International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

# DESIGN ASPECTS OF DECENTRALIZED IDENTIFIERS AND SELF-SOVEREIGN IDENTITY SYSTEMS

**NAVEEN REDDY NEMILI [1], KASARLA VIKAS [2], MUTTHAVARAPU VENKATA SAI ABHINAV [3], MODALA RAKESH [4]**

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

**ABSTRACT—** The increased digitalization of society raises concerns regarding data protection and user privacy, and criticism on how the companies handle user data without being transparent and without providing adequate mechanisms for users to control how their own data is being processed or shared. To address this problem and open the way for a secure and efficient society, where the privacy of citizens is paramount, the identity concept and proof of identity mechanisms need to be redesigned from the ground up. In this paper we discuss how the emerging Web3 technologies like distributed ledger technology (DLT), blockchain, smart contracts, decentralized storage systems, and crypto wallets can be leveraged to design and implement a decentralized digital identity system based on decentralized identifiers (DID) and self-sovereign identities (SSI). Such a system puts the users in full control over their own data while also providing a solid backbone for building interoperable systems that are secure, scalable, and efficient.

We propose different architectures for the decentralized identity infrastructure and storage layer, and also discuss the mapping of these architectures on cloud platforms. The main goal is to provide an architectural blueprint for a scalable, secure, privacy-preserving and trusted system.

*Index Terms* – Decentralized digital identity, Self-Sovereign Identity (SSI), Decentralized Identifiers (DID), Web3, blockchain, distributed ledger technology (DLT), smart contracts, decentralized storage, crypto

wallets, identity management, privacy preservation, cloud computing, interoperable identity systems.

## I. INTRODUCTION

In recent years, we are witnessing an accelerated rate of digitalization in our societies. This transformation, although it can lead to efficient societies, must be performed with great care. As more and more users get involved with online digital processes, data protection becomes extremely important. Personal data-related activities like collection, processing, storage and legal conformance pose big challenges to companies. Advancing digitalization in all fields, ranging from mobility, administration, health and financial services to entire smart cities is not possible without a well-defined digital identity for the entities that access the system (e.g., citizens, authorities, universities, public and private companies). The digital identity represents its users when interacting with digital services. Following this interaction, the service providers can acquire great amounts of personal data from users. In some countries, the management of personal data is governed by legislation (e.g., in Europe, General Data Protection Regulation (GDPR) ). Moreover, the amount of collected data increases with the level of service customization. This data is stored in data silos (on company premises, data centers, cloud etc.). However, the details regarding data storage and security measures taken to secure the data remain opaque to the end users. Most online systems rely on centralized or federated identity management systems.

## II. RELATED WORK

### *A. Why Are Companies Failing At Data Protection?*

With the rapid growth of digital technologies and online services, organizations are collecting and storing huge amounts of sensitive user data. However, many companies still fail to provide proper data protection due to weak security practices, lack of transparency, poor access control mechanisms, and inadequate privacy management. This article discusses the major reasons behind failures in protecting user information and highlights the increasing risks of data breaches, cyberattacks, identity theft, and unauthorized data sharing.

### *B. Rising To the Challenge of Modern Data Security and Growing Privacy Regulations*

With the rapid growth of digital services and online platforms, organizations are facing major challenges in protecting sensitive user information and complying with modern privacy regulations. In this article, the importance of strong data security practices and privacy-preserving technologies is discussed in detail. The study explains how increasing cyber threats, unauthorized data sharing, and lack of user control over personal information have created serious security concerns across industries. It highlights the need for secure identity management systems that can provide transparency, trust, and better control of digital data. The article also emphasizes the role of modern technologies such as encryption, decentralized systems, and secure authentication mechanisms in improving privacy protection.

