one virtual world to another, then the different identity mechanisms used by different platforms affects the immersive experience, making interoperability impossible [5].

In addition, there is no mapping available between a physical-user identity and an avatar identity in a virtual world. Considering all of these challenges, there is a serious need to implement a decentralized and interoperable identity mechanism that will address identity-related security issues such as impersonation, replay, server spoofing, mutual authentication, man-in-the-middle attack, etc. [6,7].

To address these issues, in this paper we propose a blockchain-enabled secure and interoperable authentication scheme to enhance security and protect users from diverse identity-related threats. Blockchain is a decentralized ledger technology that enables users to store transactions in a block in an immutable way. Each block is connected to the next one to form a chain of blocks. The blockchain is constructed through the linkage of blocks, which is achieved by storing the hash of the previous block in the subsequent one. Originating with the inception of Bitcoin, blockchain technology has found application in diverse scenarios. The integration of cryptography techniques within a blockchain ensures the security of transactions, rendering the entire system inherently secure and resistant to tampering [7].

In this paper, we have used blockchain to develop an authentication mechanism that will prevent identity-related attacks within a metaverse and solve the lack-of-interoperability issue among various metaverses. This authentication scheme will bring uniformity into the authentication of avatars, physical users, and devices across multiple metaverse platforms. Considering the massive increase in the number of metaverse applications currently being developed, it is essential that avatars are allowed to navigate securely across virtual worlds. Also, an avatar should be mapped to the physical identity of the user through identifiers such as such as an identity card, social security number, government identification number, etc. In the metaverse environment, avatars interact not just with other avatars but also with other devices. So, there is a need to devise a uniform identification mechanism that can be used for the identification and authentication of avatars, devices, and physical users. It could be used across multiple metaverses as well as in the physical world. For this reason, in this paper, we have proposed a blockchain-enabled secure and interoperable metaverse identity (Meta-ID) mechanism.

1.1. Contribution

The primary contributions of this paper include the following:

- We propose a system model to ensure interoperable and secure authentication among avatars, users, and devices that can address various identity-related security issues such as impersonation, server spoofing, lack of interoperability, mutual-authentication issues, replay, server spoofing, man-in-the-middle attacks, etc.

- We propose a blockchain-based decentralized authentication scheme, using a unique Meta-ID, called the Metaverse interoperable Identity Framework (MIF), which will map physical-user identities with avatar-virtual identities and establish a uniform identification mechanism across metaverses.
- We conduct an informal analysis to validate the proposed scheme's ability to safeguard against diverse attacks, encompassing impersonation, server spoofing, replay, man-in-the-middle, and mutual-authentication attacks. Furthermore, we demonstrate the scheme's capability to foster interoperability and facilitate seamless navigation across different metaverse environments.
- The security of the proposed system is evaluated through a combination of informal and formal analyses, including examinations using Burrows–Abadi–Nikoogadam (BAN) logic, the real-or-random (RoR) model, and the automated validation of internet security protocols and applications (AVISPA) simulation tool.
- Additionally, we conduct a comparative assessment of performance and security characteristics against relevant existing works, demonstrating the superiority of the proposed scheme.

1.2. Organization

This paper is structured as follows: in Section 2, we examine currently available authentication schemes suitable for the metaverse environment. Section 3 introduces significant preliminary matters. Section 4 covers the modeling of the proposed authentication scheme and the adversary model. Section 5 covers details of the scheme like user and avatar-registration phases, login, mutual authentication, etc. Section 6 conducts informal and formal security analyses of the proposed scheme, and Section 7 assesses the computation and communication costs in comparison to related works. Lastly, Section 8 summarizes the conclusions and outlines future work.

2. Related Work

When Facebook changed its name to Meta in October 2021 [8], many researchers, organizations and industries started focusing on metaverse applications. Technology is no longer perceived to be limited to gaming and related applications. Many commercial metaverse platforms have evolved in the last few years. Many metaverses are built on Minecraft, Unity, Unreal Engine, Decentraland, Roblox, etc. Apart from that, many non-commercial metaverse environments are being created. However, security is a major concern in such metaverse worlds, as discussed in many papers [9–11].

In ref. [12], K. Yang et al. proposed a secure authentication framework to guarantee the traceability of avatars in the metaverse using a two-factor authentication framework based on chameleon signatures and biometrics. It uses blockchain as a solution for traceability. However, some of the identity-related security issues in metaverse environments are not considered by this framework. For example, cross-metaverse-identity interoperability is not addressed, and server-spoofing attacks are not handled. Also, avatar-to-device mutual authentication is not considered. The framework's communication and computation costs can be reduced further.

In ref. [13], Y. Huang et al. discuss in detail various security- and privacy-related issues in metaverse environments, including personal information leakage, eavesdropping, phishing, broken authentication, and so on. Paper [14] emphasizes the importance of enabling blockchain for various metaverse applications. The potential of blockchain for security and privacy aspects of the metaverse infrastructure is also mapped out in this paper. C. T. Nguyen et al. in ref. [15] proposed a metachain framework for the interoperability of metaverse service providers and metaverse users. They have added a smart contract mechanism and novel sharding scheme to achieve the same outcomes.

In paper [16], Panda et al. propose a secure mutual authentication protocol for IoT and cloud servers based on elliptic curve cryptography. Though the research covers attacks like device privacy, impersonation attacks, replay attacks, password-guessing attacks,

and mutual-authentication attacks, there is scope to improve computational time and computational overheads. Also, the solution is designed for IoT environments and is not specific to cross-metaverse environments. Identity interoperability is also not addressed in the research.

Paper [17] by Li, Y. et al. discussed an authentication protocol based on elliptical curves and bilinear pairs. However, there is scope to improve the computational and communication costs of the protocol. Ryu J. et al. focused in ref. [18] on addressing impersonation, replay, server-spoofing, stolen-smart-device, man-in-the-middle (MITM), and insider attacks. However, identity interoperability is not discussed. Also, avatar-to-device mutual authentication is not in their scope. Kim, M. et al. in paper [19] proposed a blockchain-enabled authentication scheme. Their approach mitigates certain security and privacy concerns in the metaverse environment. In ref. [20], Shen et al. discuss an efficient block-chain-assisted secure device-authentication mechanism, BASA, for cross-domain IIoT.

A comparison of the similar solutions proposed in the literature is as shown in Table 1.

Table 1. Comparison of similar solutions proposed in the literature.

Publication	Security Challenge Addressed	Solution Proposed	What Are We Planning to Address?
[12]	Disguise, impersonation, replay	Secure authentication framework to guarantee the traceability of avatars in metaverse using two-factor authentication framework based on chameleon signature and biometrics.	• Server-spoofing attack not addressed. • Authentication time and computation costs can be reduced further. • Cross-metaverse support to be added. • Avatar-to-device mutual authentication not considered.
[16]	Device privacy, impersonation attack, replay attack, password-guessing attack, mutual authentication	Secure mutual authentication protocol for IoT and cloud servers based on elliptic curve cryptography.	• The solution is designed for the IoT environment and not for the metaverse. • Identity interoperability is not addressed. • Improvement in computational time.
[17]	Impersonation, replay, mutual authentication, centralization	An authentication protocol based on elliptic curves and bilinear pairs.	• Further improvement in computational cost. • Application to real-life scenarios.
[18]	impersonation, replay attack, server spoofing, stolen smart devices, MITM, insider attacks	Mutual authentication scheme using elliptic curve cryptography (ECC) and biometric information.	• Identity interoperability is not addressed. • Avatar-to-device authentication is not considered.
[20]	Cross-domain authentication	Blockchain-Assisted Secure Device Authentication (BASA) for Cross-Domain Industrial IoT.	• Extension to the metaverse environment.

