International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Preserving Healthcare Privacy : A fusion of Blockchain and Self Soverign Identity

[1]Ms. Monica Chawla, *[2]Dr. Alok Srivastava

Submitted:10/03/2024 **Revised**: 25/04/2024 **Accepted**: 02/05/2024

Abstract: This research delves into the intricate landscape of blockchain adoption, particularly its implications for user and data privacy concerns, especially in the context of enterprises accumulating and safeguarding user data. The transparency inherent in public blockchains raises pivotal questions surrounding data ownership and privacy. The study underscores the imperative to identify and accentuate privacy-focused blockchain technologies, proposing a standardized Blockchain Reference Model for development practices. Within the healthcare domain, the integration of self-sovereign identity (SSI) with blockchain technologies emerges as a salient focus. The research elucidates the impact of this integration on privacy-preserving mechanisms, encompassing decentralization, verifiable credentials, user control, data minimization, consent management, immutable audit trails, revocation, and secure key management. This research paper investigates the evolving landscape of blockchain technologies, with a specific focus on their integration with self-sovereign identity (SSI) in healthcare applications.. Within the healthcare sector, the integration of SSI with blockchain technology emerges as a strategic avenue. The research explores the impact of this integration on privacy-preserving mechanisms, encompassing decentralization, verifiable credentials, user control, data minimization, consent management, immutable audit trails, revocation, and secure key management. Addressing privacy and security compliance challenges in healthcare necessitates a multifaceted approach, involving technological advancements, educational initiatives, and rigorous regulatory adherence. The delicate balance between enabling data accessibility for healthcare professionals and implementing robust security measures is underscored as pivotal for successful information system management in healthcare data. The paper concludes with an in-depth examination of the symbiotic relationship between self-sovereign identity and blockchain technology. The openness of public blockchains poses critical considerations about data ownership and privacy. The report emphasizes the need of identifying and emphasizing privacy-focused blockchain technology, and it proposes a standardized Blockchain Reference Model for development procedures. The integration of self-sovereign identification (SSI) with blockchain technology is a prominent emphasis in the healthcare area. The study investigates the effect of this integration on privacy-protection methods such as decentralization, verified credentials, user control, data minimization, consent management, immutable audit trails, revocation, and secure key management. A holistic strategy to addressing privacy and security compliance issues in healthcare is being developed.

Keywords: *Blockchain technology, Privacy-Preserving mechanism, Self Soverign identity.*

1. INTRODUCTION

The potential of Self-Sovereign Identity (SSI) empowered by blockchain technology as a promising solution for safeguarding patient privacy in healthcare applications. The implementation of SSI involves four key open standards: Digital Identifier, verifiable credentials, Decentralized Key Management System (DKPI), and didauth. The SSI model, emerging in 2015 alongside blockchain technology, is defined as a decentralized identity layer that grants individuals and entities control over their identity, allowing them to request and receive credentials securely. This approach is rooted in the principles of ownership and control of private data, with blockchain technology enhancing security and privacy. The paragraph hints at the exploration of mechanisms within the research paper and raises a query about real-world implementations or case studies demonstrating the effectiveness of SSI in healthcare.

The Self-Sovereign Identity (SSI) model, emerging in 2015 alongside blockchain technology, is underpinned by essential principles, namely Differential Privacy, Attribute-Based Access Control (ABAC), and Zero-Knowledge Proofs (zkps). These principles are justified in both healthcare applications and the realm of Self-Sovereign Identity. The problem that organization can face during the implementation of the solution is primarily regarding the user experience and the related interface along with user 's education. Conventional identity management systems do not adopt a user-centric strategy that would decrease central authorities' control of user data and boost users' perceptions of trustworthiness. [1, 2], [3]. A user is typically required to to use digital services. recognize himself in several services, implying a variety of of IDs for the user to use in an analysis [3]. A Self Soverign identity relates to a new IMS in which the user is expected to be the only owner of their identification data and not require assistance from a third party [4]. This is because self-sovereign identity is highly user-centric solution to the problems that it is meant to address. Its due to this, that user should have a very friendly

[1]*Research Scholar, MVN University, Palwal,*
[2]*Associate Professor,SoET, MVN University,* [3]*Dr. Rajiv Ratan (Professor, MVN University, Palwal*

and understandable environment along with all the required information from the Getgo. For the user experience many focus groups, industry expert, and other stake holders would be required to arrive at a common conclusion on the user interface related problems. Following is the concise summary of this research paper.

