IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

Decentralized Digital ID Using Blockchain and IPFS

Mrs. Muthu Meenatchi. I[1], Vignesh Babu T D[2], Viswajith K G[3]
Assistant Professor, Dept. of Information Technology[1]
Students, Dept. of Information Technology[2,3]
K. L. N. College of Engineering, Sivaganga, India
meenatchiram28@gmail.com,vicky.it082@gmail.com,jithviswa10@gmail.com

Abstract: *Digital identity management is essential in modern digital systems, but traditional centralized approaches are vulnerable to data breaches, identity theft, and unauthorized access. This project presents a Decentralized Digital Identity System using Blockchain and IPFS to provide a secure, transparent, and user-controlled solution. The system enables users to create and manage digital identities, store documents on IPFS in a distributed manner, and maintain immutable verification records on blockchain. Smart contracts are used for secure authentication and controlled data sharing without relying on a central authority. A web-based interface allows users to access their identity wallet and perform verification efficiently. The proposed system enhances privacy, reduces fraud, and ensures data integrity, making it a scalable and reliable solution for modern digital identity management.*

Keywords: *Decentralized Identity, Blockchain, IPFS, Digital Identity Management, Data Security, Smart Contracts, Identity Verification, Distributed Systems*

I. INTRODUCTION

In today's digital era, identity management is a fundamental requirement for accessing online services such as banking, healthcare, and government platforms. Traditional identity systems rely on centralized databases, which are vulnerable to data breaches, identity theft, and unauthorized access, limiting user control over personal information. To address these challenges, this project proposes a Decentralized Digital Identity System using Blockchain and IPFS, where blockchain ensures secure and tamper-proof identity records, and IPFS provides distributed storage of user data. The system enables users to create, manage, and share their digital identities securely through a web-based interface, enhancing privacy, reducing dependency on centralized authorities, and improving trust and efficiency in digital identity verification.

II. RELATED WORK

Several approaches have been proposed for secure digital identity management. Traditional identity systems rely on centralized databases, which are efficient but vulnerable to data breaches and unauthorized access. Recent research has focused on blockchain-based identity management systems that provide immutability and transparency, reducing the risk of data tampering. Self-Sovereign Identity (SSI) models have also been introduced, allowing users to have full control over their personal data without relying on central authorities.

Additionally, IPFS-based storage solutions have been explored for decentralized data storage, improving data availability and security. Some studies have integrated smart contracts for automated identity verification and access control, enhancing system efficiency. However, many existing solutions face challenges such as scalability, interoperability, and adoption. This project aims to address these limitations by combining blockchain and IPFS to provide a secure, scalable, and user-centric digital identity management system.

DOI: 10.48175/IJARSCT-33431

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

III. METHODOLOGY

A. User Registration and Data Collection

The system begins with a secure user registration process, where individuals provide essential personal details such as name, contact information, and identification data. Users are also required to upload identity-related documents, which are necessary for verification purposes. The data is collected through a user-friendly web interface that ensures ease of use and accessibility. Validation mechanisms are applied to check for missing or incorrect inputs, ensuring that only accurate and complete data is processed. This step forms the foundation for generating a reliable and unique digital identity for each user.

B. Data Processing and Storage

Once the data is collected, it undergoes processing to ensure proper formatting and security. The system utilizes IPFS (Inter Planetary File System) for decentralized storage of user documents. Each file uploaded by the user is converted into a unique cryptographic hash, which acts as a secure reference to access the data. This content-addressable storage mechanism ensures data integrity, as even a small change in the file results in a different hash. By storing data in a distributed network, the system improves availability, reduces redundancy, and eliminates the risks associated with centralized data storage.

C. Blockchain Integration

The integration of blockchain technology plays a crucial role in ensuring data security and transparency. The unique hash generated by IPFS is stored on the blockchain along with identity-related metadata such as timestamps and verification status. Blockchain's immutable nature ensures that once data is recorded, it cannot be altered or deleted, providing a tamper-proof record of identity information. This enables secure tracking of all identity-related transactions and builds trust among users and service providers by maintaining a transparent verification process.

