Fecha de presentación: septiembre, 2022, **Fecha de Aceptación**: noviembre, 2022, **Fecha de publicación**: enero, 2023

36

ARQUITECTURA DE UN MECANISMO DE AUTENTICACIÓN SEGURO PARA EL METAVERSO EN UN ECOSISTEMA EDUCATIVO

ARCHITECTURE OF A SECURE AUTHENTICATION MECHANISM FOR THE METAVERSE IN AN EDUCATIONAL ECOSYSTEM

Sang Guun-Yoo[1]
E-mail: yoo.sang@ucacue.edu.ec
ORCID: https://orcid.org/0000-0003-1376-3843
Juan-Carlos Ortega-Castro[1]
E-mail: jcortegac@ucacue.edu.ec
ORCID: https://orcid.org/0000-0001-6496-4325
Eduardo Mauricio Campaña-Ortega[1]
E-mail: eduardo.campana@ucacue.edu.ec
ORCID: https://orcid.org/0000-0001-7720-5213
[1] Universidad Católica de Cuenca. Ecuador.

Cita sugerida (APA, séptima edición)

Guun-Yoo, S., Ortega-Castro, J-C. & Campaña-Ortega, E. M. (2023). Arquitectura de un mecanismo de autenticación seguro para el Metaverso en un Ecosistema Educativo. ***Revista Conrado, 19(90)***, 320-325.

RESUMEN

El Metaverso es una nueva tecnología que está evolucionando rápidamente en el mundo de Internet y la educación. Este servicio implica otras tecnologías novedosas como blockchain, criptomoneda, realidad virtual, avatares, gestión del conocimiento, etc., y esta situación hace necesaria la implementación de un nuevo mecanismo de seguridad que incluya un mecanismo evolucionado de autenticación de usuarios. En esta situación, este trabajo propone una nueva arquitectura, desde la educación digital, de un mecanismo de autenticación seguro para el Metaverso que incluye características de privacidad, anonimato y flexibilidad de implementación. La arquitectura propuesta incluye el servicio tradicional de infra-estructura de clave pública para permitir la facilidad de implementación, al tiempo que añade una solución de certificado pseudo-digital para permitir a los usuarios mantener el anonimato y la privacidad en los mundos virtuales del Metaverso.

Palabras clave:

Metaverso, educación digital, autenticación, conocimiento, certificado digital.

ABSTRACT

Metaverse is a new technology which is evolving rapidly in the world of Internet and education. This service involves other novel technologies such as blockchain, cryptocurrency, virtual reality, avatars, knowledge management, etc., and this situation makes it necessary the implementation of new security mechanism including an evolved user authentication mechanism. In this situation, this work proposes a new architecture, from digital education, of a secure authentication mecha-nism for the metaverse including features of privacy, anonymity and flexibility of implementation. The proposed architecture includes the traditional public key infra-structure service for allowing easiness for implementation while adding a solution of a pseudo digital certificate for allowing users to maintain anonymity and privacy in the virtual worlds of the metaverse.

Keywords:

Metaverse, digital education, authentication, knowledge, digital certificate.

INTRODUCCIÓN

El Metaverso es una nueva tecnología que está evolucionando rápidamente en el mundo de Internet. Incluso Facebook, empresa líder en tecnología, ha cambiado su nombre por Meta para seguir esta tendencia. El Metaverso es un universo tecnológico, un entorno multiusuario perpetuo y persistente que fusiona la realidad física con la realidad virtual (Mystakidis, 2022). En otras palabras, el Metaverso es un mundo virtual en el que los usuarios se conectarán mediante una serie de dispositivos que les harán creer que están realmente dentro de él, interactuando con todos sus elementos. Será como teletransportarse realmente a un mundo completamente nuevo a través de unas gafas de realidad virtual y otros accesorios que nos permitirán interactuar con él.