From the literature, it is clear that there is a need to build a secure and interoperable authentication scheme using blockchain for the cross-metaverse platforms that will cover not just avatars but device identity as well. Also, it should map the physical identity of the physical user to the avatar's virtual identities. Such an identity mechanism should not be specific to one platform but should allow meta-persons to navigate across different metaverses. This identity mechanism should address a greater number of identity-related security issues compared to the competitive work available. For this, regarding paper [2,7], we discussed earlier the various identity-related security issues that are found in metaverse environments. We also described a need for interoperability of the identity in cross-metaverse platforms. Also, the scheme should be able to achieve this with minimum computation time and communication costs. To date, there is no authentication scheme that addresses all of these issues. Therefore, we propose a secure and interoperable authentication scheme for metaverse environments.

3. Preliminaries

3.1. Commercial Metaverse Platforms

There are many commercial metaverse platforms available for users to create, collaborate, share, and transact. A commercial metaverse platform serves as a digital landscape for diverse business endeavors, enabling companies to establish a virtual presence and engage with users. Some of the widely used metaverse platforms are Roblox, Minecraft, High Fidelity, and VRChat. Such platforms focus on creating realistic and interactive virtual spaces, offering businesses opportunities for collaboration, events, and customer engagement. Additionally, development platforms like Unity and Unreal Engine play pivotal roles in building and creating immersive metaverse experiences. These platforms empower businesses to design and deploy their virtual environments, thus contributing to the metaverse's evolving landscape [21,22].

3.2. Hyperledger Fabric

Hyperledger Fabric is an open-source blockchain framework designed for enterprise-level solutions. Known for its modular architecture, Hyperledger Fabric provides a flexible and customizable platform for developing permissioned blockchain networks. It facilitates confidential transactions and smart contracts, ensuring privacy and security within business consortia. With its emphasis on scalability, efficiency, and interoperability, Hyperledger Fabric has become a preferred choice for enterprises seeking robust blockchain solutions tailored to their specific needs [23].

3.3. Smart Contracts

Smart contracts are self-executing agreements with the terms of the contract directly written into code. Operating on blockchain technology, these contracts automatically execute and enforce predefined rules without the need for intermediaries. Smart contracts facilitate secure, transparent, and tamper-resistant transactions across various sectors, from finance to supply chains. By automating processes and reducing the risk of fraud, smart contracts enhance efficiency and trust in digital interactions, making them a foundational element of decentralized systems and blockchain networks [24].

4. System Model

The proposed secure and interoperable authentication scheme using blockchain is shown in Figure 1. It demonstrates how Meta-ID will create an interoperable authentication possible and, at the same time, will ensure security across metaverse environments. The system model comprises the following components:

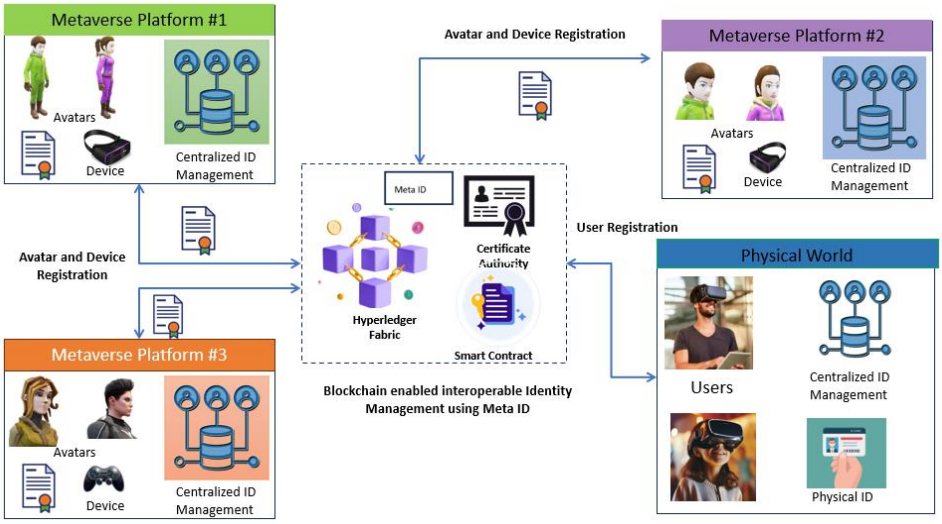

Figure 1. Proposed system model.

- Blockchain: In our system model, we have proposed the use of an enterprise blockchain platform—Hyperledger Fabric. This blockchain platform makes the identity mechanism completely decentralized. All devices, users, and avatars are registered on blockchain and are each assigned a unique ID called Meta-ID. Hyperledger Fabric helps in storing the authentication information securely. The blockchain is not owned by any single entity, making it unbiased, which can help in avoiding insider attacks. Hyperledger Fabric also gives us the flexibility to write our own smart contracts and plug in our own consensus mechanism.
- Metaverse platforms: Most of the metaverse platforms available today implement centralized identity mechanisms. The authentication mechanism on one metaverse platform is different from that on other platforms. In our proposed system, we implement decentralized identity using a blockchain identifier called Meta-ID. The metaverse platforms wanting to enhance identity-related security and to have authentication-mechanism uniformity across metaverses need to join this blockchain network. The blockchain-based Metaverse interoperable Identity Framework (MIF) will bring together multiple virtual and physical worlds.
- Certificate authority: The certificate authority is a trusted component in our system model. It ensures that unique Meta-IDs are assigned to all physical users, meta-persons, and devices. It is also responsible for initialization of the Metaverse interoperable Identity Framework and for syncing with all of the metaverse platforms that are connected to blockchain.
- User: User indicates a physical user like a student, employee, content creator, etc. The user will have an identity in the physical world such as an ID card, student roll number, employee ID, social security number, passport, etc. This physical ID will be mapped in Meta-ID to the virtual ID of an avatar or device. This will ensure that only the legitimate users enter the metaverse. The physical and behavioral attributes of each user will be mapped to an avatar in the virtual world. Other user information like email, phone number, etc., can be collected from the metaverse platform that each user registers on.
- Avatar: An avatar is a virtual representation of a user in the virtual world. Avatars have a unique ID associated with them. A user may create multiple avatars. Avatars are assigned a unique Meta-ID during the avatar-registration process. This helps them in avatar-to-avatar mutual authentication. It also helps in avatar-to-device mutual authentication.
- Device: Devices can be wearable devices that users in the physical world use to interact with virtual world. They can be AR or VR headsets, hand-held devices, smart glasses, or room-sized devices with multiple degrees of freedom. The device is registered against users and avatars. A unique Meta-ID is assigned to the device. This helps to avoid the stealing of devices or hijacking of device information.
- Meta-ID: A Meta-ID is the unique ID used to identify physical users, avatars, and devices across multiple metaverses. It is stored on blockchain to make it secure. Whenever a new avatar is created for the user, a new device is added by the user, the user enters a new metaverse platform, or any physical ID is updated for the user, the Meta-ID will be updated and then broadcast in all associated metaverse platforms to avoid security issues.
- Physical ID: A physical ID is proof that a physical user exists. The existing metaverse platforms consider authentication based on virtual IDs only. To map a physical ID with a virtual ID, in our system model, we collect proof of the Physical ID from the user during registration. Mapping a physical ID with each virtual identity will avoid attacks like avatar impersonation.

Figure 2 shows the low-level design of the Meta-ID.

