IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 25 August 2022, accepted 10 September 2022, date of publication 14 September 2022,
date of current version 23 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3206457

RESEARCH ARTICLE

Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain

JONGSEOK RYU[1], SEUNGHWAN SON[1], JOONYOUNG LEE[1], (Student Member, IEEE), YOHAN PARK[2], (Member, IEEE), AND YOUNGHO PARK[1,3], (Member, IEEE)

[1]School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, South Korea
[2]School of Computer Engineering, Keimyung University, Daegu 42601, South Korea
[3]School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea

Corresponding authors: Yohan Park (yhpark@kmu.ac.kr) and Youngho Park (parkyh@knu.ac.kr)

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2021R1I1A3059551.

ABSTRACT During the COVID-19 pandemic, engagement in various remote activities such as online education and meetings has increased. However, since the conventional online environments typically provide simple streaming services using cameras and microphones, there have limitations in terms of physical expression and experiencing real-world activities such as cultural and economic activities. Recently, metaverse environments, three-dimensional virtual reality that use avatars, have attracted increasing attention as a means to solve these problems. Thus, many metaverse platforms such as Roblox, Minecraft, and Fortnite have been emerging to provide various services to users. However, such metaverse environments are potentially vulnerable to various security threats because the users and platform servers communicate through public channels. In addition, sensitive user data such as identity, password, and biometric information are managed by each platform server. In this paper, we design a system model that can guarantee secure communication and transparently manage user identification data in metaverse environments using blockchain technology. We also propose a mutual authentication scheme using biometric information and Elliptic Curve Cryptography (ECC) to provide secure communication between users and platform servers and secure avatar interactions between avatars and avatars. To demonstrate the security of the proposed mutual authentication scheme, we perform informal security analysis, Burrows–Abadi–Needham (BAN) logic, Real-or-Random (ROR) model, and Automated Validation of Internet Security Protocols and Applications (AVISPA). In addition, we compare the computation costs, communication costs, and security features of the proposed scheme with existing schemes in similar environments. The results demonstrate that the proposed scheme has lower computation and communication costs and can provide a wider range of security features than existing schemes. Thus, our proposed scheme can be used to provide secure metaverse environments.

INDEX TERMS Metaverse, avatar, authentication, BAN logic, ROR model, AVISPA, blockchain, elliptic curve cryptography, biohashing.

I. INTRODUCTION

During the recent COVID-19 pandemic, engagement in various remote activities such as online education, meetings, and games increased rapidly to reduce the risk of infection. People can use convenient services such as real-time education, telecommuting, and video conferencing without physically contacting others in the online environment. However, conventional online environments only provide simple streaming services using cameras and microphones. As a result, such environments are limited in terms of physical expression and social, cultural, and economic activities [1], [2]. Thus, existing online services cannot provide users with experiences similar to the real world. With the recent development of computer vision and graphics processing technologies, metaverse environments are expected to

The associate editor coordinating the review of this manuscript and approving it for publication was Zijian Zhang.

overcome the limitations of online services by providing more realistic experiences.

Metaverse [3] is derived from the science fiction novel ''Snow Crash'' by Neal Stevenson in 1992. It is a combination of the words ''meta'' (meaning virtual and transcendent) and ''universe'' (meaning space and world). In a metaverse environment, users can access various virtual spaces using smart devices such as goggles and earphones, and engage in various remote and virtual activities including education, travel, and trade, using avatars. In other words, a metaverse environment can be defined as a three-dimensional virtual reality in which social, cultural, and economic activities are possible using avatars [4]. Thus, the metaverse environments can provide more immersive experiences than existing online environments and they are expected to be used widely [5], [6]. With the increasing popularity of the metaverse environments, various metaverse platforms such as Roblox, Minecraft, and Fortnite have emerged to provide virtual reality experiences using avatars. In addition, various devices such as HTC VIVE and Oculus Quest that employ AR(Augmented Reality), VR(Virtual Reality), and XR(eXtended Reality) technologies are utilized in metaverse platforms to provide realistic services using the physical information of users such as gaze and motion data.

Currently, metaverse platforms provide various services using virtual spaces and avatars, such as education, telecommuting, and gaming [7]. Users must register with the appropriate platform servers to access the desired service managed by various platforms. Then, users can communicate with the platform servers and transmit their physical information such as gaze and motion data using their smart devices. The platform servers provide various virtual spaces to the users and render the user's avatar in real-time using the received physical data. In addition, the users can utilize their avatars to communicate with other avatars for interactions such as trading and chatting through the platform server [8]. Therefore, users can express their actions and perform various activities using their avatars in metaverse environments.

Although metaverse environments can provide various appealing services, several problems must be addressed. In metaverse environments, the users and platform servers communicate through public channels. Thus, an adversary can attempt to forge and modify communication messages and attempt various security attacks such as impersonation and man-in-the-middle (MITM) attacks. In addition, users must register with each platform server to use the corresponding services. However, this is inconvenient for users because they must send information such as identifiers, passwords, and personal data every time to register with each platform server. Moreover, user identification data such as identifiers and passwords depend on each platform server, which means that the integrity of user data must be ensured because forgery and modification of the user data can cause various security problems. Furthermore, an adversary can legally create a malicious avatar to deceive people in such virtual spaces. However, an avatar cannot verify the identity of whether the other avatars are malicious. This can cause serious problems such as identity leakage, theft, and virtual asset fraud during avatar interactions.

To solve these problems, secure communication must be provided between users and platform servers. Avatar authentication is also required to provide secure avatar interactions such as trading and chatting in virtual spaces. In addition, secure and transparent management of user identification data is required. In this paper, we utilize blockchain technology to prevent the dependency of user data on each platform server and provide security of user data. Then, we design a system model using blockchain technology for metaverse environments. In our system model, we manage the user identification data in blockchain to provide user data integrity and transparency. We also propose an authentication scheme utilizing blockchain between users and platform servers and between avatars and avatars to ensure secure communication and avatar interactions in metaverse environments.

A. CONTRIBUTIONS

Our primary contributions are summarized as follows.

- We design a system model to guarantee secure communication and avatar interactions in metaverse environments. In this system model, we suggest transparent management of each user's pseudo-identity and public key using blockchain technology.
- We propose a mutual authentication scheme using Elliptic Curve Cryptography (ECC) and biometric information to provide secure communication between users and platform servers. In addition, we propose an avatar authentication scheme to provide secure avatar-to-avatar interactions.
- We perform an informal analysis to show that the proposed scheme can withstand a variety of security attacks including impersonation, stolen smart devices, MITM, and insider attacks. We also prove that the proposed scheme can guarantee mutual authentication and security of the session key utilizing the Burrows–Abadi–Needham (BAN) logic [9] and the Real-or-Random (ROR) model [10].
- We demonstrate that the proposed scheme can resist replay and MITM attacks utilizing the Automated Validation of Internet Security Protocols and Applications (AVISPA) [11]. In addition, we estimate the computation and communication costs of the proposed scheme. Finally, we compare the performance and security features of the proposed scheme with existing schemes in similar environments.

B. ORGANIZATION

The remainder of this paper is organized as follows. Related work is introduced in Section II, and relevant preliminaries including the Blockchain, ECC, Biohashing, the adversary model, and the system model are described in Section III. The proposed mutual authentication scheme to guarantee

secure communication is proposed in Section IV. The security and performance of the proposed scheme are discussed in Section V and Section VI, respectively. Finally, the paper is concluded in Section VII.

II. RELATED WORK

After the term metaverse appeared in the novel Snow Crash, developments in the computer vision and graphic fields made it possible to realize virtual reality technologies. In 2003, the Second Life platform [12] which is a client-server architecture was launched to provide a metaverse environment. In Second Life, users can participate in various activities such as avatar creation, attending virtual classes, and virtual item trading. In 2007, smart *et al.* [13] presented representative research of the metaverse. They asserted a metaverse roadmap and provided a definition of a metaverse that included four primary components, namely, augmented reality, lifelogging, mirror worlds, and virtual worlds. Their research created a broader concept of the metaverse and led to the emergence of various metaverse platforms. In the last few years, several metaverse gaming platforms have been launched, including Roblox, Fortnite, and Minecraft, and these platforms allow users to create their own avatars and interact with each other [14]. Recently, metaverse education platforms have also been studied. In 2021, Gan *et al.* [15] proposed a virtual reality teaching platform to provide immersive education for users. In 2022, Jovanovic and Milosavljevic [16] proposed the VoRtex platform to provide an educational experience and support collaborative learning activities in virtual spaces.

As metaverse research increases, several studies have discussed the security of metaverse environments [17], [18], [19], [20], [21]. In 2016, O'Brolchain *et al.* [17] claimed that privacy threats are possible in virtual reality because users perform many tasks and activities in virtual spaces, and user data are frequently communicated with servers and other users through public channels. In addition, user devices store personal data to access a virtual reality. Thus, unauthorized and malicious users can easily access user data and compromise user information. O'Brolchain *et al.* also discussed various countermeasures such as data encryption, data transparency, and end-to-end encryption to address privacy threats in virtual reality. In addition, in 2018, Falchuk *et al.* [18] asserted the importance of privacy in metaverse environments and they categorized the privacy type as personal information, behavior, and communication data. They said that personal information could be exposed to others when interacting with malicious avatars such as trading and chatting in virtual spaces. Therefore, an adversary can try various attacks such as invasion of privacy, impersonation, and identity theft, using the obtained personal information. In 2019, Guzman *et al.* [19] organized the general security and privacy requirements for virtual reality environments. They stated that device security is important because users communicate using various smart devices in virtual reality. They also claimed that data integrity, authorization, user authentication, and data confidentiality are requirements in the design of a virtual reality system to prevent various security threats. In 2022, Tan *et al.* [20] proposed using blockchain technology in metaverse environments to realize decentralization and interoperability. They said that blockchain technology can be employed to protect, store, and share data. Moreover, in 2022, Yang *et al.* [21] claimed that blockchain technology can be used to realize data transparency, openness, authenticity, and efficiency in metaverse environments. However, a specific system model and mutual authentication scheme for metaverse environments have not been proposed to date.

In the following, we introduce several existing mutual authentication schemes for guaranteeing secure communication in IoT environments that are similar to metaverse environments. In 2020, Panda and Chattopadhyay [22] proposed a mutual authentication scheme for IoT environments using ECC and a password verifier. They analyzed the security aspects of their scheme using the AVISPA tool. However, Chen *et al.* [23] asserted that the scheme proposed by Panda and Chattopadhyay does not consider various security features such as stolen smartcards and user impersonation attacks. Haq *et al.* [24] proposed a two-factor authentication protocol for 5G networks and they performed informal and formal security analyses to prove that their scheme can prevent a variety of security attacks. Unfortunately, their protocol is still vulnerable to user/server impersonations, MITM, and privileged insider attacks [25]. In 2022, Li *et al.* [26] proposed a blockchain-based mutual authentication scheme for key agreements between users and servers. They stated that their scheme can prevent impersonation and MITM attacks, and that it can provide perfect forward secrecy. However, their scheme does not handle other security features such as insider, privileged insider attacks, and user anonymity. Although [22], [24], and [26] can be utilized for a metaverse environment, these schemes lack the security features required to ensure secure communication, and they do not consider user-to-user authentication.