En los últimos años, ha surgido la idea del Metaverso como la nueva generación de Internet. Es una iteración hipotética de Internet como mundo virtual único, universal e inmersivo que se facilita mediante el uso de auriculares de realidad virtual y realidad aumentada. En palabras coloquiales, un Metaverso es una red de mundos virtuales en 3D centrada en la conexión social (Falchuk et al., 2018).

Mucha gente piensa que será sólo una nueva generación de videojuegos, pero esta tecnología implica conceptos más complejos, ya que los mundos virtuales del Metaverso tendrán una conexión directa con la realidad. Por ejemplo, el usuario podrá trabajar en el Metaverso ganando dinero en él. También será posible generar activos valiosos como criptomonedas, tokens no fungibles (NFT), etc. (Vidal-Tomás, 2022; De Jong, 2022).

El Metaverso está evolucionando rápidamente e involucra otras tecnologías novedosas como blockchain, criptomoneda, realidad virtual, avatares, etc., y esta situación hace necesaria la implementación de nuevos mecanismos de seguridad incluyendo un mecanismo evolucionado de autenticación de usuarios (Wang et al., 2022).

La autenticación de usuarios ha sido uno de los mecanismos de seguridad más importantes en los sistemas de información en la era moderna. En este sentido, se han desarrollado diferentes componentes para el proceso de autenticación de usuarios. Por ejemplo, para el proceso de identificación del usuario, se han desarrollado tres factores de autenticación diferentes, es decir, (a) algo que el usuario sabe (por ejemplo, contraseña/número de identificación personal), (b) algo que el usuario tiene (por ejemplo, dispositivo criptográfico de identificación, token, tarjeta inteligente), y (c) algo que el usuario es/hace (por ejemplo, factores biométricos como la huella dactilar, el iris del ojo, la voz) (Li et al., 2019); para el proceso de autenticación remota, se han desarrollado diferentes protocolos y tecnologías de autenticación como Kerberos (Fan et al., 2009), OpenID (Hardt, 2012), OAuth (Recordon & Reed, 2006), etc.

Aunque existen diferentes mecanismos de seguridad para la autenticación de usuarios, estas tecnologías heredadas no están optimizadas para el Metaverso, por ejemplo, es importante verificar la autenticidad del usuario, pero al mismo tiempo mantener el anonimato y la privacidad de los usuarios en algunos servicios del Metaverso, y los actuales mecanismos de autenticación de usuarios no cubren este tipo de requisitos.

En estas circunstancias, en este trabajo se estudia la arquitectura de un novedoso sistema de autenticación de usuarios para el sistema Metaverso que estará en tendencia con el advenimiento de esta nueva tecnología.

MATERIALES Y MÉTODOS

La Figura 1 muestra la metodología que utilizada en el presente trabajo. En la primera etapa, se realizó un estudio del estado del arte para conocer el estado actual de los sistemas Metaverso y sus mecanismos de seguridad. Para ello, se realizó una revisión sistemática de la literatura buscando diferentes trabajos de investigación en bases de datos científicas como IEEE Xplorer, Scopus, ScienceDirect, etc.

Una vez comprendido el estado del arte, se utilizó la Metodología de Investigación Acción, que es un proceso iterativo donde en cada ciclo se genera un nuevo conocimiento (Drummond & Themessl-Huber, 2007). En el presente trabajo, el nuevo conocimiento serán las limitaciones de la arquitectura propuesta en la última iteración que serán los requisitos de la siguiente iteración. Para reconocer las limitaciones de la arquitectura se utilizó el criterio de expertos. Los criterios serán desde la perspectiva del anonimato, la privacidad y la flexibilidad de implementación. Cuando la arquitectura no tenga limitaciones importantes, se propondrá como definitiva. Una vez con la arquitectura final, se definieron las conclusiones del trabajo propuesto.