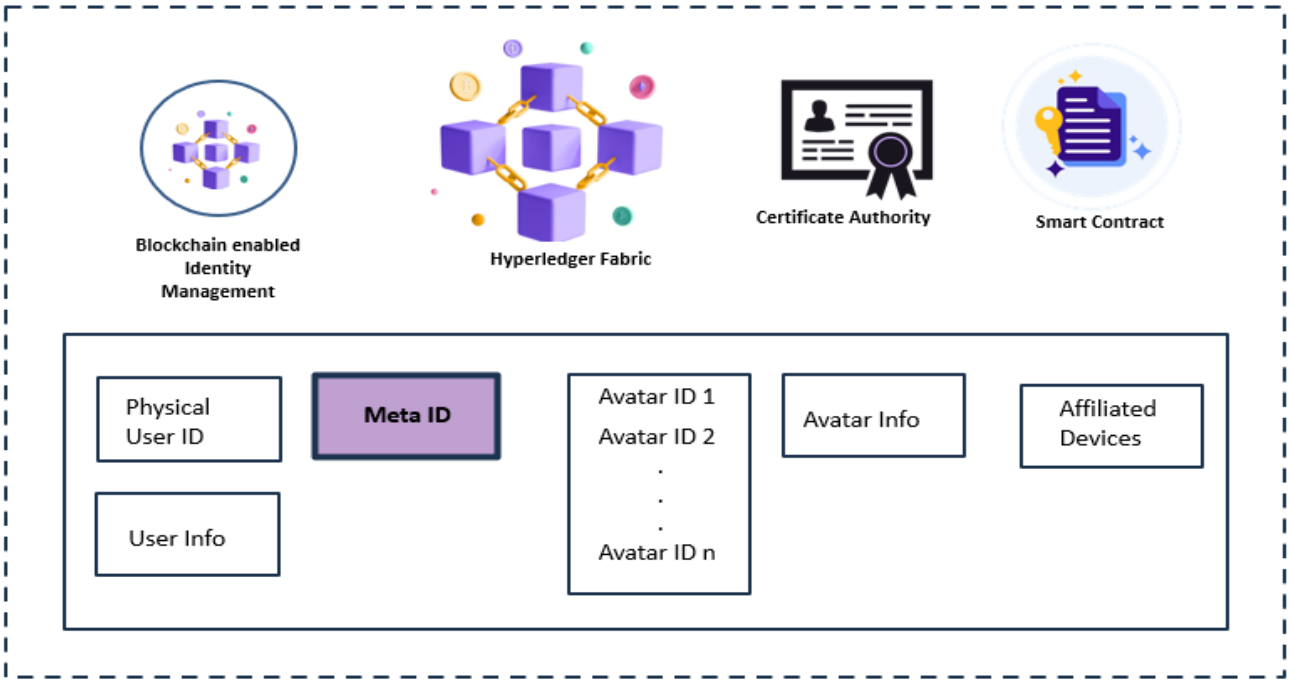

Figure 2. Low-level design with Meta-ID.

The procedural sequences of the proposed scheme are outlined as follows:

- Initialization: In the initialization phase, the CA initializes all of the system parameters, default users, avatars, etc. It syncs up all of the metaverse platforms, and all of the smart contracts are deployed in the MIF.
- User registration: Physical users can choose to register for a metaverse platform. In this phase, a user ID, a password, and other information is collected. The user is synced up with MIF through the metaverse platform server. The CA authorizes the user and then assigns a Meta-ID. This Meta-ID, a public key, and other relevant information about the user is stored in the blockchain for later verification.
- Device registration: A device registration process is required whenever any new device is identified for a user. A device ID, together with a user's physical ID, is sent for registration to the MIF. The MIF maps physical IDs, avatars, and device IDs. MIF verifies a device and assigns a Meta-ID to it.
- Avatar generation: When the user has been registered to the metaverse platform and wants to navigate across the virtual world, avatar generation is required. One physical user might be associated with multiple avatars. An avatar ID is created and mapped to the user's physical ID, and the relevant Meta-ID is assigned to an avatar. Using a public key, a session key, and an avatar ID, the user navigates across multiple metaverses.
- Login: During the user-registration phase, the user is assigned a Meta-ID that can be used in the login and authentication phases to uniquely identify this user. A session key is used during a logged-in session.
- Avatar and device mutual authentication: In the metaverse, avatars and devices can identify and interact with other avatars and devices using a Meta-ID. By using a Meta-ID, avatars and devices can interact not just within the same virtual world but within others as well.

Adversary Model

The widely used "Dolev–Yao (DY) model" [25] is instrumental in examining protocol security. According to this model, an adversary is empowered to eavesdrop, delete, and modify messages transmitted through a public channel, allowing for the execution of various security attacks. These include performing impersonation, replay, and man-in-

the-middle (MITM) attacks; acquiring a user's smart device to extract stored data through power analysis attacks [26–28]; legally creating avatars for impersonation attempts; and potentially functioning as an insider within the platform server. Additionally, we incorporate the more rigorous "Canetti–Krawczyk (CK) model" [29], which surpasses the assumptions of the DY model. Under the CK model, the adversary can acquire ephemeral and long-term values, including random numbers, private and master keys, and secret keys, through a session-hijacking attack. Moreover, the adversary crafts a replica avatar in the metaverse environment to deceive others.

5. Proposed Scheme

In this section, we propose a secure and interoperable Metaverse interoperable Identity Framework (MIF) using blockchain technology for metaverse environments. The proposed scheme is mainly divided into five phases, namely initialization, physical-user setup, device setup, avatar creation, login and authentication, and mutual authentication. The notations used in the proposed scheme are defined in Table 2

Table 2. Notations and their meanings as used in the proposed scheme.

Notation	Description
CA	Certificate authority
PUi	Physical user
MPi	Metaverse platform
PIDi	ID of physical user PUi
PNi	User name of physical user PUi
PWi	Password of physical user PUi
Di	Device ID of physical user PUi
MPS	Metaverse platform server
Ti	Random token for User Ui
Ai	Avatar identity of Ui
Sci	Smart contract for MPi
PKca, PKi	Public key of CA and Ui
Kca, Ki	Private key of CA and Ui
Ski	Session key for user Ui
H(.)	Hash function
$\oplus$	Exclusive OR
| |	Concatenation operation

5.1. Initialization Phase

In the initialization phase, the CA will initialize system parameters. The Metaverse interoperable Identity Framework will connect and sync up with all of the metaverse platforms, MPi, that are connected to it. The CA selects a base point, P, and a private key, Kca. The CA then computes a public key, PKca, as follows: PKca = Kca · P. The system parameters are published as {P, PKca, h(·)}. A sync up with all MPi for default users, PUi, and with all avatars and devices. MIF will deploy all relevant Smart Contracts Sci for all of the metaverse platforms connected to it. The initialization phase is shown in Figure 3.