D. Authentication and Smart Contracts

The system implements smart contracts to automate authentication and authorization processes. These contracts act as self-executing programs that verify identity data and enforce access control rules without human intervention. When a user requests verification or shares data, the smart contract validates the request and grants access only to authorized entities. This mechanism ensures secure and efficient identity verification while maintaining user privacy. Additionally, encryption techniques are used to protect sensitive information during transmission and access.

E. Identity Wallet and Access Management

The system provides an identity wallet that serves as a central interface for users to manage their digital identities. Through this wallet, users can view their stored credentials, monitor verification status, and control how their data is shared with third parties. The wallet also allows users to grant or revoke access permissions at any time, ensuring complete control over personal information. This feature enhances user experience, improves accessibility, and supports secure and efficient identity management in a decentralized environment.

IV. SYSTEM ARCHITECTURE

The proposed Decentralized Digital Identity System follows a multi-layered architecture designed to ensure secure, scalable, and efficient identity management using blockchain and IPFS technologies. The architecture consists of a presentation layer, application layer, blockchain layer, and data layer, each performing specific functions to support the overall system. The presentation layer provides a user-friendly web interface through which users can register, upload documents, create digital identities, and access their identity wallet. The application layer acts as the core processing unit, handling business logic, user authentication, data validation, and communication between different components of the system. It manages the interaction with IPFS for storing user documents and with the blockchain network for

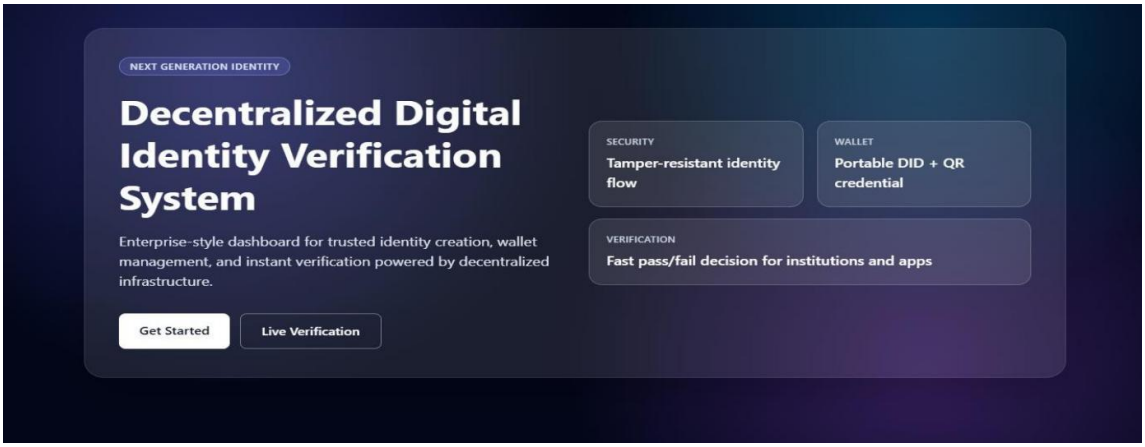
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2

recording identity verification details. The blockchain layer ensures immutability, transparency, and security by storing the hash values of user data along with verification records, preventing unauthorized modifications. The data layer utilizes IPFS for decentralized storage, where user files are stored in a distributed manner and accessed using unique cryptographic hashes. Communication between these layers is achieved through secure protocols, ensuring data privacy and integrity throughout the system. This architecture eliminates reliance on centralized systems, enhances data security, and provides a reliable framework for decentralized digital identity management.