### *C. Study: Companies Neglect Client Data Security*

With the increasing dependence on digital platforms and online services, protecting client information has become a major concern for organizations worldwide. In this study, the authors discuss how many companies fail to properly secure sensitive customer data, leading to frequent data breaches and privacy risks. The paper highlights that weak password management, poor security practices, and lack of transparency are some of the primary reasons behind the growing number of cyberattacks. It explains that users often have limited control over how their personal information is stored, accessed, and shared by organizations. The study also emphasizes the importance of implementing strong encryption techniques, secure authentication systems, and privacy-focused technologies to safeguard user data.

### *D. 64 Alarming Data Privacy Statistics Businesses Must See in 2024*

As digital transformation continues to expand across industries, concerns regarding data privacy and cybersecurity are increasing significantly. In this article, the author presents various statistical insights related to data breaches, privacy violations, and the growing risks associated with improper handling of user information. The study highlights that many businesses collect large amounts of personal data without implementing adequate security measures, which increases the possibility of cyberattacks and unauthorized access.

It explains how users are becoming more aware of privacy issues and are demanding greater transparency and control over their digital identities and personal information.

The article also discusses the financial and reputational damage organizations may face due to weak data protection practices and non-compliance with privacy regulations.

## III. PROPOSED METHODOLOGY

The proposed system introduces a secure and decentralized digital identity management platform using Blockchain Technology, Decentralized Identifiers (DIDs), and Self-Sovereign Identity (SSI) concepts. The system utilizes emerging Web3 technologies such as distributed ledger technology (DLT), blockchain, smart contracts, decentralized storage, and cryptographic mechanisms to provide secure identity and credential management. Unlike traditional centralized systems, the proposed system gives users complete control over their personal data and digital credentials. The system allows holders to request credentials from authorized issuers, while credential details are securely encrypted before storage. Issuers can verify and approve credential requests, and verifiers can validate the authenticity, expiry status, and revocation status of credentials through blockchain-based verification. Blockchain technology provides immutable, tamper-proof, and traceable storage of credential transactions, ensuring transparency, trust, and accountability. The proposed architecture supports secure credential sharing, decentralized verification, PDF based credential downloads, and trusted digital identity management. The system is designed to provide a scalable, privacy-preserving, secure, and efficient decentralized identity ecosystem.

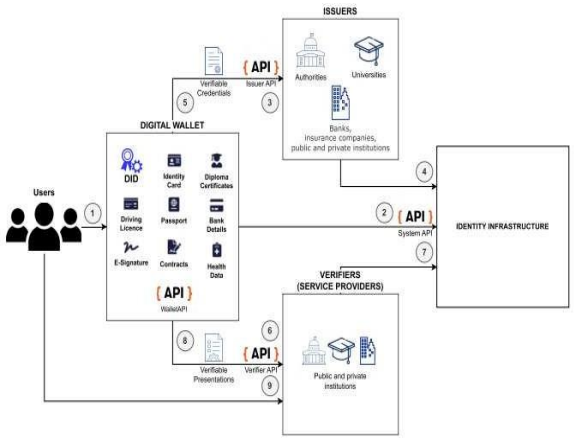


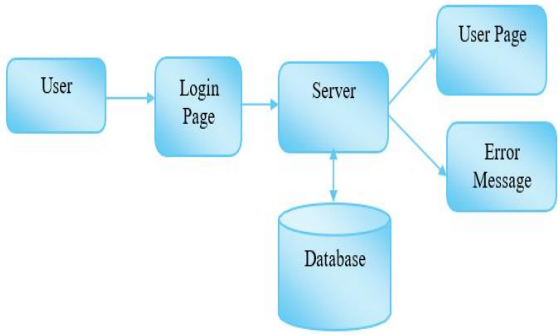

Fig. 1: System Overview

### 1. User Interface Design

Users must log in using username and password to access the system. New users can register by entering basic details like username, email, and role. After login, holders can view their DID, wallet details, and issued credentials.

