future internet

Article

MetaSSI: A Framework for Personal Data Protection, Enhanced Cybersecurity and Privacy in Metaverse Virtual Reality Platforms

Faisal Fiaz [1], Syed Muhammad Sajjad [1], Zafar Iqbal [1], Muhammad Yousaf [2] and Zia Muhammad [3,4,*]

[1] Department of Cyber Security, Air University, Islamabad 44000, Pakistan; 211835@students.au.edu.pk (F.F.); muhammad.sajjad@kc.au.edu.pk (S.M.S.); zafar.iqbal@mail.au.edu.pk (Z.I.)
[2] Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad 45210, Pakistan; muhyousaf@gmail.com
[3] Department of Computer Science, North Dakota State University, Fargo, ND 58108, USA
[4] Department of Computer Science and Technology, University of Jamestown, Jamestown, ND 58405, USA
* Correspondence: zia.muhammad@ndsu.edu

Abstract: The Metaverse brings together components of parallel processing computing platforms, the digital development of physical systems, cutting-edge machine learning, and virtual identity to uncover a fully digitalized environment with equal properties to the real world. It possesses more rigorous requirements for connection, including safe access and data privacy, which are necessary with the advent of Metaverse technology. Traditional, centralized, and network-centered solutions fail to provide a resilient identity management solution. There are multifaceted security and privacy issues that hinder the secure adoption of this game-changing technology in contemporary cyberspace. Moreover, there is a need to dedicate efforts towards a secure-by-design Metaverse that protects the confidentiality, integrity, and privacy of the personally identifiable information (PII) of users. In this research paper, we propose a logical substitute for established centralized identity management systems in compliance with the complexity of the Metaverse. This research proposes a sustainable Self-Sovereign Identity (SSI), a fully decentralized identity management system to mitigate PII leaks and corresponding cyber threats on all multiverse platforms. The principle of the proposed framework ensures that the users are the only custodians and proprietors of their own identities. In addition, this article provides a comprehensive approach to the implementation of the SSI principles to increase interoperability and trustworthiness in the Metaverse. Finally, the proposed framework is validated using mathematical modeling and proved to be stringent and resilient against modern-day cyber attacks targeting Metaverse platforms.

Keywords: cybersecurity; data privacy; metaverse; multiverse; self-sovereign identity (SSI); decentralized identity management; authentication methods; mathematical modeling; cyber threats; personally identifiable information (PII)

check for updates

Citation: Fiaz, F.; Sajjad, S.M.; Iqbal, Z.; Yousaf, M.; Muhammad, Z. MetaSSI: A Framework for Personal Data Protection, Enhanced Cybersecurity and Privacy in Metaverse Virtual Reality Platforms. *Future Internet* **2024**, *16*, 176. https://doi.org/10.3390/fi16050176

Academic Editors: Christos Troussas, Akrivi Krouska, Cleo Sgouropoulou and Jaime Caro

Received: 17 April 2024
Revised: 13 May 2024
Accepted: 16 May 2024
Published: 18 May 2024

1. Introduction

The Metaverse has been present for a while, yet many people still do not fully understand what it is or how it works. The term "Metaverse" combines the word "meta", which denotes transcending reality, and the suffix "verse", which is short for the universe. The author Neal Stephenson used the term "Metaverse" in their 1992 novel *Snow Crash*. A number of major digital corporations are vying for a piece of the Metaverse pie, including Facebook (Meta) [1], Epic Games [2], Google, and Microsoft. Online video games already include elements of Metaverse technology. Because it combines many social media elements into a persistent three-dimensional world with the user represented by an avatar, the immersive virtual reality platform "Second Life", introduced in 2003, is frequently referred to as the first Metaverse [3].

A "Metaverse" is a cosmos that exists independently of our material reality. Professionals see it as a virtual, three-dimensional version of the web that users may explore with the help of XR technology [4]. Many of the virtual reality technologies that Meta Platforms promote are still in the development phase. In the Metaverse, users take part in educational, economic, social, and cultural activities as avatars in a fully immersive, three-dimensional virtual world [5]. This is in contrast to AR and VR, which are distinct artificial worlds [6]. Some applications of the Metaverse use digital currencies, frequently cryptocurrencies, and non-fungible tokens (NFTs), which are sometimes used for trading assets in the Metaverse, and use blockchain technology to monitor ownership. Among the shared characteristics of the Metaverse are the following: identity continuity, shared surroundings, embodied avatars, synchronization, virtuality, interoperability, and an immersive user experience [7].

People in the Metaverse are represented by avatars, which may be customized in terms of looks and behavior [8]. Improvements in work efficiency, interactive educational environments, e-commerce, large-scale involvement, property investment, and fashion are among the suggested benefits and uses for Metaverse technologies. They enable computer representations of people to engage in luxurious activities like meeting friends, caring for virtual pets, designing virtual clothing, purchasing virtual real estate, going to concerts, presenting and selling or buying digital art, playing games, etc. A user may engage in a variety of activities inside the Metaverse like virtual gaming, information sharing, meetings, socializing, and asset monetization [9–11].

The Metaverse has recently emerged as a popular topic in the technology and gaming sectors. In 2020, the Metaverse market was valued at 38.5% billion, projected to grow to 478.7% billion by 2024 according to [12]. It is anticipated that the Metaverse market will expand 13.1% yearly. Adults in the United States make up 74% of those who have joined or are considering joining the Metaverse. Over USD 120 billion was invested in the Metaverse in 2022 and 79% of active members have purchased products. Four hundred million people use the Metaverse regularly, and 25% of these individuals will spend an entire hour in the Metaverse by the year 2026, with 30% of companies providing goods and services for the Metaverse. The Web 2.0 Metaverse business valuation is USD 14.8 trillion.

The Metaverse Market is anticipated to exceed USD 13 trillion by 2030. By the year 2030, there will be about 5 billion users of the Metaverse. In 2040, the Metaverse will hold 500 million people. The world of the future is the Metaverse, which mixes artificial intelligence with virtual reality. A growing number of people are drawn to the Metaverse because it makes it possible to encounter scenarios that are rare in the actual world [13].

While the Metaverse has great promise for the future, there are still certain unresolved concerns that might hinder the complete merging of the physical and virtual realms inside it. Because avatars may take on the appearance and actions of other users, and because real people are not always predictable, building trust between users is the primary concern [9,14]. The emergence of new technologies is frequently swiftly followed by cybersecurity solutions or a set of established guidelines or best practices for developers. However, this is not the case with the entrance of the Metaverse, and in a time when cyberattacks have dramatically increased, it is crucial to look into any potential security flaws. In the Metaverse, trust is considered essential for achieving one's goals. Indeed, there may be a number of challenges to a reliable system supply posed by the core characteristics of the Metaverse, including interoperability, decentralization, immersiveness, and scalability [7]. In recent years, there has been a paradigm shift in digital identity management with the introduction of innovative technologies such as Self-Sovereign Identity (SSI). SSI offers individuals greater autonomy and control over their personal data by enabling them to manage their identities independently of centralized authorities. Additionally, decentralized identifier (DID) technology has emerged as a key component of SSI, providing a method for creating globally unique identifiers that are cryptographically verifiable and under the control of the individual.