- It includes the basic concept of privacy preserving mechanism in healthcare with the integration of blockchain and self-sovereign identity.
- How will the user interface deal with any new addition to the preexisting system?
- How will the users be informed about the updates being applied to the current user interface by the new user interface of which the user is unfamiliar?

For user education outreach programmes like Seminar will have to be organized extensively. Also, multiple vedio content like how to – video's, basics set-ups, and user responsibility, should be easily available on the platform as well as on rest of the internet too.

Differential Policy: Differential privacy is imperative in healthcare applications due to the highly sensitive nature of medical data. It offers a rigorous mathematical assurance of privacy protection by anonymizing individual data contributors within aggregated results. This is particularly significant in sharing medical data for research while upholding patient confidentiality. For Self-Sovereign Identity, differential privacy aligns seamlessly with principles, allowing individuals to selectively disclose attributes, maintaining overall privacy. By applying it to verifiable credentials, individuals can control attribute noise, balancing privacy and data accuracy.

Attribute-Based Access Control (ABAC): ABAC is pivotal in healthcare due to the varied sensitivity of data. It enables selective attribute disclosure based on access policies, ensuring healthcare providers access only necessary patient data while keeping sensitive attributes private. In Self-Sovereign Identity, ABAC complements principles by empowering individuals to set access policies for verifiable credentials. Users can grant specific attribute access to entities, reinforcing data control and privacy.

Zero-Knowledge Proofs (ZKPs): ZKPs play a crucial role in healthcare for authentication and authorization without exposing sensitive information. In Self-Sovereign Identity, ZKPs align with principles by enabling individuals to assert their identity and attributes without relying on central authorities. This cryptographic tool empowers users to demonstrate verifiable credentials' validity without revealing the underlying attributes, preserving privacy and user autonomy. In summary, the chosen privacy-preserving techniques—differential privacy, ABAC, and ZKPs—offer robust solutions for healthcare applications within the Self-Sovereign Identity framework. These techniques facilitate secure data sharing, selective disclosure, and verifiable authentication, ensuring individuals maintain control over their data in a privacy-centric healthcare ecosystem.

2. Research Objectives:

1. To investigate the effectiveness of privacy-preserving techniques in healthcare applications with self-sovereign identity: The primary objective is to assess the efficacy of various privacy preserving techniques, such as zero-knowledge proofs, differential privacy, attribute-based access control, etc., in ensuring the privacy and security of patient data within a self-sovereign identity framework.

2. To evaluate the impact of privacy-preserving techniques on data sharing and collaboration: The research aims to examine how the adoption of privacy-preserving techniques influences the willingness of patients to share their health data and the extent to which healthcare providers and researchers can access and use this data for collaborative purposes.

3. To explore the trade-offs between privacy and data utility: The research seeks to identify the balance between preserving patient privacy and enabling data analytics and research advancements. It will investigate the extent to which privacy-preserving techniques may affect data accuracy and utility in healthcare applications.

4. To assess the user acceptance and trust in a privacy-preserving self-sovereign identity system: The research will evaluate how patients and healthcare professionals perceive and trust the privacy-preserving self-sovereign identity system. It aims to identify any barriers to adoption and explore ways to improve user acceptance.

Motivation behind Adopting Privacy-Preserving Techniques:

1. Patient Privacy Protection: The foremost motivation is to protect the privacy of patients' sensitive health information. Privacy-preserving techniques ensure that individual patients have control over their data, and only authorized parties can access it.

2. Regulatory Compliance: In the healthcare industry, there are strict regulations and laws concerning patient data privacy, such as HIPAA and GDPR. Adopting privacy-preserving techniques is essential to comply with these regulations and avoid legal consequences.

3. Building Trust: Privacy-preserving techniques are vital in building trust between patients, healthcare providers, and other stakeholders. When patients know their data

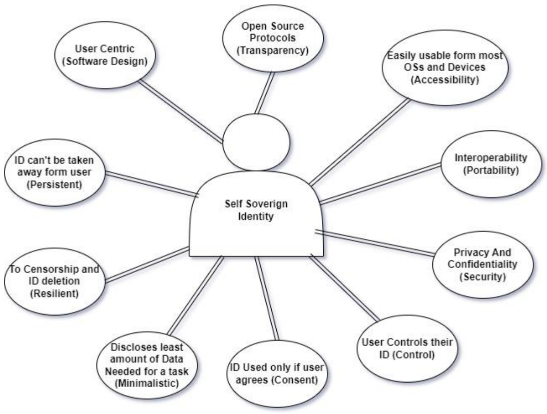
is secure and handled with care, they are more likely to participate in self-sovereign identity systems and share necessary information.