Users can request credentials such as Passport, Driving License, and Degree from authorized issuers. The entered details are encrypted before storing in the database. Issuers verify and approve the requests, and the credential data is stored securely in the

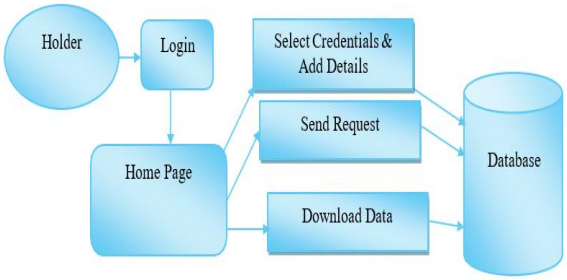
blockchain ledger. Holders can also download credentials in PDF or QR format and check credential validity. The interface is simple, secure, and easy to use.




## 2. Holder Module

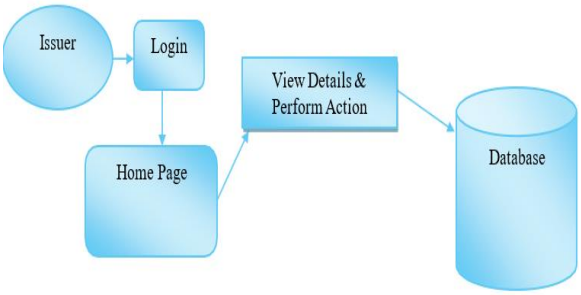
The Holder module allows users to securely manage their digital identity credentials using the SSI wallet system. Users first register and log in using their username and password. After successful login, the holder dashboard displays personal DID (Decentralized Identifier), wallet details, and issued credentials.

The holder can request credentials such as Passport, Driving License, Bachelor Degree, and Bank Statement from authorized issuers. Before sending the request, the holder enters details like name, ID number, and expiry information. These details are encrypted for security before being stored in the database. The holder can also view blockchain transaction details, credential status, expiry date, and download credentials in PDF. This module provides a simple and secure interface for users to control and manage their digital identity credentials safely.




## 3. Issuer Module

The Issuer module is responsible for verifying and issuing digital credentials to holders. Authorized issuers log in to the system and access the issuer dashboard. The dashboard displays all pending credential requests sent by holders. The issuer can decrypt and preview holder details such as candidate name, ID number, and expiry date before approval. After verification, the issuer approves the request, and the credential information is securely stored in the blockchain ledger with a unique transaction hash. The issuer can also revoke credentials if required. This module ensures that only trusted organizations can issue valid credentials securely and transparently.




### 4. Verifier Module

The Verifier module is used to validate whether a credential is genuine, active, expired, or revoked. The verifier enters the transaction hash, or credential details to check its authenticity. The system verifies the credential information from the blockchain ledger without exposing sensitive holder.

### 5. JSP Dashboard

This module provides the front-end interface of the system using JSP pages. It allows holders, issuers, and verifiers to interact with the decentralized identity platform through attractive web pages.

The dashboard displays wallet information, credential requests, blockchain transactions, approval status, verification results, and downloadable credentials. It acts as the communication layer between users and the backend system.

### 6. MySQL Database

This module stores all project-related data such as user details, DID information, credential requests, encrypted holder data, blockchain transaction records, issued credentials, and verification history. It ensures proper data management, secure storage, and quick retrieval of information whenever required by the system modules.

## IV. EXPERIMENTAL RESULTS AND ANALYSIS

The analysis shows that the proposed decentralized identity architecture effectively enables user-controlled identity management using Decentralized Identifiers (DIDs) and Self-Sovereign Identity (SSI). The integration of blockchain, smart contracts, decentralized storage, and crypto wallets enhances privacy, security, interoperability, and scalability. The proposed cloud-based architecture demonstrates the feasibility of deploying trusted and efficient decentralized identity systems. Overall, the framework provides a robust foundation for secure and privacy-preserving digital identity management in Web3 environments.

