A Comprehensive Decentralized Digital Identity System: Blockchain, Artificial Intelligence, Fuzzy Extractors, and NFTs for Secure Identity Management

Oleksandr Kuznetsov[1,2], Emanuele Frontoni[1,3], Viktor Katrich[4], Olena Kobylianska[2], and Svetlana Pshenichnaya[4]

[1] *Department of Political Sciences, Communication and International Relations, University of Macerata, 30/32 Via Crescimbeni, Macerata, 62100, Italy*
[2] *Department of Information and Communication Systems Security, School of Computer Sciences, V. N. Karazin Kharkiv National University, 4 Svobody sq., Kharkiv, 61022, Ukraine*
[3] *Department of Information Engineering, Marche Polytechnic University, 12 Via Brecce Bianche, Ancona, 60131, Italy*
[4] *School of Radiophysics, Biomedical Electronics and Computer Systems, V. N. Karazin Kharkiv National University, 4 Svobody sq., Kharkiv, 61022, Ukraine*

Abstract

Existing digital identification systems are often vulnerable to attacks as they are commonly based on authentication methods such as passwords, PIN codes, biometric data, etc., which can be easily forged or compromised. In this letter, we propose a digital identification system based on a unique set of user biometric data processed by Artificial Intelligence (AI) and fuzzy extractors to generate a cryptographically secure password linked to a unique Non-Fungible Token (NFT). Our system provides decentralized identification based on blockchain technology, which eliminates problems associated with centralized identification systems, such as cyber-attacks on central servers and data leaks. Our proposed system offers a higher level of user identification security by linking the user to their data through a unique NFT, generating a cryptographically secure password, and processing large volumes of biometric data using AI and fuzzy extractors. Our system provides a solution to many of these problems, making it important and relevant to many industries, including banking, medical, and financial sectors. The use of decentralized storage of information on the blockchain provides a high level of protection against hacking and reduces the likelihood of data breaches, making our system particularly relevant in the field of financial services and personal data protection.

Keywords

Decentralized digital identification, NFT, AI, fuzzy extractors, blockchain, biometrics, cryptography.

1. Introduction

The need for a global decentralized digital identity has arisen due to the increasing demand for identity verification and authentication in various fields such as e-government, e-commerce, and online services [1–2]. However, the centralized nature of traditional identification systems creates several problems such as lack of functional compatibility, privacy risks, and vulnerability to cyberattacks [3–4]. Furthermore, traditional identification systems are not always accessible for marginalized groups, exacerbating issues of identity verification and access to services. This problem is compounded by the fact that many countries have their own identification systems, which

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: kuznetsov@karazin.ua (O. Kuznetsov); emanuele.frontoni@unimc.it (E. Frontoni); vkatrich@karazin.ua (V. Katrich); kobol1801@gmail.com (O. Kobylianska); s.pshenychna@karazin.ua (S. Pshenichnaya)
ORCID: 0000-0003-2331-6326 (O. Kuznetsov); 0000-0002-8893-9244 (E. Frontoni); 0000-0001-5429-6124 (V. Katrich); 0000-0003-3405-3429 (O. Kobylianska); 0000-0002-6212-7280 (S. Pshenichnaya)

are not compatible with each other, making cross-border identification difficult [5–6].

In this paper, we propose the development of a global decentralized digital identification system based on Non-Fungible Tokens (NFTs) technology [7–8], Artificial Intelligence (AI) methods [9–10], and fuzzy extractors [11–14]. The use of blockchain technology provides immutable and secure identity verification, making it an appropriate solution for embedded systems. The proposed system utilizes AI methods to process biometric data and fuzzy extractors, which are cryptographic tools, to generate cryptographic keys based on user biometric data. The keys will be used for encryption and decryption of identification data, providing an additional layer of security to the system.

The proposed system is designed to be decentralized, relying on a network of nodes that will be responsible for storing and verifying identification data [15]. This approach will help ensure the system's resilience to attacks and provide security and confidentiality for user data. The use of NFTs will enable the creation of unique digital certificates that cannot be reproduced or duplicated, preventing identity theft and fraud.

Overall, the proposed system is tailored for use in embedded systems, where security and efficiency are of paramount importance. By utilizing NFT technology, AI methods, and fuzzy extractors, we aim to develop a decentralized identification system that can be used across various embedded platforms and services, providing an efficient and secure means of identity verification.

2. State-of-the-Art

The problem of decentralized digital identification has been addressed in many related articles.

The proposed Idenx system in [16] is a promising approach to mitigating supply chain attacks in the smart grid. However, the article does not address the challenges of scalability and performance in implementing a blockchain-based identity management system in the context of a large-scale smart grid. Additionally, the article does not discuss the issue of secure key management, which is critical to ensuring the integrity and authenticity of smart grid components and services.