The majority of new technologies typically have the same security flaws as their predecessors while also creating opportunities for new kinds of attacks. The structure of the Metaverse is not an exception; its structure makes it vulnerable to unusual and more sophisticated attacks. How users' identities, data, and avatars may be shared across different Metaverse virtual worlds is an important concern. Users can easily go to other Metaverse virtual worlds and transfer their data and assets to anywhere they choose. The user's data, avatars, and identity might be restricted to a single virtual service provider (VSP) if there is an incompatible collection of virtual worlds. Concerns about security and privacy will not only increase but also fundamentally change. There has been little research on the security implications of the Metaverse; concerns like how vulnerable this new technology is have not been adequately studied, and if they have, the answers are scarce. This paper's key contributions can be outlined as:

1. This article investigates the security and privacy concerns prevalent in the Metaverse, with a particular focus on the limitations and challenges of existing centralized identity systems and certificate-based authentication methods.
2. We explore the concept of SSI and its potential applications, highlighting its advantages over traditional identity systems, and propose a novel SSI-based authentication mechanism for the Metaverse, named MetaSSI, designed to enhance user control and interoperability.
3. We demonstrate the practicality and effectiveness of MetaSSI through rigorous proof of work and mathematical formulation. Finally, we propose a comparative analysis of the existing authentication methods and our proposed SSI model against standard SSI evaluation frameworks, validating the superiority of MetaSSI.

Section 2 introduces the components of SSI and the key role of SSI in the Metaverse. We offer a concise overview of cyber security challenges, user privacy, and identity management within the Metaverse in Section 3. Section 4 explores additional requirements for implementation and the proposed solutions. An evaluation and results are presented in Section 5. Finally, in Section 6, we wrap up and provide a glimpse into future directions for this work.

2. Background

This section will cover the elements of SSI, its essential role in the Metaverse, and the requirements for implementing the Metaverse.

2.1. Components of SSI

The management and application of digital identities can be transformed by SSI in the Metaverse. Users are empowered, privacy and security are improved, trust and interoperability are fostered, innovation is stimulated, and inclusivity is expanded. This revolutionary method of identity management is the cornerstone of a Metaverse ecosystem that is more flexible, safe, and user-oriented.

In the Metaverse, DIDs offer unique, pseudonymous identities that are connected to cryptographic keys. They enable users to create and manage their digital identities throughout the Metaverse while remaining anonymous. DIDs give users the freedom to manage and resolve their identifiers on their own without depending on centralized authorities. In addition to ensuring autonomy, this decentralization lowers the possibility of identity theft and manipulation. Because IDs are meant to be compatible with various Metaverse platforms, users can use the same one and keep their virtual identity constant [15].

SSI in the Metaverse places users in control of their identities, emphasizing user autonomy, privacy, and security. SSI ensures the trustworthiness and authenticity of identity-related information, fostering secure interactions and transactions within virtual environments. Adoption of SSI standards in the Metaverse encourages innovation, supports new use cases, and fosters the growth of a vibrant ecosystem with diverse virtual identities and credentials [16]. SSI in the Metaverse represents a paradigm shift in identity management, offering users unprecedented control, privacy, and security in their digital interactions across immersive virtual worlds.

SSI in the Metaverse grants users true ownership and control over their digital identities and personal data. Users have the authority to manage, share, and revoke access to their identity information across different virtual spaces. SSI empowers users to provide explicit consent for sharing specific attributes or credentials [17], ensuring they disclose only relevant information required for interactions or transactions within the Metaverse. Users can seamlessly carry their digital identities and credentials across various Metaverse platforms, fostering continuity and persistence of their online personas regardless of the virtual environment.

SSI reduces reliance on centralized databases and authorities, mitigating the risks associated with single points of failure, data breaches, and unauthorized access. This decentralized approach enhances security and privacy. SSI enables the use of zero-knowledge proofs, allowing users to prove possession of certain information without revealing the information itself [18]. This cryptographic method enhances privacy while validating credentials or attributes. Storing identity-related data on decentralized ledgers ensures immutability and tamper-resistance, enhancing trust and confidence in the authenticity of digital identities and credentials.

While the concept of the Metaverse is still in its infancy, various implementations of VWs such as Second Life, Meta Horizons, Fortnite, Decentraland, Roblox, Otherside, and The Sandbox are being built using different technologies and do not intend for their avatars, ecosystems, and currencies to be interoperable with one another [6]. The future Metaverse is imagined as a single, fully connected, decentralized 3D network where all the sub-Metaverses coexist in a manner that users can easily traverse from one section to another, offering the greatest possible experience for users who wish to navigate the virtual world via their avatar, and nobody owns it [12].

2.2. *Standards Related to the Metaverse*

The following standards pertaining to the Metaverse have been identified in earlier research [19].

- IEEE 2888: A set of rules for communicating across the digital and physical worlds; these standards form a family. For example, 2888.1, 2888.2, 2888.3, 2888.4, 2888.5, and 2888.6 are all part of the standard set. Generally speaking, these standards provide the language, criteria, metrics, data formats, or application programming interfaces (APIs) for collecting data from sensors, which allows for the creation of cyber–physical interfaces. The development and operation of the Metaverse are anticipated to be greatly impacted by the IEEE 2888 standard [20].
- ISO/IEC 23005: The purpose of this standard is to allow interactions between digital contents and the actual environment by providing an architecture and defining related information representations. As a result, virtual worlds are able to work together more easily. This standard has the potential to improve a number of Metaverse-based applications, including those that deal with audiovisual content and rendered sensory effects [19].

Two well-established methods in the field of digital identity verification are self-sovereign authentication and certificate-based authentication, which stand out as contrasting approaches [21]. While self-sovereign authentication allows users to take control of their identities using decentralized identifiers and Verifiable Credentials without relying on central authorities, certificate-based authentication uses digital certificates issued by trusted authorities (Certificate Authorities) to validate identities. Self-sovereign authentication is decentralized and puts user control, privacy, and interoperability across digital platforms first, whereas certificate-based authentication is centralized and requires trust in the Certificate Authority.

2.3. *Drawbacks of Certificate-Based Asymmetric Authentication*

Here are some drawbacks of this authentication model.

- Centralized points of failure are produced when certificate issuance and management are left to Certificate Authorities (CAs). A CA's certificates are all at risk if the CA itself is compromised.

- Digital certificate acquisition and management can be expensive and complicated, particularly for smaller businesses or individuals. The process of renewing certificates contributes to continuous maintenance.
- It can be difficult to revoke compromised certificates and make sure the network recognizes the revocation. There may be additional latency when checking Online Certificate Status Protocols (OCSPs) or Certificate Revocation Lists (CRLs).
- Identity data found in certificates may be exposed during the authentication procedure. Users' ability to control when and how their identity information is shared is restricted.

2.4. How Self-Sovereign Identity Addresses These Issues

- By using decentralized networks like blockchains, SSI reduces its dependency on a single authority. Decentralization improves security and resilience to disruptions and attacks.
- Users are in total control of the information about themselves. They choose what details they want to share and to whom. To improve privacy, SSI employs zero-knowledge proofs and selective disclosure.
- By doing away with the need for intermediaries like CAs, SSI reduces the cost of issuing and managing certificates. Identity verification becomes easier to use and more efficient.
- SSI frameworks are designed to work with various networks and systems. This enables users to interact with different services and platforms more seamlessly.
- Revocation and identity credential recovery mechanisms can be implemented more effectively by SSI systems. Even if a user loses their device or login credentials, they can still retrieve their identity using decentralized recovery mechanisms.
- Systems for SSI based on blockchain technology can effectively manage a large volume of identity verifications. Numerous identity-management-related procedures can be automated through the use of smart contracts and decentralized applications (DApps).

Self-Sovereign Identity solves many of the drawbacks of conventional certificate-based systems and provides a more user-centric approach to digital identity. Through the utilization of blockchain technology and a focus on user control and privacy, SSI offers a digital identity management framework that is more efficient, secure, and adaptable. This is especially helpful in the ever-changing digital landscape, where seamless and secure identity verification is essential in places like the Metaverse.