4. Enabling Secure Data Sharing: Privacy-preserving techniques allow for secure data sharing between patients and healthcare providers. By ensuring that only relevant and authorized data is shared, healthcare professionals can make accurate and informed decisions.

5. Advancing Medical Research: Research and innovation in healthcare often require access to patient data. Privacy-preserving techniques enable researchers to access anonymized data without compromising patient privacy, encouraging advancements in medical research.

6. Preventing Data Breaches: With the increasing number of data breaches in healthcare, adopting privacy-preserving techniques helps safeguard against unauthorized access and protect sensitive patient data from falling into the wrong hands.

Overall, adopting privacy-preserving techniques in healthcare applications with self-sovereign identity is essential for ensuring patient privacy, regulatory compliance, building trust, facilitating data sharing, enabling medical research, and protecting sensitive data from breaches and misuse. These techniques support the fundamental principles of self-sovereign identity and strengthen the healthcare ecosystem.


User Centric (Software Design)
Open Source Protocols (Transparency)
Easily usable form most OSs and Devices (Accessibility)
ID can't be taken away form user (Persistent)
Self Soverign Identity
Interoperability (Portability)
To Censorship and ID deletion (Resilient)
Privacy And Confidentiality (Security)
Discloses least amount of Data Needed for a task (Minimalistic)
ID Used only if user agrees (Consent)
User Controls their ID (Control)

3. RELATED WORK

3.1 First, Wu et al. [5] provided a detailed survey on how zero-knowledge proofs gradually improved in the last 20 years. Authors studied the basic principles, application, and efficiency improvement of the non-interactive zero-knowledge proof system. They summarize the research progress achieved by the non-interactive zero-knowledge proof system on the following aspects:

3.1 a non-interactive zero-knowledge proof system of NP problems, the definition, and related models of the non-interactive zero- knowledge proof system, non-interactive statistical and perfect zero-knowledge, the connection between interactive zero-knowledge proof system, non-interactive zero-knowledge proof system. One of the first research works that adopted ZKP technique in DLT and blockchain is Zerocoin. Miers et al. [6] proposed cryptographic extension to Bitcoin named Zerocoin. The protocol used in Zerocoin allows for fully anonymous currency transactions without requiring a trusted setup. Further, they explained Zerocoin's cryptographic construction, its integration into Bitcoin, and examine its performance both in terms of computation and impact on the Bitcoin protocol. Some of the recent work on privacy issue can be found in I wendi et al. [7] and Patel et al. [8] and others [9–11]. Furthermore, Boudot et al. [12] provided the efficient (less than 20 exponentiation to perform and less than 2 Kilobytes to transmit) and exactly zero knowledge range-proofs to show that a committed number belongs to an interval without revealing the number itself. Their proofs has potential application in different areas such as electronic cash, group signatures, publicly verifiable secret encryption, etc. Similarly, Camenisch et al. [13] proposed two different way of building set-membership zero-knowledge proofs. The first membership proof is based on bilinear group assumptions while, the second is based on a strong RSA assumption. Depending on the application, for example, when membership set is a published set of values such as frequent flyer clubs, cities, etc., these alternative proofs provide privacy-preserving solutions. In terms of range-proof techniques, Peng et al. [14] also proposed a range-proof technique that needs a constant cost and is more efficient than the Boudot et al. [12] range-proof schemes. Therefore, their technique improves the efficiency of range-proof without further compromising security. Koens et al. [15] proposed a more efficient zero-knowledge range-proof and compared it with the.

3.2 Nowadays, digital identity management system plays a vital role in providing various services to the citizens by the government. Singapore, for example, has developed the National Digital Identity (NDI) system as part of its Smart Nation Initiative, which is expected to help people securely access e-government services [20].

3.3 Exactly, in traditional Internet-based systems, the communication model typically follows a one-to-one interaction between a client and a server [21]. Digital identity is increasingly prevalent in online services, leading to a growing reliance on Identity Management Systems (IDMS) for establishing, verifying, and managing digital identities [22]. The raw data, which contains incomplete information in certain tuples, requires cleaning before analysis [23]. The research suggests that achieving high cyber security levels requires state control over cyberspace and the availability of a national strategy [24].