V. RESULTS AND DISCUSSION

A. Home Page

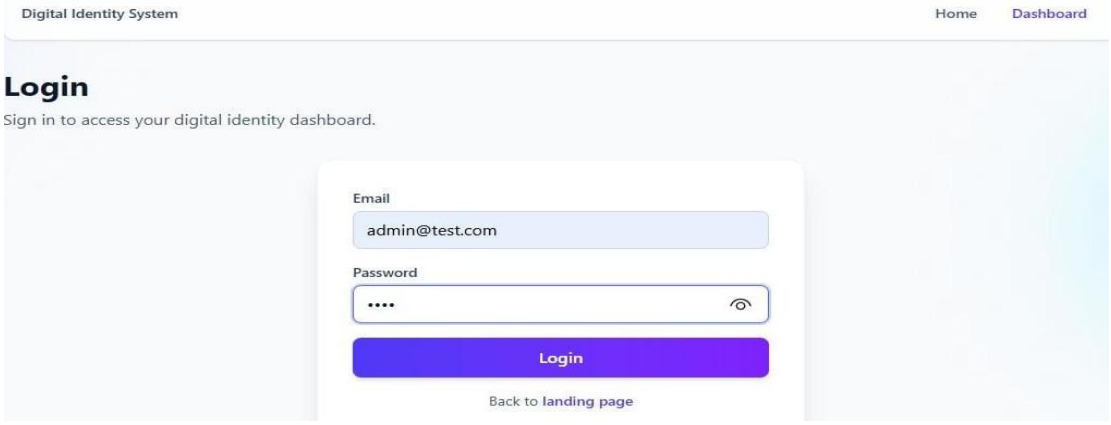
The landing page of the Decentralized Digital Identity Verification System presents a modern and user-friendly interface that highlights the core features of the platform, including secure identity creation, identity wallet management, and real-time verification. It provides a clear overview of the system with sections showcasing tamper-resistant identity flow, portable digital identity (DID) with QR credentials, and fast verification capabilities for institutions. The page includes interactive options such as "Get Started" for new users to create their digital identity and "Live Verification" for instant authentication. Designed with a clean and responsive layout, the landing page ensures easy navigation and effectively communicates the purpose and benefits of the decentralized identity system.



B. Login Page

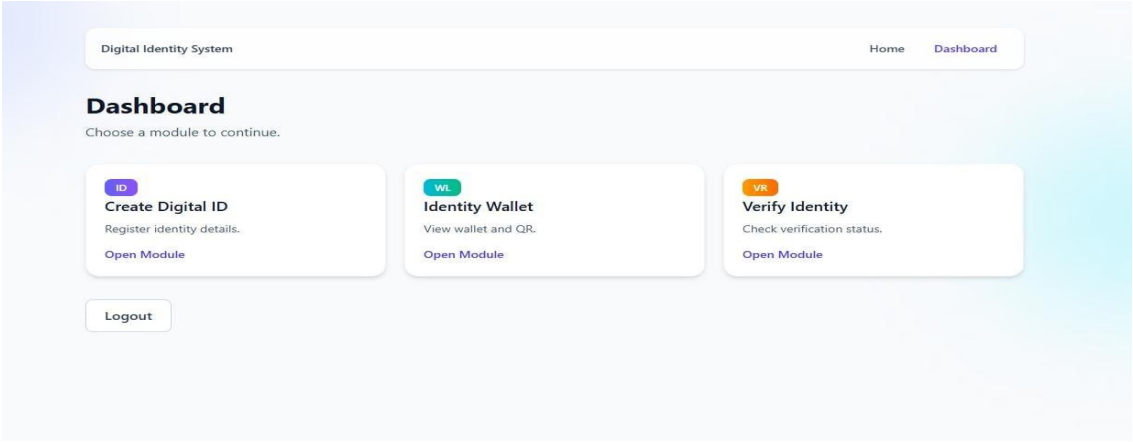
The Login Page of the Decentralized Digital Identity System provides a secure and simple interface for users to access their identity dashboard. It includes input fields for email and password, along with validation features to ensure correct credentials. The page is designed with a clean and responsive layout, allowing users to easily sign in and navigate the system. It also includes options such as password visibility toggle and a link to return to the landing page, enhancing usability and accessibility. This page ensures secure authentication and acts as a gateway for users to manage their digital identities.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2