The proposed Casper platform appears to provide a secure and decentralized solution for digital identity management using blockchain and a self-sovereign identity-based approach [17]. However, the paper does not provide a comprehensive analysis of the potential limitations of this approach, such as scalability, interoperability, and regulatory compliance. In addition, the paper does not address the potential challenges associated with the adoption and integration of this platform in existing systems. Therefore, further research is required to evaluate the effectiveness and feasibility of this approach in real-world scenarios.

The paper [18] evaluates the compliance of Self-Sovereign Identity (SSI) systems with the key principles of GDPR and compares two different SSI ecosystems. However, it does not address the issue of secure and decentralized storage of biometric data, which is a critical concern for digital identity systems. Additionally, it does not explore the potential of AI and fuzzy extractors in improving the accuracy and security of identity verification. These are important areas of research that could significantly enhance the security and usability of digital identity systems.

While the proposed digital identity platform "Trust Pass" [19] offers high accuracy in document validation and biometric authentication, it does not address the issue of centralized identity verification and storage, which can still be vulnerable to hacks and data breaches. Additionally, the article does not mention how the system handles the issue of user consent and control over their data.

The article [20] focuses on the concept of SSI and the challenges of identity management in a distributed digital environment. While it provides a comprehensive overview of different authentication and verification solutions, it falls short in addressing the vulnerabilities of centralized digital entities and the limitations of current identity management approaches.

The papers [21–22] provide a critical analysis of the current digital identity landscape and focus on the SSI based on blockchain as a potential solution. However, the paper does not address the limitations of SSI implementation, such as the difficulty of

managing large volumes of biometric data and the complexity of integrating SSI into existing systems. Additionally, the paper does not offer a comprehensive solution for secure and convenient access to user data.

The proposed SmartDID system [23] is an innovative blockchain-based distributed identity management system that aims to provide strong privacy preservation and SSI to IoT devices. However, the article mentions continuing issues related to resource limitations for IoT devices, security, and privacy, which are not adequately addressed by SmartDID. Additionally, the paper does not incorporate the use of advanced AI and fuzzy extractor methods, which we have implemented in our decentralized digital identity system, allowing for improved accuracy and security.

The papers [9, 24] describe systems that use NFTs and smart contracts for document traceability, which aims to prevent fraud, corruption, tampering, and counterfeiting in identity and document verification. These approaches have similarities with our proposed decentralized digital identity system, as both use NFTs and smart contracts to ensure a secure and transparent solution. However, compared to our solution, they lack details on AI-based biometric processing, fuzzy extractors, decentralized architecture, and user control over data, which may result in weaker security measures and limited user privacy.

There are numerous works and studies in the field of decentralized identity, but many unresolved issues remain. Our decentralized digital identity system based on NFT, AI methods, and fuzzy extractors addresses some of these issues, including the ability to process large volumes of biometric data using AI and fuzzy extractors, generating cryptographically secure passwords, and utilizing blockchain technology for decentralized identity management. Additionally, our system offers the convenience of remote access to personal data and eliminates the need for special equipment.

3. Methodology

The methodology used in this paper for global digital identification involves the integration of blockchain technology, NFTs, AI methods, and fuzzy extractors.

Blockchain is a decentralized and immutable digital ledger that can be used to securely store and manage identity-related information. By using blockchain, it is possible to create a tamper-proof and transparent record of identity-related transactions.

NFTs are unique digital assets that are used to represent a particular object or item. In the context of digital identification, NFTs can be used to represent a person's identity and associated attributes. The use of NFTs ensures that each identity is unique, non-interchangeable, and can be easily verified.

AI methods such as deep learning-based face recognition can be used to authenticate a person's identity based on biometric data. The use of AI can improve the accuracy and efficiency of the authentication process, which is crucial for large-scale digital identification systems.

Finally, fuzzy extractors can be used to extract a secure cryptographic key from biometric data, such as a fingerprint or iris scan. This key can then be used to securely verify a person's identity without exposing their biometric data. Fuzzy extractors can help address privacy concerns associated with the use of biometric data in digital identification systems. The integration of these technologies provides a robust and secure framework for global digital identification.

4. Basic System Components

The identification blockchain system proposed in this paper is based on distributed ledger technology, which ensures transparency and security in digital identification. The main components of the system are digital wallets, smart contract signatures, data transmission protocols, and NFT creation and verification systems. Digital wallets are used to store digital assets and personal user data, while smart contract signatures automate the identity verification process and the agreement of terms for the use of personal data. Data transmission protocols are used to ensure the secure transfer of information between users and the system, and the NFT creation and verification system ensures the

uniqueness and tamper-proof nature of digital identification.