III. PRELIMINARIES

In this section, we describe simple preliminary concepts including Blockchain, ECC, and Biohashing. We then explain the adversary model and system model used in this paper.

A. BLOCKCHAIN

The blockchain [27] is a distributed ledger that provides data transparency, integrity, and tamper resistance. Blockchain can be classified into permissionless (public) blockchains and permissioned blockchains [28], [29]. In a permissionless blockchain such as Bitcoin and Ethereum, anyone can read data, write data, and participate in the consensus process. Note that anyone can freely enter or leave the network without authorization, including potentially malicious adversaries. Permissioned blockchains can be divided into private permissioned blockchains (e.g., Hyperledger Fabric) and public permissioned blockchains (e.g., Sovrin). In both private and public permissioned blockchains, participation in the writing

and consensus processes is limited. Here, the consensus process is performed by a selected group of trusted nodes. However, private permissioned blockchains restrict read access, and public permissioned blockchains allow anyone to read the data. Therefore, we utilize a public permissioned blockchain to manage user pseudo-identity and public keys transparently in metaverse environments.

B. ELLIPTIC CURVE CRYPTOGRAPHY

ECC, which employs an elliptic curve over a large finite field, provides better security performance with smaller key sizes than existing public-key cryptography techniques [30], [31]. Assume that p is a large prime, F_p represents prime fields, $u, r \in F_p$, and $4u^3 + 27r^2 \neq 0 \ (mod\ p)$. Then, a nonsingular elliptic curve $E_p(u, r)$ over F_p is denoted $E_p(u, r) : y^2 = x^3 + ux + r \ (mod\ p)$. In addition, assume that Q is a base point on $E_p(u, r)$ and a positive integer $t \in F_p$. Then, the point multiplication is denoted $t \cdot Q = Q + \cdots + Q$ (t times). ECC security is based on the following problems.

- Elliptic Curve Discrete Logarithm Problem (ECDLP). Assume that P and Q are two points on $E_p(u, r)$ and $x \in F_p$. However, it is computationally difficult to determine x from $Q = x \cdot P$.
- Elliptic Curve Diffie-Hellman Problem (ECDHP). Assume that P, $x_1 \cdot P$, and $x_2 \cdot P$ are three points on $E_p(u, r)$. However, it is computationally difficult to determine $x_1 \cdot x_2 \cdot P$.
- Elliptic Curve Decisional Diffie-Hellman Problem (ECDDHP). Assume that $P, x_1 \cdot P, x_2 \cdot P$, and $x_3 \cdot P$ are four points on $E_p(u, r)$ and $x_1, x_2, x_3 \in Z_p^*$. However, it is difficult to determine whether $x_3 \cdot P = x_1 \cdot x_2 \cdot P$.

C. BIOHASHING

Biometric information of the user can be used as an additional factor in an authentication system and is a suitable way to identify a real user. Jin *et al.* [32] introduced a biohashing function using fingerprint data to verify users, and they demonstrated that fingerprint data of users can be converted to a bit form using biohashing.

- The biometric feature is extracted from the fingerprint and represented as a vector $v \in R^n$.
- A set of pseudo-random numbers $r_i \in R^n (i = 1, \ldots, n)$ is generated the using Blum–Blum–Shub methods.
- Apply the Gram-Schmidt procedure with generated pseudo-random number to transform the basis r_i into an $or_i \in R^n (i = 1, \ldots, n)$.
- Calculate the inner product operation between v and or_i. As a result, the biohash code b_i is computed as follows.

$$b_i = \begin{cases} 0, & if\ \langle v|or_i\rangle \leq \tau \\ 1, & if\ \langle v|or_i\rangle > \tau, \end{cases}$$

where τ is a preset threshold.

D. ADVERSARY MODEL

We consider the widely used "Dolev-Yao(DY) model" [33], [34] for analyzing protocol security. Following this model, an adversary has complete control of all messages communicated via public channels and can eavesdrop, delete, and modify these messages. Thus, the adversary can attempt various security attacks. The abilities of the adversary can be defined as follows.

- An adversary can perform security attacks such as impersonation, replay, and MITM attacks.
- An adversary can obtain a user's smart device. Then, the adversary can extract all data stored on the smart device using power analysis attacks [35], [36], [37].
- An adversary can legally create an avatar and attempt to impersonate other avatars.
- An adversary can be an insider in the platform server.

Furthermore, we also adopt the "Canetti-Krawczyk (CK) model" [38], which has a stronger assumption than the DY model. In the CK model, an adversary can obtain ephemeral values such as random numbers or long-term values such as private and master keys. Then, the adversary can attempt to compute the session key by conducting the ephemeral secret leakage attack.

E. SYSTEM MODEL

The system model for a metaverse environment consists of the certificate authority, users, platform servers, and a blockchain, as represented in Figure 1.

- Certificate authority: The certificate authority is a fully-trusted entity that initializes system parameters and publishes public information. The certificate authority receives the user's pseudo-identity, public key, and personal information from the user. Then, the certificate authority uses the received personal information to verify the user's identity once and stores the user's pseudo-identity and public key in the blockchain. In addition, the certificate authority creates user credential values that must be authenticated between the user and the platform servers, and the certificate authority transmits the credential values to the user.
- User: The user sends the pseudo-identity, public key, and personal information to the certificate authority for identity verification to participate in the metaverse environment. Then, the user can communicate with various platform servers through an authentication process that uses the user's pseudo-identity and credential values. Afterward, the user can create an avatar and access various virtual spaces managed by the platform servers. In addition, the user can authenticate with the other avatars using the pseudo-identity and the public key stored in the blockchain to achieve secure avatar-to-avatar interaction in virtual spaces.
- Platform server: Each platform server provides different immersive services such as education and game services to users through various virtual spaces. If a user attempts to access the platform server, the platform server verifies their credential value and pseudo-identity using the blockchain and the public key of the certificate authority.

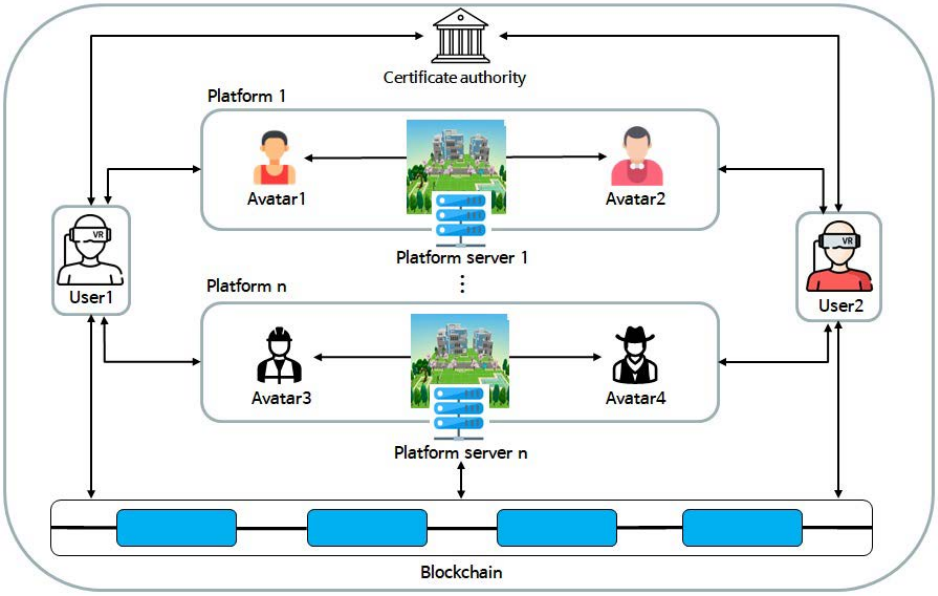

FIGURE 1. The proposed system model for a metaverse environment.

In addition, each platform server is responsible for forwarding request and response messages in their virtual spaces for avatar authentication processes.

- Blockchain: The public permissioned blockchain is adopted in our scheme. Thus, any node can read the data in the blockchain; however, only a selected group of entities such as the certificate authority and platform servers can participate in the consensus process. In our system model, we manage identification data of users such as the pseudo-identity and public key in blockchain to provide data integrity and data transparency. Users must transmit their personal information to the certificate authority for uploading their identification data. After a certificate authority verifies the user's identity, the certificate authority uploads the pseudo-identity and public key of users to the blockchain. Then, the blockchain transparently manages the user's pseudo-identity and public keys. As a result, the platform servers can verify whether users are legitimate using the data stored in the blockchain. Furthermore, a user can verify another avatar's identity through the avatar authentication phase using the blockchain in virtual spaces.

The process of the proposed system model is as follows.

1) The user transmits their pseudo-identity, public key, and personal information to the certificate authority to verify their identity and obtain credential values to participate in the metaverse environments.
2) The user can create an avatar on each platform server using their pseudo-identity, public key, and credential values. Afterward, the user transmits an authentication message to the appropriate platform server for entering the corresponding virtual spaces.
3) If the authentication phase is completed successfully, the platform server sends a session key to the user, and then the user and platform server communicate using the session key to guarantee secure communication.
4) A user who has already entered a virtual space using an avatar can interact with the other avatars. For secure avatar-to-avatar interactions, the user can perform the avatar authentication phase.

IV. PROPOSED SCHEME

In this section, we propose a secure mutual authentication scheme using blockchain technology for metaverse environments. In addition, we consider the avatar authentication phase to guarantee secure avatar-to-avatar interactions in virtual spaces. The proposed scheme comprises five main phases, namely, the initialization, user setup, avatar generation, login and authentication, and avatar authentication phases. The notations used in the proposed scheme are defined in Table 1.

A. INITIALIZATION PHASE

In the initialization phase, CA selects a nonsingular elliptic curve $E_p(u, r)$ over F_p. Afterward, CA selects a base point P on $E_p(u, r)$ and a private key k_{ca}. CA then computes a public key $PK_{ca} = k_{ca} \cdot P$ and publishes the system parameters $\{E_p(u, r), P, PK_{ca}, h(\cdot), h_b(\cdot)\}$.

B. USER SETUP PHASE

In the user setup phase, U_i must verify the identity from CA to obtain the credentials required to participate in the metaverse environment. The process of the user setup phase is shown in Figure 2 and is described as follows.

TABLE 1. Notations of our scheme.