Table 1 COMPARISON OF PROPOSED SOLUTION WITH EXISTING DECENTRALIZED IDENTITY METHODS

S.No.	**Criteria**	**Existing Decentralized Identity Methods**	**Proposed Methods**
1.	Privacy	Varied Privacy Safeguards, Pseudonimyzation strategies	Differential Policy, ZKP's, ABAC, Selective attribute disclosure
2.	Security	Dependent on Specific Protocols, Vulnerabilities possible	BlockChain, Cryptographic Techniques, Zero knowledge proofs
3.	User-Control	Variances in user control, potential reliance in central authorities.	User centric principles, Individual control over access policies
4.	Practicality	Adaptability Challenges, Integration complexities	Emphasis on Interoperability, Flexibility with differential policy
5.	Adoption Challenges	Resistance to change, Integration Intricacies	Education Imperative, Privacy centric features as adoption incentives.
6	Sovrin[16]	No Remote Admin and no Policy Management,	It consist of Consent, Basic security, Multilateral Security and Privacy standard.
7	Zhou et al. [17] proposed	An identity management method	user registration, authorization, verification, and key recovery easier.
8	Liu et al. [25].	compared Sovrin, uPort, and ShoCard	using Cameron's law of identity
9	Mundhe et al.[26]	various authentication and privacy-preserving techniques in VANETS	including decentralized blockchain-based schemes,

4. PORPOSED MODELLING

Algorithm for Blockchain and SSI integration => User Identity Creation (Public and Private Key Pair)+Blockchain Registration(Public key Identity Information) + Authentication(Digital Signature) + Verification of Blockchain(Validation result) + Self-sovereign Identity(Zero knowledge proofs or tokens) + Consensus (Agreement or proof of Work)

Healthcare IAM. Authenticate
Healthcare. Blockchain.add_transaction

Create_ DID

Sign_with_private _key

Generate_Access_tokens

Generate Access tokens

```
# Pseudocode for Privacy-Preserving IAM with Blockchain and SSI in Healthcare

function authenticate_user(patient_id, patient_credentials):
    # IAM Process
    if HealthcareIAM.authenticate(patient_id, patient_credentials):
        # Privacy Measures
        encrypted_health_data = encrypt(patient_id, health_information)
        # Blockchain Transaction
        healthcare_blockchain.add_transaction(encrypted_health_data)
        # SSI
        patient_did = create_did(patient_id)
        patient_credentials_proof = sign_with_private_key(patient_did, patient_credentials)
        # Access Control
        access_token = generate_access_token(patient_did, healthcare_roles)
        return {
```

```
        "credentials_proof": patient_credentials_proof,
        "access_token": access_token
    }
else:
    return "Authentication Failed"
```

3. Privacy – Preserving Mechanisms:

4.1. **Decentralization and Elimination of Central Authorities:** Blockchain – based SSI systems distribute identity management across a decentralized network, reducing the reliance on a central authority. This minimizes the risk of unauthorized access and single point of failure.

4.2 **Verifiable Credentials**: Verifiable Credentials are digital proofs contain attributes. These credentials can be shared selectively without revealing the underlying data, ensuring and sensitive information remains private.

4.3 **Zero-Knowledge Proofs:** It enables the verification of claims without disclosing the actual data. This mechanism enhances privacy by allowing individuals to prove specific attributes.

4.4. **Data Minimization and Selective Disclosure:** It enforces the principle of least privilege, ensuring that only necessary information is shared for a specific transaction.

4.5 **Consent Management**: It enables users to provide explicit consent before their identity information is accessed or shared.

4.6. **Revocation and immutable Audit Trail:** It enhances the transparency and accountability in data management.

4.7. **Pseudonymity and Secure Key Management**: It practices further protect individuals' identities.

5. **Challenges and Consideration:**

5.1. Regulatory Compliance Adhering to Healthcare: Regulations such as HIPAA (Healthinsurance Portability and Accountability Act) is critical.

5.2. User Education and Adoption: User education plays a significant role in ensuring individuals understand how SSI works and how to manage their identities effectively.

5.3. Technological Considerations: Choosing the appropriate blockchain platform, consensus mechanism and cryptographic techniques is essential for building a robust and secure SSI system.

6**. Blockchain Platforms:**

6.1**. Ethereum:** A popular Blockchain Platform with Smart Contract capabilities widely used for self-sovereign identity and healthcare data sharing applications.