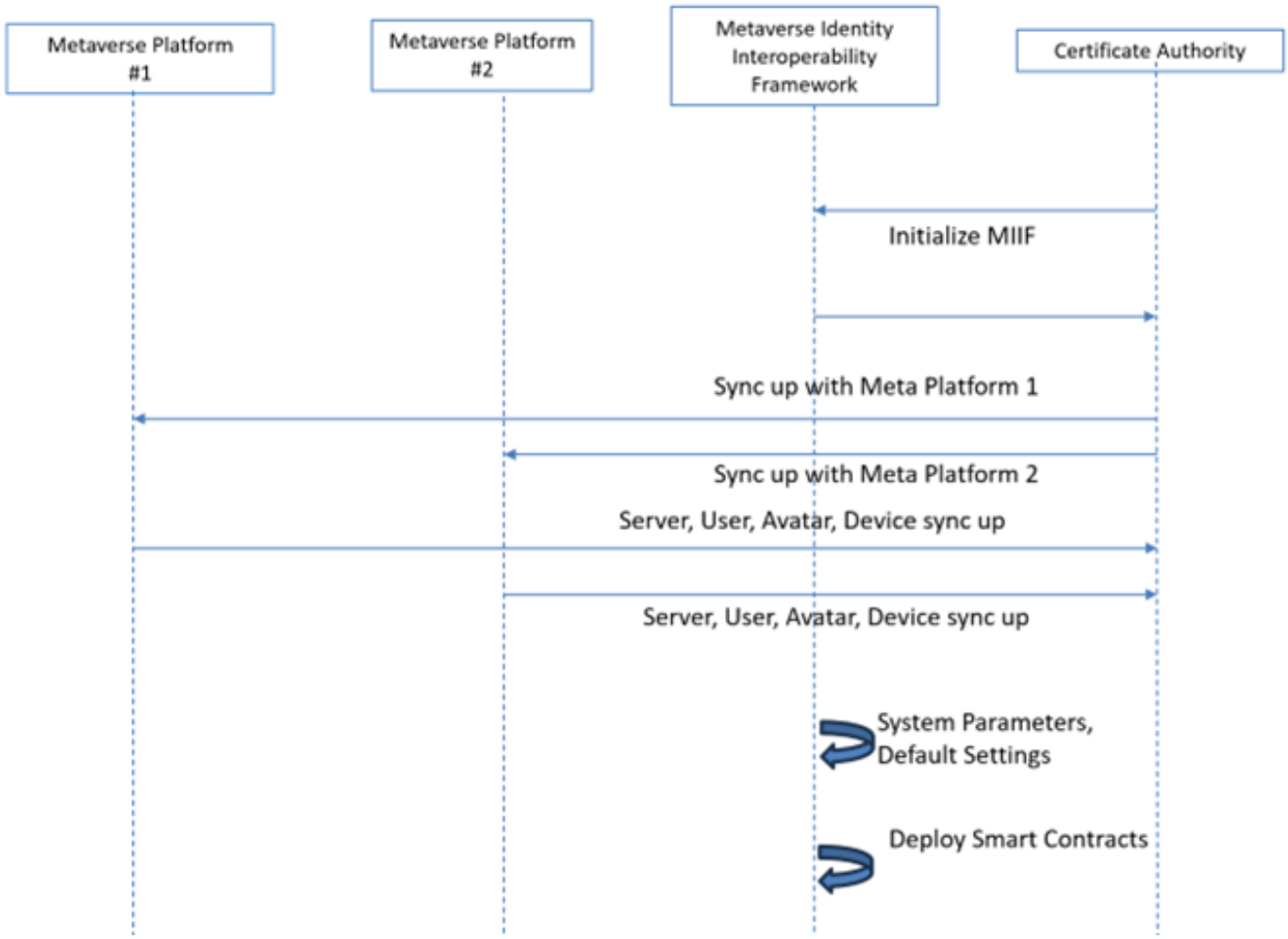

Figure 3. Initialization phase.

5.2. User-Registration Phase

In the user-registration phase, Ui enters the username UNi, Password PWi and other information, infoi, in the metaverse platform, MPi. MPi registers the user and relevant user information in the metaverse platform server, MPSi. A Smart Contract, SC1, on MIF will trigger an event for MPi to sync up if any new user has been registered. MPi will send PUi details and MP-Server-MPSi details to the MIF. The MIF will create a random token Ti for the user, PUi. The MIF will send a random token, Ti, to the PUi and send a request to enter physical ID PIDi (like ID card, social security number, etc.). After this, PUi will compute a public key, PKi, as follows: PKi = Ki · P. Then, PUi will transmit { h(UNi, PWi, MPSi, Ti,), PIDi, PKi, infoi} to the CA for verification.

The CA will check the uniqueness of { h(UNi, PWi, MPSi, Ti), PIDi, PKi, infoi } in the blockchain and verify the request. On success, the CA will generate signature Sigca-i for user Ui to confirm that the user has been verified by the CA. The CA will then generate a random token, ti, and compute Zi =ti · P. The CA will then generate Meta-ID MIDi, a 256-bit hash for {PIDi, UNi, PWi, PKi, infoi, MPSi}. The response, R = (Sigca-i, Zi, MIDi), will be sent to the user Ui, and the CA will store MIDi on the blockchain.

The user-registration process is shown in Figure 4.

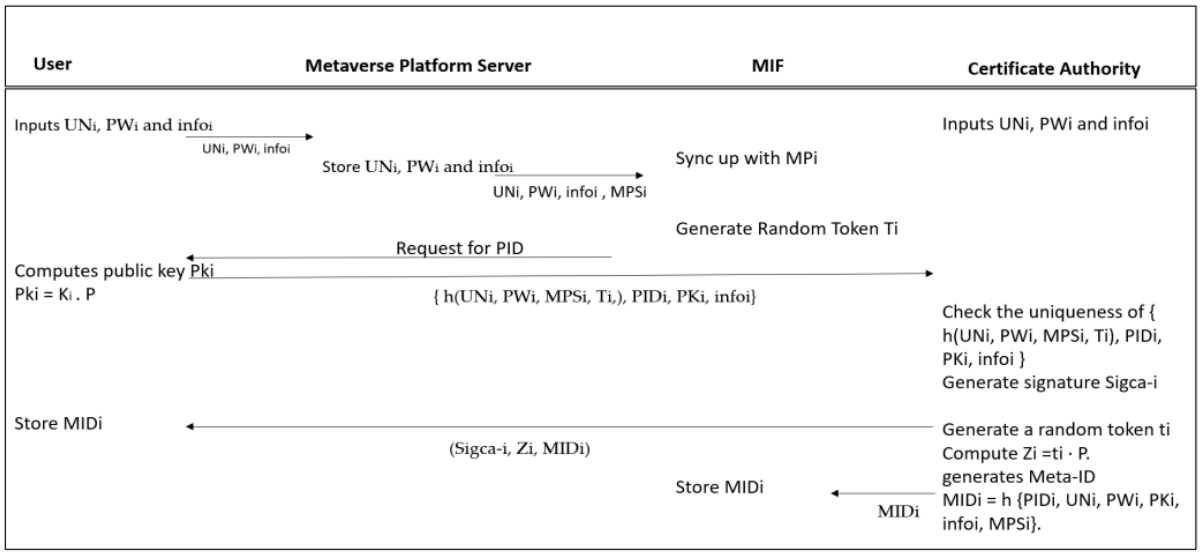

Figure 4. User-registration phase.

5.3. Avatar-Generation Phase

Physical users can create avatars in the metaverse environment for navigation in the virtual world. One physical user can generate multiple avatars. The following steps can be followed to generate an avatar for a user.

A physical user, PUi, enters UNi and PWi to login to the metaverse platform MPi. If the user is wearing device Di and Di is already registered with the user, then the user will be logged in to MPi. If Di is not already registered, then the device registration flow is initiated, and an avatar is created with an unique avatar identity, Ai.

The MIF Smart Contract triggers an event with MPSi to sync up with new-avatar generation. The physical user's UNi, PWi, MPi, Meta-ID MIDi, Di and Ai are sent to the MIF for verification.

The MIF checks in the blockchain for MIDi and retrieves the PKi. If {Ai, PKi} is unique in the blockchain, then {Ai, MPSi} is stored in the blockchain. The Avatar generation phase is shown in Figure 5.

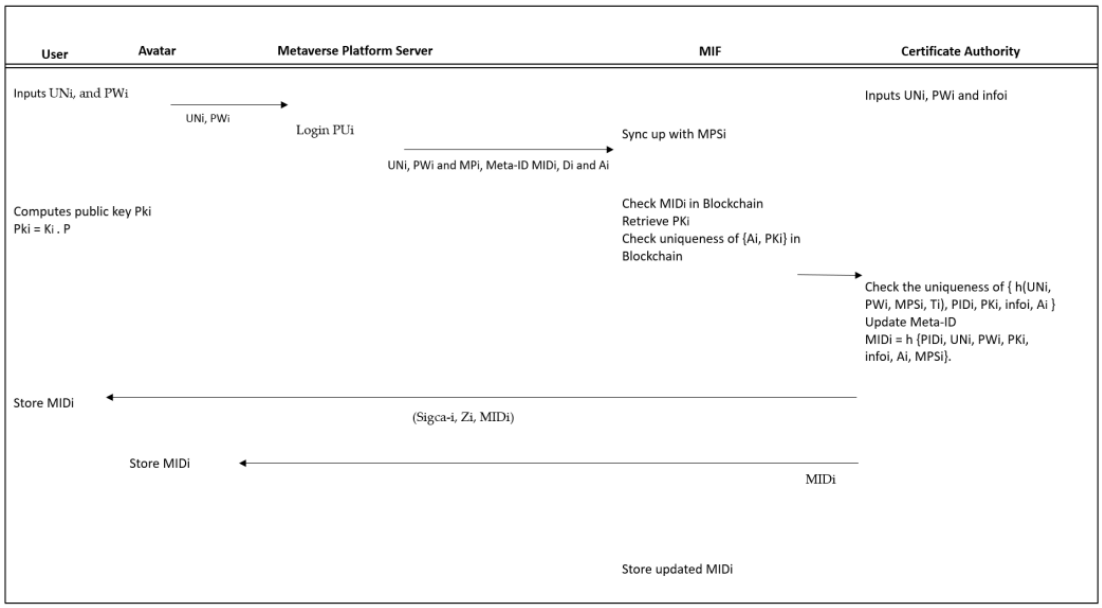

Figure 5. Avatar-generation phase.