Notaion	Definition
CA	Certificate authority
U_i	User
S_t	Platform server
ID_i	Identity of U_i
PID_i	Pseudo-identity of U_i
PW_i	Password of U_i
B_i	Biometric information of U_i
SD_i	Smart device of U_i
$avatar_i$	Avatar identity of U_i
$info_i$	Personal information of U_i
PK_{ca}, PK_i, PK_{st}	Public key of CA, U_i, and S_t
k_{ca}, k_i, k_{st}	Private key of CA, U_i, and S_t
Sig_{i-ca}	Signature value generated by CA
$RN_i, x_i, n_i, n_1, n_2, n_3, n_4$	Random numbers
T_1, T_2, T_3, T_4	Timestamps
SK	Session key
SYE_k/SYD_k	Symmetric encryption/decryption
$h(\cdot)$	One-way hash function
$h_b(\cdot)$	Biohash function
$\oplus$	Exclusive or operation
$\|\|$	Concatenation operation

1) U_i inputs ID_i, PW_i, and B_i in SD_i and generates a random number RN_i and private key k_i. Thereafter, U_i computes a pseudo-identity $PID_i = h(ID_i||RN_i)$ and public key $PK_i = k_i \cdot P$. Afterward, U_i transmits the message $\{PID_i, PK_i, info_i\}$ to CA via a secure channel, where $info_i$ is the personal information of U_i.
2) CA checks the uniqueness of (PID_i, PK_i) in the blockchain and verifies $info_i$. If this process is completed successfully, CA generates a random number x_i and computes $X_i = x_i \cdot P$ and $Sig_{i-ca} = x_i + h(PID_i||PK_i||X_i) \cdot k_{ca}$, where Sig_{i-ca} is the signature value used to confirm that U_i is verified by CA. Then, CA sends $V_i = (X_i, Sig_{i-ca})$ to U_i and stores (PID_i, PK_i) in the blockchain.
3) U_i computes $HPW_i = h(ID_i||PW_i||h_b(B_i))$, $RPW_i = h(PW_i||h_b(B_i)||RN_i)$, $Z_1 = RN_i \oplus HPW_i$, $Z_2 = h(ID_i||HPW_i||RPW_i||RN_i)$, and $Z_3 = V_i \oplus RPW_i$, and then stores $\{Z_1, Z_2, Z_3\}$ on SD_i.

C. AVATAR GENERATION PHASE

In the avatar generation phase, U_i can generate an avatar using SD_i to enter the virtual space managed by S_t. Figure 3 presents the avatar generation phase, which is described in detail as follows.

1) U_i inputs ID_i, PW_i, and B_i in SD_i. Then, U_i computes $HPW_i = h(ID_i||PW_i||h_b(B_i))$, $RN_i = Z_1 \oplus HPW_i$, $RPW_i = h(PW_i||h_b(B_i)||RN_i)$, and $Z_2^* = h(ID_i||HPW_i||RPW_i||RN_i)$, and checks $Z_2^* \stackrel{?}{=} Z_2$.
2) If it is equal, U_i generates a random number n_i and $avatar_i$, where $avatar_i$ is the unique ID used in S_t. U_i then computes $V_i = Z_3 \oplus RPW_i$, $N_i = n_i \cdot P$, $S_i = k_i \cdot PK_{st}$, $C_i = n_i + h(avatar_i||PID_i||X_i||Sig_{i-ca}) \cdot k_i$, and $EM_i = (N_i||C_i||X_i||Sig_{i-ca}) \oplus h(avatar_i||PID_i||S_i)$. Thereafter, U_i sends $\{avatar_i, PID_i, EM_i\}$ to S_t through the secure channel.
3) S_t checks PID_i in the blockchain and retrieves PK_i. Then, S_t verifies the uniqueness of $(avatar_i, PK_i)$ in the database and computes $S_i^* = k_{st} \cdot PK_i$ and $(N_i||C_i||X_i||Sig_{i-ca}) = EM_i \oplus h(avatar_i||PID_i||S_i^*)$. Afterward, S_t verifies $C_i \cdot P \stackrel{?}{=} N_i + h(avatar_i||PID_i||X_i||Sig_{i-ca}) \cdot PK_i$ and $Sig_{i-ca} \cdot P \stackrel{?}{=} X_i + h(PID_i||PK_i||X_i) \cdot PK_{ca}$. If it is equal, S_t stores $(avatar_i, PK_i)$ in the database and publishes $(avatar_i, PK_i)$ in the virtual space.

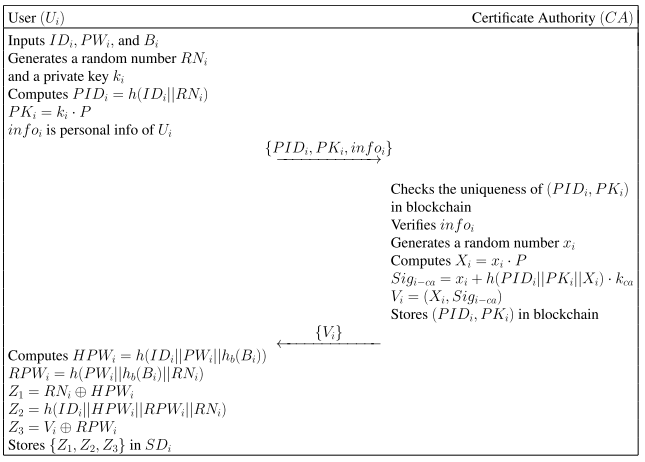

FIGURE 2. User setup phase of our scheme.

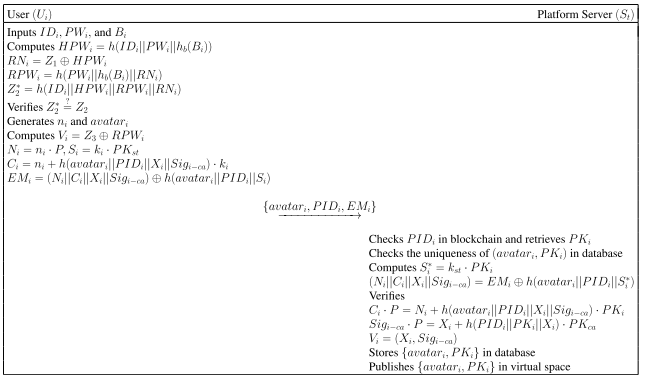

FIGURE 3. Avatar generation phase of our scheme.

D. LOGIN AND AUTHENTICATION PHASE

U_i can login to S_t with $avatar_i$ to enter the virtual space. U_i and S_t perform the following steps to obtain the session key to realize secure communication. Figure 4 describes the login and authentication phase.

1) U_i inputs ID_i, PW_i, and B_i in SD_i. Then, U_i calculates $HPW_i = h(ID_i||PW_i||h_b(B_i))$, $RN_i = Z_1 \oplus HPW_i$, $RPW_i = h(PW_i||h_b(B_i)||RN_i)$, and $Z_2^* = h(ID_i||HPW_i||RPW_i||RN_i)$, and verifies $Z_2^* \stackrel{?}{=} Z_2$.

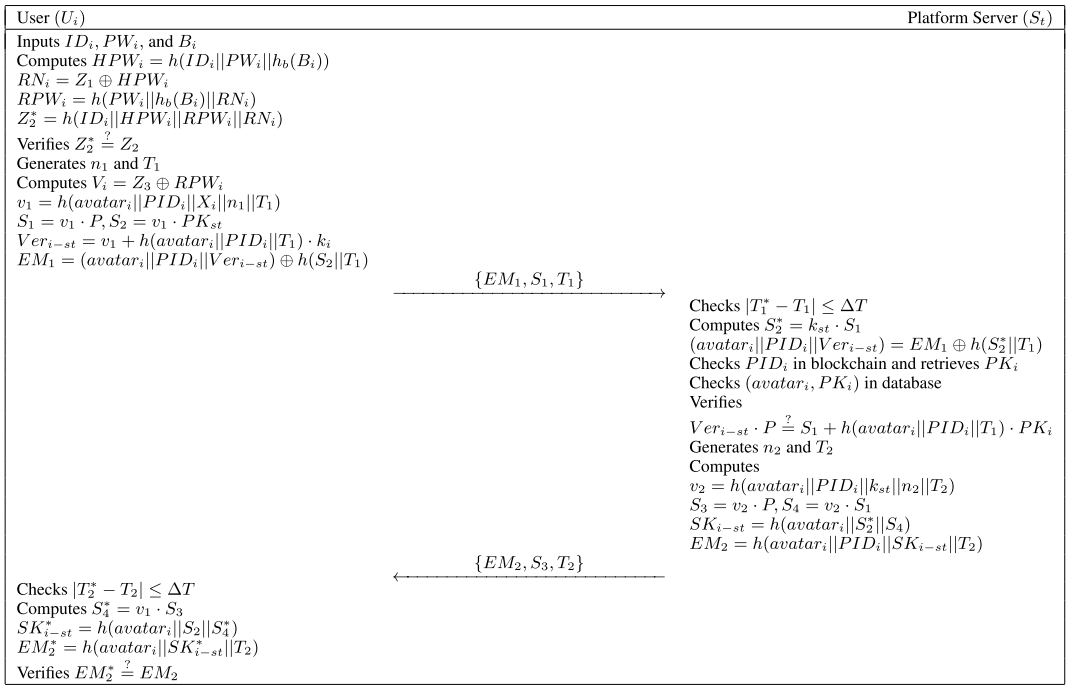

FIGURE 4. Login and authentication phase of our scheme.

2) If it is same, U_i generates a random number n_1 and timestamp T_1. Afterward, U_i calculates $V_i = Z_3 \oplus RPW_i$, $v_1 = h(avatar_i||PID_i||X_i||n_1||T_1)$, $S_1 = v_1 \cdot P$, $S_2 = v_1 \cdot PK_{st}$, $Ver_{i-st} = v_1 + h(avatar_i||PID_i||T_1) \cdot k_i$, and $EM_1 = (avatar_i||PID_i||Ver_{i-st}) \oplus h(S_2||T_1)$. Then, U_i sends the message $\{EM_1, S_1, T_1\}$ to S_t via the public channel.
3) After receiving $\{EM_1, S_1, T_1\}$ from U_i, S_t checks T_1 by the condition $|T_1^* - T_1| \leq \Delta T$. Thereafter, S_t computes $S_2^* = k_{st} \cdot S_1$ and $(avatar_i||PID_i||Ver_{i-st}) = EM_1 \oplus h(S_2^*||T_1)$. Then, S_t verifies that $Ver_{i-st} \cdot P \stackrel{?}{=} S_1 + h(avatar_i||PID_i||T_1) \cdot PK_i$.
4) If it is equal, S_t computes $v_2 = h(avatar_i||PID_i||k_{st}||n_2||T_2)$, $S_3 = v_2 \cdot P$, $S_4 = v_2 \cdot S_1$, $SK_{i-st} = h(avatar_i||S_2^*||S_4)$, and $EM_2 = h(avatar_i||PID_i||SK_{i-st}||T_2)$. Then, S_t transmits the message $\{EM_2, S_3, T_2\}$ to U_i via the public channel.
5) After obtaining $\{EM_2, S_3, T_2\}$ from S_t, U_i checks whether $|T_2^* - T_2| \leq \Delta T$. If this is valid, U_i calculates $S_4^* = v_1 \cdot S_3$, $SK_{i-st}^* = h(avatar_i||S_2||S_4^*)$, and $EM_2^* = h(avatar_i||SK_{i-st}^*||T_2)$. Afterward, U_i verifies the condition that $EM_2^* \stackrel{?}{=} EM_2$. If the equation is the same, U_i and S_t have successfully finished the login and authentication phase. In the future, U_i and S_t use SK_{i-st} for their secure communication.