7.2. Hyperledger Indy: A permissioned blockchain platforms specifically designed for self -sovereign identity.

Architecture:

Our goal is to explore the potential of blockchain technology in managing self-sovereign identity, a topic of interest among researchers and academicians [25]. Our solution is considered suitable for public adoption due to its Self-Sovereign Identity, legally valid status, and acceptable performance [26]. In addition, the distributed design of SSI makes it difficult to ensure reliability and integrity [28]. The architecture of a healthcare application with self-sovereign identity and privacy-preserving mechanisms is designed to ensure that patients have control over their health data while maintaining privacy and security. Below is a high-level overview of the architecture:

1. **User Interface (UI):**
    - The UI is the front-end of the application, providing an interface for users to interact with the system. It includes user registration, login, and dashboard functionalities.
    - Users can manage their digital identity, verifiable credentials, and consent settings through the UI.
    - The UI facilitates data sharing requests and displays notifications related to data access and usage.
2. **Identity Management:**
    - The identity management component is responsible for handling user registration, authentication, and the creation of decentralized identifiers (DIDs) for each user.
    - Users create their digital identity, which is associated with a unique DID and cryptographic keys.
3. **Decentralized Identity (Self-Sovereign Identity):**
    - The decentralized identity component allows users to store their verifiable credentials (e.g., medical records, prescriptions) and selectively share them with trusted entities.
    - Verifiable credentials are issued by trusted issuers (e.g., healthcare providers) and can be cryptographically verified by relying parties (e.g., other healthcare providers, researchers).

4. **Privacy-Preserving Techniques**:
   - The privacy-preserving techniques layer incorporates the selected methods such as differential privacy, attribute-based access control, and zero-knowledge proofs to protect sensitive data.
   - Differential privacy adds noise to aggregated statistics to ensure individual data privacy during data analysis.
   - Zero-knowledge proofs allow users to prove certain statements about their data without revealing the actual data.
5. **Blockchain Infrastructure:**
   - The blockchain infrastructure provides a decentralized and immutable ledger for recording verifiable credentials, user consent, and data access logs.
   - Blockchain platforms like Ethereum or Hyperledger Indy are commonly used for their smart contract capabilities and data transparency.
6. **Data Storage and Encryption:**
   - Healthcare data, including electronic health records (EHRs), medical reports, and sensitive information, is stored in encrypted databases.
   - Data encryption techniques (e.g., AES, RSA) are used to protect data both at rest and during transmission.
7. **Access Control and Policy Engine:**
   - The access control component enforces access policies based on the user's consent and identity attributes.
   - Attribute-based access control (ABAC) is applied to determine which users or entities can access specific data attributes.

7. Results and Discussions

Challenges in healthcare applications with self-sovereign identity:

Privacy and security are of paramount importance in healthcare applications with self-sovereign identity. Here are some key reasons why they are crucial:

1. **Protecting Patient Confidentiality**: Healthcare applications deal with sensitive personal and medical information. Maintaining privacy ensures that patients' data is not exposed to unauthorized individuals, protecting their confidentiality, and preventing potential harm or discrimination.
2. **Preventing Medical Identity Theft and Fraud**: Robust security measures in healthcare applications with self-sovereign identity help prevent identity theft, ensuring that only authorized users can access and modify patient data. This protects patients from potentially fraudulent activities.
3. **Building Patient Trust**: Privacy and security are essential in building and maintaining patient trust. Patients are more likely to engage with healthcare systems that demonstrate a commitment to protecting their privacy and keeping their data secure.
4. **Avoiding Data Breaches:** Healthcare data breaches can have severe consequences, including financial losses, legal penalties, and damage to the organization's reputation. Robust security measures help prevent data breaches and protect patient information.
5. **Encouraging Data Accuracy**: Privacy and security measures can foster trust between patients and healthcare providers. Patients are more likely to provide accurate and comprehensive health information when they are confident in the protection of their data.
6. **Enabling Research and Innovation**: Protecting patient privacy is vital in healthcare research. Privacy-preserving techniques allow researchers to access anonymized data while respecting patients' privacy, fostering medical advancements and innovation.

Overall, sovereign identity addresses the challenges of data security, privacy, and interoperability, improving the quality of healthcare services and patient experiences**.**

Overall, adopting privacy-preserving techniques in healthcare applications with self-sovereign identity is essential for ensuring patient privacy, regulatory compliance, building trust, facilitating data sharing, enabling medical research, and protecting sensitive data from breaches and misuse. These techniques support the fundamental principles of self-sovereign identity and strengthen the healthcare ecosystem.

Research methods tools used for the practical implementation**.**The practical implementation of privacy-preserving techniques in healthcare applications with self-sovereign identity involves a combination of cryptographic methods, secure programming practices, and robust infrastructure. Below is an overview of the methods and tools commonly used for the practical implementation:

1. **Cryptographic Libraries:** Utilize cryptographic libraries and frameworks that provide ready-to use implementations of privacy-preserving techniques.

