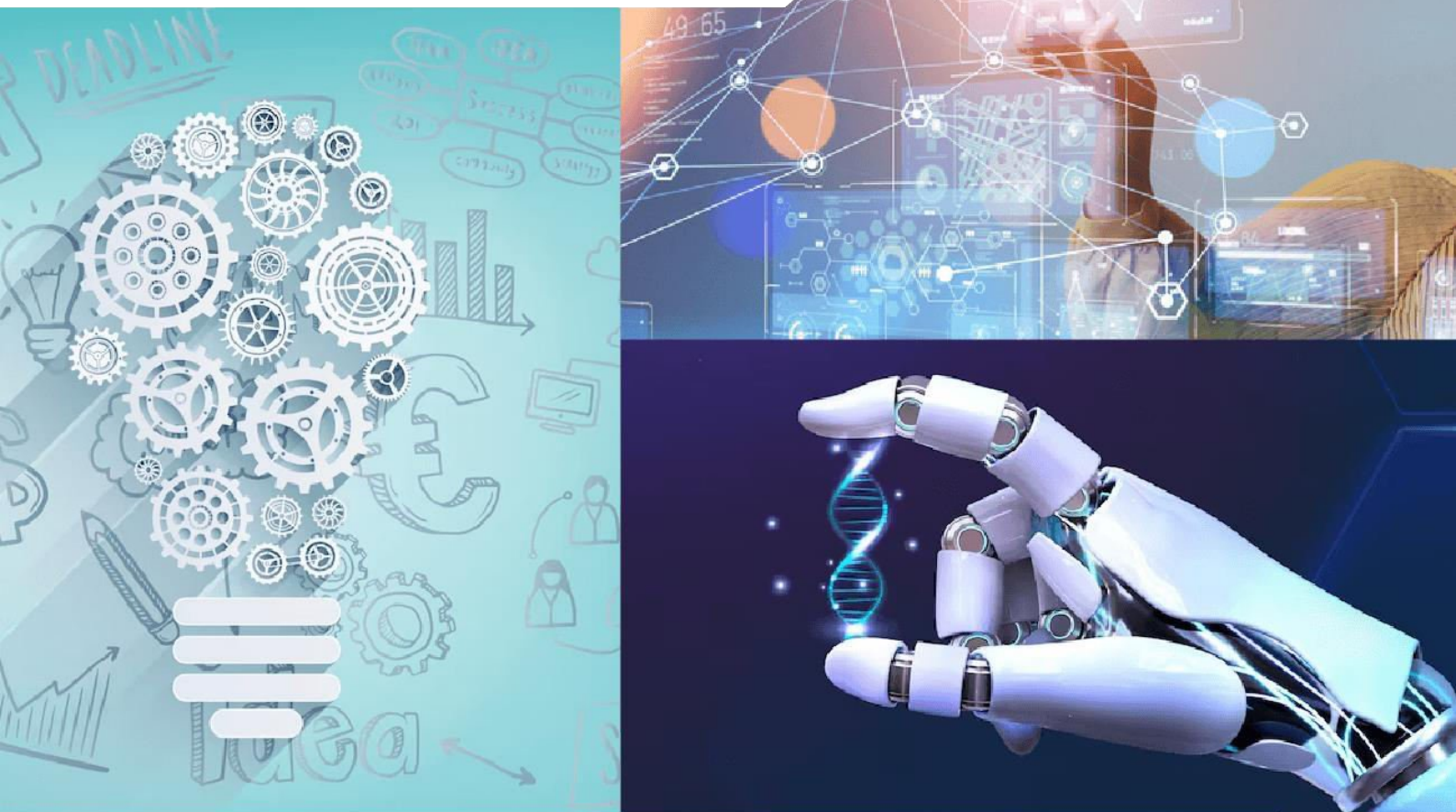




International Journal of Advanced Research in Education and Technology (IJARETY)

Volume 13, Issue 2, March - April 2026

Impact Factor: 8.152



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



An Open-Source Web Application Data Management

Shaikh Mohamad¹, Pamula Nithin Kumar², Pathi Raghav Reddy³, Sougani Manichandh⁴

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India¹

Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India^{2, 3, 4}

ABSTRACT: Managing posthumous digital data is increasingly challenging, and existing solutions lack transparency, flexibility, and proper access control. This paper presents “Beyond Life,” a cross-platform digital will management system for secure handling of digital assets after death. The system is built on a customized PD-CP-ABE encryption scheme, enabling fine-grained and scalable access control. It ensures user control, transparency, and independence from service providers. Additionally, the solution is portable, allowing users to switch platforms while maintaining secure data management.