The blockchain identification system works as follows: when a user creates an account in the system, their data is hashed and stored on the blockchain. The system then creates an NFT, which is linked to this personal data, and sends it to the user's digital wallet. Every time the user wants to use their data to authenticate themselves in online services or other systems, the system requests access to the corresponding NFT. If the user grants permission to use the NFT, the smart contract signature is used to verify the authenticity of the user's data.

To ensure security and protect the confidentiality of user data, the system uses AI methods such as machine learning and deep learning to detect and prevent fraud and cyberattacks. Fuzzy extractors are used to compress and store user biometric data in a secure format [25–26].

Thus, the blockchain identification system developed in this paper represents an innovative and secure approach to global digital identification.

4.1. System Formalization

Let U be the set of users, D be the set of their data, $H: D \to H(D)$ be the hash function for hashing personal data, W be the set of digital wallets, N be the set of NFTs, T be the set of smart contract rules, and P be the set of data transmission protocols.

Then, the identification system can be represented as a tuple (U, D, H, W, N, T, P), where: each user $u \in U$ has their account associated with their data $d \in D$, which is hashed by the function H and stored in the blockchain; each user also has their digital wallet $w \in W$, where their data and NFTs tied to them are stored; each NFT $n \in N$ is linked to a specific user and is used for authentication and authorization when requesting access to their data; each smart contract $t \in T$ represents rules for using the user's data and automatically verifies the authenticity of that data; each data transmission protocol $p \in P$ ensures secure transmission of information between the user and the system; when using the system, each user u provides access to the corresponding NFT n, which is automatically verified by the smart contract t

4.2. Elements of Digital Identification

When creating an account in the identification system, the user provides their data d_u, which is hashed using a hash function H, i.e., $h_u = H(d_u)$. The resulting hash value h_u is then stored in the blockchain registry of the system. Mathematical notation of the step: $h_u = H(d_u)$, $h_u \in \{0,1\}^l$, $d_u \in D$, $u \in U$, where: h_u is the hash value of the user's data u; H is the hash function; d_u is the user's data; D is the set of personal data; U is the set of users; l is the length of the hash value (in bits).

To generate unique digital identifiers for users, biometric data is used. Let B be the set of fuzzy biometric data, $F: B \to F(B)$ be an AI function that extracts essential features from the fuzzy data, $E: F(B) \to E(F(B))$ be a fuzzy extractor that processes the features and generates a cryptographically secure password (key), and N be the set of NFTs, where each element $n \in N$ is associated with a user's password.

The procedure for creating an NFT for the user can be described as follows:

1. The user u provides their fuzzy biometric data $b \in B$.
2. The AI function F is used to extract essential features from the user's biometric data: $f = F(b)$.
3. The fuzzy extractor E processes the extracted features f and generates a cryptographically secure password p: $p = E(f)$.
4. A unique NFT n is created, associated with the user's password p: $n = createNFT(p)$.
5. The NFT n is sent to the user's digital wallet for further use in the authentication process.

Thus, this process ensures the uniqueness and security of the user's identifier, using their fuzzy biometric data and a cryptographically secure password.

4.3. Implementation of Digital Identification as Smart Contracts

To implement digital identification in a decentralized system, we will use smart contracts that provide automatic verification of users' data and coordination of the conditions for their use. Specifically, we will use smart contracts that can verify the authenticity of a user's identifier based on the NFT associated with their data. These contracts will contain rules for the use of personal data and automatically verify them for compliance with these rules when requesting access to this data.

Also, to ensure the security and protection of data, we can use smart contracts that can perform operations for processing and storing users' data in a secure and protected manner, using cryptographic methods and data transmission protocols.

The smart contract for user registration and NFT generation is a part of the software code that is executed upon user account creation in the identification system. Its main task is to create a unique NFT that will be used for user authentication in the future.

The structure of the smart contract can be described as follows: $Contract : RegisterUser(u,b) \to n$, where: u is a user who creates an account; b is fuzzily defined biometric data of the user; n is a unique NFT linked to the user's password.

The smart contract itself consists of three main steps:

1. Generation of a cryptographically secure password based on the user's biometric data: $p = E(F(b))$, where F there is an AI function that extracts essential features from fuzzy biometric data and E is a fuzzy extractor that processes the extracted features and generates a cryptographically secure password.
2. Creation of a unique NFT linked to the generated password: $n = createNFT(p)$, where $createNFT$ is a function that creates a unique NFT based on the cryptographically secure password.
3. Saving the created NFT in the user's digital wallet and returning it as the result of the smart contract execution: $saveNFT(u,n)$, where $saveNFT$ is a function that saves the created NFT in the user's digital wallet.