2. **Zero-Knowledge Proof (ZKP) Libraries**: For implementing ZKPs, employ specialized ZKP libraries like libsnark (C++), zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge), or zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge) These libraries simplify the generation and verification of ZKPs.

3. **Attribute-Based Encryption (ABE) Libraries:** ABE is useful for selective disclosure of data attributes. Consider using libraries like Charm-Crypto (Python) or jPBC (Java) that support various ABE schemes such as KP-ABE (Key-Policy ABE) or CP-ABE (Ciphertext-Policy ABE).

4. **Secure Multi-Party Computation (MPC) Frameworks:** If secure data aggregation is required, consider using MPC frameworks like Sharemind, Secure Multi-Party Computation Library (SMPC), or the SCALE-MAMBA library to perform computations across multiple parties without revealing individual data.

5. **Blockchain Platforms:** For self-sovereign identity implementations, consider blockchain platforms like Ethereum, Hyperledger Indy, or Sovrin. These platforms provide decentralized identity management and enable secure and auditable data storage.

6. **Secure Communication:** Use secure communication protocols like TLS/SSL to encrypt data during transit between different system components, ensuring that sensitive information is protected against eavesdropping and man-in-the-middle attacks.

7. **Data Encryption Techniques:** Apply encryption techniques like AES (Advanced Encryption Standard) or RSA (Rivest–Shamir–Adleman) to protect sensitive data stored in databases or transmitted between components.

8. **Testing and Debugging Tools:** Use testing frameworks like JUnit, pytest, or Mocha to test the privacy-preserving features and ensure correct implementation. Debugging tools like GDB and Wireshark can help identify and resolve issues during development.

By combining these methods and tools, a practical implementation of privacy-preserving techniques in healthcare applications with self-sovereign identity can be achieved, providing patients with greater control over their data while maintaining privacy and security.

Fig 2 REPRESENTATION OF BLOCKCHAIN IN HEALTH CAREAPPLICATIONS.

(i) **Understanding Privacy Requirements:**

Identify the specific privacy requirements and objectives of the application. Consider factors like data sensitivity, legal and regulatory constraints (e.g., HIPAA, GDPR), and user expectations regarding privacy.

(ii) Data Sensitivity Assessment:

. Determine the sensitivity of the data to be protected. Classify data into different categories based on their level of sensitivity, and assess the potential impact of a data breach.

(iii)Privacy-Preserving Goals:

Define the desired privacy-preserving goals for the application. These goals may include data minimization, selective disclosure, data aggregation with privacy guarantees, or secure data sharing.

(iv)Technique S**uitability Evaluation:**

Evaluate each privacy-preserving technique (e.g., zero-knowledge proofs, attribute-based access control, differential privacy) against the identified privacy requirements and goals.

8, Results and Future Scope

1. Data Protection and Patient Privacy: Healthcare data contains highly sensitive and personal information, including medical history, diagnoses, and treatment plans. Privacy-preserving techniques ensure that patient data remains confidential and is shielded from unauthorized access or misuse. By safeguarding patient privacy, individuals can trust that their sensitive health information is secure and used only for authorized purposes.

2. User-Centric Data Control: Self-sovereign identity empowers patients to manage their own digital identities and consent to data sharing. Privacy-preserving techniques align perfectly with this principle by allowing users to selectively disclose attributes and control the level of information shared with different entities. Patients retain full control over their data, promoting a user-centric approach to data management.

3. Ethical and Regulatory Compliance: Healthcare providers are subject to stringent data protection regulations, such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). Privacy-preserving techniques ensure compliance with these regulations by applying robust privacy measures and minimizing the risk of data breaches and unauthorized access.

4. Secure Data Sharing and Collaboration: In the healthcare ecosystem, data sharing and collaboration among healthcare providers, researchers, and patients are essential for improved outcomes. Privacy-preserving techniques enable secure data sharing while ensuring that individual patient information remains private. This promotes a collaborative environment for medical research and advances without compromising patient confidentiality.

5. Transparency and Accountability: Privacy-preserving techniques often come with auditability features, such as data access logs and traceability. Patients and regulatory bodies can verify that data access and sharing are compliant with established privacy policies and that data usage is transparent and accountable.

6. **Resilience to Data Breaches**: Privacy-preserving techniques introduce an additional layer of protection against data breaches. Even if a breach occurs, the data shared through these techniques is often anonymized or encrypted, reducing the risk of re-identification and potential harm to patients.