E. AVATAR AUTHENTICATION PHASE

The avatar authentication phase is only available to users logged into and exchanged session keys with the platform server for secure avatar interaction in the virtual space. In this phase, the platform server is only responsible for forwarding request and response messages. In the virtual space, avatars can perform mutual authentication according to the following process. Figure 5 indicates the avatar authentication phase.

1) U_i generates n_3 and T_3. Then, U_i computes $v_3 = h(avatar_i||PID_i||X_i||n_3||T_3)$, $S_5 = v_3 \cdot P$, $S_6 = v_3 \cdot PK_j$, $Ver_i = v_3 + h(avatar_i||avatar_j||S_6||T_3) \cdot k_i$, $EM_3 = (PID_i||Ver_i) \oplus h(S_6||T_3)$, and $Req = SYE_{SK_{i-st}}(avatar_j, EM_3, S_5, T_3)$. Afterward, U_i sends the authentication request message Req to S_t.
2) After receiving Req from U_i, S_t calculates $(avatar_j, EM_3, S_5, T_3) = SYD_{SK_{i-st}}(Req)$. Then, S_t encrypts Req_{ij} using the session key between U_j and S_t such as $Req_{ij} = SYE_{SK_{j-st}}(EM_3, S_5, T_3)$. Thereafter, S_t transmits Req_{ij} to U_j.
3) U_j computes $(EM_3, S_5, T_3) = SYD_{SK_{j-st}}(Req_{ij})$, $S_6^* = k_j \cdot S_5$, and $(PID_i||Ver_i) = EM_3 \oplus h(S_6^*||T_3)$. Afterward, U_j checks PID_i in the blockchain and retrieves PK_i. Then, U_j verifies $Ver_i \cdot P \stackrel{?}{=} S_5 + h(avatar_i||avatar_j||S_6^*||T_3) \cdot PK_i$.
4) If it is same, U_j generates n_4 and T_4. Then, U_j calculates $v_4 = h(avatar_j||PID_j||X_j||n_4||T_4)$, $S_7 = v_4 \cdot P$, $S_8 = v_4 \cdot S_5$, $Ver_j = v_4 + h(avatar_j||avatar_i||S_8||T_4) \cdot k_j$, $EM_4 = (PID_j||Ver_j) \oplus h(S_8||T_4)$, and $Res = SYE_{SK_{j-st}}(avatar_i, EM_4, S_7, T_4)$. Afterward U_j sends the response message Res to S_t.
5) After receiving Res from U_j, S_t calculates $(avatar_i, EM_4, S_7, T_4) = SYD_{SK_{j-st}}(Res)$. Then, S_t encrypts Res_{ij} using the session key between U_i and S_t such as

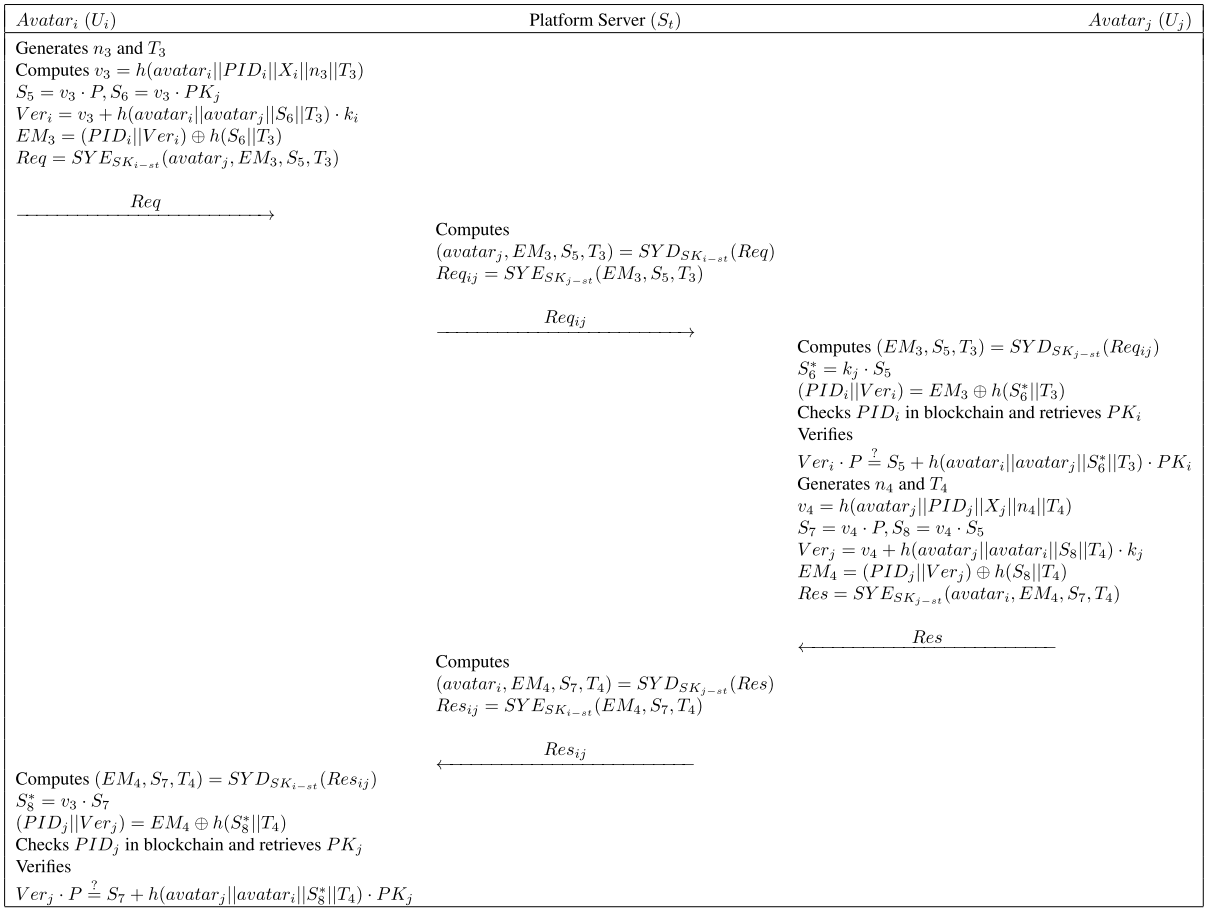

FIGURE 5. Avatar authentication phase of our scheme.

$Res_{ij} = SYE_{SK_{i-st}}(EM_4, S_7, T_4)$. Thereafter, S_t transmits Res_{ij} to U_i.

6) U_i computes $(EM_4, S_7, T_4) = SYD_{SK_{i-st}}(Res_{ij})$, $S_8^* = v_3 \cdot S_7$, and $(PID_j||Ver_j) = EM_4 \oplus h(S_8^*||T_4)$. Then, U_i checks PID_j in the blockchain and retrieves PK_j. Afterward, U_i verifies $Ver_j \cdot P \stackrel{?}{=} S_7 + h(avatar_j||avatar_i||S_8^*||T_4) \cdot PK_j$. If all steps are completed successfully, U_i and U_j can prove that $avatar_i$ and $avatar_j$ are their own.

V. SECURITY ANALYSIS

In this section, we present an informal security analysis of the proposed scheme. In addition, we present a formal security analysis of the proposed scheme using the AVISPA tool, BAN logic, and ROR model. As a result, we prove that the proposed scheme can resist various security attacks.

A. INFORMAL SECURITY ANALYSIS

Through this informal security analysis, we demonstrate that the proposed scheme is resistant to various security attacks including stolen smart devices, offline password guessing, impersonation, platform server spoofing, reply, MITM, insider, privileged insider, and ephemeral secret leakage (ESL) attacks. Furthermore, we demonstrate that the proposed scheme guarantees perfect forward secrecy, user anonymity, and mutual authentication.

1) STOLEN SMART DEVICES ATTACK

Following the adversary model, assume that an adversary obtains SD_i and can extract the stored parameters $\{Z_1, Z_2, Z_3\}$. However, all the parameters are masked with hash and XOR operations using ID_i, PW_i, and B_i so that the adversary cannot obtain sensitive information about U_i. Thus, our scheme can protect against stolen smart device attacks.

2) OFFLINE PASSWORD GUESSING ATTACK

Assume that an adversary eavesdrops transmitted messages $\{EM_1, S_1, T_1\}$, and $\{EM_2, S_2, T_2\}$ through the public channel and extracts the parameters $\{Z_1, Z_2, Z_3\}$ stored on SD_i. Then, the adversary can try to compute the sensitive information of U_i. However, the adversary cannot calculate any sensitive information such as $Z_1 = RN_i \oplus h(ID_i||PW_i||h_b(B_i))$ and $Z_3 = V_i \oplus h(PW_i||h_b(B_i)||RN_i)$ without knowing ID_i, PW_i, and B_i. Therefore, our scheme is resistant to offline password guessing attacks.

3) IMPERSONATION ATTACK

Suppose that an adversary can eavesdrop on the transmitted message via the public channel. If an adversary wants to impersonate U_i, they should create a login request message $\{EM_1, S_1, T_1\}$. However, the adversary cannot create the login request message because they do not know U_i's identity ID_i, password PW_i, biometric information B_i, random numbers RN_i, n_1, and private key k_i. As a result, our scheme can withstand impersonation attacks.

4) PLATFORM SERVER SPOOFING ATTACK

An adversary can intercept messages $\{EM_1, S_1, T_1\}$ and $\{EM_2, S_3, T_2\}$ through an insecure channel for spoofing S_t. Then, the adversary attempts to deceive legitimate users by generating a response message $\{EM_2^*, S_3^*, T_2^*\}$. However, under the proposed scheme, the adversary cannot generate the response message because they cannot compute S_2, S_3, and v_2 without the random number n_2 and private key k_{st}. Thus, our scheme can resist platform server spoofing attacks.

5) REPLAY AND MITM ATTACKS

Assume that the adversary eavesdrops on the transmitted messages $\{EM_1, S_1, T_1\}$ and $\{EM_2, S_3, T_2\}$ via the public channel. However, the adversary cannot reuse these messages for the login and authentication phase because they verify the timestamps $\{T_1, T_2\}$ and random numbers $\{n_1, n_2\}$ to confirm the freshness of the messages. In addition, the adversary cannot calculate EM_1, S_1, EM_2, and S_3 without knowing the random numbers n_1, n_2 and private keys k_i, k_{st}. Therefore, our scheme is resistant to both replay and MITM attacks.

6) PERFECT FORWARD SECRECY

Let be the adversary can intercept messages $\{EM_1, S_1, T_1\}$ and $\{EM_2, S_3, T_2\}$ via an insecure channel and obtain long-term secret keys $\{k_i, k_{st}\}$. Then, the adversary can attempt to compute $SK_{i-st} = h(avatar_i||S_2||S_4)$. However, the adversary cannot calculate $v_2 = h(avatar_i||PID_i||k_{st}||n_2||T_2)$ and $S_4 = v_2 \cdot P$ without knowing random number n_2. As a result, our scheme provides perfect forward secrecy.