3. Literature Review

The Metaverse, a virtual reality environment, presents a range of cybersecurity challenges. Many researchers have focused on the security and privacy of the Metaverse. There have been numerous survey articles from various aspects of the Metaverse. Cybersecurity challenges in the Metaverse include identity theft, spying, social engineering, data security, privacy, and the security of virtual assets [22]. The Metaverse poses asymmetric risks such as terrorism and crypto-laundering, and potential military applications may impact global security [23]. Cybersecurity threats faced by the Metaverse in relation to visualization technologies include emerging threats related to VR and AR [24]. The Metaverse faces security and privacy issues, such as attacks on user authentication and impersonation, and the research agenda includes biometric-based authentication and federated learning for protecting user privacy [25]. These studies suggest that cybersecurity issues in the Metaverse involve identity theft, spying, social engineering, data security, privacy, security of virtual assets, asymmetric risks, visualization technologies, user authentication, financial cybercrime, and challenges in security defenses and privacy preservation.

The Metaverse, a virtual world that mirrors the real world, raises significant privacy concerns due to the collection and processing of personal data [26]. These concerns are particularly pronounced in the use of non-fungible token (NFT) avatars, which contain personal information and behavioral footprints [27]. The legal landscape of the Metaverse is complex, with challenges in intellectual property, privacy, and jurisdiction [28]. Furthermore, the Metaverse presents unprecedented privacy risks, with attackers able to covertly obtain personal data attributes from users [29]. These studies collectively highlight the need for robust privacy measures and legal frameworks to protect users in the Metaverse.

Personal identity in the Metaverse is transforming, causing ethical and legal implications and privacy concerns, with digital identity becoming an integral part of our lives [30]. The virtual self in the Metaverse, linked to a social networking account, forms a contiguous connection between lived VR experiences and identity data gathered through social media [31]. The Metaverse, a fusion of human and artificial intelligence, offers a unique opportunity for digital art and identity to merge, resulting in a new digital culture [32].

The Metaverse offers potential for improved well-being and social control, but also potential for individual identity, privacy, and political consciousness to be manipulated [33]. The concept of identity in the Metaverse is a complex and multifaceted issue, as highlighted by several recent studies. Awadallah [34] and Wang [35] both emphasize the importance of digital identity in the Metaverse, with the former focusing on the potential risks and cybersecurity threats, and the latter discussing the need for a balance between anonymity and pseudonymity. Zhang [36] suggests the establishment of a unified digital identity authentication system to address privacy and security concerns. The proposed two-factor authentication framework based on chameleon signatures and biometric-based authentication effectively guarantees the consistency and traceability of the avatar's identity in the Metaverse, enabling virtual–physical tracking [37].

Decentralized authentication mechanisms are presented as being able to overcome the limitations of centralized approaches [38]. Blockchain-enabled architectures are suggested to ensure decentralized authentication and traceability of avatars and users. The design of secure mutual authentication schemes using blockchain and biometric information is also explored [39]. They highlight the need for secure access, data privacy, and interoperability in the Metaverse environment. These studies collectively underscore the need for a comprehensive approach to managing identity in the Metaverse, one that prioritizes security, privacy, and user control. The use of Self-Sovereign Identity (SSI) is suggested as a solution to address these challenges [19].

4. Proposed Framework

The Metaverse, a communal virtual shared place, is blossoming as a platform for social and economic interactions. Ensuring safe and independent user interactions inside this environment is crucial. We propose a complete Self-Sovereign Identity (SSI)-based authentication architecture aimed to empower individuals with control over their digital identities, boost security, and encourage interoperability across multiple Metaverse platforms. Because it is decentralized and requires compatibility across multiple platforms, the Metaverse poses unique problems for identity authentication. Due to their inadequacies, traditional centralized authentication techniques compromise user privacy and are vulnerable to failure points. One possible answer is an SSI-based architecture, which gives people full control over their identity and eliminates the need for a governing body.

Figure 1 demonstrates the components of SSI, which rely on decentralized identifiers (DIDs) and Verifiable Credentials (VCs). A DID is a string created by the user, which is linked to their public key, and it uniquely identifies them as a Metaverse Service Provider (MSP). On the other hand, Verifiable Credentials consist of attribute names and values about a user that are cryptographically signed and are issued by the Credential Granting Authority. The issuer signs the VCs using their private key before sending them to the user, who stores them in a wallet. This user is also known as the holder in SSI, and they interact with an MSP by presenting their VCs, which the MSP verifies as a verifier. The sharing of DIDs happens through a DID document, which contains relevant metadata such as the DID and associated cryptographic public keys. These documents are saved in a data registry, implemented as a blockchain for its immutable and decentralized nature. The process in SSI involves entities establishing connections and the Credential Granting Authority issuing a VC to the holder through the established connection. The holder then stores the VC in their wallet. Upon receiving a presentation request from a Metaverse service, the user prepares a presentation, sends it to the Metaverse service through the established connection, and subsequently verifies each VC in the presentation to proceed accordingly.

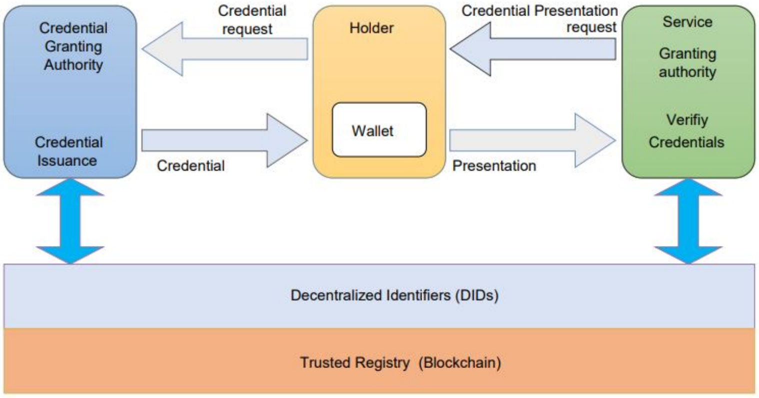
Credential Granting Authority
Credential Issuance
Credential request
Credential
Holder
Wallet
Credential Presentation request
Presentation
Service
Granting authority
Verifiy Credentials
Decentralized Identifiers (DIDs)
Trusted Registry (Blockchain)

Figure 1. Components of the proposed framework.

The operational flow of the framework is shown in Figure 2. Users create and store their DIDs and VCs in their Identity Wallet. Holder requests the CGA to attest specific claims. The CGA demands specific data to validate the claim. The user will provide specific data to the CGA. After validation of a claim, the CGA will cryptographically sign a set of data and attest the holder's claim using their public key. When accessing a service in the Metaverse, the SGA requests authentication. Users present specific VCs with the service provider. The service provider verifies the VCs against the Trust Registry using authentication protocols. Upon successful verification, access is granted, and the user's activity within the service is pseudonymously recorded to maintain privacy.