Thus, the smart contract for registering an account and generating an NFT ensures the security and uniqueness of the user's identifier based on their fuzzily defined biometric data and a cryptographically secure password.

Fig. 1 depicts a UML sequence diagram for the registration of a user account and the generation of an NFT.

The smart contract for verifying the authenticity of a user's identifier based on NFT consists of the following elements:

- A data structure containing information about the user and their NFT: $Auth(u) = (n_u, d_u, t_u)$ where: n_u is the identifier of the NFT associated with the user's data u; d_u is the personal data of the user u, which must correspond to the data associated with the NFT n_u; t_u is the time of the last update of the user's data u.
- Method for authenticating a user's data: $authenticate(u,n,d) \to bool$ where: u is the user attempting to access their data; n is the NFT identifier provided by the user u for authentication.
- d is the personal data that the user u wants to use for authentication. Algorithm for updating a user's data: $update(u,d) \to bool$ where: u is the user whose personal data needs to be updated; d is the new personal data of the user.

When attempting to access a user's data u, the smart contract first extracts information about the user u and their NFT n_u from the $Auth(u)$ structure. Then it calls the $authenticate(u,n,d)$ method to authenticate the personal data provided by the user u, using their NFT n_u and stored personal data d_u. If the data is authentic, the smart contract returns the value $true$ and updates the time of the last update of the personal data t_u in the $Auth(u)$ structure. If the data is invalid, the smart contract returns the value $false$. If there is a need to update a user's data, the smart contract calls the $update(u,d)$ method to update the personal data in the $Auth(u)$ structure and the associated NFT. If the update is successful, the method returns the value $true$, otherwise—the value $false$. Thus, the structure of the smart contract for verifying the authenticity of a user's identifier based on NFT consists of three main elements: data structure, authentication method, and personal data update method.

In Fig. 2, a UML sequence diagram for the user identity authenticity verification based on NFT is presented.

The smart contract for processing and storing personal user data includes the following components:

1. A data structure for storing personal data: let D_u be the set of personal data of the user u. We will use a data structure, such as an array or hash table, to store the user's data. Suppose we use the hash table DHT_u, where each element stores a key-value pair (k,v), where k is the identifier of the data and v is the data itself. Thus, $DHT_u[k]=v$.
2. An encryption function for personal data: let E be the encryption function that converts personal data $d \in D_u$ into encrypted form $e=E(d)$.
3. A data structure for storing encrypted personal data: let E_u be the set of encrypted personal data of the user u. We will use a data structure, such as an array or hash table, to store the encrypted personal data of the user. Suppose we use the hash table EHT_u, where each element stores a key-value pair (k,v), where k is the identifier of the data and v is the encrypted data. Thus, $EHT_u[k]=v$.
4. An authenticity verification function for user data: let C be the function for verifying the authenticity of user data. The smart contract will use the function C to verify the authenticity of the user's data that will be requested by other network participants.

Thus, the smart contract for processing and storing personal user data can be formalized as follows:

$$DHT_u[k]=d, \text{ where } d \in D_u;$$
$$EHT_u[k]=e, \text{ where } e=E(d);$$
$$C(e,key)=\begin{cases}1, & \text{if } E(key)=e\\ 0, & \text{else}\end{cases};$$

where: k is the identifier of the data; key is the key for decrypting the data; D_u is the set of personal data of user u; E is the encryption function; E_u is the set of encrypted personal data of user u; C is the function for verifying the authenticity of user data; DHT_u is the hash table for storing personal data.

This diagram depicts the interaction between the user, the personal data processing and storage smart contract (DSC), the digital signature smart contract (DSS), and the Blockchain Registry (BR).

The main scenario starts with the user's request to store personal data, to which the DSC encrypts the data and stores them in the blockchain registry. The DSC then returns the data identifier to the user. When the user requests access to personal data, the DSC finds the data in the registry, decrypts it, and requests a digital signature from the DSS. The DSS verifies the authenticity of the user and signs the data, after which the DSC returns them to the user.

The UML Component diagram (Fig. 4) provides a comprehensive visualization of the main components and their relationships within the decentralized digital identity system. Each component plays a crucial role in the overall functionality and security of the system.