7) INSIDER ATTACK

According to the adversary model, a malicious adversary can generate a malicious avatar and access S_t. In addition, the adversary can intercept messages $\{EM_1, S_1, T_1\}$ and $\{EM_2, S_3, T_2\}$. However, the adversary cannot calculate the parameters required to impersonate U_i such as $v_1 = h(avatar_i||PID_i||X_i||n_1||T_1)$ and $Ver_{i-st} = v_1 + h(avatar_i||PID_i||T_1) \cdot k_i$, without the private key k_i and random number n_1. Furthermore, assume that the adversary obtains the messages Req, Req_{ij}, Res, and Res_{ij}. However, since the adversary does not know the session keys SK_{i-st} and SK_{j-st}, they cannot obtain the information required to impersonate avatars. Thus, our scheme can withstand insider attacks.

8) PRIVILEGED INSIDER ATTACK

Suppose that a malicious adversary is a privileged insider user of S_t. Then, the adversary can obtain the message $\{avatar_i, PID_i, EM_i\}$ in the avatar generation phase. Furthermore, the adversary can intercept messages $\{EM_1, S_1, T_1\}$ and $\{EM_2, S_3, T_2\}$ via the public channel. However, the adversary cannot generate any information to impersonate U_i such as v_1, Ver_{i-st}, and EM_1 without knowing n_1 and k_i. In addition, assume the adversary obtains the messages Req, Req_{ij}, Res, and Res_{ij}. However, the adversary cannot obtain vital information required to impersonate avatars without n_3, n_4, k_i, and k_j. Hence, our scheme can protect against privileged insider attacks.

9) EPHEMERAL SECRET LEAKAGE ATTACK

As described in Section III-D, the adversary can obtain the ephemeral and long-term secret values. Then, the adversary can attempt to compute the session key $SK_{i-st} = h(avatar_i||S_2||S_4)$ generated between U_i and S_t. This scenario is described in detail as follows.

- Assume the adversary obtains the ephemeral secret values n_1 and n_2 to compute SK_{i-st}. However, the adversary cannot calculate $S_2 = v_1 \cdot PK_{st}$ and $S_4 = v_2 \cdot S_1$ because v_1 and v_2 are generated with long-term secret values X_i, k_i, and k_{st}.
- Assume the adversary obtains long-term secret values X_i, k_i and k_{st} to compute SK_{i-st}. Although the adversary can obtain $S_2, S_4 = v_1 \cdot S_3 = v_2 \cdot S_1$ cannot be obtained without knowing the ephemeral values n_1 and n_2.

As a result, the adversary must have both the ephemeral and long-term secret values to compute SK_{i-st}. Therefore, our scheme can prevent ESL attacks.

10) USER ANONYMITY

Assume that the adversary can intercept transmitted messages and obtain SD_i. However, they cannot obtain the real identity ID_i. Under the proposed scheme, U_i utilizes a pseudo-identity $PID_i = h(ID_i||RN_i)$ rather than ID_i in the metaverse environments so that ID_i is never revealed to any entity. Therefore, our schemes can provide user anonymity.

11) MUTUAL AUTHENTICATION

In the authentication phase, U_i sends the login request message $\{EM_1, S_1, T_1\}$ to S_t. Then, S_t obtains Ver_{i-st} by decrypting EM_1 and retrieves PK_i from the blockchain using PID_i. Then, S_t verifies $Ver_{i-st} \cdot P \stackrel{?}{=} S_1 + h(avatar_i||PID_i||T_1) \cdot PK_i$. If it is same, S_t can authenticate U_i, and S_t sends message $\{EM_2, S_3, T_2\}$ to U_i. Afterward, U_i computes EM_2^* and authenticates S_t by verifying that $EM_2^* \stackrel{?}{=} EM_2$.

In addition, our scheme provides the avatar authentication phase to realize secure avatar-to-avatar interactions in virtual spaces. If $Avatar_i$ and $Avatar_j$ want to authenticate each other, they exchange the request message Req_{ij} and response message Res_{ij} through S_t. Afterward, $Avatar_i$ obtains Ver_j through EM_4 and retrieves PK_j from the blockchain using PID_j. Then,

U_i checks $Ver_j \cdot P \stackrel{?}{=} S_7 + h(avatar_j||avatar_i||S_8^*||T_4) \cdot PK_j$. If the equation is true, $Avatar_i$ can authenticate $Avatar_j$. Similarly, $Avatar_j$ can authenticate $Avatar_i$ by checking $Ver_i \cdot P \stackrel{?}{=} S_5 + h(avatar_i||avatar_j||S_6^*||T_3) \cdot PK_i$. Therefore, our scheme can ensure mutual authentication.

B. FORMAL SECURITY ANALYSIS USING BAN LOGIC

BAN logic is widely used to demonstrate the mutual authentication of a protocol [39], [40], [41]. In this section, we utilize BAN logic to prove that the proposed scheme guarantees mutual authentication. We also introduce logical postulates, goals, idealized forms, and assumptions to conduct the BAN logic proof. Table 2 defines the notations using in BAN logic.

TABLE 2. Notaions of BAN logic.

Notaion	Definition
A_1, A_2	Two principals
D_1, D_2	Two statements
$A_1\| \equiv D_1$	A_1 believes D_1
$A_1\| \sim D_1$	A_1 once said D_1
$A_1 \triangleleft D_1$	A_1 receives D_1
$A_1 \Rightarrow D_1$	A_1 controls D_1
SK	Session key
$\#D_1$	D_1 is fresh
$\{D_1\}_K$	D_1 is encrypted by K
$A_1 \stackrel{K}{\leftrightarrow} A_2$	A_1 and A_2 communicate via shared key K

1) LOGICAL POSTULATES

The logical postulates of BAN logic are summarized as follows.

- Message meaning rule (MMR):

$$\frac{A_1| \equiv A_1 \stackrel{K}{\leftrightarrow} A_2, A_1 \triangleleft \{D_1\}_K}{A_1| \equiv A_2| \sim D_1}$$

- Nonce verification rule (NVR):

$$\frac{A_1| \equiv \#(D_1), A_1| \equiv A_2| \sim D_1}{A_1| \equiv A_2| \equiv D_1}$$

- Jurisdiction rule (JR):

$$\frac{A_1| \equiv A_2 \Rightarrow D_1, A_1| \equiv A_2| \equiv D_1}{A_1| \equiv D_1}$$

- Belief rule (BR):

$$\frac{A_1| \equiv (D_1, D_2)}{A_1| \equiv D_1}$$

- Freshness rule (FR):

$$\frac{A_1| \equiv \#(D_1)}{A_1| \equiv \#(D_1, D_2)}$$

2) GOALS

The goals of the proposed scheme to prove mutual authentication are expressed as follows.

$$\begin{aligned}
&\textit{Goal 1: } S_t| \equiv (U_i \stackrel{SK_{i-st}}{\longleftrightarrow} S_t)\\
&\textit{Goal 2: } S_t| \equiv U_i| \equiv (U_i \stackrel{SK_{i-st}}{\longleftrightarrow} S_t)\\
&\textit{Goal 3: } U_i| \equiv (U_i \stackrel{SK_{i-st}}{\longleftrightarrow} S_t)\\
&\textit{Goal 4: } U_i| \equiv S_t| \equiv (U_i \stackrel{SK_{i-st}}{\longleftrightarrow} S_t)
\end{aligned}$$

3) IDEALIZED FORMS

We can express our login and authentication messages $\{EM_1, S_1, T_1\}$ and $\{EM_2, S_3, T_2\}$ as follows.

$$\begin{aligned}
&\textit{Message 1: } U_i \rightarrow S_t : \{avatar_i, PID_i, S_1, T_1\}_{S_2}\\
&\textit{Message 2: } S_t \rightarrow U_i : \{avatar_i, PID_i, S_3, T_2\}_{S_4}
\end{aligned}$$

4) ASSUMPTIONS

The assumptions considered in the proposed scheme are summarized as follows.

$$\begin{aligned}
&A_1\text{: } S_t| \equiv (U_i \stackrel{S_2}{\longleftrightarrow} S_t)\\
&A_2\text{: } S_t| \equiv \#(T_1)\\
&A_3\text{: } U_i| \equiv (U_i \stackrel{S_4}{\longleftrightarrow} S_t)\\
&A_4\text{: } U_i| \equiv \#(T_2)\\
&A_5\text{: } S_t| \equiv U_i \Rightarrow (U_i \stackrel{SK_{i-st}}{\longleftrightarrow} S_t)\\
&A_6\text{: } U_i| \equiv S_t \Rightarrow (U_i \stackrel{SK_{i-st}}{\longleftrightarrow} S_t)
\end{aligned}$$

5) BAN LOGIC PROOF

The BAN logic proof is performed using the above logical postulates, idealized forms, and assumptions to prove the stated goals.

- We can obtain E_1 from *Message* 1.

$$E_1 : S_t \triangleleft \{avatar_i, PID_i, S_1, T_1\}_{S_2}$$

- We apply the MMR using E_1 and A_1 to obtain E_2.

$$E_2 : S_t| \equiv U_i| \sim (avatar_i, PID_i, S_1, T_1)$$

- We apply the FR using E_2 and A_2 to obtain E_3.

$$E_3 : S_t| \equiv \#(avatar_i, PID_i, S_1, T_1)$$

- We apply the NVR using E_2 and E_3 to obtain E_4.

$$E_4 : S_t| \equiv U_i| \equiv (avatar_i, PID_i, S_1, T_1)$$

- We apply the BR using E_4 to obtain E_5.

$$E_5 : S_t| \equiv U_i| \equiv (avatar_i, PID_i, S_1)$$

- We can obtain E_6 from *Message* 2.

$$E_6 : U_i \triangleleft \{avatar_i, PID_i, S_3, T_2\}_{S_4}$$

- We apply the MMR using E_6 and A_3 to obtain E_7.

$$E_7 : U_i| \equiv S_t| \sim (avatar_i, PID_i, S_3, T_2)$$

- We apply the FR using E_7 and A_4 to obtain E_8.

$$E_8 : U_i| \equiv \#(avatar_i, PID_i, S_3, T_2)$$

- We apply the NVR using E_7 and E_8 to obtain E_9.

$$E_9 : U_i| \equiv S_t| \equiv (avatar_i, PID_i, S_3, T_2)$$

- We apply the BR using E_9 to obtain E_{10}.

$$E_{10} : U_i| \equiv S_t| \equiv (avatar_i, PID_i, S_3)$$

- We can obtain E_{11} using E_5. S_t can calculate $v_2 = h(avatar_i||PID_i||k_{st}||n_2||T_2)$, $S_2 = k_{st} \cdot S_1$, and $S_4 = v_2 \cdot S_1$. Then, S_t can successfully generate the session key $SK_{i-st} = h(avatar_i||S_2||S_4)$.

$$E_{11} : S_t| \equiv U_i| \equiv (U_i \overset{SK_{i-st}}{\longleftrightarrow} S_t) \quad (Goal\ 2)$$

- We apply the JR using E_{11} and A_5 to obtain E_{12}.

$$E_{12} : S_t| \equiv (U_i \overset{SK_{i-st}}{\longleftrightarrow} S_t) \quad (Goal\ 1)$$

- We can obtain E_{13} using E_{10}. U_i can calculate $v_1 = h(avatar_i||PID_i||X_i||n_1||T_1)$, $S_2 = v_1 \cdot PK_{st}$, and $S_4 = v_1 \cdot S_3$. Then, U_i can successfully generate the session key $SK_{i-st} = h(avatar_i||S_2||S_4)$.

$$E_{13} : U_i| \equiv S_t| \equiv (U_i \overset{SK_{i-st}}{\longleftrightarrow} S_t) \quad (Goal\ 4)$$

- We apply the JR using E_{10} and A_6 to obtain E_{14}.

$$E_{14} : U_i| \equiv (U_i \overset{SK_{i-st}}{\longleftrightarrow} S_t) \quad (Goal\ 3)$$

As a result, the proposed scheme guarantees mutual authentication between U_i and S_t.