7. **Patient Trust and Adoption:** Privacy concerns are a significant barrier to adopting digital health solutions. By implementing robust privacy-preserving mechanisms, healthcare applications with self-sovereign identity can build patient trust and confidence in digital health technologies, leading to greater adoption and engagement.

8. **Future-Proofing Data Privacy**: As technology advances and new privacy threats emerge, privacy-preserving techniques offer a flexible and adaptive approach to data protection. By incorporating these techniques, healthcare applications can future-proof their privacy strategies and stay ahead of evolving privacy challenges.

   In conclusion, privacy-preserving techniques are crucial in healthcare applications with self-sovereign identity to protect patient data, empower individuals with data control, comply with regulations, facilitate secure collaboration, and build patient trust in digital health solutions. By integrating these techniques, healthcare systems can strike the right balance between privacy and data sharing, ensuring that patient privacy remains a top priority in the rapidly evolving landscape of healthcare technology.

   Researchers and practitioners can explore several avenues for further research and improvements in privacy-preserving techniques to enhance data protection, user control, and data utility.

9. CONCLUSION

This will pave the way for future development of publicly used blockchains which would be readily available to every individual of the society. This will also change the way current public system work, ie based on Full disclosure of information (Identification documents like id's, old health care records etc) will not be required for the individual to access these institutions / services

References

[1] K. Gilani *et al.*, "Self-sovereign identity management framework using smart contracts To cite this version : HAL Id : hal-03563470 Self-sovereign Identity Management Framework using Smart Contracts," *HAL Open Sci.*, 2022.

[2] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, "Privacy-Preserving Solutions for Blockchain: Review and Challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019, doi: 10.1109/ACCESS.2019.2950872.

[3] "Technical exploration Ledger-based Self Sovereign Identity," vol. 31, no. 0.

[4] P. J. Windley, "SELF-SOVEREIGN IDENTITY The Architecture of Personal Autonomy," no. March, 2022.

[5] R. Singh, A. Dhar, and R. Rao, "Privacy-preserving ledger for blockchain and Internet of," *Comput. Electr. Eng.*, vol. 103, no. August, p. 108290, 2022, doi: 10.1016/j.compeleceng.2022.108290.

[6] R. Singh, A. D. Dwivedi, R. R. Mukkamala, and W. S. Alnumay, "Privacy-preserving ledger for blockchain and Internet of Things-enabled cyber-physical systems," *Comput. Electr. Eng.*, vol. 103, no. July, p. 108290, 2022, doi: 10.1016/j.compeleceng.2022.108290.

[7] R. Singh, A. Dhar, and R. Rao, "Privacy-preserving ledger for blockchain and Internet of," *Comput. Electr. Eng.*, vol. 103, no. August, p. 108290, 2022, doi: 10.1016/j.compeleceng.2022.108290.

[8] N. Zapoglou, I. Patsakos, G. Drosatos, and K. Rantos, "Privacy-Preserving Blockchain-Based Solutions in the Internet of Things," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 372, no. December, pp. 386–405, 2021, doi: 10.1007/978-3-030-76063-2_27.

[9] R. Antwi et al., “A Survey on Network Optimization Techniques for Blockchain Systems,” Algorithms, vol. 15, no. 6, p. 193, 2022, doi: 10.3390/a15060193.

[10] J. Xi et al., “A Comprehensive Survey on Sharding in Blockchains,” Mob. Inf. Syst., vol. 2021, 2021, doi: 10.1155/2021/5483243.

[11] M. Monti and S. Rasmussen, “RAIN: A Bio-Inspired Communication and Data Storage Infrastructure,” *Artif. Life*, vol. 23, no. 4, pp. 552–557, 2017, doi: 10.1162/ARTL_a_00247.

[12] J. Kaneriya and H. Patel, “a Comparative Survey on Blockchain,” pp. 1150–1155, 2020.

[13] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, “Blockchain with Internet of Things: Benefits, challenges, and future directions,” *Int. J. Intell. Syst. Appl.*, vol. 10, no. 6, pp. 40–48, 2018, doi: 10.5815/ijisa.2018.06.05.

[14] C. V. Priscilla and T. Devasena, “Blockchain based Identity Management System - A Survey (1),” vol. 11, no. 5, pp. 29–36, 2021, doi: 10.9790/9622-1105052936.