C. Dashboard Page

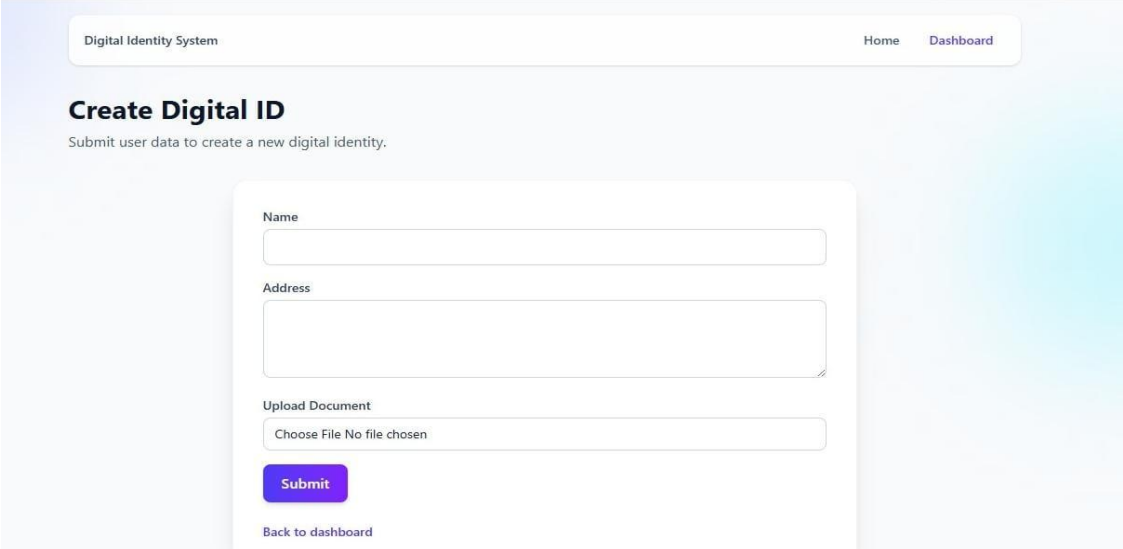
The Dashboard Page of the Decentralized Digital Identity System acts as the central hub where users can access different modules of the application. It provides options such as creating a digital ID, accessing the identity wallet, and verifying identity, all in a structured and user-friendly layout. Each module is clearly displayed with navigation links, allowing users to quickly choose and perform required actions. The page also includes a logout option and ensures smooth navigation across the system, improving overall usability and efficiency.



D. Create Digital ID

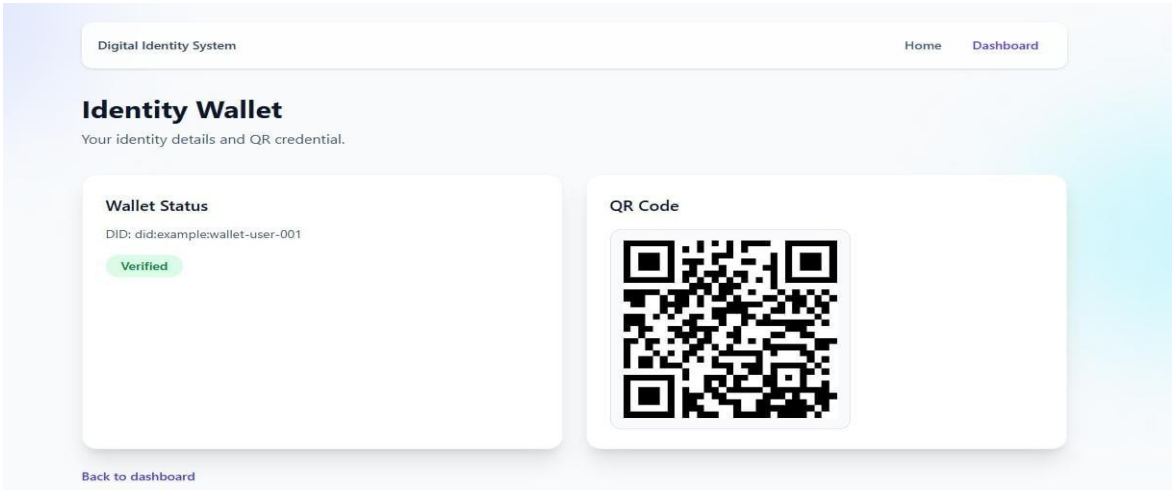
The Create Digital ID Page allows users to register their personal information and upload necessary documents to generate a digital identity. It includes input fields for user details such as name and address, along with a file upload option for documents. The page ensures proper data validation before submission and provides a simple interface for users to complete the process. This page plays a key role in initiating the identity creation process securely within the system.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2