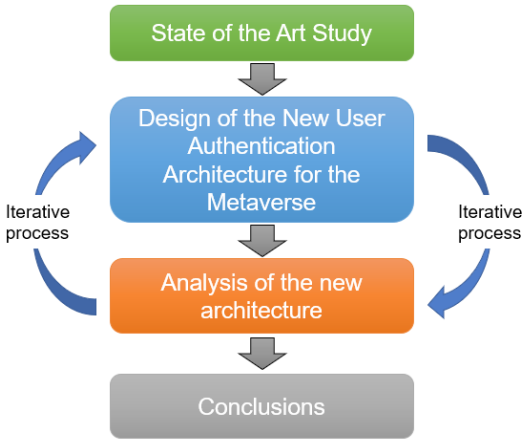

Figura 1. Metodología del presente trabajo.

RESULTADOS Y DISCUSIÓN

Dado que el Metaverso es un concepto nuevo y que no existe un sistema real que cumpla todas sus características, la propuesta de mecanismo de seguridad para el Metaverso es muy limitada. En esta sección, se describirán los trabajos previos relacionados con el mecanismo de seguridad para Metaverso con el objetivo de comprender el estado del arte en esta área.

Una de las tecnologías más utilizadas para asegurar el Metaverso es blockchain. La tecnología blockchain se ha utilizado para hacer frente a diferentes retos de desarrollo de aplicaciones Metaverso. Por ejemplo, en la referencia (Nguyen et al., 2022), se propuso una solución llamada Meta-Chain, que puede gestionar y automatizar eficazmente interacciones complejas entre el proveedor de servicios Metaverso y los usuarios Metaverso. Otro ejemplo del uso de blockchain para el Metaverso es la Ref. (Goldman Sachs LLC, 2021). En este trabajo, los autores proponen un nuevo sistema de dinero electrónico similar al Bitcoin, pero especializado para el Metaverso.

Otro trabajo desarrollado por Yang et al. (2022), hacen un estudio de cómo la inteligencia artificial y el blockchain pueden ser utilizados en el Metaverso concluyendo que se espera que estas tecnologías se conviertan en una de las principales herramientas para dicho entorno, permitiendo a los usuarios participar de forma segura y libre en actividades sociales y económicas en el mundo virtual.

Wang & Kumar (2022), proponen una Identificación Humana en Metaverso Usando Reconocimiento Egocéntrico del Iris los autores desarrollaron una base de datos pública de imágenes del iris, de 384 sujetos diferentes para el reconocimiento del iris usando un dispositivo AR/VR generalizado. La intención de este trabajo es reconocer a un usuario utilizando el iris del ojo leído por el dispositivo AR/VR. Mientras que otro trabajo propone un protocolo de autenticación e intercambio de claves de baja latencia para el Internet de las Cosas de la energía en la era Metaverse (Zhang et al., 2022).

Propuesta del nuevo mecanismo de autenticación de usuarios para el Metaverso

La intención de esta sección es describir la arquitectura propuesta del mecanismo de autenticación de usuarios para el Metaverso que proporciona las características de seguridad, anonimato y privacidad para los usuarios. La arquitectura general del mecanismo propuesto se muestra en la Figura 2; con una interacción entre cuatro entidades: el usuario U, la Autoridad de Certificación CA, el Servidor de Autenticación AS, el Servidor Metaverso MS y la Blockchain. En la primera etapa, el usuario se comunica con la CA a través del Protocolo de Emisión de Certificados para recibir un Certificado con su pseudo identificación. Una vez recibido el Certificado, U se comunica con AS para crear una cuenta que le permita acceder a los Servicios Metaversos proporcionados por MS. Una vez creada la cuenta de usuario que mantiene el anonimato y la privacidad del usuario (los detalles se explican en la sección Protocolo de Emisión de Certificados), el usuario puede crear los avatares en la MS y utilizar sus servicios a través de cualquier mecanismo existente de inicio de sesión único (SSO) como Kerberos, OAuth, SAML u OpenID.

A continuación, se describen en detalle el protocolo de emisión de certificados y el protocolo de registro de usuarios propuestos. Estos protocolos se explican utilizando la notación descrita en la Tabla 1.

Tabla 1. Notaciones.