6. Security Analysis

In this section, we demonstrate the robustness of the proposed system against malicious security attacks through an informal analysis and AVISPA simulation. Additionally, we employ BAN logic [30,31], a widely recognized formal-security-analysis method, to establish that the proposed scheme ensures secure mutual authentication. Following that, we validate the session key's confidentiality using the real-or-random (ROR) model.

6.1. Informal Security Analysis

- Impersonation attack: An adversary can create a fake login username, PU, and password, PW. However, it is not possible to get access to tokens, Ti, that are used at the time of user registration. Also, the Meta-ID that is a 256-bit hash used to uniquely identify users is also mapped to login credentials. To change the Meta-ID, consensus has to achieved in the blockchain network. So, it is not possible to manipulate it using an impersonation attack. Therefore, our scheme prevents impersonation attack.
- Replay attack: The replay attack allows an adversary to eavesdrop on the messages being exchanged between users and avatars. However, an adversary will not be able to get access to the private keys and MID of the user and avatar. In our proposed model, the replay attack is avoided using an MIF-sync up with relevant Metaverse server platforms (MPs). Blockchain in the MIF maintains the timestamp of the transaction and also the session key that is being used, SKi, to identify each session. Therefore, the combination of the Meta-ID and session key will prevent s replay attack.
- Fake-avatar attack: In this type of attack, the virtual world creates a false avatar to imitate an actual avatar. In order to do this, an adversary is required to possess the Meta-ID and avatar ID (Ai). Also, it would need to be able to verify the PKi with the CA and the MIF, which is highly infeasible as PKi is created using tokens. Also, avatars are mapped to the PID of the PU for which an avatar is created. This means that a fake avatar would need to able to get access to the physical ID of the user. It is highly unlikely that a fake avatar can get access to all of these parameters. Therefore, our scheme is fake-avatar-attack proof.
- Stolen-device attack: An adversary can steal a head-mounted device, hand-held device or other related device. However, the device ID is stored in a block masked with a hash. Also, it is combined with a Meta-ID that is stored in the blockchain. Therefore, an adversary cannot gain access to the user information, infoi, through a stolen device.
- Stolen-password attack: The user and avatar authentication processes in our scheme are not based only on a password. This authentication requires a physical PID and a metaverse-platform-specific username and password. The Meta-ID hash is generated based on all of the associated parameters. Thus, it is difficult to crack the password of the user by adversary. Therefore, our scheme is stolen-password-attack proof.
- Server-spoofing attack: An adversary can intercept messages shared among users and avatars and generate a response message as if it is coming from the legit server MPSi. However, a response message cannot be generated without the private keys of users and avatars. Also, the Meta-ID is added to the messages being sent. Thus, our scheme can resist platform-server-spoofing attacks.
- Denial-of-service attack: An adversary can send multiple request messages and transmit them to the MIF or CA for verification. This may lead to a network bottleneck. However, as the metaverse platform checks for the timestamp of the request and session key, the attacker cannot create new request messages. Even if the adversary tries to resend past messages, the MPS will treat them as invalid. Therefore, the proposed scheme guarantees robustness against denial-of-service attacks.
- Man-in-the-middle attack: An adversary may try to reuse previously shared messages that have been captured by an attacker. However, the timestamp and Meta-ID mechanisms in our scheme will prevent responses to such invalid requests. Thus, our scheme takes care of MITM attacks.

- Non-traceable-avatar attack: All of the messages shared among the users and devices are protected by session keys, SKi, and time stamps, ts. Also, there are unique random numbers associated with users or avatars. That is why our proposed scheme provides non-traceability.
- Lack of interoperability: Due to a lack of interoperability, an adversary may try to impersonate a user in different platforms with different identities. There is no uniformity in the identification of the user or avatar. The unique security feature provided by our scheme is interoperable identity. This will avoid the security issues caused by lack-of-identity interoperability.
- Mutual authentication: If an adversary tries to fake authentication while communicating with other users or avatars, it will not be validated in our proposed scheme. Because of the Meta-ID, Metaverse server platforms are registered while enrolling the user. Also, session keys and timestamps are used while sharing messages. Consequently, the proposed system provides secure mutual authentication.
- Stolen user- or avatar-information attack: The user information is protected by a Meta-ID and session key. Even if an adversary tries to steal user or avatar information, when it is being used somewhere else, session key will be invalid. Hence, our scheme protects users and avatars from stolen-information attacks.
- Session-key-disclosure attack: In the framework proposed, the session key is maintained per session and is used in combination with a Meta-ID. If an adversary tries to disclose the session key, then it would not be possible to use against another Meta-ID. Thus, our scheme is not susceptible to session-key-disclosure attack.
- Perfect forward secrecy: An adversary will not be able to perform a perfect forward secrecy attack on our proposed scheme. Even if the private key used in an individual session are stolen, then the attacker will not be obtain access to the Meta-ID for that user and device. Hence, an adversary will not be able to access data from other sessions.
- Insider attack: In the insider attack, an adversary can impersonate an avatar, Ai, or a ser, PUi. However, in our proposed scheme, without knowing session keys and a Meta-ID, it is difficult for any avatars or users to perform an impersonation attack. Hence, our scheme can prevent insider attacks.

6.2. Formal Security Analysis

BAN Logic

After an informal security analysis, it is essential to formally analyze the proposed scheme. Out of the all of the security issues addressed, mutual authentication among the avatars and devices can be ensured using BAN logic. BAN logic is an analysis method commonly used to verify mutual authentication protocols. Before we start with actual BAN logic analysis, we introduce logical postulates, rules, and goals. Then we prove the mutual authentication protocol using BAN logic. The Table 3 introduces the BAN logic notations used in our analysis.

Table 3. Notations for BAN logic analysis.

Notation	Description
P_1, P_2	Two principals
S_1, S_2	Two statements
K	The session key
$P_1 \mid\equiv S_1$	P_1 believes S_1
$P_1 \mid\sim S_1$	P_1once said S_1
$P_1 \Rightarrow S_1$	P_1controls S_1
$P_1 \triangleleft S_1$	P_1 receives S_1
$\#S_1$	S_1 is fresh
$\{S_1\}_K$	S_1 is encrypted with K
$P_1 \overset{K}{\longleftrightarrow} P_2$	P_1 and P_2 have shared key K

Logical postulates of BAN logic are given below.