- **User Interface.** The User Interface serves as the point of interaction for users and service providers. It receives input, displays relevant information, and facilitates communication with other components in the system.
- **Blockchain System.** The Blockchain System is responsible for managing the decentralized network, ensuring the immutability and security of the digital identity system. It connects the nodes in the network and maintains the overall architecture.
- **Node.** Nodes are responsible for storing and verifying identity data within the blockchain network. They contribute to the decentralized nature of the system and provide redundancy and resilience against attacks.
- **Smart Contract.** Smart Contracts automate and enforce the rules and processes of the digital identity system. They interact with the Identity Data Storage and NFT Management components to create, verify, and manage digital identities.
- **AI Biometric Processor.** The AI Biometric Processor processes

biometric data, such as facial recognition, to enable secure and efficient identity verification. It extracts unique biometric features and passes them to the Fuzzy Extractor.

- **Fuzzy Extractor.** Fuzzy Extractors generate cryptographic keys based on the biometric features provided by the AI Biometric Processor. These keys enhance the security of the system by providing an additional layer of protection for identity data.
- **Identity Data Storage.** The Identity Data Storage securely stores user data and is accessed by Smart Contracts. It maintains user information while ensuring data privacy and protection against unauthorized access.
- **NFT Management.** NFT Management creates unique digital identities using NFTs. These digital identities cannot be replicated or duplicated, thus preventing identity theft and fraud.
- **Biometric Features.** Biometric Features represent the unique characteristics of users, such as fingerprints or facial features. They are used as input for the Fuzzy Extractor to generate cryptographic keys.
- **Cryptographic Keys.** Cryptographic Keys are generated from biometric features and are used to encrypt and decrypt identity data. These keys provide a secure mechanism to protect user data and authenticate users within the system.
- **User Data.** User Data contains the personal information of users and is protected by cryptographic keys. It is securely stored in the Identity Data Storage and can be accessed only through proper authentication.
- **Service Provider.** Service Providers interact with the system to authenticate and authorize users for various services. They rely on the decentralized digital identity system to ensure secure and efficient access to their platforms.

In summary, the UML Component diagram offers a clear representation of the decentralized digital identity system's components, their relationships, and their roles. The diagram highlights the system's decentralized architecture, which leverages blockchain technology, AI-based biometric processing, fuzzy extractors, and NFTs to create a secure and efficient digital identity management solution.