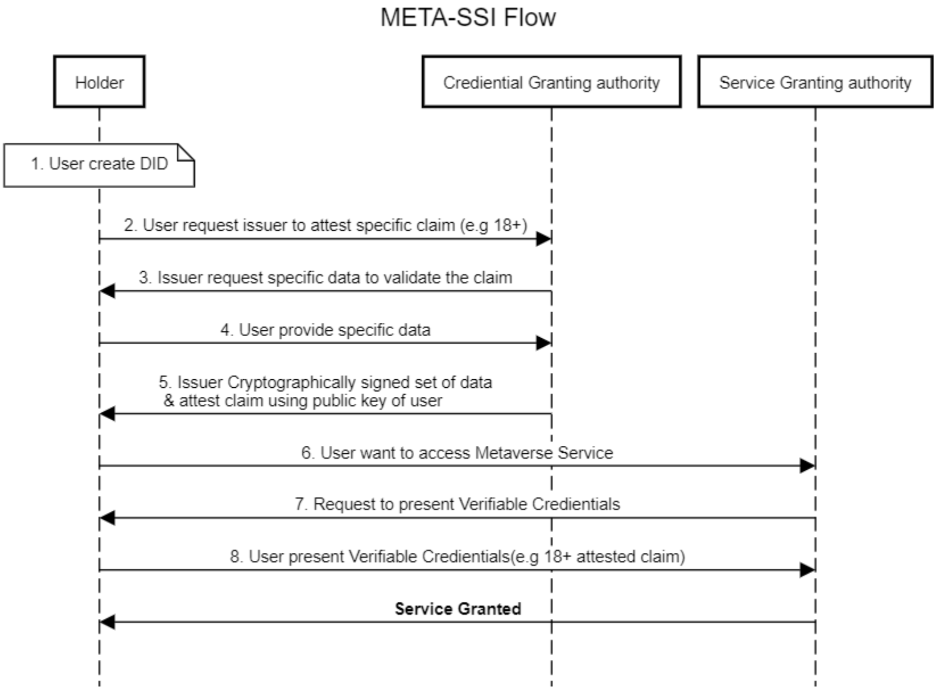
META-SSI Flow
Holder
Credential Granting authority
Service Granting authority
1. User create DID
2. User request issuer to attest specific claim (e.g 18+)
3. Issuer request specific data to validate the claim
4. User provide specific data
5. Issuer Cryptographically signed set of data & attest claim using public key of user
6. User want to access Metaverse Service
7. Request to present Verifiable Credientials
8. User present Verifiable Credientials(e.g 18+ attested claim)
Service Granted

Figure 2. Proposed framework flow.

Identity Creation and Management Using a convenient UI, users start by establishing their digital identity. In order to create their decentralized identifiers (DIDs), a pair of cryptographic keys must be generated. The user's Identity Wallet, which can be an independent program or integrated into already existing Metaverse interfaces, is where the private key is safely kept. The distributed ledger stores the public key, which establishes the user's DID without disclosing any personal information.

- Credential Issuance: Verifiable Credentials (VCs) are granted to users by trusted organizations, such as academic institutions. These documents may serve as identification or as proof of a professional qualification. The issuer's public key allows third parties to independently verify the VCs, which are signed using the issuer's private key. These VCs are given to users, who keep complete control over who can access them by storing them in their Identity Wallet.
- Authentication Request: The service provider asks for authentication when a user wants to use a service inside the Metaverse. The credentials that are needed to gain access are listed in this request (e.g., age verification and membership status). The request reaches the user's Identity Wallet, which asks for permission to share particular VCs.
- Consent and Privacy Management: Users can examine the authentication request and decide which credentials to share using the Identity Wallet as a Consent Layer. Users have the option to divulge only the information required to complete the transaction. By using zero-knowledge proofs, the framework enables users to validate identity claims without disclosing the actual credentials.
- End-to-end Encryption: Every exchange of credentials and personal data within the framework, in particular, is end-to-end encrypted. This prevents information from being intercepted or accessed by unauthorized parties because only the intended recipient can decrypt and view the data.
- Zero-Knowledge Proofs: A party can prove to another that a statement is true without revealing any information except that the statement is true by employing cryptography. Within the framework of SSI, it permits users to authenticate themselves or certain aspects of their identity without disclosing their personal information.
- Blockchain Technology: A decentralized, unchangeable ledger is made possible by using blockchain technology to record DIDs and VCs. This stops historical records from being altered or tampered with, in addition to guaranteeing the authenticity and non-repudiation of the identity data.
- Minimising Data and Obtaining Consent: The framework processes personal data only to the extent necessary for the specific purpose for which the user has granted consent, in accordance with the data minimization principle. Users are guaranteed fine-grained control over what data they share and with whom thanks to the Consent Layer.
- Anonymity and Pseudonymity: Pseudonyms are a convenient way for users to communicate in the Metaverse without having to reveal their true identities. This makes it possible to engage in digital activities while protecting one's privacy. **Interoperability and Standardization:** The framework conforms to the World Wide Web Consortium's (W3C) global standards for DIDs and VCs in order to guarantee a seamless user experience throughout the Metaverse. Open protocols and APIs make it simple for service providers to be integrated. Cross-chain interoperability is present to enable DIDs and VC verification between various blockchain networks governed by international laws. Standardization and interoperability are essential to the SSI framework's functionality and broad acceptance across various Metaverse platforms. The following measures are proposed:
- Adherence to W3C Standards: The framework will be developed in accordance with the standards for DIDs and VCs set forth by the World Wide Web Consortium (W3C), guaranteeing a standardized and open model for digital identities that is suitable for widespread adoption.
- Open APIs and Protocols: The framework makes it simple for different service providers to integrate with the Metaverse by offering open APIs and standardized protocols, which promotes a consistent user experience across platforms and services.

- Cross-Chain Compatibility: Cross-chain interoperability will be supported by the framework, making it possible to verify DIDs and VCs between various blockchain networks. This guarantees that users, irrespective of the blockchain technology utilized, can preserve a singular identity on various platforms.

  Governance and Evolution

  The framework will be governed by a decentralized autonomous organization (DAO), in which decision-making will involve participation from stakeholders from all over the Metaverse. The development of protocols and standards will be supervised by the DAO. New, reliable organizations will be added to the Trust Registry.
- Policy and Compliance: The DAO will be in charge of making sure the framework complies with international rules, such as identity standards and privacy laws. Additionally, it will create guidelines for how the framework should be used and operated.
- Continuous Improvement: Through user feedback and adaptation to technological advancements, the DAO will support ongoing framework improvement. This entails maintaining the Trust Registry and revising protocols and standards.
- Stakeholder Engagement: All stakeholders will be encouraged to actively participate in the framework to make sure it satisfies the wide range of needs of the Metaverse community. This involves transparent channels of communication, feedback systems, and frequent consultations.

  The suggested SSI-based authentication framework seeks to offer a user-centric, secure, private, and interoperable identity solution for the Metaverse that can adjust to its changing needs and dynamic nature through these governance structures and considerations.

  Ongoing Identity Management:

  As they engage with various services and entities in the Metaverse, users can keep receiving and managing new venture capital. The Identity Wallet makes it possible to renew and revoke login credentials, guaranteeing that the user's identity is safe and current.
- Audit and Compliance: The framework incorporates mechanisms for conducting compliance checks and auditing transactions to guarantee that all operations comply with the set privacy and security standards. To keep the Trust Registry as a trustworthy source of verification and to preserve the integrity of the authentication procedure, audits are carried out regularly. By allowing the user to maintain control over, give permission for use of, and manage their identity throughout the Metaverse, this operational flow guarantees that the user stays at the center of the authentication process. A secure foundation is provided by the application of blockchain technology and cryptographic proofs, and interoperability and a seamless user experience are enabled by the architecture of the framework.
- Regular Security Audits: Independent third-party security firms will regularly audit the framework to ensure that the highest security standards are maintained. By locating and fixing possible vulnerabilities, these audits contribute to the framework's resistance to changing cyber threats.
- Security and Privacy Considerations: Security and privacy are given top priority by the framework, which encrypts identity data from beginning to end. Zero-knowledge proofs allow for verification while hiding the underlying information. Blockchain technology is used for tamper identification and consistent DID and VC recording. Frequent framework updates and security audits are necessary to handle new threats. Security and privacy are given top priority in the design of the suggested SSI-based authentication framework, guaranteeing that users can trust the system with their digital identities. A secure, user-controlled, and interoperable identity management system is essential, and this need is met by the suggested SSI-based authentication framework for the Metaverse. The framework makes sure that users can navigate the Metaverse with confidence in the security and privacy of their digital identities by utilizing blockchain technology and abiding by international standards.