C. FORMAL SECURITY ANALYSIS USING ROR MODEL

The ROR model is widely used to prove the security of session keys of various authentication protocols [42], [43], [44]. In this section, we analyze the session key security of our scheme using the ROR model. We define $P_{U_i}^{t_1}$ and $P_{S_t}^{t_2}$ as participants such as user and platform server, where t_i is the instance of the participants. Under the ROR model, an adversary can use *Execute*, *CorruptSD*, *Send*, and *Test* queries to perform various security attacks. These queries are described as follows.

- $Execute(P_{U_i}^{t_1}, P_{S_t}^{t_2})$: The adversary can intercept messages transmitted via the public channel between $P_{U_i}^{t_1}$ and $P_{S_t}^{t_2}$.
- $CorruptSD(P_{U_i}^{t_1})$: The adversary can obtain SD_i of $P_{U_i}^{t_1}$ and extract the stored information.
- $Send(P^t, Message)$: The adversary transmits the request message to other participants and receives the response message.
- $Test(P^t)$: There is an unbiased coin b representing 0 or 1. If the adversary performs *Test* query, P^t obtains a random number when $c = 0$ and a session key SK_{i-st} when $c = 1$; otherwise, P^t obtains a null ($\perp$). If the adversary cannot distinguish between the session key and random number, we can guarantee our scheme's security of the session key.

1) SECURITY PROOF

Theorem 1: We define $Adv_S(t)$ as the probability of breaking the session key security of the proposed scheme S in running time t. In addition, l, q_h, q_s, $|Hash|$, $|D_i|$, and $|D_p|$ denote the number of bits in the biometric information, the number of hash queries, the number of send queries, the range space of the hash function, the size of the identity dictionary, and the size of the password dictionary, respectively. We also define $Adv_S^{ECDDHP}(t)$ as the probability of breaking *ECDDHP*. We then can derive the following result.

$$Adv_S(t) \leq \frac{q_h^2}{|Hash|} + 2\left(\frac{q_s}{2^l \cdot |D_i| \cdot |D_p|} + Adv_S^{ECDDHP}(t)\right)$$

Proof: We conduct five games G_n, where $n = 0, 1, 2, 3, 4$. We also define Suc_n^{ad} as the adversary winning probability of G_n. In addition, $Pr_S[Suc_n^{ad}]$ is the advantage of Suc_n^{ad}. The detailed steps of each game are described as follows.

- G_0: In G_0, the adversary has no information and does not perform a query. Thus, the adversary chooses the random bit b. Through semantic security, we derive the following result.

$$Adv_S(t) = |2Pr_S[Suc_0^{ad}] - 1| \tag{1}$$

- G_1: The adversary performs $Execute(P_{U_i}^{t_1}, P_{S_t}^{t_2})$ query and intercepts messages $\{EM_1, S_1, T_1\}$ and $\{EM_2, S_3, T_2\}$. Then, the adversary runs the *Test* query to obtain the return value and guesses whether the return value is SK_{i-st} or not. To compute $SK_{i-st} = (avatar_i||S_2||S_4)$, the adversary requires random numbers n_1, n_2, and the secret values X_i, k_{st}. However, these values are still unknown to the adversary. Therefore, we derive the following result.

$$Pr_S[Suc_0^{ad}] = Pr_S[Suc_1^{ad}] \tag{2}$$

- G_2: The adversary conducts both *Hash* and *Send* queries to calculate SK_{i-st}. Here, the adversary can also use messages $\{EM_1, S_1, T_1\}$ and $\{EM_2, S_3, T_2\}$. However, these messages are masked by hash functions and random numbers. Therefore, the adversary must find the hash collision to obtain information about SK_{i-st}. We then derive the following result according to the birthday paradox.

$$|Pr_S[Suc_2^{ad}] - Pr_S[Suc_1^{ad}]| \leq \frac{q_h^2}{2|Hash|} \tag{3}$$

- G_3: The adversary can try to obtain SK_{i-st} using *CorruptSD* query. Then, the adversary can extract the stored parameters $\{Z_1, Z_2, Z_3\}$, where $Z_1 = RN_i \oplus HPW_i$, $Z_2 = h(ID_i||HPW_i||RPW_i||RN_i)$, and $Z_3 = V_i \oplus RPW_i$. To compute SK_{i-st}, the adversary requires RN_i and X_i which are masked with ID_i, PW_i, and B_i. Thus, the adversary can attempt to guess the values to compute SK_{i-st} using the biometric information of l bits, the

identity dictionary, and the password dictionary. Then, we derive the following result.

$$|Pr_S[Suc_3^{ad}] - Pr_S[Suc_2^{ad}]| \leq \frac{q_s}{2^l \cdot |D_i| \cdot |D_p|} \quad (4)$$

- G_4: The adversary can try to calculate $SK_{i-st} = h(avatar_i||S_2||S_4)$, using messages $\{EM_1, S_1, T_1\}$ and $\{EM_2, S_3, T_2\}$. Although the adversary can utilize S_1 and S_3, they cannot calculate S_2 and S_4 due to *ECDDHP* such as $S_4 = v_1 \cdot v_2 \cdot P$. Thus, we derive the following result.

$$|Pr_S[Suc_4^{ad}] - Pr_S[Suc_3^{ad}]| \leq Adv_S^{ECDDHP}(t) \quad (5)$$

The adversary guesses bit b by performing *Test* query. Then, we derive the following result.

$$Pr_S[Suc_4^{ad}] = \frac{1}{2} \quad (6)$$

We can derive the following equation according to (1), (2), and (6).

$$\begin{aligned} \frac{1}{2}Adv_S(t) &= |Pr_S[Suc_0^{ad}] - \frac{1}{2}| \\ &= |Pr_S[Suc_1^{ad}] - \frac{1}{2}| \\ &= |Pr_S[Suc_1^{ad}] - Pr_S[Suc_4^{ad}]| \end{aligned} \quad (7)$$

We can transform (7) into the following equation using the triangular inequality and (3), (4), and (5).

$$\begin{aligned} |Pr_S[Suc_1^{ad}] - Pr_S[Suc_4^{ad}]| &\leq |Pr_S[Suc_1^{ad}] - Pr_S[Suc_3^{ad}]| \\ &\quad + |Pr_S[Suc_3^{ad}] - Pr_S[Suc_4^{ad}]| \\ &\leq |Pr_S[Suc_1^{ad}] - Pr_S[Suc_2^{ad}]| \\ &\quad + |Pr_S[Suc_2^{ad}] - Pr_S[Suc_3^{ad}]| \\ &\quad + |Pr_S[Suc_3^{ad}] - Pr_S[Suc_4^{ad}]| \\ &\leq \frac{q_h^2}{2|Hash|} + \frac{q_s}{2^l \cdot |D_i| \cdot |D_p|} \\ &\quad + Adv_S^{ECDDHP}(t) \end{aligned} \quad (8)$$

As a result, we can derive (9) from (7) and (8).

$$Adv_S(t) \leq \frac{q_h^2}{|Hash|} + 2\left(\frac{q_s}{2^l \cdot |D_i| \cdot |D_p|} + Adv_S^{ECDDHP}(t)\right) \quad (9)$$

Thus, we can prove *Theorem* 1.

D. FORMAL SECURITY ANALYSIS USING AVISPA

AVISPA is a formal security simulation tool that can be used to verify the security of various protocols against replay and MITM attacks. The AVISPA tool has been employed in many studies to demonstrate protocol security [45], [46], [47]. The AVISPA tool uses the High-Level Protocols Specifications Language (HLPSL) to specify the actions of each participant. Afterward, the HLPSL code of the protocol is transformed to the Intermediate Format (IF) using the HLPSL2IF translator. Then, IF is input to one of four backends, namely, the On-the-fly-Model-Checker (OFMC), the CL-based Attack Searcher (CL-AtSe), the SAT-based Model-Checker (SATMC), or the Tree-Automata-based Protocol Analyzer (TA4SP), to obtain Output Format (OF). In this paper, we performed an AVISPA simulation of the proposed scheme using OFMC and CL-AtSe backends, which provide the XOR operation. If the SUMMARY part of OF is SAFE, the proposed scheme can defend against replay and MITM attacks.

1) HLPSL CODES OF THE PROPOSED SCHEME

In this section, we use the HLPSL language to implement the proposed scheme for the basic roles of user U, platform server S, and certificate authority CA. Figure 6 indicates the role of the session and environment. Note that we declare all basic roles and channels in the role of the session. Then, we declare all constants and variables used in the codes, and we define the intruder knowledge, secrecy goals, and authentication goals in the role of the environment.

```
%%%% Role Session %%%%
role session(U,S,CA:agent,SKuca,SKus:symmetric_key,H,ADD,MUL:hash_func)
def=
local SN1,SN2,SN3,RV1,RV2,RV3:channel(dy)
composition
user(U,S,CA,SKuca,SKus,H,ADD,MUL,SN1,RV1)
/\server(U,S,CA,SKuca,SKus,H,ADD,MUL,SN2,RV2)
/\cauthority(U,S,CA,SKuca,SKus,H,ADD,MUL,SN3,RV3)
end role

%%%% Role environment %%%%
role environment()
def=
const u,s,ca:agent,
skuca,skus:symmetric_key,
h,add,mul:hash_func,
idi,pwi,bi,infoi,rni,pidi,ki,pki,hpwi,rpwi,avatari,
z1,z2,z3,ni,nni,ci,xi,xxi,n1,n2,t1,t2,vi,v1,v2,si,s1,s2,s3,s4,
sigica,emi,em1,em2,veris,kca,ks,pks,sk,p:text,
sp1,sp2,sp3,sp4,sp5,sp6,
u_s_n1,s_u_n2:protocol_id

intruder_knowledge={u,s,ca,pidi,pki,pks,s1,s3,t1,t2,p,h,add,mul}
composition
session(u,s,ca,skuca,skus,h,add,mul)
/\session(i,s,ca,skuca,skus,h,add,mul)
/\session(u,i,ca,skuca,skus,h,add,mul)
/\session(u,s,i,skuca,skus,h,add,mul)
end role

%%% goal %%%%
goal
secrecy_of sp1,sp2,sp3,sp4,sp5,sp6
authentication_on u_s_n1
authentication_on s_u_n2
end goal

environment()
```

FIGURE 6. Role of session, environment, and goal.