Notation	Description
U	User
CA	Certificate Authority
AS	Authentication Server
$PubK_U$	User's public key
$PriK_U$	User's private key
$Info_U$	User's personal information
PID_U	User's pseudo identification
$Cert_U$	User's certificate
$Nonce_U$	Nonce for U
$E_K(M)$	Asymmetric encryption of the plaintext M using key K

$D_K(M)$	Asymmetric decryption of the ciphertext *C* using key *K*
ID_U	Identification of the user
PW_U	Password of the user

Protocolo de emisión de certificados

Dado que el usuario debe ser verificado utilizando su información real, se realiza el proceso de emisión de la certificación (Figura 3). Para ello, el usuario genera su propia clave pública PubKU y su clave privada PriKU. A continuación, se envía la PubKU a la Autoridad de Certificación (CA) con la información personal del usuario InfoU y la pseudoidentificación seleccionada por el usuario PIDU.

La CA, una vez recibido el paquete del usuario U, verifica si la InfoU es correcta. También verifica que el PIDU es único y no ha sido utilizado por otro usuario. Si el PIDU está repetido, CA informa al usuario para que cambie su PIDU. Cuando se selecciona un PIDU único y se verifica la validez del InfoU, la CA genera el certificado del usuario CertU utilizando el PIDU en lugar del InfoU; esto se hace para mantener el anonimato y la privacidad del usuario. Sin embargo, la CA puede verificar la validez del usuario y del CertU.

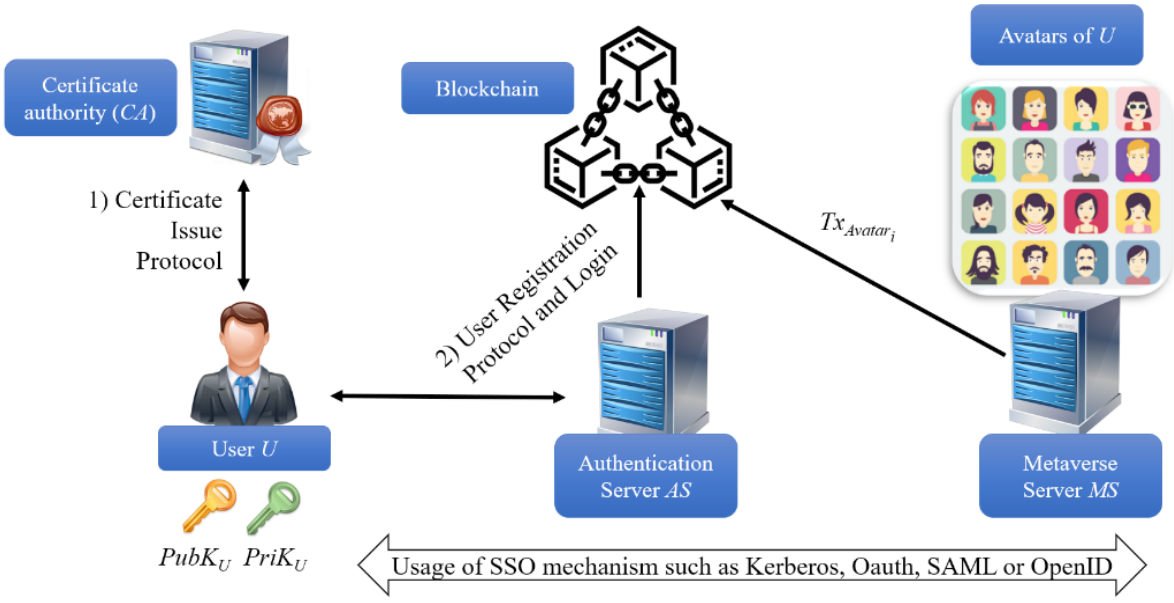

Figura 2. Arquitectura propuesta para la identificación de usuarios.