1. Message meaning rule:

$$\frac{P1 \mid \equiv S1 \overset{K}{\leftrightarrow} P1, P2 \triangleleft S1}{P1 \mid \equiv P2 \mid \sim S1}$$

2. Nonce verification rule:

$$\frac{P1 \mid \equiv \#(S1),\ A1 \mid \equiv A2 \mid \sim S1}{P1 \mid \equiv P2 \mid \equiv S1}$$

3. Jurisdiction rule:

$$\frac{P1 \mid \equiv P2 \mid \Longrightarrow S1, P1 \mid \equiv P2 \mid \equiv S1}{P1 \mid \equiv S1}$$

4. Freshness rule:

$$\frac{P1 \mid \equiv \#(S1)}{P1 \mid \equiv \#(S1, S2)}$$

5. Belief rule:

$$\frac{P1 \mid \equiv (S1, S2)}{P1 \mid \equiv S1}$$

Goals

The goals are to prove mutual authentication in the proposed scheme. The goals can be expressed as follows:

Goal 1: MPS $\mid \equiv$ (Ui SKi$-$MPS $\leftarrow\rightarrow$ MPS)
Goal 2: MPS $\mid \equiv$ Ui $\mid \equiv$ (Ui SKi$-$MPS $\leftarrow\rightarrow$ MPS)
Goal 3: Ui $\mid \equiv$ (Ui SKi$-$MPS $\leftarrow\rightarrow$ MPS)
Goal 4: Ui $\mid \equiv$ MPS $\mid \equiv$ (Ui SKi$-$MPS $\leftarrow\rightarrow$ MPS)
We can express our login and authentication messages,
{M1, MPS1, ts1} and {M2, MPS2, ts2}, as follows:
Message 1: Ui $\rightarrow$ MPS1 : { Ai, , PIDi, , MPS1, ts1}MPS2
Message 2: St $\rightarrow$ Ui : {Ai , PIDi, MPS3, ts2}MPS4
The relevant assumptions are as follows:
A1: MPS $\mid \equiv$ (Ui $\leftarrow\rightarrow$ MPS2 MPS)
A2: MPS $\mid \equiv$ #(ts)
A3: Ui $\mid \equiv$ (Ui $\leftarrow\rightarrow$ MPS4 MPS)
A4: Ui $\mid \equiv$ #(ts2)
A5: MPS $\mid \equiv$ Ui $\Rightarrow$ (Ui SKi$-$MPS $\leftarrow\rightarrow$ MPS)
A6: Ui $\mid \equiv$ MPS $\Rightarrow$ (Ui SKi$-$st $\leftarrow\rightarrow$ MPS)
Proof

The BAN logic method can be used to prove the four goals using the assumptions and rules mentioned above.

• To obtain E1 from Message 1.
E1 : MPS $\triangleleft$ {Ai , PIDi , MPS1, t1}MPS2
• Applying MMR using E1 and A1 to obtain E2.
E2 : MPS $\mid \equiv$ Ui $\mid \sim$ (Ai , PIDi , MPS1, t1)
• Applying FR using E2 and A2 to obtain E3.
E3 : MPS $\mid \equiv$ #(Ai , PIDi , MPS1, t1)
• Applying NVR using E2 and E3 to obtain E4.
E4 : MPS $\mid \equiv$ Ui $\mid \equiv$ (Ai , PIDi , MPS1, t1)
• Applying BR using E4 to obtain E5.

E5 : MPS$|\equiv$ Ui $|\equiv$ (Ai , PIDi , MPS1)

• To obtain E6 from Message 2.

E6 : Ui $\triangleleft$ {Ai , PIDi , MPS3, t2}MPS4

• Applying MMR using E6 and A3 to obtain E7.

E7 : Ui $|\equiv$ St$|\sim$ (Ai , PIDi , MPS3, t3)

• Applying FR using E7 and A4 to obtain E8.

E8 : Ui $|\equiv$ #(Ai , PIDi , MPS3, t2)

• Applying NVR using E7 and E8 to obtain E9.

E9 : Ui $|\equiv$ MPS$|\equiv$ (Ai , PIDi , MPS3, t2)

• Applying BR using E9 to obtain E10.

E10 : Ui $|\equiv$ MPS$|\equiv$ (Ai , PIDi , MPS3)

• To obtain E11 using E5. MPS can calculate v2 = h(Ai$||$PIDi$||$k$||$ t2), MPS2 = k $\cdot$ MPS1, and MPS4 = v2 $\cdot$ MPS1. Then, MPS can successfully generate the session key SKi$-$MPS = h(Ai $||$MPS2$||$MPS4).

E11 : MPS$|\equiv$ Ui $|\equiv$ (Ui SKi$-$MPS $\longleftrightarrow$ MPS) (Goal 2)

• Applying JR using E11 and A5 to obtain E12.

E12 : MPS$|\equiv$ (Ui SKi$-$MPS $\longleftrightarrow$ MPS) (Goal 1)

• To obtain E13 using E10. Ui can calculate v1 = h(Ai $||$PIDi $||$Xi $||$t1), S2 = v1 $\cdot$ PK, and MPS4 = v1 $\cdot$ MPS3. Then, Ui can successfully generate the session key SKi$-$MPS = h(Ai $||$MPS2$||$MPS4).

E13 : Ui $|\equiv$ MPS$|\equiv$ (Ui SKi$-$MPS $\longleftrightarrow$ MPS) (Goal 4)

• Applying JR using E10 and A6 to obtain E14.

E14 : Ui $|\equiv$ (Ui SKi$-$MPS $\longleftrightarrow$ MPS) (Goal 3)

Thus, we proved that our scheme guarantees secure mutual authentication between Ui and MPS.

6.3. ROR Model

The real-or-random (ROR) model, which is grounded in probabilistic game theory, is extensively employed for assessing the semantic security of authenticated key agreements [32–34]. Employing the ROR model, we illustrate that our proposed scheme guarantees session key security against a malicious adversary within probabilistic polynomial time. We begin by outlining the foundational aspects of the ROR model in Table 4, followed by a demonstration of the session key security for our proposed scheme.

Table 4. Various queries and descriptions for the ROR model.

Query	Description
Execute	Two principals
Send	Two statements
Reveal	The session key
Test	P_1 believes S_1
Corrupt	P_1 once said S_1

6.4. AVISPA

AVISPA is a commonly used security-simulation tool focused on assessing the resistance of protocols to replay and man-in-the-middle (MITM) attacks [35–38]. The language used in AVISPA is High-Level Protocol Specification Language (HLPSL). AVISPA outlines the actions of each participant. Subsequently, the HLPSL code is translated into Intermediate Format (IF) using the HLPSL2IF translator. The IF data are then input into AVISPA, employing one of four backends, namely, the CL-based attack searcher (CL-AtSe), the on-the-fly model checker (OFMC), the tree-Automata-based protocol analyzer (TA4SP), and the SAT-based model checker (SATMC).