KEYWORDS: Digital Will Management, Posthumous Data Security, Attribute-Based Encryption (CP-ABE), PD-CP-ABE, Access Control, Data Privacy, Cross-Platform Systems

I. INTRODUCTION

In today’s digital era, individuals generate and store a vast amount of personal data across various online platforms. However, managing these digital assets after a person’s death remains a major challenge due to lack of proper systems and security mechanisms. Existing solutions are often centralized, closed source, and provide limited control over data access and distribution. To address these issues, this project introduces “**Beyond Life**,” a secure and open-source digital will management system. The system uses advanced encryption techniques like PD-CP-ABE to ensure fine-grained access control over digital assets. It also supports decentralization and portability, giving users full control over their data. This project aims to provide a transparent, secure, and scalable solution for posthumous data management.

II. LITERATURE SURVEY

Reeves,A.,Shaghghi,A.,Krebs,S.,&Ashenden,D. (2025) This study explores how digital data becomes a legacy after death and highlights the lack of clear policies for managing posthumous data. It shows that users prefer trusted individuals or independent systems over social media platforms due to privacy concerns. The research emphasizes the need for transparent and user-controlled solutions. It suggests developing third-party systems that enable secure preservation and distribution of digital assets.

Doyle,D.T.,&Brubaker,J.R. (2025) This paper presents a comprehensive review of digital legacy research and identifies key stages in the lifecycle of digital data after death. It highlights gaps in current systems, particularly in handling multi-user access and long-term data management. The study emphasizes the importance of designing systems that support secure sharing and preservation of digital assets. It provides a foundation for developing more effective and user-centric digital legacy solutions.

Allegri,M.R. (2025) This article examines the challenges of enforcing data privacy laws, particularly the “right to be forgotten,” in a global digital environment. It discusses conflicts between different legal systems and the difficulty of applying consistent data protection policies across borders. The study highlights the importance of strong privacy frameworks to protect sensitive information. It emphasizes the need for balanced solutions to ensure secure and ethical data management.

Bethencourt,J.,Sahai,A.,&Waters,B. (2025) This paper introduces Ciphertext-Policy Attribute-Based Encryption (CP-ABE), a method for enforcing fine-grained access control on encrypted data. It allows data owners to define access policies based on user attributes, ensuring only authorized users can decrypt information. The approach improves security even in untrusted storage environments and prevents unauthorized access. This concept forms the foundation for advanced secure data-sharing systems like digital will management.

III. EXISTING SYSTEM

The storage and communication of quantum information are still difficult experimentally, but they will probably become easier and less expensive in the future. Classical secret sharing, in which secrets and shares are both classical information, is nowadays used in practice, for example, in distributed storage systems. In a distributed storage system, data are stored in multiple storages, which increases the risk of data leakage. Secret sharing schemes decrease that risk with multiple storage.

Existing System Disadvantages

- Increased risk of **data leakage** due to storage across multiple locations. **No fine-grained access control** over who can access or reconstruct data.
- Uses **traditional security methods**, which may not handle modern threats well. Limited transparency and flexibility in managing access policies