4.1. Mathematical Formulation

Within the framework of our studies on authentication based on Self-Sovereign Identity (SSI), we have further explored the mathematical characterization of the underlying mechanisms. We have clarified the roles and relationships through in-depth analysis, offering a thorough grasp of how every part interacts with the system as a whole. Digital identity creation, credential issuance and signing, credential verification, and access decision-making are some of these functions. We have also described the relationships that exist between credentials and the corresponding signatures, as well as between entities and credentials. This mathematical framework clarifies the nuances of important operations and how they interact with one another within the system, providing insightful information about the mechanics of SSI-based authentication.

The Algorithm 1 represents the process of SSI-based authentication. It starts with the creation of digital identities for each entity in the system. Then, for each entity and each credential type, credentials are issued and signed. Finally, service providers verify the authenticity of the received credentials. This algorithm provides a clear and concise representation of the SSI-based authentication process. Here, we present a more detailed step-by-step mathematical representation of the proposed framework.

Algorithm 1 Detailed Self-Sovereign Identity (SSI)-based authentication

```
procedure SSI AUTHENTICATION
    for each entity $e$ in $\mathcal{E}$ do
        $(k_{\text{priv}}, k_{\text{pub}}) \leftarrow \text{CreateIdentity}(e)$
        $\text{Register}(e, k_{\text{pub}})$
    end for
    for each entity $e$ in $\mathcal{E}$ do
        for each credential type $t$ in $\mathcal{T}$ do
            $c \leftarrow \text{IssueCred}(e, t)$
            $s \leftarrow \text{Sign}(c, k_{\text{priv}})$
            Add $(e, c)$ to $\mathcal{R}_{\text{ec}}$
            Add $(c, s)$ to $\mathcal{R}_{\text{cs}}$
        end for
    end for
    for each service provider do
        $\text{Verify}(c, s)$
        GrantAccess(verification result)
    end for
end procedure
```

4.1.1. Functions

Create Digital Identity: $\text{CreateIdentity} : \mathcal{E} \to \mathcal{K} \times \mathcal{K}$ maps an entity (user, trusted entity, etc.) to a pair of private and public keys.

Issue Credential: The function $\text{IssueCred} : \mathcal{E} \times \mathcal{T} \to \mathcal{C}$ maps an entity $e \in \mathcal{E}$ and a credential type $t \in \mathcal{T}$ to a Verifiable Credential c in the set of all credentials $\mathcal{C}$.

Sign Credential: $\text{Sign} : \mathcal{C} \times \mathcal{K} \to \mathcal{S}$ takes a credential c and a private key k_{priv} from the set of keys $\mathcal{K}$ and produces a signature s in the set of signatures $\mathcal{S}$.

Verify Credential: The function $\text{Verify} : \mathcal{C} \times \mathcal{S} \to \{\text{True}, \text{False}\}$ takes a credential c and its associated signature s and determines their authenticity.

Register Entity: $\text{Register} : \mathcal{E} \times \mathcal{K} \to \mathcal{L}$ maps an entity e and its public key k_{pub} to an entry in the set of distributed ledgers $\mathcal{L}$.

Request Authentication: $\text{RequestAuth} : \mathcal{E} \times 2^{\mathcal{T}} \to 2^{\mathcal{C}}$ takes an entity e and a set of desired credential types $\{t_1, t_2, \ldots, t_n\} \subseteq \mathcal{T}$ and returns a subset of credentials $\{c_1, c_2, \ldots, c_m\} \subseteq \mathcal{C}$.

Grant Access: $\text{GrantAccess} : \{\text{True}, \text{False}\} \to \{\text{Access Granted}, \text{Access Denied}\}$ takes a verification result and determines the access decision.

4.1.2. Relations

Entity–Credential Relation: $\mathcal{R}_{\text{ec}} \subseteq \mathcal{E} \times \mathcal{C}$ represents the relation between entities and their held credentials.

Credential–Signature Relation: $\mathcal{R}_{\text{cs}} \subseteq \mathcal{C} \times \mathcal{S}$ signifies the relation between credentials and their associated signatures.

4.1.3. Process Overview

Identity Creation: For each entity e in the set of entities $\mathcal{E}$, the function $\text{CreateIdentity}(e)$ generates a unique pair of cryptographic keys $(k_{\text{priv}}, k_{\text{pub}})$.

Credential Issuance and Signing: Trusted entities issue specific credentials to entities/users, represented by $\text{IssueCred}(e, t)$, and subsequently sign them with $\text{Sign}(c, k_{\text{priv}})$.

Credential Verification: Service providers use $\text{Verify}(c, s)$ to verify the authenticity of received credentials c with their associated signatures s.

Access Decision: Based on the verification results, $\text{GrantAccess}(\text{verification result})$ decides whether to grant or deny access to the service.

4.2. Simulation

Figure 3 shows our simulation of a primarily Self-Sovereign Identity (SSI)-based authentication system for the Metaverse using Hyperledger Aries. The process follows in the following sequence.

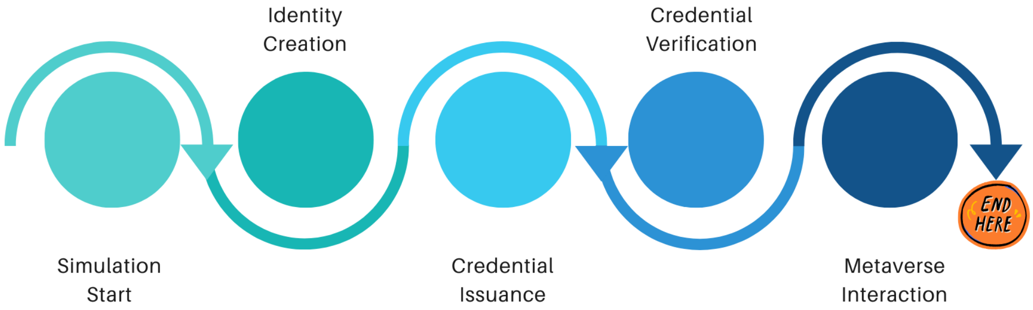

Figure 3. Simulation process flow.

- **Setting Up the Simulation Environment**
  First, we install Git, Python, and Docker. In containerized environments, Docker is essential for navigating Hyperledger Aries and streamlining the setup and deployment process. Next, we use Git to clone the essential Hyperledger Aries repositories. The hardware and scripts required for our simulation are contained in these repositories.
- **Launching Aries Agents**
  Docker Compose, which is found inside the cloned repositories, is used to launch multiple Aries sellers. Within the SSI version, each agent represents a unique entity, such as an identity holder, issuer, or verifier. We set each agent up to perform specific tasks within the SSI environment. For example, one agent acts on behalf of the identity company, another acts as the verifier, and a third represents an individual within the Metaverse.
- **Simulating SSI Scenarios**
  Using the issuer agent and their attractiveness via the user agent, we simulate the issuance of digital credentials. This is an essential step in verifying the credential issuance procedure within the Metaverse. The integrity and validity of the SSI model are then confirmed through testing the verification process of these credentials with the help of the verifier agent. Furthermore, we replicate credential revocation and confirm that the verifier agent can properly encounter and handle revoked credentials.
- **Integration with the Metaverse** We combine the Aries retailers to control authentication inside a digital environment (such as one created in Unity or Unreal Engine)

for the Metaverse. Through APIs or SDKs, this integration makes it possible for the Metaverse utility and the Aries dealers to communicate with one another.

- **Development and Testing**
  We expand custom scripts or applications that utilize Aries dealers to model accurate interactions in the Metaverse, specifically designed to meet the requirements of the SSI version. The marketers are controlled programmatically by the Hyperledger Aries APIs, which replicate different SSI operations relevant to the Metaverse.
- **Performance Monitoring and Analysis**
  To gain insight into the SSI interactions and transactions, we monitor the Aries sellers' logs and outputs throughout the simulation. The scalability and efficiency of the SSI version in a Metaverse environment are assessed using key performance metrics like response time, throughput, and aid utilization.
- **Utilizing Community Resources**
  We refer to the Hyperledger Aries documentation when looking for exact instructions and best practices. Part of our strategy involves interacting with the Hyperledger community, especially for troubleshooting and obtaining insights unique to the current state of the Metaverse.