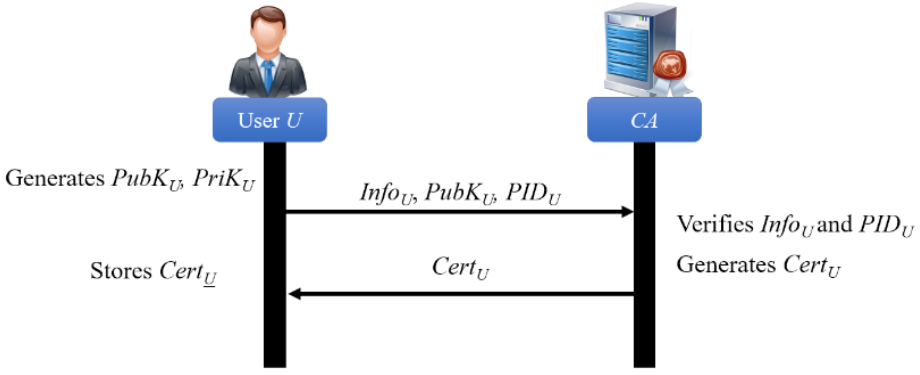

Figura 3. Protocolo de expedición de certificados.

Protocolo de registro de usuarios e inicio de sesión

En la Figura 4 se ilustra el proceso de registro de usuarios que consta de los siguientes pasos. Una vez recibido el CertU, U solicita al Servidor de Autenticación AS la creación de una cuenta enviando el mensaje de solicitud REQU. AS, una vez recibido REQU, genera un nonce NonceU y lo envía a U. A continuación, U cifra el NonceU con su PriKU y lo envía a AS acompañado del CertU y del IDU seleccionado, PWU. Una vez recibido el mensaje, AS verifica la validez del CertU con CA. A continuación, AS extrae el PubKU del CertU y descifra el EPriKU(NonceU) utilizando el PubKU y compara el resultado con el NonceU; con esta verificación AS puede asegurar que la petición proviene del propietario del CertU. Una vez validada la autenticidad de U, AS registra IDU y PWU del usuario en el servidor y registra el IDU en la Blockchain.

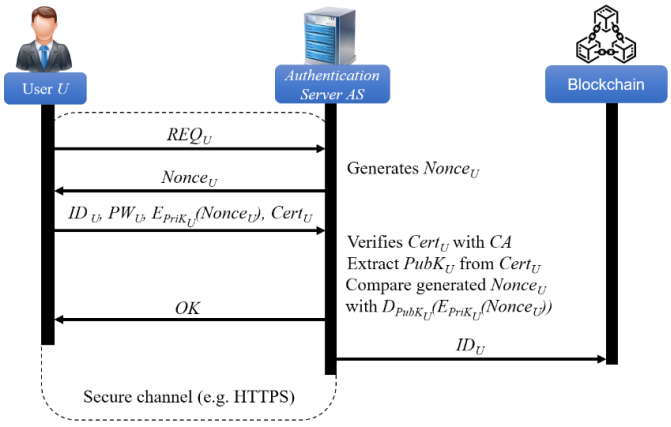

Figura 4. Protocolo de registro de usuarios.

Una vez registrado el usuario, el proceso de inicio de sesión es igual al proceso tradicional basado en identificación y contraseñas.

Verificación de las prestaciones

Como se indica al principio de este trabajo, el análisis de la arquitectura propuesta desde la perspectiva del anonimato, la privacidad y la flexibilidad.

Anonimato y Privacidad: El uso de PIDU en lugar de InfoU para la generación del Certficado CertU, permite al usuario ocultar su identidad a la AS, MS y otros usuarios del Metaverso. Sólo la CA (que podría estar controlada por el Gobierno, por ejemplo) podría conocer la identidad real del usuario cuando fuera necesario. Sin embargo, incluso la CA podría conocer la identidad real del usuario sólo con la colaboración del AS, ya que requiere hacer la correspondencia entre CertU e IDU.

Flexibilidad de implementación: Dado que la arquitectura propuesta se basa en la Infraestructura de Clave Pública (PKI) tradicional, su implementación es sencilla y no requiere la implantación de nuevas infraestructuras. Además, AS no requiere la modificación del proceso de inicio de sesión tradicional basado en contraseña. Sólo necesita añadir un proceso para verificar el Certificado CertU enviado por el usuario con la CA, lo que no es un problema importante.