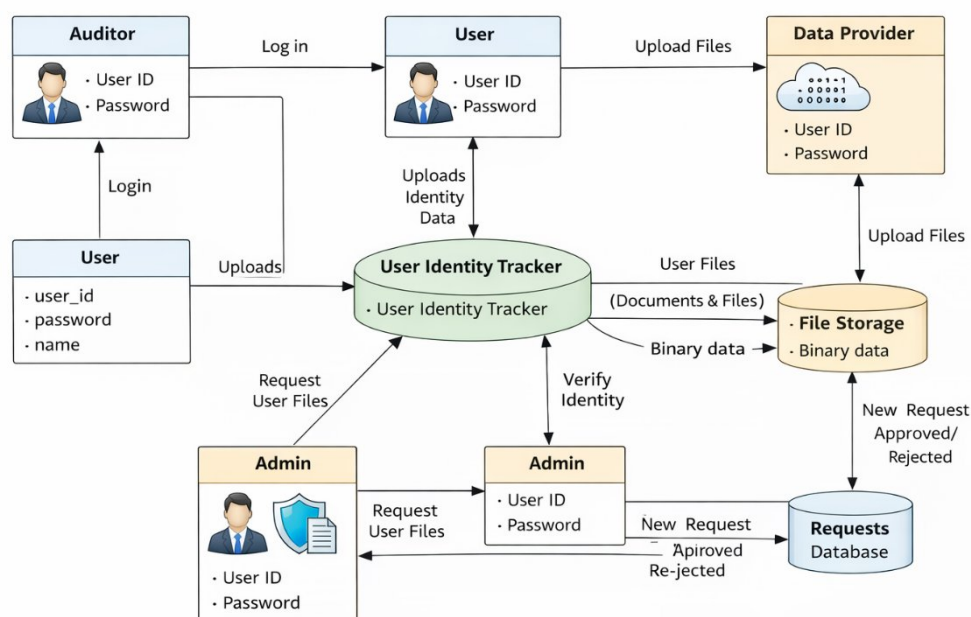
Proposed System

This paper proposes “Beyond Life”, an open-source Privacy Enhancing Technology (PET) solution for posthumous data management. The proposed solution automatically manages and distributes digital assets according to preset policies after the user’s demise. Using a newly designed encryption scheme, data access rights can be flexibly and efficiently controlled on the content level. The system combines blockchain technology and multi-load storage mechanisms to ensure transparency in the digital will system and reduce trust assumptions between entities. The proposed solution allows users to move their digital will between different service providers and generate their will content.

Advantages:

- Provides **secure posthumous data management** by automatically executing digital wills based on predefined policies, reducing manual intervention and errors.
- Enables **fine-grained access control** using advanced encryption, ensuring only authorized users can access specific parts of the data.
- Ensures **high data privacy and protection** at the content level
- Uses **blockchain technology** to maintain transparency and build trust between users and service providers

IV. SYSTEM ARCHITECTURE



System Architecture

DOI:10.15680/IJARETY.2026.1302091

The proposed system architecture is designed to securely manage user identities and digital files through four main entities: Auditor, User, Data Provider, and Admin, all connected through a centralized Cloud Server and Database. The Auditor module is responsible for identity tracking and generation. The auditor logs into the system using a user ID and password. After authentication, the auditor creates a tracker that generates a unique user identity. This tracker helps in monitoring user activities and supports later identity verification during data access and auditing processes.

V. METHODOLOGY

The core of the proposed system is a **secure, decentralized digital will management framework** that combines **PD-CP-ABE encryption, blockchain integration, and cloud-based storage**. The methodology focuses on ensuring **privacy, fine-grained access control, and secure posthumous data distribution**.

MODULES NAME:

1. User Interface
2. Authentication & Authorization
3. Identity Management
4. File Management
5. Verification & Approval
6. Encryption & Security
7. Database Management
8. Tracking & Logging

Modules Explanation:

1. User Interface:

- The user interface provides a simple and interactive platform for all system users. It includes login pages, dashboards, file upload forms, and access controls.
- The interface ensures ease of use, allowing users to manage their digital assets without requiring technical expertise.

2. Authentication & Authorization:

- This module ensures secure system access by validating user credentials such as user ID and password.
- It implements role-based access control, ensuring that Users, Admins, Auditors, and Data Providers have access only to their respective functionalities.

3. Identity Management:

- The identity management module handles user identity verification and tracking.
- The Auditor generates unique identity trackers for users, which are used for authentication, access control, and monitoring system activities. This ensures accountability and prevents identity misuse.

4. File Management:

- This module manages the upload, storage, and retrieval of files. Data Providers upload documents, which are converted into binary format and securely stored.
- Users can access files based on permissions, ensuring controlled data sharing.

5. Verification & Approval:

- The admin uses this module to verify user identities and approve or reject file access requests.
- It ensures that only verified users can access sensitive data, maintaining system integrity and security.

6. Encryption & Security:

- This module implements the PD-CP-ABE encryption scheme to secure data.
- It ensures that data is encrypted before storage and can only be accessed by users whose attributes satisfy the defined access policies. It also integrates blockchain for transparency and tamper-proof operations.

7. Database Management:

- The database stores user data, identity details, files, requests, and tracker information. It supports efficient data retrieval and ensures data consistency and reliability across the system.

8. Tracking & Logging:

- This module records all system activities, including user actions, access requests, and verification processes. The Auditor uses this information to monitor system behavior, ensuring transparency, accountability, and security.

VI. IMPLEMENTATION

The implementation of “**Beyond Life: An Open-Source Web Application for Data Management**” focuses on building a secure and scalable system for managing posthumous digital assets. The system is designed to ensure privacy, controlled access, and efficient data handling using advanced encryption techniques. It integrates identity management, file storage, verification, and access control into a unified platform.