Through this comprehensive setup and simulation technique, we aim to comprehensively check and validate the SSI-based total authentication model for the Metaverse, making sure it meets the necessary requirements for security, scalability, and personal experience.

5. Comparative Analysis and Results

Many authors have suggested frameworks, covering all the bases when it comes to SSI needs, including privacy, data integrity, and security. This research has made use of Abylay Satybaldy's [40] "Self-Sovereign Identity Evaluation Framework". In order to assess how well the existing and proposed identity systems adhere to these standards, this study evaluates the identity system for the Metaverse based on this framework. We used this evaluation framework as a reference to evaluate the current state of Self-Sovereignty in the published and proposed authentication solution for the Metaverse. In this analysis, we assess five proposed solutions for Metaverse authentication: a secure authentication framework to guarantee the traceability of avatars in the Metaverse (SMC) [37], a Secure and Privacy-Preserving Authentication Scheme Using Decentralized Identifiers in a Metaverse Environment (DIM) [41], gaze-based authentication (GBA) [42], and knowledge-based authentication (KBA) [43], in addition to evaluating MetaSSI.

The proposed Metaverse authentication model (SMC) addresses some SSI principles but lacks clarity on user data control and consent. It emphasizes limiting shared information but needs more detail on decentralization and transparency. The DIM framework ties virtual and physical identities, raising privacy and decentralization concerns. It lacks clarity on scalability and interoperability. Gaze-based authentication (GBA) has potential but required strong encryption and transparency. KBA methods like passwords and PINs lack user control and scalability, presenting usability challenges in AR and VR environments. Paired accounts show promise but require further development to align with principles.

Our proposed framework, which uses blockchain technology as a distributed identity repository, was set out to create guidelines and a structure for autonomous identities in the Metaverse. The proposed solution is based on the idea that users ought to be in total control of their online personas. Attribute credentials can be made more visible and accessible at the user level. The selective disclosure makes use of zero-knowledge proof, an advanced technique for enhancing privacy. To protect user privacy without sacrificing functionality, we also use decentralized identifiers and public and private keys for every relationship. Since each DID is intrinsically linked to a private agent's network address, users can securely exchange information, including verified claims, with one another over an encrypted private channel. These private investigators can choose to operate on edge devices or in the cloud. Our ledger complies with security requirements since it does not store any personally identifiable information. No third party should ever have access to a user's personal information, regardless of how trustworthy or committed to serving their best interests it may be. The protocol layer bears the responsibility of carrying out all necessary verifications and assurances. The problems of openness and trust are addressed by the webs of trust and reputation. The private information that consumers have opted to keep on their devices or with an agent will never be accessible through any of the systems or databases of the service providers.

Identity owners can recover their credentials and private keys in the event of loss because we provide a decentralized method of revocation using cryptographic accumulators. It is used in a manner independent of systems to enable data portability across providers. The ability to remove certain operational data from the SSI system is a necessary component of an individual's right to be forgotten; as such, it is best if identities can remain active indefinitely or for as long as the owner desires. Wherever you go, you can carry your identity services and personal data with you. Transportable identities ensure that the user keeps control over their identity while also improving identity persistence over time. The owner of an identity can still obtain their private keys and login information in the event that they misplace or have their primary access device stolen. Protocols and systems do not have any secret goals. An identity network's operational, managerial, and update processes are transparent thanks to the systems used for them. The algorithms are well known and compatible with all types of architectures. Our scheme makes use of only open-source licenses for all software and standards, which can be downloaded for free from the internet. The non-profit self-governing trust framework is made up of stewards, or volunteer specialists, in digital identity, privacy, and policy around the world. It is sometimes mentioned that having a portable identity is a requirement that needs to be met. We have designed our proposed identities for maximum usability. Global identities are made possible by our SSI system, enabling them to cross national boundaries and different system deployments. As a result of our identity systems' remarkable scalability, we are able to meet our users' growing needs. The number of end users or the availability of resources, for example, will not significantly affect the effectiveness of our SSI system. It is imperative that the user experience fulfils the expectations and demands of the user. Identity owners need a consistent user experience across various platforms and services. The question of how this will occur remains unanswered. Before the smart cryptographic tools of the identity system are made available to end users, they must be improved in terms of usability. It is crucial that services integrating with the virtual ecosystem and Metaverse developers focus on the user experience as they continue to improve their plans.

We conducted a comparative analysis based on the principles outlined in the SSI evaluation framework; the results are shown in Table 1.

Table 1. Evaluation results.

SSI Requirements	MetaSSI	SMC	DIM	GBA	KBA
User control and consent	yes	No	No	No	No
Privacy and protection	yes	No	No	yes	yes
No trust in a central authority	yes	yes	No	yes	No
Portability and persistence	yes	yes	No	No	No
Transparency	yes	yes	yes	yes	yes
Interoperability	yes	No	yes	yes	yes
Scalability	yes	No	yes	yes	No
Usability	yes	No	No	No	No

It is clear that the proposed framework completely fulfils the requirements of all SSI evaluation framework requirements.

5.1. Discussion

In the rapidly evolving Metaverse, the significance of robust and user-centric authentication models cannot be overstated. This study assessed four proposed Metaverse authentication models by contrasting them with the eight recognized Self-Sovereign Identity (SSI) principles to guarantee user autonomy and security in digital interactions. Every model that was looked at used a different technique for user authentication, ranging from centralized database approaches to blockchain-based solutions. However, there were differences in how closely they followed the SSI principles, necessitating an in-depth review.

The evaluation made it clear that although certain models performed well in certain areas, they fell short in critical domains like user consent and interoperability. For instance, one model performed an excellent job of ensuring data minimization, but it lacked a robust mechanism that would allow users to control their preferences concerning data sharing. Another, even with advanced cryptography techniques, had limited interoperability, making it less useful in a heterogeneous Metaverse ecosystem.

In response to these shortcomings, we unveiled our proposed model, which includes sophisticated consent processes that provide users with granular control over their data. Compared to the existing models, which frequently ignore the user′s right to privacy when sharing data, this feature is a significant improvement. Furthermore, our model solves the critical interoperability issue that many prior models faced by utilizing standards that are compatible with one another, ensuring seamless integration on various Metaverse platforms. The comparative evaluation revealed that our model adheres more closely to the SSI principles of user control and consent than the current models do. It gives users more power by allowing them to share their data selectively—a feature prominently missing from some of the evaluated models. Moreover, its interoperable framework ensures that users can move between different Metaverse environments without risking their identity security or privacy.

In our authentication mechanism, zero-knowledge proofs are automatically achieved through the cryptographic operations performed during the authentication process. When a user presents their Verifiable Credentials, they utilize cryptographic techniques such as blind signatures and selective disclosure. These techniques allow the user to provide only the necessary information to prove their identity, without revealing any additional details to the verifying party. This ensures that the user maintains privacy and confidentiality, as the verifying party only receives the minimal information required for authentication. By incorporating these cryptographic principles into our system design, we ensure that zero-knowledge proofs are seamlessly integrated into the authentication process, providing users with enhanced privacy and security.

These findings suggest that the Metaverse is experiencing a paradigm shift towards more user-centric authentication models following the international movement for digital identity sovereignty. Our model enhances user privacy and control while paving the way for a more interconnected and user-friendly Metaverse. Its practical applications' robustness and user-centricity will require continual examination and improvement, paving the way for a more user-centered, secure, and interoperable digital future.