Figure 7 describes the role of U. In transition 1, U performs the setup phase in state 0 and updates the state from 0 to 1. Then, U sends $\{PID_i, PK_i, Info_i\}$ to CA via the secure channel. After receiving $\{V_i\}$ in transition 2, U updates the state from 1 to 2. U then computes $\{Z_1, Z_2, Z_3\}$ and stores it on SD_i. Thereafter, U sends $\{avatar_i, PID_i, EM_i\}$ to S. To perform the login and authentication process, U transmits $\{EM_1, S_1, T_1\}$ and defines $witness(U, S, u\_s\_n_1, N_1)$. In transition 3, U receives $\{EM_2, S_3, T_2\}$ from S and updates the state from 2 to 3. Finally, U computes SK, and defines $request(S, U, s\_u\_n_2, N_2)$.

```
%%%% User %%%%
role user(U,S,CA:agent,SKuca,SKus:symmetric_key,H,ADD,MUL:hash_func,SN,RV:channel(dy))
played_by U
def=
local State:nat,
      IDi,PWi,Bi,INFOi,RNi,PIDi,Ki,PKi,HPWi,RPWi,AVATARi:text,
      Z1,Z2,Z3,Ni,NNi,Ci,Xi,XXi,N1,N2,T1,T2,Vi,V1,V2,Si,S1,S2,S3,S4:text,
      SIGica,EMi,EM1,EM2,VERis,Kca,Ks,PKs,SK,P:text
const sp1,sp2,sp3,sp4,sp5,sp6,u_s_n1,s_u_n2:protocol_id
init State:=0
transition

%%%% Setup phase %%%%
1. State=0 /\RV(start)=|>
State':=1 /\RNi':=new()
/\PIDi':=H(IDi.RNi') /\PKi':=MUL(Ki.P)
/\SN({PIDi'.PKi'.INFOi}_SKuca)
/\secret({IDi.PWi.Bi.Ki.RNi'},sp1,{U})
/\secret({INFOi},sp2,{U,CA})

2.State=1
/\RV({MUL(Xi'.P).ADD(Xi'.MUL(H(H(IDi.RNi').MUL(Ki.P).MUL(Xi'.P)).Kca))}_SKuca)=|>
State':=2 /\HPWi':=H(IDi.PWi.H(Bi))
/\RPWi':=H(PWi.H(Bi).RNi')
/\Z1':=xor(RNi',HPWi') /\Z2':=H(IDi.HPWi'.RPWi'.RNi') /\Z3':=xor((MUL(Xi'.P).ADD(Xi'.MUL(H(H(IDi.RNi')
.MUL(Ki.P).MUL(Xi'.P)).Kca))),RPWi')

%%%% Avatar generation phase %%%%
/\Ni':=new() /\AVATARi':=new()
/\NNi':=MUL(Ni'.P) /\Si':=MUL(Ki.PKs)
/\Ci':=ADD(Ni'.MUL(H(AVATARi'.H(IDi.RNi').Si').Ki))
/\EMi':=xor((NNi'.Ci'.MUL(Xi'.P).ADD(Xi'.MUL(H(H(IDi.RNi').MUL(Ki.P).MUL(Xi'.P)).Kca))),
H(AVATARi'.H(IDi.RNi').Si'))
/\SN({AVATARi'.H(IDi.RNi').EMi'}_SKus)
/\secret({Ni'},sp3,{U})
/\secret({EMi'},sp4,{U,S})

%%%% login & authentication phase %%%%
/\N1':=new() /\T1':=new()
/\V1':=H(AVATARi'.H(IDi.RNi').MUL(Xi'.P).N1'.T1')
/\S1':=MUL(V1'.P) /\S2':=MUL(V1'.PKs)
/\VERis':=ADD(V1'.MUL(H(AVATARi.H(IDi.RNi').T1').Ki))
/\EM1':=xor((AVATARi'.H(IDi.RNi').VERis'),H(S2'.T1'))
/\SN(EM1',S1',T1')
/\witness(U,S,u_s_n1,N1')

3.State=2
/\RV(H(AVATARi.H(IDi.RNi').H(AVATARi'.MUL(Ks.MUL(H(AVATARi'.H(IDi.RNi').MUL(Xi'.P).N1'.T1').P)).
MUL(H(AVATARi'.H(IDi.RNi').Ks.N2'.T2').MUL(H(AVATARi'.H(IDi.RNi').MUL(Xi'.P).N1'.T1').P))).T2').
MUL(H(AVATARi'.H(IDi.RNi').Ks.N2'.T2').P).T2')=|>

State':=3
/\S4':=MUL(H(AVATARi'.H(IDi.RNi').MUL(Xi'.P).N1'.T1').MUL(H(AVATARi'.H(IDi.RNi').Ks.N2'.T2').P))
/\SK':= H(AVATARi'.MUL(H(AVATARi'.H(IDi.RNi').MUL(Xi'.P).N1'.T1').PKs).S4')
/\request(S,U,s_u_n2,N2')
end role
```

FIGURE 7. Role of user.

2) RESULT OF AVISPA SIMULATION

The OF for the proposed scheme obtained after applying the OFMC and CL-AtSe backends is shown in Figure 8. We represent the OF of our scheme after conducting the OFMC and CL-AtSe backends in Figure 8. Because the SUMMARY parts are SAFE, the proposed scheme can prevent both replay and MITM attacks.

```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/Seok(Metaverse).if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 2.67s
 visitedNodes: 130 nodes
 depth: 6 plies
```