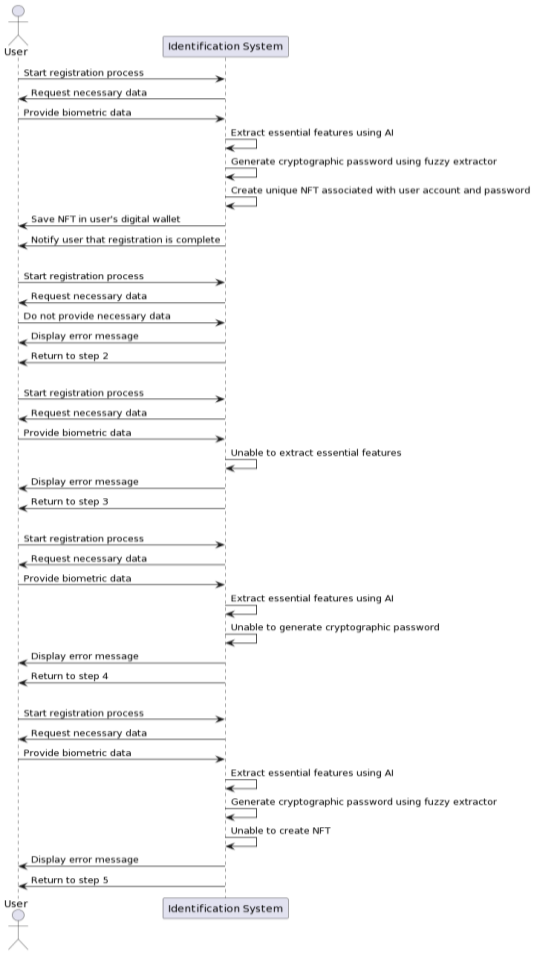

Figure 1: UML sequence diagram for user account registration and NFT generation

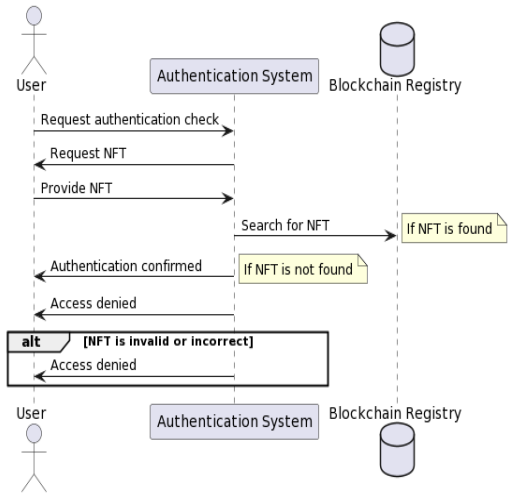

Figure 2: UML Sequence Diagram of NFT-Based User ID Authentication

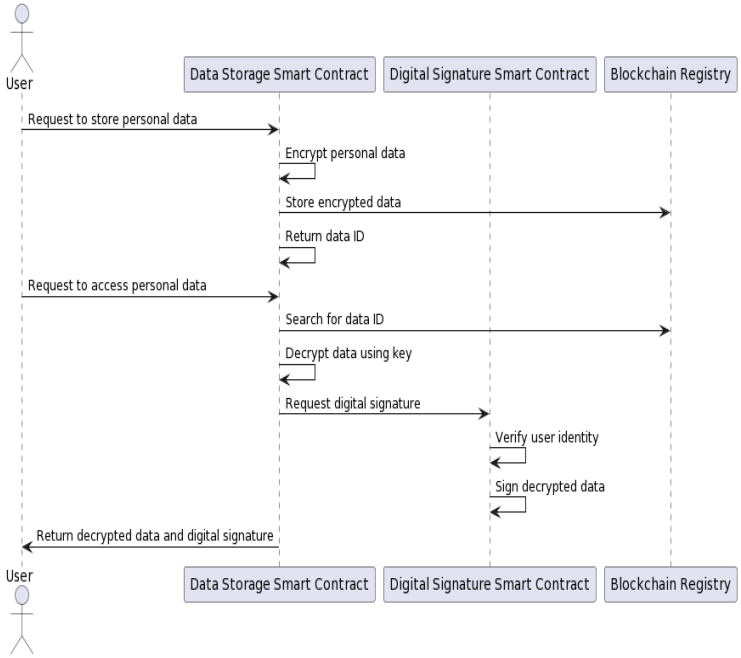

Figure 3: UML Sequence diagram for Personal Data Processing and Storage Smart Contract

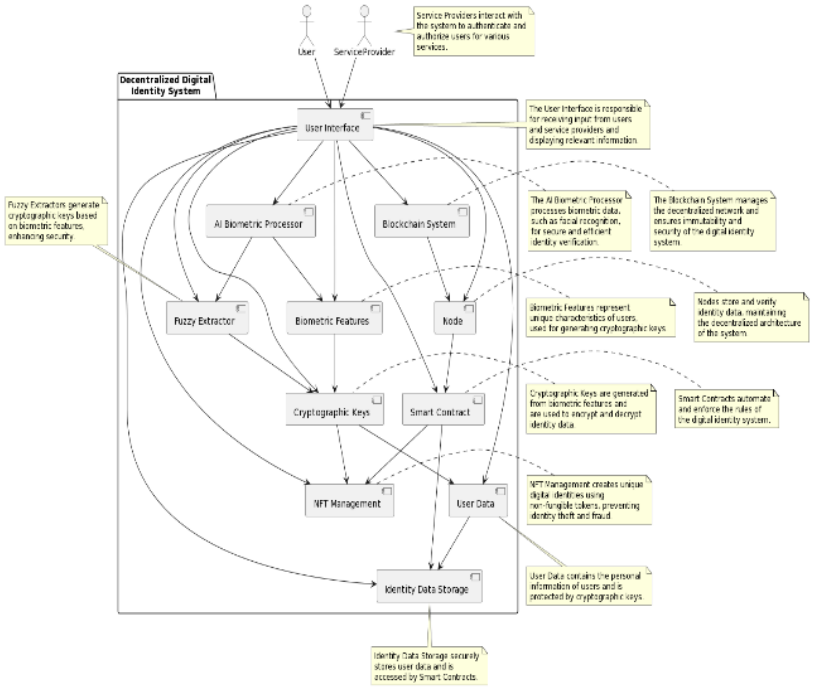

Figure 4: UML Component diagram for the decentralized digital identity system.

Table 1
Comparison of results

Feature	Our Solution	Solution A	Solution B	Solution C
Decentralized	Yes	No	Yes	Partially
Enhanced Security	Yes	Yes	Partially	No
Improved Privacy	Yes	Partially	No	Yes
Cross-platform Compatibility	Yes	No	Yes	Partially
AI-based Biometric Processing	Yes	No	Yes	No
Fuzzy Extractor Integration	Yes	No	No	No
NFT-based Identity	Yes	No	Partially	No

5. Discussion and Comparison of Results

In this research, we have addressed the pressing need for a secure, efficient, and user-centric digital identity management system. Our proposed solution leverages the advantages of blockchain technology, AI techniques for biometric data processing, and fuzzy extractors for cryptographic key generation. This unique combination of technologies offers a novel approach to digital identity management that sets it apart from existing solutions in the market.