We acknowledge that the remarks represent the subjective opinions of the authors derived from a qualitative analysis rather than established facts in the literature. We employed qualitative methods to evaluate existing frameworks against specified criteria, leading to the identification of perceived weaknesses. While these assessments are subjective in nature, they are grounded in the analysis conducted within the scope of this study.

5.2. Demonstrating the Excellence of MetaSSI

Self-sovereign authentication in the Metaverse presents cost-effectiveness over other authentication mechanisms through various means. Firstly, it eliminates intermediaries, enabling users to manage their digital identities directly, thus reducing the costs associated with third-party services. Secondly, it cuts down infrastructure expenses by leveraging decentralized technologies like blockchain, which diminishes the need for centralized infrastructure maintenance. Additionally, MetaSSI ensures enhanced security through cryptographic techniques and decentralized identifiers, mitigating risks of data breaches and compliance costs. It also enhances user experience by empowering users to control their digital identities, leading to decreased support costs related to forgotten passwords. Scalability is another advantage, as self-sovereign authentication can naturally grow with the Metaverse, avoiding substantial additional expenses. Moreover, it opens up monetization opportunities through new models of data sharing, creating revenue streams for both users and service providers. Despite the potential initial implementation costs, the long-term benefits in terms of cost-effectiveness, security, scalability, and user experience outweigh these investments, especially in the dynamic landscape of the Metaverse.

MetaSSI proves to be time-effective in the Metaverse due to several key factors. Firstly, it facilitates faster onboarding processes by streamlining identity creation and management, thus reducing the time typically spent on lengthy registration procedures. Additionally, its simplified authentication workflows eliminate the need for users to remember multiple passwords, enabling swift authentication through single-click actions or biometric verification. Efficient account recovery further saves time by empowering users to independently recover their accounts using decentralized identifiers and cryptographic keys, bypassing lengthy verification steps and support interactions. Real-time updates and access control capabilities enable users to manage their personal information promptly and efficiently, reducing administrative overheads and enabling swift interaction with digital environments. Furthermore, self-sovereign authentication can be seamlessly integrated with emerging technologies like augmented reality (AR) and virtual reality (VR), ensuring frictionless authentication experiences within immersive digital environments. Overall, by reducing authentication-related friction and streamlining identity management processes, MetaSSI optimizes the user experience in the Metaverse, saving time for both users and service providers.

6. Conclusions

In summary, this research represents a significant step forward in addressing the complexities of digital identity management within the developing Metaverse field. This study emphasizes the need for a user-centric, more secure approach by thoroughly analyzing the disadvantages of centralized identity systems. The Self-Sovereign Identity (SSI) model is a robust solution that offers users in the Metaverse enhanced privacy, autonomy, and security. The utility of this research is demonstrated by the development and simulation of an SSI-based authentication method tailored to the specific needs of the Metaverse. This strategy not only aligns with the decentralized Metaverse culture, but also creates a benchmark for improved digital identity management in virtual spaces. The comprehensive examination of four distinct authentication methods and the proposed SSI model demonstrates the thoroughness and precision of this research.

Most importantly, the extent to which the proposed SSI model adheres to widely used SSI evaluation frameworks determines its viability and effectiveness. This alignment guarantees the model's applicability and relevance in real-world scenarios in addition to validating it. This study establishes beyond a reasonable doubt that SSI can be used in the Metaverse, offering a solution that is both innovative and crucial given how quickly the digital landscape is changing.

Essentially, this work contributes to the scholarly discourse on digital identity management and provides a workable, proven path for the implementation of Self-Sovereign Identity in the Metaverse. By providing frameworks and insights that could influence the direction of digital interactions in virtual worlds, it acts as a guide for further research and advancement in this field. This work has broad implications that could influence the creation of more private, secure, and user-friendly digital environments.

Future Work

There are a few directions that could be taken in the future to improve the suggested self-sovereign authentication system for the Metaverse. First off, a more thorough examination of the suggested framework's performance in varied circumstances can be facilitated by expanding the simulation to include more extensive scenarios and parameters. To better understand scalability and efficiency aspects, this could involve simulating larger-scale Metaverse environments with more users and a variety of interaction patterns. We will focus on simulating real-time scenarios to validate the speed and accuracy of our proposed method in practical applications. In our future work, we plan to conduct real-time simulations of our proposed solution to validate its speed and accuracy in real-world scenarios and to identify and compute objective values that can prove the efficiency and excellence of the proposed model. Furthermore, investigating how to incorporate cutting-edge technologies like virtual reality (VR) and augmented reality (AR) into the authentication procedure can improve user experience and security in the Metaverse. Additionally, research into cutting-edge cryptography methods and decentralized identity management systems may provide an improved privacy and attack resistance in the dynamic Metaverse environment. Working together with Metaverse platform developers and industry stakeholders can also help to make the suggested authentication mechanism more feasible to implement and validate in the real world. When every factor is considered, future research projects ought to focus on addressing the changing opportunities and problems in the Metaverse domain, opening the door for more reliable, safe, and user-centered authentication solutions.

Author Contributions: Conceptualization, Z.I.; Methodology, F.F. and M.Y.; Validation, S.M.S., M.Y. and Z.M.; Formal analysis, S.M.S., M.Y. and Z.M.; Writing—original draft, F.F. and S.M.S.; Writing—review & editing, Z.I. and Z.M.; Visualization, F.F.; Supervision, Z.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available in this article.

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

References

1. Fernandez, P. Facebook, Meta, the metaverse and libraries. *Libr. Hi Tech. News* **2022**, *39*, 1–5. [CrossRef]
2. Jungherr, A.; Schlarb, D.B. The extended reach of game engine companies: How companies like epic games and Unity technologies provide platforms for extended reality applications and the metaverse. *Soc. Media Soc.* **2022**, *8*, 20563051221107641. [CrossRef]
3. Rymaszewski, M. *Second Life: The Official Guide*; John Wiley & Sons: Hoboken, NJ, USA, 2007.
4. Vitón-Castillo, A.A.; Fajardo Quesada, A.J.; Romero Valdes, Y.d.l.C.; Batista Rivero, L. Metaverse: An Emerging Research Area. Available online: https://mr.saludcyt.ar/index.php/mr/article/view/3 (accessed on 15 May 2024).
5. Ball, M. The Metaverse: What It Is. Where Find It, Who Will Build It, Fortnite. Available online: https://www.matthewball.co/all/themetaverse (accessed on 15 May 2024).
6. Tian, X. Scanning the literature–from ar/vr to metaverse. *IEEE Netw.* **2021**, *35*, 8–9. [CrossRef]
7. Ning, H.; Wang, H.; Lin, Y.; Wang, W.; Dhelim, S.; Farha, F.; Ding, J.; Daneshmand, M. A Survey on the Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges. *IEEE Internet Things J.* **2023**, *10*, 14671–14688.
8. Cheong, B.C. Avatars in the metaverse: Potential legal issues and remedies. *Int. Cybersecur. Law Rev.* **2022**, *3*, 467–494. [CrossRef]
9. Park, S.M.; Kim, Y.G. A metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access* **2022**, *10*, 4209–4251. [CrossRef]
10. Saleem, B.; Zia, M.M.; Zahra, M.; Ahmad, F.; Muhammad, Z. Smart Cities: A Novel Framework for Energy Production and Harvesting using Renewable Energy. In Proceedings of the 2023 International Conference on IT and Industrial Technologies (ICIT), Orlando, FL, USA, 4–6 April 2023; IEEE: New York, NY, USA, 2023; pp. 1–6.
11. Iesar, H.; Iqbal, W.; Abbas, Y.; Umair, M.Y.; Wakeel, A.; Illahi, F.; Saleem, B.; Muhammad, Z. Revolutionizing Data Center Networks: Dynamic Load Balancing via Floodlight in SDN Environment. In Proceedings of the 2024 5th International Conference on Advancements in Computational Sciences (ICACS), Lahore, Pakistan, 19–20 February 2024; IEEE: New York, NY, USA, 2024; pp. 1–8.
12. Design, J.; Cover, D.; de Villiers, L.L.; Miller, E.T.; Rowles, H.G.; Shadows, O. Sue McFadden, MLS Beth South, MLS. Available online: https://scholarworks.iu.edu/journals/index.php/jsriue/issue/download/2305/266 (accessed on 15 May 2024).
13. Han, E.; Miller, M.R.; DeVeaux, C.; Jun, H.; Nowak, K.L.; Hancock, J.T.; Ram, N.; Bailenson, J.N. People, places, and time: A large-scale, longitudinal study of transformed avatars and environmental context in group interaction in the metaverse. *J. Comput.-Mediat. Commun.* **2023**, *28*, zmac031. [CrossRef]
14. Irfan, M.; Ali, S.T.; Ijlal, H.S.; Muhammad, Z.; Raza, S. Exploring The Synergistic Effects of Blockchain Integration with IOT and AI for Enhanced Transparency and Security in Global Supply Chains. *Int. J. Contemp. Issues Soc. Sci.* **2024**, *3*, 1326–1338.
15. Reed, D.; Sporny, M.; Longley, D.; Allen, C.; Grant, R.; Sabadello, M.; Holt, J. Decentralized identifiers (dids) v1.0. In *Draft Community Group Report*; W3C: Cambridge, MA, USA, 2020.