CONCLUSIONES

El Metaverso está evolucionando rápidamente y se espera que se convierta en la próxima versión de Internet. Dado que el Metaverso requiere mantener el anonimato y la privacidad de los usuarios en las transacciones normales, pero reconocer si el usuario es válido cuando se requiere, es necesario crear una nueva arquitectura de autenticación de usuarios.

Ante esta situación, en el presente trabajo se ha desarrollado un nuevo esquema de autenticación de usuarios que cumple los requisitos mencionados. La arquitectura presentada permite a los usuarios mantener el anonimato y la privacidad en los mundos virtuales del Metaverso, a la vez que permite una rápida implementación sin grandes cambios en los actuales sistemas de autenticación de usuarios. La educación digital docentes se infiere como el conjunto de conocimientos, capacidades, habilidades y destrezas relacionadas con el uso de la tecnología, aplicada a los contextos y procesos educativos, con el fin de alcanzar uno o varios objetivos.

REFERENCIAS BIBLIOGRÁFICAS

De Jong, H. (2022). The Political Economy of the Metaverse. https://quantoz.com/publications/the-economy-of-the-metaverse/

Drummond, J. S., & Themessl-Huber, M. (2007). The cyclical process of action research: The contribution of Gilles Deleuze. ***Action Research, 5***(4), 430–448.

Falchuk, B., Loeb, S., & Neff, R. (2018). The social metaverse: Battle for privacy. ***IEEE Technology and Society Magazine, 37***(2), 52–61.

Fan, K., Li, H., & Wang, Y. (2009). Security analysis of the kerberos protocol using BAN logic. ***2009 Fifth International Conference on Information Assurance and Security, 2***, 467–470.

Goldman Sachs LLC. (2021). ***Overview of Digital Assets and Blockchain***. https://1e9.community/uploads/short-url/yK2ONzAH0NdeYL8lyFJN7QfKYte.pdf

Hardt, D. (2012). *The OAuth 2.0 authorization framework*. https://www.rfc-editor.org/rfc/rfc6749

Li, X., Peng, J., Obaidat, M. S., Wu, F., Khan, M. K., & Chen, C. (2019). A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. *IEEE Systems Journal, 14*(1), 39–50.

Mystakidis, S. (2022). Metaverse. *Encyclopedia*, *2*(1), 486-497.

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., & Dutkiewicz, E. (2022). *Metachain: A novel blockchain-based framework for metaverse applications*. https://arxiv.org/pdf/2201.00759.pdf

Recordon, D., & Reed, D. (2006). *OpenID 2.0: a platform for user-centric identity management. Proceedings of the Second ACM Workshop on Digital Identity Management*. https://dl.acm.org/doi/10.1145/1179529.1179532

Vidal-Tomás, D. (2022). The new crypto niche: NFTs, play-to-earn, and metaverse tokens. *Finance Research Letters*, 47.

Wang, K., & Kumar, A. (2022). *Human Identification in Metaverse Using Egocentric Iris Recognition*. https://www.techrxiv.org/articles/preprint/Human_Identification_in_Metaverse_Using_Egocentric_Iris_Recognition/19750411/1/files/35094070.pdf

Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T. H., & Shen, X. (2022). *A Survey on Metaverse: Fundamentals, Security, and Privacy*. https://arxiv.org/pdf/2203.02662.pdf

Yang, Q., Zhao, Y., Huang, H., Xiong, Z., Kang, J., & Zheng, Z. (2022). Fusing blockchain and AI with metaverse: A survey. *IEEE Open Journal of the Computer Society, 3*, 122–136.

Zhang, X., Huang, X., Yin, H., Huang, J., Chai, S., Xing, B., Wu, X., & Zhao, L. (2022). Llakep: A low-latency authentication and key exchange protocol for energy internet of things in the metaverse era. *Mathematics, 10*(14).