The key innovations of our solution include:

- **Decentralization.** Our digital identity system is built on a decentralized architecture, eliminating reliance on a central authority or organization. This ensures better resilience against attacks and minimizes the risk of data breaches and identity theft.
- **Enhanced Security.** The use of AI techniques for processing biometric data, fuzzy extractors for generating cryptographic keys, and NFTs for creating unique digital identities significantly enhances the overall security of the system. These features prevent unauthorized access, duplication, and forgery of identity data.
- **Improved Privacy.** By allowing users to maintain full control over their digital identities and sharing only the necessary information with service providers, our system ensures better privacy for users. It also reduces the risk of unauthorized data access and misuse.
- **Cross-platform Compatibility.** Our solution is designed to be used across various platforms and services, enabling seamless integration with embedded systems in different sectors such as finance, healthcare, and e-commerce.

To illustrate the advantages of our proposed digital identity system compared to other known solutions, we present the comparison in Table 1.

As seen in the comparison table, our proposed digital identity system stands out in terms of decentralization, enhanced security, improved privacy, cross-platform compatibility, AI-based biometric processing, fuzzy extractor integration, and the use of NFTs for creating unique digital identities. While other solutions may offer some of these features, our approach provides a more comprehensive and robust solution to digital identity management.

In the comparison table, we referred to three hypothetical digital identity management solutions:

- **Solution A:** Centralized Digital Identity Management Systems (e.g., traditional single sign-on systems).
- **Solution B:** SSI platforms (e.g., Sovrin, uPort).
- **Solution C:** Federated identity management systems (e.g., OAuth, OpenID Connect).

These examples represent well-known digital identity management solutions currently in use. While each of these solutions has its merits, our proposed decentralized digital identity system offers a more comprehensive approach, combining the advantages of blockchain technology, AI-based biometric processing, fuzzy extractors, and NFTs for creating unique digital identities.

6. Conclusions

Existing identification systems often rely on authentication methods such as passwords, PIN codes, biometric data, and so on [27–28]. However, these methods are often easily counterfeited or compromised [29–30].

The proposed NFT-based digital identification system, utilizing AI and fuzzy extractor methods, provides a higher level of user identification security. It uses a unique set of user biometric data, processed with AI and fuzzy extractors, to generate a cryptographically secure password linked to a unique NFT.

Firstly, our system utilizes a unique NFT to link the user with their data. This eliminates the possibility of data forgery or alteration and ensures the security of data storage and transmission.

Secondly, by utilizing AI and fuzzy extractors, our system can process large volumes of biometric data and extract the most significant features from them. This improves identification accuracy and reduces the probability of errors, which is especially

important for systems used in the banking and medical sectors.

Thirdly, our system generates a cryptographically secure password linked to the user's unique NFT, ensuring the security of data transmission and storage. This is critical for systems used in the financial services and personal data protection fields.

Finally, our system provides a high degree of convenience and accessibility for users, as it does not require specialized equipment and provides remote access to personal data.

Thus, our NFT-based digital identification system utilizing AI and fuzzy extractors provides reliability, security, and user convenience, making it an attractive option for a wide range of users and organizations.

7. Acknowledgments

This project has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No. 101007820—TRUST. This publication reflects only the author's view and the REA is not responsible for any use that may be made of the information it contains.

References

[1] S. Van Staden, P. Sheetekela, Unified Cooperative Population Identification Architecture to Enhance the National Identity Ecosystem of Developing Countries, iIST-Africa Week Conference (2018).

[2] H. L'Amrani et al., Identity Management Systems: Laws of Identity for Models7 Evaluation, 4th IEEE Int. Colloq. Inf. Sci. Technol. (2016) 736–740. doi:10.1109/CIST.2016.7804984.

[3] N. Poluyanenko, et al., The Problem of Double Costs in Blockchain Systems, Adv. Comput. Sci. Eng. Educ. III, (2021) 640–652. doi:10.1007/978-3-030-55506-1_57.

[4] N. Poluyanenko, et al., Extrapolation to Calculate the Probability of a Double Spending Attack, in: Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems vol. 2608 (2020) 610–620. doi:10.32782/cmis/2608-47.

[5] K. Isirova, et al., Decentralized Electronic Voting System Based on Blockchain Technology Developing Principals, in: Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems vol. 2608 (2020) 211–223. doi:10.32782/cmis/2608-17.

[6] A. Kuznetsov, et al., Cryptographic Transformations in a Decentralized Blockchain Environment, Inf. Secur. Technol. Decent. Distrib. Netw. (2022) 89–113. doi:10.1007/978-3-030-95161-0_4.

[7] Ethereum.Org, Non-fungible tokens (NFT) (2023). URL: https://ethereum.org.