The implementation is divided into multiple components, including **frontend, backend, database, and security layers**. The frontend provides a user-friendly interface for Users, Admins, Auditors, and Data Providers to interact with the system. The backend handles business logic such as authentication, identity verification, file management, and request processing. The database stores user details, files, and verification data, while the security layer enforces encryption and access control mechanisms.

Algorithm Used

Existing Algorithm

Traditional CP-ABE (Ciphertext-Policy Attribute-Based Encryption):

Traditional CP-ABE is a cryptographic technique used to enforce access control by embedding policies into encrypted data. It allows users with matching attributes to decrypt the data, but it relies on a centralized authority for key management. This creates issues such as single points of failure, limited scalability, and difficulty in handling dynamic access changes. Additionally, it may expose user attribute information and lacks flexibility for large-scale distributed systems.

Proposed Algorithm

PD-CP-ABE (Partially Decryptable Ciphertext-Policy Attribute-Based Encryption):

The proposed system uses PD-CP-ABE, an enhanced version of CP-ABE, to provide fine-grained and scalable access control for digital assets. It allows partial decryption based on user attributes, ensuring that only authorized users can access specific parts of the data. The algorithm supports decentralized key management, reducing dependency on a single authority and improving security. It also enhances privacy by protecting user attributes and supports dynamic access policies, making it suitable for secure and real-time digital will management systems.

VII. EXPERIMENTAL RESULTS

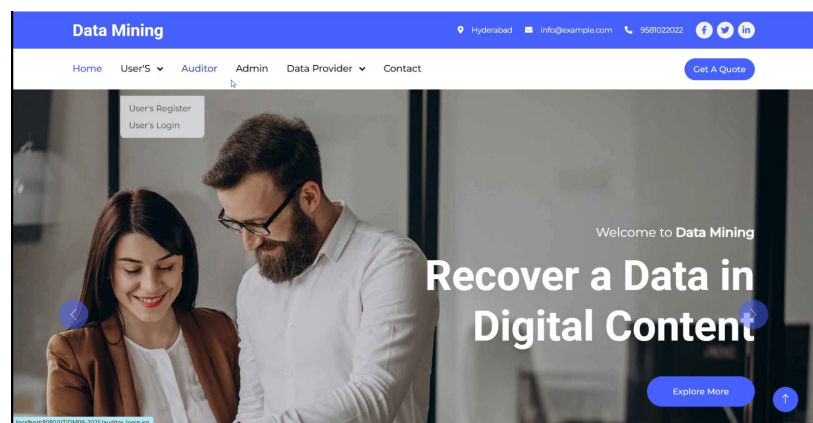


Figure 1: Home Page

This screen represents the **home page of the system**, providing a centralized entry point for all users including User, Auditor, Admin, and Data Provider. It contains a navigation menu with role-based access options such as login and registration, enabling controlled access to different system functionalities. The interface highlights the core purpose of the project—secure digital data management—through a clear heading and call-to-action section.

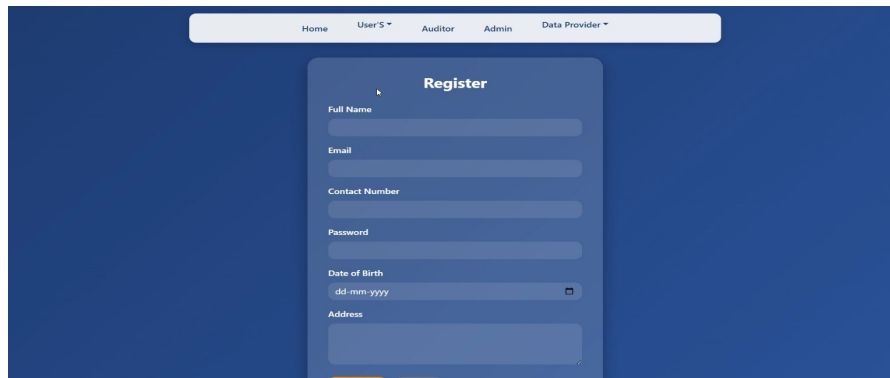


Figure 2: Data Provider Register Page

This screen represents the registration page where users enter details such as name, email, contact number, password, date of birth, and address. It is used to create a secure account in the system. All actors including User, Admin, and Auditor must register once before accessing the application. After registration, they can log in using their credentials whenever required. This page ensures secure authentication and controlled access to the system.