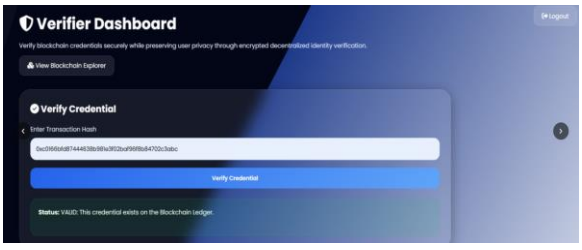



Fig. 2: Verify Credential

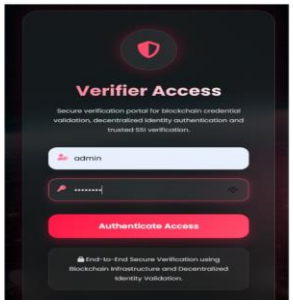



Fig. 3: Login

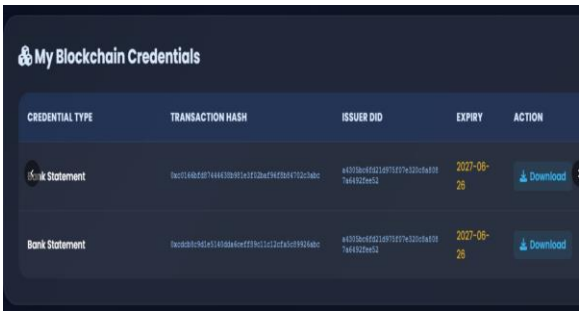



Fig. 4: Block Chain Credentials

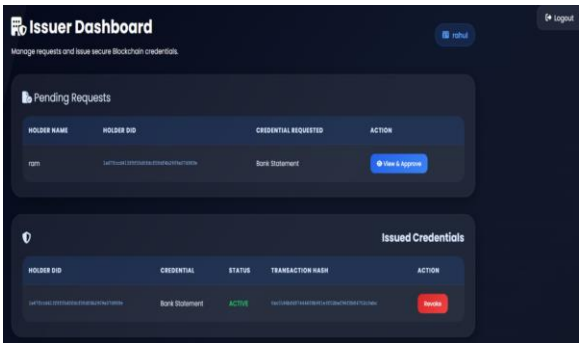



Fig. 5: Pending Request

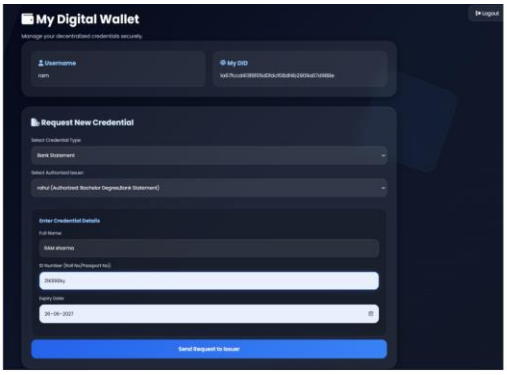



Fig. 6: Digital Wallet




Fig. 6: Certificate of Bank Statement

## V. CONCLUSION

This project presents a secure and decentralized digital identity management system using Blockchain, Decentralized Identifiers (DID), and Self-Sovereign Identity (SSI) technologies. The proposed system improves privacy, security, and transparency by giving users full control over their personal credentials. Holders can securely request credentials such as Passport, Driving License, Bachelor Degree, and Bank Statement from authorized issuers through a digital wallet. The credential details are encrypted before storage to protect sensitive information from unauthorized access. Issuers verify and approve the requests, and the approved credentials are securely stored in the blockchain ledger with transaction details. The blockchain provides immutability, tamper-proof storage, traceability, and reliable credential verification. The system also supports credential preview, expiry management, PDF

download, and QR-based verification for better usability and demonstration. Verifiers can easily check whether a credential is valid, revoked, or expired without exposing private user data. Compared to traditional centralized identity systems, the proposed approach provides better trust, security, and user privacy. Overall, the project offers a secure, efficient, and practical framework for modern decentralized digital identity management applications.