16. Truong, V.T.; Le, L.; Niyato, D. Blockchain meets metaverse and digital asset management: A comprehensive survey. *IEEE Access* **2023**, *11*, 26258–26288. [CrossRef]
17. Lai, Y.; Yang, J.; Liu, M.; Li, Y.; Li, S. Web3: Exploring Decentralized Technologies and Applications for the Future of Empowerment and Ownership. *Blockchains* **2023**, *1*, 111–131. [CrossRef]
18. Maesa, D.D.F.; Lisi, A.; Mori, P.; Ricci, L.; Boschi, G. Self sovereign and blockchain based access control: Supporting attributes privacy with zero knowledge. *J. Netw. Comput. Appl.* **2023**, *212*, 103577. [CrossRef]
19. Ghirmai, S.; Mebrahtom, D.; Aloqaily, M.; Guizani, M.; Debbah, M. Self-sovereign identity for trust and interoperability in the metaverse. In Proceedings of the 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta), Haikou, China, 15–18 December 2022; IEEE: New York, NY, USA, 2022; pp. 2468–2475.
20. Yoon, K.; Kim, S.-K.; Jeong, S.P.; Choi, J.-H. Interfacing cyber and physical worlds: Introduction to IEEE 2888 standards. In Proceedings of the 2021 IEEE International Conference on Intelligent Reality (ICIR), Piscataway, NJ, USA, 12–13 May 2021; pp. 49–50.
21. Ahmed, M.R.; Islam, A.M.; Shatabda, S.; Islam, S. Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. *IEEE Access* **2022**, *10*, 113436–113481. [CrossRef]
22. Jaipong, P.; Siripipattanakul, S.; Sriboonruang, P.; Sitthipon, T.; Jaipong, P.; Siripipattanakul, S.; Sriboonruang, P.; Sitthipon, T. A Review of Metaverse and Cybersecurity in the Digital Era. *Int. J. Comput. Sci. Res.* **2023**, *7*, 1125–1132. [CrossRef]
23. Metz, D.; Gurău, M.M. Emerging and Disruptive Technologies: The Metaverse. Implications on Global Security. *Land Forces Acad. Rev.* **2022**, *27*, 411–422. [CrossRef]
24. Chow, Y.W.; Susilo, W.; Li, Y.; Li, N.; Nguyen, C. Visualization and Cybersecurity in the Metaverse: A Survey. *J. Imaging* **2022**, *9*, 11. [CrossRef] [PubMed]
25. Cheng, R.; Chen, S.; Han, B. Towards Zero-trust Security for the Metaverse. *IEEE Commun. Mag.* **2023**, *6*, 156–162. [CrossRef]
26. Canbay, Y.; Utku, A.; Canbay, P. Privacy concerns and measures in metaverse: A review. In Proceedings of the 2022 15th International Conference on Information Security and Cryptography (ISCTURKEY), Ankara, Turkey, 19–20 October 2022; IEEE: New York, NY, USA, 2022; pp. 80–85.
27. Zelenyanszki, D.; Hóu, Z.; Biswas, K.; Muthukkumarasamy, V. A privacy awareness framework for NFT avatars in the metaverse. In Proceedings of the 2023 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 20–22 February 2023; IEEE: New York, NY, USA, 2023; pp. 431–435.
28. Kalyvaki, M. Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction. *J. Metaverse* **2023**, *3*, 87–92. [CrossRef]
29. Nair, V.; Garrido, G.M.; Song, D.; O'Brien, J. Exploring the privacy risks of adversarial VR game design. In Proceedings of the 24th Privacy Enhancing Technologies Symposium, Bristol, UK, 15–20 July 2024; pp. 238–256.
30. Mitrushchenkova, A.N. Personal Identity in the Metaverse: Challenges and Risks. *Kutafin Law Rev.* **2023**, *9*, 793–817. [CrossRef]
31. Saker, M.; Frith, J. Contiguous identities: The virtual self in the supposed metaverse. *First Monday* **2022**, *27*, 12471. [CrossRef]
32. Giannini, T.; Bowen, J.P.; Michaels, C.A.; Smith, C.H. Digital art and identity merging human and artificial intelligence: Enter the metaverse. In Proceedings of the EVA London 2022, BCS Learning & Development, London, UK, 4–8 July 2022; pp. 1–7.
33. Cambronero, M.L. Metaverse, Religions and Metahumans: A Window to a Hypercontrolled Post-pandemic World. *Sci. Et Fides* **2023**, *11*, 121–135. [CrossRef]
34. Awadallah, A.M.; Damiani, E.; Zemerly, J.; Yeun, C.Y. Identity Threats in the Metaverse and Future Research Opportunities. In Proceedings of the 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 7–8 March 2023; IEEE: New York, NY, USA, 2023; pp. 1–6.
35. Wang, S.; Wang, W. A review of the application of digital identity in the Metaverse. *IEEE Trans. Mob. Comput.* **2023**, *2*, 2023009. [CrossRef]
36. Wu, H.; Zhang, W. Digital identity, privacy security, and their legal safeguards in the Metaverse. *Secur. Saf.* **2023**, *2*, 2023011. [CrossRef]
37. Yang, K.; Zhang, Z.; Tian, Y.; Ma, J. A secure authentication framework to guarantee the traceability of avatars in metaverse. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 3817–3832. [CrossRef]
38. 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), Pune, India, 7–9 April 2023; IEEE: New York, NY, USA, 2023; pp. 1–8.
39. 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]
40. Satybaldy, A.; Nowostawski, M.; Ellingsen, J. Self-sovereign identity systems: Evaluation framework. In *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Windisch, Switzerland, August 19–23 2019, Revised Selected Papers 14*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 447–461.
41. 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]

42. Kürtünlüoğlu, P.; Akdik, B.; Karaarslan, E. Security of virtual reality authentication methods in metaverse: An overview. *arXiv* **2022**, arXiv:2209.06447.
43. Stephenson, S.; Pal, B.; Fan, S.; Fernandes, E.; Zhao, Y.; Chatterjee, R. Sok: Authentication in augmented and virtual reality. In Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 22–26 May 2022; IEEE: New York, NY, USA, 2022; pp. 267–284.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.