北 京 科 技 大 学

硕士学位研究生
选题报告及文献总结

论文题目:

RESEARCH ON DECENTRALIZED AND SELF-SOVEREIGN IDENTITY AND MUTUAL AUTHENTICATION IN METAVERSE;

元宇宙分布式自主标识与双向认证研究

指导教师：黄旗明副教授
单位：计算机与通信工程学院通信工程系
学号：M202161026
作者：MUHAMMAD FAIZAN 飞赞
专业名称：信息与通信工程
入学时间：2021 年 9 月
2022 年 12 月 30

TABLE OF CONTENTS

1. Introduction

As the global industrial complex gears toward fulfilling the tenets of Industry 4.0 and beyond, technologies such as distributed ledger, digital twins, and artificial intelligence become pivotal enablers. With the emergence of concepts such as Metaverse and Web 3.0, digital identity plays a very important role as one of its infrastructures. In centralized identity management system, the owner of the digital identity does not actually control his own identity, and there is a risk of easy disclosure and theft of identity information. Self-sovereign Identity (SSI) as a logical alternative to traditional centralized identity management systems. The decentralized identity management scheme based on blockchain technology has the characteristics of distributed data storage, point-to-point transmission, encryption security, consensus confirmation, etc., which can effectively solve the problems of identity verification and operation authorization.

Authentication is a key factor in blockchain based SSI metaverse platform. With the growing number of users, there's a need of some reliable authentication scheme. Mutual Authentication scheme based on the blockchain using biometric information and Elliptic Curve Cryptography provides secure communication between users and platform servers and secure avatar interactions in the metaverse.

1.1. Metaverse

The metaverse is a vision of what many in the computer industry believe is the next iteration of the internet: a single, shared, immersive, persistent, 3D virtual space where humans experience life in ways they could not in the physical world. Some of the technologies that provide access to virtual world, such as virtual reality headsets and augmented reality (AR) glasses, are evolving quickly; other critical components of the metaverse, such as adequate bandwidth or interoperability standards, are probably years off or might never materialize.

1.2. Digital Identity

A digital identity is an online or networked identity adopted or claimed in cyberspace by an individual, organization or electronic device. These users may also project more than one digital identity through multiple communities. In terms of digital identity management, key areas of concern are security and privacy.

The development of digital identity from centralized to decentralized has gone through the following stages:

- **Centralized Identity** is that we use usernames and passwords to log in to all websites
- **Federated Identity** is actually cross-platform login
- **User-centric identities** give users control over their identities
- **SSI model** allows users to not only control their identity but also the data associated with it.

1.3. Blockchain

A blockchain is a tamper-resistant distributed ledger that's used to validate and store digital transactional records. No single authority is responsible for maintaining a Blockchain. Instead, computers in a peer-to-peer (P2P) network each store a copy of the ledger and transactions are verified through a decentralized consensus mechanism.

1.4. Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is a modern type of public-key cryptography wherein the encryption key is made public, whereas the decryption key is kept private. This particular strategy uses the nature of elliptic curves to provide security for all manner of encrypted products.

1.5. Mutual Authentication

Mutual authentication is a security process in which both client and server authenticate each other's identities before actual communication occurs. This is to ensure that clients are communicating exclusively with legitimate entities or servers and so the servers can be certain that the client attempting access has a legitimate purpose.

1.6. Blockchain Based Digital Identity

In the blockchain-enabled digital identity, with the help of asymmetric encryption, the private key owner uses his public key as the unique identifier of the identity, and then associates the identity attributes through smart contracts. Blockchain Based Digital Identity is based on the following approaches:

- **Distributed Authentication** is based on Public Key Infrastructure and its core is digital certificate and the certification authority. The accounting and maintenance of the blockchain can be done jointly by all certificate holders in the system or a blockchain can be formed between CAs, so that the CAs do not have to trust each other, and the issuance and management of digital certificates are completed in consensus manner.
- The core idea of **Cross-agency Security Identity Authorization** is to identify and recognize each other's login requests and authorize access to the corresponding user data through the form of consortium blockchain, forming a trusted and secure identity information interoperability system.

1.7. Blockchain Based Mutual Authentication

A secure mutual authentication scheme using blockchain technology for metaverse environments is based on the avatar authentication phase to guarantee secure avatar-to-avatar interactions in virtual spaces. This scheme comprises five main phases, namely, the initialization, user setup, avatar generation, login and authentication, and avatar authentication phases.