## REFERENCES

[1]General Data Protection Regulation (GDPR) Compliance Guidelines. GDPR.eu. Accessed: Dec. 7, 2023. [Online]. Available: https://gdpr.eu/

[2]A.AlexandrescuandG.Butnaru,‘‘Anarchit ectureofidentity management and thirdparty integration for online teaching in a university,’’ in Proc. 24th Int. Conf. Syst. Theory, Control Comput. (ICSTCC), Sinaia, Romania, Oct. 2020, pp. 850–855, doim10.1109/ICSTCC50638.2020.92596 52.

[3]N. Perlroth. (Oct. 2017). All 3 Billion Yahoo Accounts Were Affected By 2013 Attack. The New York Times. Accessed: Dec. 7, 2023. [Online]. Available: https://www.nytimes.com/2017/10/03/tec hnology/yahoo-hack 3-billion-users.html

[4]885 Million Records Exposed Online: Bank Transactions, Social Security Numbers, and More. Gizmodo. Accessed: Dec. 7, 2023. [Online]. Available: https://gizmodo.com/885-million- sensitive-records leaked-online-bank- trans-1835016235

[5](2022). Roth, E. Meta Fined $276 Million Over Facebook Data Leak Involving More Than 533 Million Users. The Verge. Accessed: Dec. 7, 2023. [Online]. Available: https://www.theverge. com/ 2022/11/28/23481786/met fine-facebook- data-leak-ireland-dpc gdpr

[6](2022). Meta Settles Cambridge Analytica Scandal Case for $725m. BBC News. Accessed: Dec. 7, 2023. [Online]. Available: https://www.bbc. com/news/technology-64075067

[7]Hackers Leak LinkedIn 700 Million Data Scrape. Accessed: Dec. 7, 2023. [Online]. Available:https://therecord.media/hackers -leak-linkedin-700 million-data-scrape

[8]J. S.-G. Perlroth. (2014). Matthew Goldstein and Nicole. JPMorgan Chase Hacking Affects 76 Million Households. DealBook. Accessed: Dec. 7, 2023.

[Online]. Available: https://dealbook. nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security issues/

[9]N. Lomas. (2020). U.K. Watchdog Reduces Marriott Data Breach Fine To $23.8M, Down From $123M. TechCrunch. Accessed: Dec. 7, 2023. [Online]. Available: https://techcrunch .com/2020/10/30/uk-watchdog reduces-marriott-data-breach-fine-to-23-8m-down-from-123m/

[10] (Oct. 30, 2013). Adobe Hack: At Least 38 Million Accounts Breached. BBC News. Accessed: Dec. 7, 2023. [Online]. Available: https://www.bbc.com/news/technology-24740873.

[11] Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219

[12] Kolla, S. H., Nagabhyru, K. C., & Kummari, D. N. (2026). Letter to the Editor re:"CurvAssist: An AI assisted pipeline for penile shaft segmentation/curvature measurement in children with hypospadias". Journal of Pediatric Urology.

[13] Kandula, S. T. R., Boyapati, P. K., & Susarla, R. S. (2025, April). Optimized Cloud Resource Management Using Deep Dendritic Artificial Neural Networks Integrated with Kubernetes and Terraform. In International Conference on Computer Vision and Robotics (pp. 454-465). Cham: Springer Nature Switzerland.

[14] Shashank A. (2025). Metadata-driven data integration framework: Automating enterprise data integration through declarative approaches. European Modern Studies Journal, 9(4), 9.

**AUTHORS Profile**



**Dr. NAVEEN REDDY NEMILI** has received his MCA from Osmania University, Hyderabad in 2010, M.Tech degree in Computer science from JNTUH, Hyderabad in 2014 and Ph.D degree awarded in Computer Science from SSSUTMS, Madhyapradesh in 2024 He is dedicated to teaching field from the last 12 years. His research area Cloud Computing. At present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



**Mr. KASARLA VIKAS** pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



**Mr. MUTTHAVARAPU VENKATA SAI ABHINAV** pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



**Mr. MODALA RAKESH** pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.