E. Identity Page

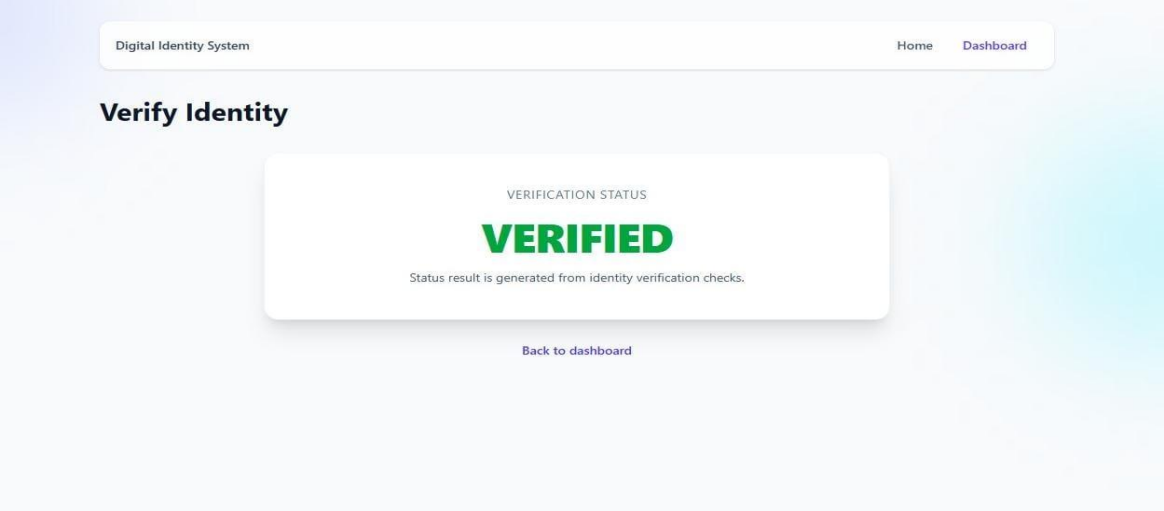
The Identity Wallet Page provides users with a secure view of their digital identity details and credentials. It displays information such as the Decentralized Identifier (DID), verification status, and a QR code that can be used for quick identity sharing and verification. The page is designed to give users full control over their identity data, allowing them to access and present their credentials easily while maintaining privacy and security.



F. Verification Page

The Verify Identity Page enables users or institutions to check the authenticity of a digital identity. It displays the verification result clearly, indicating whether the identity is verified or not. The page ensures a quick and reliable verification process by using blockchain-based validation, providing trust and transparency. Its simple design allows users to understand the verification status instantly, making it efficient for real-time identity checks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, April 2026
Impact Factor: 8.2



VI. CONCLUSION

The Decentralized Digital Identity System using Blockchain and IPFS provides a secure, transparent, and user-centric solution for managing digital identities in modern digital environments. By replacing traditional centralized systems, the proposed approach ensures enhanced data security, privacy, and integrity through the use of blockchain for immutable record keeping and IPFS for decentralized data storage. The system enables users to create digital identities, store documents securely, and manage credentials through an identity wallet, while also supporting fast and reliable identity verification. Features such as smart contract-based authentication and controlled data sharing reduce the risk of fraud and unauthorized access. The implementation of a user-friendly web interface further improves accessibility and usability across different platforms. Overall, the system demonstrates improved efficiency, reduced dependency on intermediaries, and strong potential for real-world applications in sectors such as banking, healthcare, and government services, making it a scalable and effective solution for decentralized digital identity management.

ACKNOWLEDGMENT

The authors would like to thank Mrs.I.Muthu Meenatchi,M.E.,(CSE) , K.L.N. College of Engineering, for her continuous guidance, valuable suggestions, and support throughout the development of this project. Her expertise and encouragement played a significant role in the successful completion of this work.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[2] J. Benet, “IPFS - Content Addressed, Versioned, P2P File System,” arXiv:1407.3561, 2014.
[3] M. Sporny, D. Longley, and D. Chadwick, “Verifiable Credentials Data Model 1.0,” W3C Recommendation, 2019.
[4] C. Allen, “The Path to Self-Sovereign Identity,” 2016.
[5] A. M. Antonopoulos, Mastering Bitcoin, O’Reilly Media, 2017.
[6] Ethereum Foundation, “Ethereum Whitepaper,” 2014.
[7] NIST, “Digital Identity Guidelines,” National Institute of Standards and Technology, 2017.
[8] Sovrin Foundation, “Self-Sovereign Identity and Decentralized Trust,” 2018.
[9] Hyperledger Fabric Documentation, Hyperledger Foundation, 2021.
[10] K. Cameron, “The Laws of Identity,” Microsoft Corporation, 2005.