In our analysis, we have used OFMC. Various phases used in our scheme like setup, user registration, and login are analyzed for attacks like replay and MITM. The output screenshots for our proposed scheme are shown in Figure 6.

```
%%%%%%% Role UA %%%%%%
role usera(UA,SP,CA : agent, SKuanc,SKuans :symmetric_key, H,ADD,MUL: hash_func, SND, RCV : channel(dy))
played_by UA
def=
local State: nat,
        IDi,PWi,BIOi,DIDi,PKi,SKi,RRi,INFOi,HPWi,HVCi,AAi,REGi,HRIDi,HBii,Aii,Xi,T1,MS1,MS2,SKus:text,

VCi,P: text,
        RIDi,SKsp,PKsp,BBi,Bii,Ysp,RIDnew,MS3,MS4,SKsu,T2:text

const sp1,sp2,sp3,sp4,ua_sp_xi,sp_ua_ysp: protocol_id
init State:=0
transition
%%%%% Set up phase %%%%%%%
1. State=0 /\RCV(start)=|>
State':=1 /\SKi':=new()
        /\DIDi':=new() /\RRi':=new() /\PKi':=MUL(SKi.P)
        /\SND({DIDi'.INFOi}_SKuanc)
        /\secret({IDi.PWi.BIOi.SKi'.RRi'},sp1,{UA})
        /\secret({INFOi},sp2,{UA,CA})
2. State=1 /\RCV({VCi'}_SKuanc)=|>
State':=2 /\HPWi':=H(IDi.PWi.RRi') /\HVCi':=xor(VCi',H(RRi'.IDi.PWi))
%%%%% Registration phase %%%%%
/\AAi':=H(MUL(SKi'.PKsp')) /\REGi':=H(DIDi'.HPWi'.AAi')
/\SND({DIDi'.HPWi'.REGi'}_SKuans)
3. State=2 /\RCV({H(DIDi'.H(IDi.PWi.RRi').SKsp).H(BBi'.H(DIDi'.H(IDi.PWi.RRi').SKsp).SKsp)}_SKuans)=|>
State':=3 /\HRIDi':=xor(H(DIDi'.H(IDi.PWi.RRi').SKsp),H(IDi.HPWi'.AAi'))
        /\HBii':=xor(H(BBi'.H(DIDi'.H(IDi.PWi.RRi').SKsp).SKsp),H(HPWi'.RRi'.IDi))
        /\Aii':=H(H(DIDi'.H(IDi.PWi.RRi').SKsp).H(BBi'.H(DIDi'.H(IDi.PWi.RRi').SKsp).SKsp).RRi'.HPWi')
%%%%% Login phase %%%%%%
/\Xi':=new() /\T1':=new()
/\MS1':=xor(Xi',H(H(DIDi'.H(IDi.PWi.RRi').SKsp).H(BBi'.H(DIDi'.H(IDi.PWi.RRi').SKsp).SKsp).T1'))
/\MS2':=H(H(DIDi'.H(IDi.PWi.RRi').SKsp).Xi'.H(BBi'.H(DIDi'.H(IDi.PWi.RRi').SKsp).SKsp).DIDi'.T1')
/\SND(H(DIDi'.H(IDi.PWi.RRi').SKsp),MS1',MS2',T1')
/\witness(UA,SP,ua_sp_xi,Xi')
4. State=3 /\RCV(xor({Ysp'.H(DIDi'.Ysp'.Bii')},H(Xi'.DIDi'.Bii')),H(Xi'.Ysp'.RIDi'.H(DIDi'.Ysp'.Bii').H(Xi'.Ysp'.Bii'.DIDi').T2'),
T2')=|>
State':=4
        /\SKus':=H(Xi'.Ysp'.H(DIDi'.H(IDi.PWi.RRi').SKsp).H(DIDi'.Ysp'.Bii').DIDi')
        /\request(UA,SP,sp_ua_ysp,Ysp')
end role
```

Figure 6. User role and various phases of AVISPA analysis.

7. Performance Analysis

In this section, we perform a comparative analysis with the other related schemes. We compare our proposed scheme to other schemes with respect to computation cost, communication cost, and security issues addressed [16–19]. In this paper, we follow the execution time of the cryptographic operation measured by [39,40] using 2048 MB of RAM with an Intel Pentium Dual CPU E2200 2.20 GHz and the Ubuntu 12.04.1 LTS 32-bit operating system.

7.1. Computation Cost Analysis

The following table shows the comparison of computation costs of various schemes proposed earlier [16–19] with our proposed scheme. It is clear that the computation cost is substantially reduced in our scheme. The total computation cost of our scheme is 50.115 ms. Table 5 compares the computation cost of various other schemes and our scheme.

Table 5. Comparison of computation costs of various schemes.

Schemes	User	Server	Total Cost
Panda and Chattopadhyay [16]	44.1190 ms	29.4136 ms	73.5326 ms
Li et al. [17]	36.7759 ms	36.7837 ms	73.5596 ms
Ryu et al. [18]	51.4723 ms	88.2458 ms	139.7181 ms
Kim et al. [19]	29.4438 ms	36.7755 ms	66.2193 ms
Our proposed scheme	27.3357 ms	22.7758 ms	50.1115 ms

7.2. Communication Cost Analysis

Table 6 shows the comparison of the communication cost of the previously proposed schemes [16–19] with that of our scheme. The communication cost is reduced to 1256 bits in our scheme.

Table 6. Comparison of communication costs of various schemes.

Schemes	Communication Cost	Messages
Panda and Chattopadhyay [16]	1440 bits	3
Li et al. [17]	1728 bits	2
Ryu et al. [18]	1888 bits	3
Kim et al. [19]	1344 bits	2
Our proposed scheme	1256 bits	2

7.3. Security-Features Comparison

Table 7 compares the various security features addressed in the proposed schemes. Our proposed scheme has addressed the security issues mentioned in the earlier schemes in addition to extra security issues.

Table 7. Security-features comparison (X—Security issue not addressed; Tick—Security issue addressed).

Security Feature	Panda and Chattopadhyay [16]	Li et al. [17]	Ryu et al. [18]	Kim et al. [19]	Our Proposed Scheme
Impersonation	✓	✓	✓	✓	✓
Avatar Impersonation	X	X	✓	✓	✓
Mutual authentication	X	✓	✓	✓	✓
Server Spoofing	✓	x	✓	✓	✓
Replay	✓	X	✓	✓	✓
Stolen Device	X	x	✓	✓	✓
Offline Password Guessing	✓	X	✓	✓	✓
Insider Attack	✓	X	✓	X	✓
Session Key Disclosure	✓	✓	✓	✓	✓
Perfect Forward Secrecy	✓	✓	✓	✓	✓
Man-in-the-Middle	✓	✓	✓	✓	✓
Insider Attack	✓	X	✓	✓	✓
Ephemeral Secret Leakage	X	✓	✓	✓	✓
Anonymity	✓	X	✓	✓	✓
Privacy Preservation	X	X	X	✓	✓
Untraceability	✓	X	✓	✓	✓
Denial of Service	X	✓	X	✓	✓
Lack of Interoperability	X	X	X	X	✓

8. Conclusions

In this paper, we introduced a robust interoperable authentication framework tailored for cross-metaverse platforms, aiming to guarantee secure user and avatar interactions and defend against a wide set of security threats. Our approach leverages blockchain-enabled interoperable metaverse identity, enabling users to assert a uniform identity mechanism across multiple metaverse platforms. This framework is applicable not only to virtual worlds but is applicable to physical users as well. Extensive security analyses, including ROR-oracle-security analyses, AVISPA simulations, and BAN logic analyses, attest to the

resilience of our scheme against diverse security attacks such as stolen XR devices and impersonation. Notably, our solution exhibits lower computation and communication costs compared to existing metaverse schemes, making it a practical choice for heightened security and privacy preservation. Our future research agenda involves applying and testing the proposed scheme in various use cases.