[15] N. Fotiou, V. A. Siris, G. Xylomenos, and G. C. Polyzos, “IoT Group Membership Management Using Decentralized Identifiers and Verifiable Credentials,” *Futur. Internet*, vol. 14, no. 6, 2022, doi: 10.3390/fi14060173.

A. Giannopoulou and F. Wang, “Self-sovereign identity,” *Internet Policy Rev.*, vol. 10, no. 2, pp. 1–10, Apr. 2021, doi: 10.14763/2021.2.1550.

[16] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, and S. Guerreiro, “SSIBAC: Self-sovereign identity based access control,” *Proc. - 2020 IEEE 19th Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2020*, pp. 1935–1943, 2020, doi: 10.1109/TrustCom50675.2020.00264.

[17] D. Pöhn and W. Hommel, “Universal identity and access management framework for future ecosystems,” *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl.*, vol.12, no. 1, pp. 64–84, 2021, doi: 10.22667/JOWUA.2021.03.31.064.

[18] J. A. Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, and K. Dahal, “DNS-IdM: A blockchain identity management system to secure personal data sharing in a network,” *Appl. Sci.*, vol. 9, no. 15, 2019, doi: 10.3390/app9152953.

[19] C. V. Priscilla and T. Devasena, “Blockchain based Identity Management System - A Survey (1),” vol. 11, no. 5, pp. 29–36, 2021, doi: 10.9790/9622-1105052936.

[20] N. Fotiou, V. A. Siris, G. Xylomenos, and G. C. Polyzos, “IoT Group Membership Management Using Decentralized Identifiers and Verifiable Credentials,” *Futur. Internet*, vol. 14, no. 6, 2022, doi: 10.3390/fi14060173.

[21] M. Shuaib *et al.*, “Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison,” *Mob. Inf. Syst.*, vol. 2022, 2022, doi: 10.1155/2022/8930472.

[22] S. Agrawal, S. Banerjee, and S. Sharma, “Privacy and security of aadhaar: A computer science perspective,” *Econ. Polit. Wkly.*, vol. 52, no. 37, pp. 93–102, 2017.

[23] N. A. Samion, “Innovation of National Digital Identity: A Review,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 1.2, pp. 151–159, 2020, doi: 10.30534/ijatcse/2020/2391.22020.

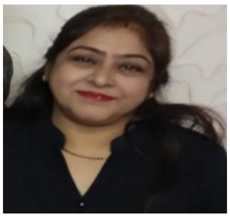
[24] J. Kaneriya and H. Patel, “a Comparative Survey on Blockchain,”

[25] Stokkink and J. Pouwelse, “Deployment of a Blockchain-Based Self-Sovereign Identity,” no. February, 2021, doi: 10.1109/Cybermati

[26] J. A. Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, and K. Dahal, “DNS-IdM: A blockchain identity management system to secure personal data sharing in a network,” *Appl. Sci.*, vol. 9, no. 15, 2019, doi: 10.3390/app9152953.

[27] M. Tabor, “Self Sovereign ,” *Leg. Tech*, no. November 2021, doi: 10.5771/922834-407.

Authors



- Ms.Monica Chawla. BSc, A-level (Doeacc), MBA(IT),M.Phil., MTech, Pursuing Ph.D. in computer science from MVN university, Palwal. Published 6 research paper in papers and 1 book on computer applications in management for MBA1st semester. She is working as a Designation of an Assistant Professor having 20 years of experience in MCA Department in Institute of Management, Faridabad.

Dr. Alok Srivastava received a Ph.D. degree in on topic Design & Analysis of Efficient Co-Operative Communication System from MVN university Palwal in 2021. He has Design patent published for “SOIL TESTING DEVICE INTEGRATED WITH IOT UNIT” Design No 388628-001 Date 19/06/2023 Application Number: 388628-001 Filing Date: 5/19/2023. Also Design patent published for “OT BASED AIR QUALITY SENSING DEVICE” Design No 388351- 001 Date 14/06/2023 . Design patent published for “PORTABLE SMART EXTERNAL HARD DISK DRIVE” Application no 368860-001 cbr date 05/08/2022. Design patent published for “AN APPARATUS FOR SECURE AND CONSISTENT PATH SELECTION IN WIRELESS COOPERATIVE COMMUNICATION AND IMPROVED METHOD THEREOF” Application no 202211015718 Date 06/05/2022. Germany Utility Patent Granted for the invention of “INTELLIGENT SYSTEM FOR DETECTING EDITED IMAGES USING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING” on 25th April 2022. He has also published and been granted different patents in India, Australia & Germany. He has published more than 10 papers in scoopers journal.