[8] nell'Enciclopedia Treccani, Non Fungible Token (NFT) (2023). URL: https://www.treccani.it/enciclopedia/non-fungible-token.

[9] M. Eltuhami, M. Abdullah, B. Talip, Identity Verification and Document Traceability in Digital Identity Systems using Non-Transferable Non-Fungible Tokens, Int. Visual. Inform. Technol. Conf. (IVIT) (2022) 136–142. doi:10.1109/IVIT55443.2022.10033362.

[10] J. Brownlee, Probability for Machine Learning: Discover How To Harness Uncertainty With Python, Machine Learning Mastery (2019).

[11] N. Li, et al., Fuzzy Extractors for Biometric Identification, IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS), 2017: pp. 667–677. doi:10.1109/ICDCS.2017.107.

[12] A. Jana, et al., Neural Fuzzy Extractors: A Secure Way to Use Artificial Neural Networks for Biometric User Authentication, Proc. Priv. Enhancing Technol. 4 (2022) 86–104. doi:10.56553/popets-2022-0100.

[13] B. Bebeshko, et al., Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency, Journal of Theoretical and Applied Information Technology 100(24) (2022) 7390–7404.

[14] K. Khorolska, et al., Application of a Convolutional Neural Network with a Module of Elementary Graphic Primitive Classifiers in the Problems of Recognition of Drawing Documentation and Transformation of 2D to 3D Models, Journal of Theoretical and Applied

Information Technology 100(24) (2022) 7426–7437.
[15] V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.
[16] A. Sani, et al., Idenx: A Blockchain-based Identity Management System for Supply Chain Attacks Mitigation in Smart Grids, IEEE Power & Energy Society General Meeting (2020) 1–5. doi: 10.1109/PESGM41954.2020.9281929.
[17] E. Bandara, et al., A Blockchain and Self-Sovereign Identity Empowered Digital Identity Platform, Int. Conf. Comput. Commun. Netw. (ICCCN), (2021) 1–7. doi:10.1109/ICCCN52240.2021.9522184.
[18] N. Naik, P. Jenkins, Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity, 7th Int. Conf. Behav. Social Comput. (2020) 1–6. doi: 10.1109/BESC51023.2020.9348298.
[19] K. Dissanayake, et al., "Trust Pass"—Blockchain-Based Trusted Digital Identity Platform Towards Digital Transformation, 2nd Int. Inform. Software Eng. Conf. (2021) 1–6. doi: 10.1109/IISEC54230.2021.9672336.
[20] K. Gilani, et al., A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data, 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (2020) 97–101. doi: 10.1109/BRAINS49436.2020.9223312.
[21] K. Moriyama, A. Otsuka, Permissionless Blockchain-Based Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Processors, IEEE Int. Conf. Blockchain (2022) 1–10. doi: 10.1109/Blockchain55522.2022.00012.
[22] Y. Bai, et al., Decentralized and Self-Sovereign Identity in the Era of Blockchain: A Survey, IEEE Int. Conf. Blockchain (2022) 500–507. doi: 10.1109/Blockchain55522.2022.00077.
[23] J. Yin, et al., SmartDID: A Novel Privacy-Preserving Identity Based on Blockchain for IoT, IEEE Internet Th. J. (2022) 1–1. doi:10.1109/JIOT.2022.3145089.
[24] K. Gilani, et al., Self-sovereign Identity Management Framework using Smart Contracts, NOMS 2022–2022 IEEE/IFIP Netw. Oper. Manag. Symp. (2022) 1–7. doi:10.1109/NOMS54207.2022.9789831.
[25] Z. B. Hu, et al., Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388. doi:10.1007/978-3-030-80472-5_31
[26] V. Zhebka, et al., Optimization of Machine Learning Method to Improve the Management Efficiency of Heterogeneous Telecommunication Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 149–155.
[27] S. Banerjee, et al., A Provably Secure and Lightweight Anonymous User Authenticated Session Key Exchange Scheme for Internet of Things Deployment, IEEE Internet Th. J. 6 (2019) 8739–8752. doi:10.1109/JIOT. 2019.2923373.
[28] R. Amin, et al., Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues, Bio-Inspiring Cyber Secur. Cloud Services: Trends Innov. (2014) 423–446. doi:10.1007/978-3-662-43616-5_16.
[29] T.V. hamme, et al., AI for Biometric Authentication Systems, Security and Artificial Intelligence (2022) 156–180. doi:10.1007/978-3-030-98795-4_8.
[30] Z. Qin, et al., A Fuzzy Authentication System Based on Neural Network Learning and Extreme Value Statistics, IEEE Trans. Fuzzy Syst. 29(3) (2021) 549–559. doi:10.1109/TFUZZ.2019.2956896.