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/Seok(Metaverse).if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed  : 2 states
 Reachable  : 0 states
 Translation: 0.26 seconds
 Computation: 0.00 seconds
```

FIGURE 8. Simulation results.

VI. PERFORMANCE ANALYSIS

In this section, we analyze the computation costs, communication costs, and security features of the proposed scheme. Then, we compare the computation costs, communication costs, and security features of the proposed scheme with existing schemes in similar environments [22], [24], [26].

A. COMPUTATION COSTS

We compare the computation costs of the proposed scheme with [22], [24], and [26]. In this paper, we follow the execution time of cryptographic operation measured by [48] using Visual C++ 2008 and MIRACL library on Intel(R) Core(TM) 2 T6570 2.1GHz, 4GB memory, and Win7 32-bit operating system environment. Depending on [48] and [49], we denote the execution times of bilinear pairing, EC point multiplication, EC point addition, symmetric encryption/decryption, the hash function, and the biohashing function as T_{bp} ($\approx$ 22.0587 ms), T_{em} ($\approx$ 7.3529 ms), T_{ea} ($\approx$ 0.009 ms), T_{sye} ($\approx$ 0.1303 ms), T_h ($\approx$ 0.0004 ms), and T_{bh} ($\approx$ 0.01 ms), respectively. In the login and authentication phase of the proposed scheme, U_i performs the operation to send the login request message, which has an execution cost of $4T_{em}+T_{ea}+8T_h+2T_H$. After receiving the login request message, S_t performs the operation, which requires time as $5T_{em}+T_{ea}+5T_h$ for responding to U_i. Table 3 shows the total computation costs of the compared authentication schemes.

TABLE 3. Computation costs of each scheme.

Schemes	User	Server	Total costs
Panda and Chattopadhyay [22]	$6T_{em}+$ $4T_h$ $\approx$ 44.1190 ms	$4T_{em}+$ $5T_h$ $\approx$ 29.4136 ms	73.5326 ms
Haq et al. [24]	$5T_{em}+$ $T_{ea}+$ $6T_h$ $\approx$ 36.7759 ms	$5T_{em}+$ $2T_{ea}+$ $3T_h$ $\approx$ 36.7837 ms	73.5596 ms
Li et al. [26]	$7T_{em}+$ $5T_h$ $\approx$ 51.4723 ms	$2T_{bp}+$ $6T_{em}+$ $T_{ea}+$ $5T_h$ $\approx$ 88.2458 ms	139.7181 ms
Our scheme	$4T_{em}+$ $T_{ea}+$ $8T_h+$ $2T_H$ $\approx$ 29.4438 ms	$5T_{em}+$ $T_{ea}+$ $5T_h$ $\approx$ 36.7755 ms	66.2193 ms

B. COMMUNICATION COSTS

We evaluate the communication costs of the proposed scheme and [22], [24], and [26]. In the proposed scheme, the EC point, hash function output, avatar identity, random number, symmetric encryption/decryption, and timestamp require 320, 160, 160, 128, 128, and 32 bits, respectively. In the proposed scheme's login and authentication phase, we transmit messages $\{EM_1, S_1, T_1\}$ and $\{EM_2, S_3, T_2\}$ between U_i and S_t which require $(480+320+32)$ bits and $(160+320+32)$ bits, respectively. As a result, the total communication cost of the login and authentication scheme is $(832+512)=1344$ bits. Table 4 shows the total communication costs and number of exchanged messages for each authentication scheme.

C. SECURITY FEATURES

The security features of the compared schemes [22], [24], [26], and the proposed scheme are listed in Table 5. Following Table 5, the proposed scheme can withstand stolen smart cards/devices, offline password guessing, impersonation, server spoofing, replay, MITM, insider, and privileged

TABLE 4. Communication costs of each scheme.

Schemes	Communication costs	Messages
Panda and Chattopadhyay [22]	1440 bits	3
Haq et al. [24]	1728 bits	2
Li et al. [26]	1888 bits	3
Our scheme	1344 bits	2

TABLE 5. Security features of each scheme.

Security features	Panda and Chattopadhyay [22]	Haq et al. [24]	Li et al. [26]	Our scheme
SF_1	-	○	-	○
SF_2	○	○	-	○
SF_3	-	×	○	○
SF_4	○	×	○	○
SF_5	○	×	○	○
SF_6	○	×	○	○
SF_7	-	-	-	○
SF_8	○	×	-	○
SF_9	○	○	○	○
SF_{10}	○	○	×	○
SF_{11}	○	○	○	○
SF_{12}	-	-	-	○

○: Secure; ×: Insecure; −: Not considered; SF_1: Stolen smart card/device attack; SF_2: Offline password guessing attack; SF_3: User impersonation attack; SF_4: Sever spoofing attack; SF_5: Replay attack; SF_6: MITM attack; SF_7: Insider attack; SF_8: Privileged insider attack; SF_9: Perfect forward secrecy; SF_{10}: User anonymity; SF_{11}: User-to-server mutual authentication; SF_{12}: User-to-user mutual authentication

insider attacks. In addition, our scheme provides perfect forward secrecy, user anonymity, and user-server mutual authentication. The proposed scheme also provides user-to-user mutual authentication to guarantee secure avatar interactions. Therefore, the proposed scheme offers a more diverse set of security features than the existing schemes [22], [24], and [26].

VII. CONCLUSION

In this paper, we designed a system model that provides secure communication and avatar interactions in metaverse environments. In this system model, user identification data are managed transparently using blockchain technology. In addition, we proposed a secure mutual authentication scheme between users and platform servers and between avatars and avatars using ECC and biometric information. The informal security analysis was also performed to evaluate the proposed secure mutual authentication scheme. The results demonstrate that the proposed scheme is resistant to various security attacks such as stolen smart devices, offline password guessing, and impersonation attacks. In addition, we performed formal security analyses using the BAN logic and the ROR model to show that the proposed scheme provides mutual authentication and session key security. We also demonstrated that the proposed scheme can prevent replay and MITM attacks utilizing the AVISPA tool. Finally, we compared the computation costs, communication costs, and security features of the proposed scheme and existing schemes in similar environments. We found that the proposed scheme has lower computation costs and communication costs. Moreover, the proposed scheme offers a richer set of security features than the existing schemes. Thus, we expect that the proposed scheme can be used to provide secure metaverse environments.

REFERENCES

[1] 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.

[2] H. Yoo, J. Jang, H. Oh, and I. Park, "The potentials and trends of holography in education: A scoping review," *Comput. Educ.*, vol. 186, Sep. 2022, Art. no. 104533.

[3] S. Mystakidis, "Metaverse," *Encyclopedia*, vol. 2, no. 1, pp. 486–497, 2022.

[4] S. M. Park and Y. G. Kim, "A Metaverse: Taxonomy, components, applications, and open challenges," *IEEE Access*, vol. 10, pp. 4209–4251, 2022.

[5] S. Park and S. Kim, "Identifying world types to deliver gameful experiences for sustainable learning in the metaverse," *Sustainability*, vol. 14, no. 3, p. 1361, Jan. 2022.

[6] B. Shen, W. Tan, J. Guo, L. Zhao, and P. Qin, "How to promote user purchase in metaverse? A systematic literature review on consumer behavior research and virtual commerce application design," *Appl. Sci.*, vol. 11, no. 23, p. 11087, Nov. 2021.

[7] M. Zyda, "Let's rename everything 'the metaverse,'" *Computer*, vol. 55, no. 3, pp. 124–129, Mar. 2022.

[8] D. Griol, A. Sanchis, J. M. Molina, and Z. Callejas, "Developing enhanced conversational agents for social virtual worlds," *Neurocomputing*, vol. 354, pp. 27–40, Aug. 2019.

[9] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990.

[10] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. 8th Int. Workshop Theory Pract. Public Key Cryptogr.*, Jan. 2005, pp. 65–84.

[11] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron, "The AVISPA tool for the automated validation of internet security protocols and applications," in *Proc. Int. Conf. Comput. Aided Verification*, Jul. 2005, pp. 281–285.

[12] S. Kumar, J. Chhugani, C. Kim, D. Kim, A. Nguyen, P. Dubey, B. Christian, and Y. Kim, "Second life and the new generation of virtual worlds," *Computer*, vol. 41, no. 9, pp. 46–53, Sep. 2008.

[13] J. Smart, J. Cascio, J. Paffendorf, C. Bridges, J. Hummel, J. Hursthouse, and R. Moss, "A cross-industry public foresight project," in *Proc. Metaverse Roadmap Pathways (3DWeb)*, 2007, pp. 1–28.

[14] 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, 2022.

[15] L. Gan, D. Wang, C. Wang, D. Xiao, M. Zhang, Z. Wang, and F. Li, "Design and implementation of multimedia teaching platform for situational teaching of music appreciation course based on virtual reality," *Int. J. Electr. Eng. Educ.*, Apr. 2021.

[16] A. Jovanović and A. Milosavljević, "VoRtex metaverse platform for gamified collaborative learning," *Electronics*, vol. 11, no. 3, p. 317, Jan. 2022.

[17] F. O'Brolcháin, T. Jacquemard, D. Monaghan, N. O'Connor, P. Novitzky, and B. Gordijn, "The convergence of virtual reality and social networks: Threats to privacy and autonomy," *Sci. Eng. Ethics*, vol. 22, no. 1, pp. 1–29, 2016.

[18] B. Falchuk, S. Loeb, and R. Neff, "The social metaverse: Battle for privacy," *IEEE Technol. Soc. Mag.*, vol. 37, no. 2, pp. 52–61, Jun. 2018.

[19] J. A. D. Guzman, K. Thilakarathna, and A. Seneviratne, "Security and privacy approaches in mixed reality: A literature survey," *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–37, Jan. 2020.

[20] T. F. Tan, Y. Li, J. S. Lim, D. V. Gunasekeran, Z. L. Teo, W. Y. Ng, and D. S. Ting, "Metaverse and virtual health care in ophthalmology: Opportunities and challenges," *Asia–Pacific J. Ophthalmol.*, vol. 11, no. 3, pp. 237–246, 2022.

[21] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing blockchain and AI with metaverse: A survey," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 122–136, 2022.

[22] P. K. Panda and S. Chattopadhyay, "A secure mutual authentication protocol for IoT environment," *J. Reliable Intell. Environments*, vol. 6, no. 2, pp. 79–94, 2020.

[23] F. Chen, Z. Xiao, T. Xiang, J. Fan, and H. L. Truong, "A full lifecycle authentication scheme for large-scale smart IoT applications," *IEEE Trans. Depend. Secure Comput.*, early access, May 26, 2022, doi: 10.1109/TDSC.2022.3178115.
[24] I. Ul Haq, J. Wang, and Y. Zhu, "Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multiserver 5G networks," *J. Netw. Comput. Appl.*, vol. 161, Jul. 2020, Art. no. 102660.
[25] P. Kumar and H. Om, "A secure and efficient authentication protocol for wireless applications in multi-server environment," *Peer Peer Netw. Appl.*, vol. 15, pp. 1939–1952, May 2022.
[26] Y. Li, M. Xu, and G. Xu, "Blockchain-based mutual authentication protocol without CA," *J. Supercomput.*, early access, pp. 1–23, May 2022.
[27] S. Yu and Y. Park, "A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions," *IEEE Internet Things J.*, early access, May 2, 2022, doi: 10.1109/JIOT.2022.3171791.
[28] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.
[29] K. Wüst and A. Gervais, "Do you need a blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, 2018, pp. 45–54.
[30] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[31] J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, and Y. Park, "Secure ECC-based three-factor mutual authentication protocol for telecare medical information system," *IEEE Access*, vol. 10, pp. 11511–11526, 2022.
[32] A. T. B. Jin, D. N. C. Ling, and A. Goh, "BioHashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, Apr. 2004.
[33] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[34] D. Chattaraj, B. Bera, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Designing fine-grained access control for software-defined networks using private blockchain," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1542–1559, Jan. 2022.
[35] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 1666. Berlin, Germany: Springer, Aug. 1999, pp. 388–397.
[36] M. Wazid, A. K. Das, K.-K.-R. Choo, and Y. Park, "SCS-WoT: Secure communication scheme for web of things deployment," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10411–10423, Jul. 2022.
[37] S. Son, Y. Park, and Y. Park, "A secure, lightweight, and anonymous user authentication protocol for IoT environments," *Sustainability*, vol. 13, no. 16, p. 9241, Aug. 2021.
[38] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, Amsterdam, The Netherlands, 2002, pp. 337–351.
[39] D. Kwon, S. Son, Y. Park, H. Kim, Y. Park, S. Lee, and Y. Jeon, "Design of secure handover authentication scheme for urban air mobility environments," *IEEE Access*, vol. 10, pp. 42529–42541, 2022.
[40] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1346–1358, May 2022.
[41] I. A. Kamil and S. O. Ogundoyin, "A lightweight mutual authentication and key agreement protocol for remote surgery application in tactile internet environment," *Comput. Commun.*, vol. 170, pp. 1–18, Mar. 2021.
[42] Y. Cho, J. Oh, D. Kwon, S. Son, S. Yu, Y. Park, and Y. Park, "A secure three-factor authentication protocol for E-governance system based on multiserver environments," *IEEE Access*, vol. 10, pp. 74351–74365, 2022.
[43] J. Lee, G. Kim, A. K. Das, and Y. Park, "Secure and efficient honey list-based authentication protocol for vehicular ad hoc networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2412–2425, Jun. 2021.
[44] Y. Guo and Y. Guo, "FogHA: An efficient handover authentication for mobile devices in fog computing," *Comput. Secur.*, vol. 108, Sep. 2021, Art. no. 102358.
[45] M. Kim, J. Lee, J. Oh, K. Park, Y. Park, and K. Park, "Blockchain based energy trading scheme for vehicle-to-vehicle using decentralized identifiers," *Appl. Energy*, vol. 322, Sep. 2022, Art. no. 119445.
[46] R. Shashidhara, M. Lajuvanthi, and S. Akhila, "A secure and privacy-preserving mutual authentication system for global roaming in mobile networks," *Arabian J. Sci. Eng.*, vol. 47, no. 2, pp. 1435–1446, 2022.
[47] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, and Y. Park, "A secure and lightweight authentication protocol for IoT-based smart homes," *Sensors*, vol. 21, no. 4, p. 1488, Feb. 2021.
[48] N. Ravanbakhsh and M. Nazari, "An efficient improvement remote user mutual authentication and session key agreement scheme for E-health care systems," *Multimedia Tools Appl.*, vol. 77, no. 1, pp. 55–88, 2018.
[49] S. K. Islam and G. P. Biswas, "A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks," *Ann. téléCommunications-Annales Des Telecommun.*, vol. 67, no. 11, pp. 547–558, 2012.

JONGSEOK RYU received the B.S. degree in software from Kyungpook National University, Sangju, South Korea, in 2021. He is currently pursuing the M.S. degree with the Kyungpook National University of Electronic and Electrical Engineering, Daegu, South Korea. His research interests include authentication, cryptography, and communication security.

SEUNGHWAN SON received the B.S. degree in mathematics and the M.S. degree in electronic and electrical engineering from Kyungpook National University, Daegu, South Korea, in 2019 and 2021, respectively. He is currently pursuing the Ph.D. degree with the School of Electronic and Electrical Engineering. His research interests include blockchain, cryptography, and information security.

JOONYOUNG LEE (Student Member, IEEE) received the B.S. and M.S. degrees in electronics engineering from Kyungpook National University, Daegu, South Korea, in 2018 and 2020, respectively, where he is currently pursuing the Ph.D. degree with the School of Electronic and Electrical Engineering. His research interests include authentication, the Internet of Things, and information security.

YOHAN PARK (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 2006, 2008, and 2013, respectively. He is currently an Assistant Professor with the Department of Computer Engineering, College of Engineering, Keimyung University, Daegu. His research interests include computer networks, mobile security, blockchain, and the IoT.

YOUNGHO PARK (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 1989, 1991, and 1995, respectively. From 1996 to 2008, he was a Professor with the School of Electronics and Electrical Engineering, Sangju National University, South Korea. From 2003 to 2004, he was a Visiting Scholar with the School of Electrical Engineering and Computer Science, Oregon State University, USA. He is currently a Professor with the School of Electronic and Electrical Engineering, Kyungpook National University. His research interests include computer networks, multimedia, and information security.