Author Contributions: Conceptualization, S.P.; Methodology, S.P.; Software, S.P.; Validation, S.P.; Formal analysis, S.P.; Resources, S.P.; Writing—original draft, S.P.; Writing—review & editing, S.P.; Supervision, S.B.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Wang, Y.; Su, Z.; Zhang, N.; Xing, R.; Liu, D.; Luan, T.H.; Shen, X. A survey on metaverse: Fundamentals, security, and privacy. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 319–352. [CrossRef]
2. Patwe, S.; Mane, S. Blockchain enabled architecture for secure authentication in the metaverse environment. In Proceedings of the 2023 IEEE 8th International Conference for Convergence in Technology (I2CT), Lonavla, India, 7–9 April 2023; pp. 1–8.
3. A Researcher's Avatar was Sexually Assaulted on a Metaverse Platform Owned by Meta, Making Her the Latest Victim of Sexual Abuse on Meta's Platforms, Watchdog Says. Available online: https://www.businessinsider.in/tech/news/a-female-researchers-avatar-was-sexually-assaulted-on-a-metaverse-platform-owned-by-meta-making-her-the-latest-victim-of-sexual-abuse-on-metas-platforms-watchdog-says/articleshow/91884508.cms (accessed on 13 January 2024).
4. Falchuck, B.; Loeb, S.; Neff, R. The social metaverse: Battle for privacy. *IEEE Technol. Soc. Mag.* **2018**, *37*, 52–61. [CrossRef]
5. Yu, S.; Lee, J.; Park, Y.; Park, Y.; Lee, S.; Chung, B. A secure and efficient three-factor authentication protocol in global mobility networks. *Appl. Sci.* **2020**, *10*, 3565. [CrossRef]
6. Lee, L.-H.; Braud, T.; Zhou, P.; Wang, L.; Xu, D.; Lin, Z.; Kumar, A.; Bermejo, C.; Hui, P. All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv* **2021**, arXiv:2110.05352.
7. Patwe, S.; Mane, S. Blockchain Enabled Architecture for Secure Authentication in the Metaverse Environment: A Student Training Use Case. In Proceedings of the IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), Kyoto, Japan, 26–28 June 2023; pp. 413–417.
8. Why Has Facebook Changed its Name to Meta and What is the Metaverse? Available online: https://www.newscientist.com/article/2295438-why-has-facebook-changed-its-name-to-meta-and-what-is-the-metaverse/ (accessed on 13 January 2024).
9. Wang, Y.; Su, Z.; Zhang, N.; Liu, D.; Xing, R.; Luan, T.H.; Shen, X. A Survey on Metaverse: Fundamentals, Security, and Privacy. *arXiv* **2022**, arXiv:abs/2203.02662. [CrossRef]
10. Aks, S.M.; Karmila, M.; Givan, B.; Hendratna, G.; Setiawan, H.S.; Putra, A.S.; Winarno, S.H.; Kurniawan, T.A.; Simorangkir, Y.N.; Taufiq, R.; et al. A Review of Blockchain for Security Data Privacy with Metaverse. In Proceedings of the 2022 International Conference on ICT for Smart Society (ICISS), Online, 10–11 August 2022; pp. 1–5. [CrossRef]
11. Gadekallu, T.R.; Huynh-The, T.; Wang, W.; Yenduri, G.; Ranaweera, P.; Pham, Q.V.; da Costa, D.B.; Liyanage, M. Blockchain for the Metaverse: A Review. *arXiv* **2022**, arXiv:2203.09738v2.
12. Yang, K.; Zhang, Z.; Tian, Y.; Ma, J. A Secure Authentication Framework to Guarantee the Traceability of Avatars in Metaverse. In Proceedings of the IEEE Transactions on Information Forensics and Security, Nürnberg, Germany, 4–7 December 2023; Volume 18, pp. 3817–3832. [CrossRef]
13. Huang, Y.; Li, Y.J.; Cai, Z. Security and privacy in metaverse: A comprehensive survey. *Big Data Min. Anal.* **2023**, *6*, 234–247. [CrossRef]
14. Truong, V.T.; Le, L.; Niyato, D. Blockchain meets metaverse and digital asset management: A comprehensive survey. *IEEE Access* **2023**, *11*, 26258–26288. [CrossRef]
15. Nguyen, C.T.; Hoang, D.T.; Nguyen, D.N.; Dutkiewicz, E. Metachain: A novel blockchain-based framework for metaverse applications. *arXiv* **2021**, arXiv:2201.00759.
16. Panda, P.K.; Chattopadhyay, S. A secure mutual authentication protocol for IoT environment. *J. Reliable Intell. Environ.* **2020**, *6*, 9–94. [CrossRef]
17. Li, Y.; Xu, M.; Xu, G. Blockchain-based mutual authentication protocol without CA. *J. Supercomput.* **2022**, *78*, 17261–17283. [CrossRef]
18. Ryu, J.; Son, S.; Lee, J.; Park, Y.; Park, Y. Design of secure mutual authentication scheme for metaverse environments using blockchain. *IEEE Access* **2022**, *10*, 98944–98958. [CrossRef]
19. Kim, M.; Oh, J.; Son, S.; Park, Y.; Kim, J.; Park, Y. Secure and Privacy-Preserving Authentication Scheme Using Decentralized Identifier in Metaverse Environment. *Electronics* **2023**, *12*, 4073. [CrossRef]

20. Shen, M.; Liu, H.; Zhu, L.; Xu, K.; Yu, H.; Du, X.; Guizani, M. Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 942–954. [CrossRef]
21. Ryu, J.; Oh, J.; Kwon, D.; Son, S.; Lee, J.; Park, Y.; Park, Y. Secure ECC-Based Three-Factor Mutual Authentication Protocol for Telecare Medical Information System. *IEEE Access* **2022**, *10*, 11511–11526. [CrossRef]
22. Xu, M.; Ng, W.C.; Lim, W.Y.B.; Kang, J.; Xiong, Z.; Niyato, D.; Yang, Q.; Shen, X.; Miao, C. A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 656–700. [CrossRef]
23. Yang, Q.; Zhao, Y.; Huang, H.; Xiong, Z.; Kang, J.; Zheng, Z. Fusing blockchain and AI with metaverse: A survey. *IEEE Open J. Comput. Soc.* **2022**, *3*, 122–136. [CrossRef]
24. Huynh-The, T.; Gadekallu, T.R.; Wang, W.; Yenduri, G.; Ranaweera, P.; Pham, Q.V.; Costa, D.B.; Liyanage, M. Blockchain for the metaverse: A review. *Futur. Gener. Comp. Syst.* **2023**, *143*, 401–419. [CrossRef]
25. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [CrossRef]
26. Masud, M.; Gaba, G.S.; Choudhary, K.; Hossain, M.S.; Alhamid, M.F.; Muhammad, G. Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. *IEEE Internet Things J.* **2022**, *9*, 2649–2656. [CrossRef]
27. Bhattacharya, M.; Roy, S.; Chattopadhyay, S.; Das, A.K.; Jamal, S.S. ASPA-MOSN: An efficient user authentication scheme for phishing attack detection in mobile online social networks. *IEEE Syst. J.* **2023**, *17*, 234–245. [CrossRef]
28. Son, S.; Kwon, D.; Lee, S.; Jeon, Y.; Das, A.K.; Park, Y. Design of secure and lightweight authentication scheme for UAV-enabled intelligent transportation systems using blockchain and PUF. *IEEE Access* **2023**, *11*, 60240–60253. [CrossRef]
29. Canetti, R.; Krawczyk, H. Universally composable notions of key exchange and secure channels. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, 28 April–2 May 2002; pp. 337–351.
30. Soni, P.; Pardhan, J.; Pal, A.K.; Islam, S.K.H. Cybersecurity attack-resilience authentication mechanism for intelligent healthcare system. IEEE Trans. *Ind. Inform.* **2023**, *19*, 830–840. [CrossRef]
31. Oh, J.; Yu, S.; Lee, J.; Son, S.; Kim, M.; Park, Y. A secure and lightweight authentication protocol for IoT-based smart homes. *Sensors* **2021**, *21*, 1488. [CrossRef]
32. Hosseinzadeh, M.; Ahmed, O.H.; Ahmed, S.H.; Trinh, C.; Bagheri, N.; Kumari, S.; Lansky, J.; Huynh, B. An enhanced authentication protocol for RFID systems. *IEEE Access* **2020**, *8*, 126977–126987. [CrossRef]
33. Lee, J.; Kim, G.; Das, A.K.; Park, Y. Secure and efficient honey list-based authentication protocol for vehicular ad hoc networks. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2412–2425. [CrossRef]
34. Chen, C.M.; Chen, Z.; Kumari, S.; Lin, M.C. LAP-IoHT: A lightweight authentication protocol for the internet of health things. *Sensors* **2022**, *22*, 5401. [CrossRef] [PubMed]
35. Wang, D.; Cheng, H.; Wang, P.; Huang, X.; Jian, G. Zipf's law in passwords. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2776–2791. [CrossRef]
36. AVISPA. Automated Validation of Internet Security Protocols and Applications. Available online: http://www.avispa-project.org/ (accessed on 22 August 2023).
37. SPAN: A Security Protocol Animator for AVISPA. Available online: https://people.irisa.fr/Thomas.Genet/span/ (accessed on 22 August 2023).
38. Kilinc, H.H.; Yanik, T. A survey of SIP authentication and key agreement schemes. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 1005–1023. [CrossRef]
39. Ravanbakhsh, N.; Nazari, M. An efficient improvement remote user mutual authentication and session key agreement scheme for E-health care systems. *Multimed. Tools Appl.* **2018**, *77*, 55–88. [CrossRef]
40. Gope, P.; Sikdar, B. Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. *IEEE Internet Things J.* **2019**, *6*, 580–589. [CrossRef]