2. SSI Architecture & SSI Industrial Application

2.1. SSI Architecture

The core technology of SSI is distributed ledgers and cryptography, which can be combined with distributed digital identity identifiers and verifiable credentials to create nonrepudiation and tamper-resistant identity records.

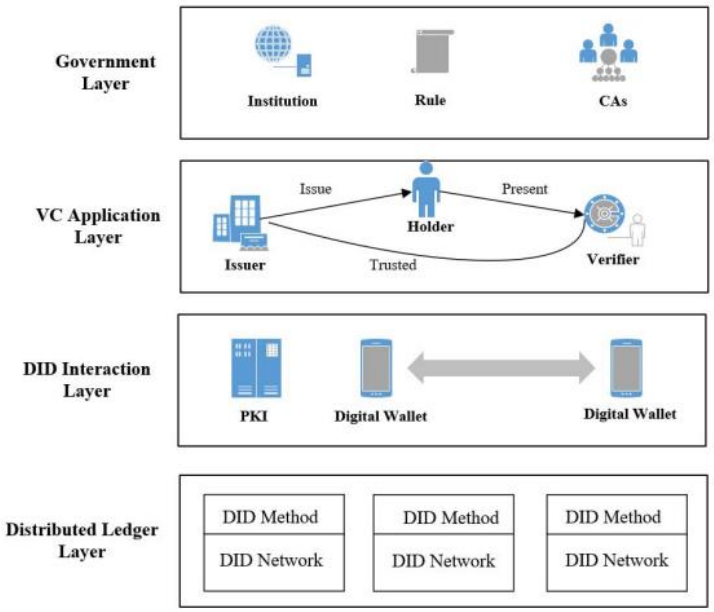

Fig1: SSI Architecture

The four-layer architecture of SSI is discussed below:

- **Distributed Ledger Layer:** The first layer of the SSI architecture is the distributed ledger, which is used as a registry of distributed digital identity identifiers so that no third party can have access to the identifier as long as it ensures that the identity owner maintains control of his or her private key. The characteristic of non-tamping of the distributed ledger makes it suitable for both the publication and maintenance of distributed digital identity data and for verifier verification of credential authenticity.
- **DID Interaction Layer:** The second layer is the combination of the PKI system based on distributed ledger and digital wallet to realize end-to-end interaction between users and perform activities such as certificate application, issuance, update and revocation. As a personal repository, digital wallets can realize user identity information and VC off-chain storage, so that the control of the identity truly returns to the user's hands.
- **VC Application Layer:** The third layer is the VC application layer, which implements the VC interaction of the three entity roles of the issuer, holder and verifier. In the SSI model, users are the central administrators of their identities, and they have far more control over their own data and information than anyone else owns, knows about, or shares.
- **Government Layer:** The fourth layer is the governance layer, where business and legal protocols need to be established to build human trust in a distributed network. In

current implementations of digital identity solutions, the governance model establishes principles, policies, terminology, standards, and responsibilities that define who is a certificate authority and where to find a list of trusted.

2.2. SSI Industrial Application

A scheme for SSI Industrial Application has been discussed. Firstly, generic architecture will be discussed and after that different use cases for industry 4.0 will also be discussed.

2.2.1. Generic Architecture

As per the architecture, there is no entity (e.g., IdP) that issues identities to the users. Each user provides and controls their own identity by using their wallet to generate an identity for a particular (meta)verse (also known as Virtual World or VW in short). In Figure 2, such virtual worlds are represented:

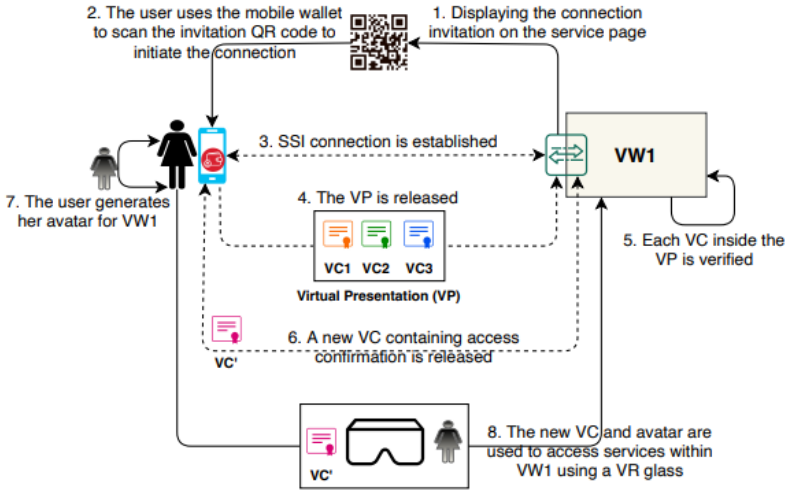

Fig2: Generic SSI Industrial Implementation

1) The VW1 needs to be equipped with an SSI agent to facilitate SSI functionalities. The SSI agent generates a connection invitation which is then displayed as a QR code on the VW1 page.
2) The user uses her mobile wallet to scan the QR code and initiate the connect establishes process between the user and the VW1.
3) DIDs of each entity are exchanged and the corresponding DID Docs are resolved from the blockchain and finally validated. At this point, the connection is established between the user and VW1.
4) The user prepares a VP (Virtual Presentation) consisting of one VC or several VCs to access the service by VW1. This VP is then released to the VW1 using the previously established connection.
5) The VW1 retrieves each VC from the VP and verifies them.
6) The VW1 generates and shares a new VC (denoted with VC ') that is then stored in the wallet of the user.
7) The user generates an avatar for her.
8) The user shares VC ' to access services using the previously created avatar and a VR device.

3. Decentralized Mutual Authentication Protocols

3.1. One-Party Authentication Protocol

The one-party authentication protocol implements dynamic authentication based on a challenge-response mechanism to ensure the consistency of avatar's virtual and physical identities. As shown in Fig. 3: 1) avatar A as a prover claims that his identity is valid; 2) avatar B as a verifier checks the validity of A's virtual identity and throws a random challenge to A to confirm whether A's physical identity matches its virtual identity; 3) avatar A's manipulator provides his biometric feature and corresponding check parameters as a response; 4) avatar B checks the validity of the parameters to determine the consistency of avatar's virtual and physical identities.

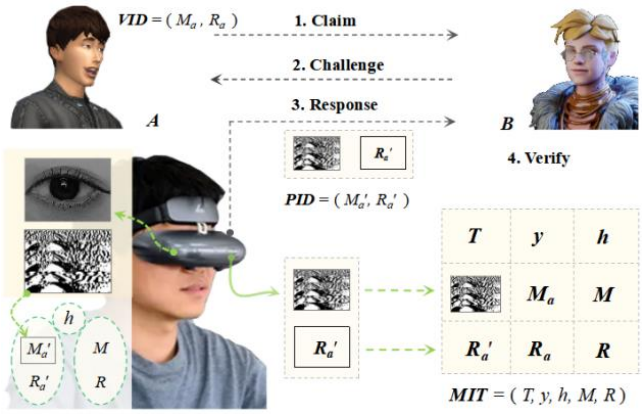

Fig3: Interaction process of one-party authentication protocol

3.2. Two-Party Authentication Protocol

A two-party authentication protocol is designed to realize the decentralized mutual authentication between avatars. The designed protocol adds a session key negotiation based on the one-party protocol to achieve secure communication between avatar A and avatar B. The detailed processes are in the following three phases:

- **Round 1:** In this phase, first avatar A submits an identity claim to avatar B, then B submits a claim of B's identity and a challenge to A.
- **Round 2:** In round 2, first avatar A submits his physical identity parameters as a response and throws a challenge to avatar B, then B submits his own physical identity parameters as a response and sends a session parameter to A.
- **Session Key Establishment:** After A checking the validity of B's physical identity, A establishes the session key K using his private key to realize secure communication.

4. Challenges

Some of the challenges in building a viable and effective SSI architecture and mutual authentication scheme for metaverse are explained below:

- **User Experience:** It includes high threshold for private key management and use of

identifiers. If the user uses multiple DIDs in order to further improve privacy and security, then each identity information corresponds to a DID. It will be doubly difficult to manage DIDs and less acceptable to users. Once the private key is lost, the corresponding data will be lost.

- **Regulation:** More and more criminal organizations are using encrypted information to complete illegal transactions, and since blockchain only guarantees that data information cannot be tampered after it is uploaded, but it cannot guarantee the authenticity and timeliness of information before it is uploaded. The SSI model cannot meet the requirements of regulators when they ask blockchain to provide encrypted information or tamper with related non-compliant transaction records.
- **Right to be Forgotten:** It means having to know exactly where the data is, and also be able to identify yourself to those who own it so they can ask them to delete it, and there is no personal data in an immutable and decentralized registry. Digital wallets should provide easy ways to track where and for what purpose a person's identifiers are used, allowing requests for deletion.
- **Commercial Landing Promotion:** It's the realistic conflict between user data privacy and enterprise data realization. Due to the tendency to protect user data privacy, information disclosure is minimized, and only authentication results are shared. However, at present, a large number of internet companies implement business models based on user big data analysis, such as advertising business, financial business, e-commerce business, etc. These businesses need to be carried out based on the user's identity information. There are real conflicts in conservation that are difficult to reconcile. Companies with data as their core business model have no incentive to participate in such a decentralized digital identity system, so many current SSI applications have not been very successful.

5. Research Methodology

In this section, proposed methodology will be discussed to accomplish the work as follows:

5.1. Literature Review

Literature review is the most important part in carrying out quality research. To get better understanding of the concepts, leading published research papers related to SSI and Mutual Authentication for metaverse will be reviewed. By following this method, various loop holes in the research can be identified and a better solution can be proposed.

5.2. Simulation & Experimentation

After getting deeper understanding of the SSI implementation schemes and Mutual Authentication implementation schemes, they can be simulated on Metaverse Simulation Platforms such as Robox and Cryptovoxels. Already existing schemes and techniques will be simulated as per instructions. After performing different experiments, research gaps xan be found.

5.3. Analysis & Output

After simulation and detecting the research gaps, both formal and informal analysis related to security and us as performance can be carried out. Formal security analysis can be done by using BAN logic proof, ROR model, AVISPA etc. while informal analysis includes MTM attack, offline password guess, Platform server spoofing etc. In performance analysis, computation cost, communication costs can be calculated based on different scenarios and security features can be analyzed as well. Legislation and regulation rules for SSI model can also be proposed for better interoperability. After detailed analysis, most innovative solutions to the current issues can be put forward.

6. Research Objectives

Research objectives has been discussed below:

- Find loop holes in existing work.
- Carry out performance and security tests over existing schemes.
- Address the importance of regulations and legislation for SSI Model.
- Implement different protocols to optimize the models.
- Emerging issues to protect user data and privacy.
- Find easy ways to restrict unauthorized access to personal data od user.
- Improve the interoperability of consortium blockchain.
- Investigate mutual authentication schemes based on blockchain.

7. Research Significance

This research focuses on the field of SSI models, an emerging concept where users have absolute control over personal data information, which makes it more desirable than the current way data is stored in the metaverse. SSI has the potential to solve data security and privacy concerns because it does not require storing personal information in a central database, but instead gives individuals control over the information they store and share. This level of proven and decentralized trust is essential to bring data elements together for a unified and open metaverse. This research work will help to improve supporting interoperability between different solutions, data portability, pseudonymization, traceability, scalability, etc., and will introduce innovative solutions for managing personal digital identities.

In the emerging social ecosystems, however, malicious players frequently violate the safety of other avatars, posing a huge challenge to the healthy development of metaverse. For this issue, various Mutual Authentication Schemes such as two-factor authentication framework based on chameleon signature and biometrics and mutual authentication using ECC and biometric information which guarantees the virtual-physical traceability that tracking an avatar in virtual space to its manipulator in physical world will be tested on real-time metaverse environment and innovative solutions will help to optimize them.

8. Reference List

H. Lee, D. Woo, and S. Yu, ‘‘Virtual reality metaverse system supplementing remote education methods: Based on aircraft maintenance simulation,’’ Appl. Sci., vol. 12, no. 5, p. 2667, Mar. 2022.

S. M. Park and Y. G. Kim, ‘‘A Metaverse: Taxonomy, components, applications, and open challenges,’’ IEEE Access, vol. 10, pp. 4209–4251, 2022

Chen Jidong 濒 Legal Imagination Beyond the Metaverse: Digital Identity, NFT and Multiple Regulations [J/OL], Research on the Rule of Law, 2022(5), pp. 1-12.

L.H. Lee, T. Braud, P. Zhou, Lin Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, P. Hui, “All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda,” 2021, arXiv:2110.05352

E. Bandara, X. Liang, P. Foytik, S. Shetty and K. D. Zoysa, "A Blockchain and Self-Sovereign Identity Empowered Digital Identity Platform," 2021 International Conference on Computer