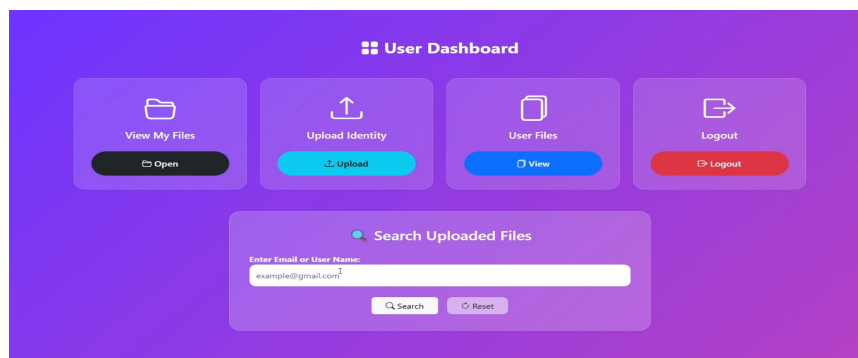
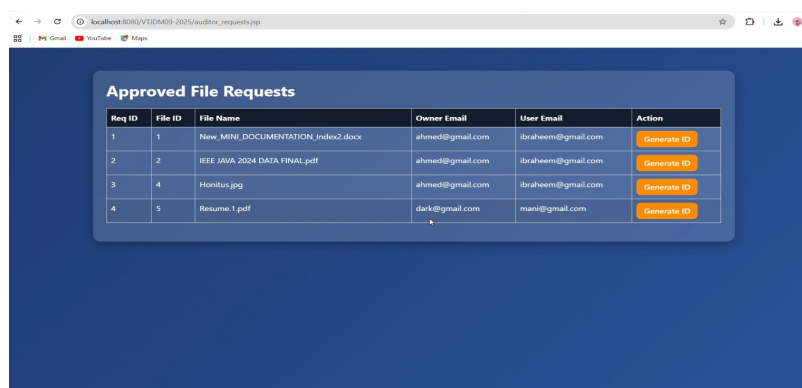


Figure 3: User Dashboard

This screen represents the **User Dashboard**, which provides all essential functionalities for the user in a single interface. It includes options such as **View My Files**, **Upload Identity**, and **User Files** for managing personal data securely. The user can upload identity details to enable verification and gain access to protected files. A search feature is also provided to find uploaded files using email or username. The dashboard includes a logout option for secure session termination. This page improves user convenience by organizing all actions in one place. It ensures controlled access to data based on verification status. Overall, it enhances usability, security, and efficient data management for the user.



Req ID	File ID	File Name	Owner Email	User Email	Action
1	1	New_MINI_DOCUMENTATION_Index2.docx	ahmed@gmail.com	ibraheem@gmail.com	Generate ID
2	2	IEEE JAVA 2024 DATA FINAL.pdf	ahmed@gmail.com	ibraheem@gmail.com	Generate ID
3	4	Honitus.jpg	ahmed@gmail.com	ibraheem@gmail.com	Generate ID
4	5	Resume.1.pdf	dark@gmail.com	mani@gmail.com	Generate ID

Figure 3: Audit Service Page

This screen represents the **Audit Service Page**, where the auditor manages approved file access requests. It displays details such as request ID, file ID, file name, owner email, and user email for tracking purposes. The auditor can generate a unique identity or tracker ID using the “**Generate ID**” option for each request. This helps in monitoring user activities and maintaining accountability within the system. The page ensures that all approved requests are properly recorded and traceable. It plays an important role in identity generation and audit logging. This functionality enhances transparency and strengthens system security. Overall, it supports effective tracking and verification of file access operations.

VIII.CONCLUSION

Our project “**Beyond Life**” an open-source Privacy Enhancing Technology (PET) for secure digital will management. It enables efficient posthumous distribution of digital assets using the PD-CP-ABE encryption scheme for fine-grained access control. The system addresses key challenges such as decentralization, portability, and cross-platform support. By integrating blockchain and multi-cloud storage, it ensures transparency and builds user trust. The solution supports flexible deployment models, allowing local or remote processing. However, legal, usability, and advanced security aspects require further improvement. Overall, Beyond Life provides a practical foundation for future scalable digital will management systems.

IX. ACKNOWLEDGMENT

I would like to express my sincere gratitude to my project guide and faculty members for their continuous support and guidance during the completion of my project titled “An Open-source Web application Data Management” Their valuable suggestions and encouragement helped me successfully complete this work. I am also thankful to my friends and teammates for their cooperation and support throughout the project.

REFERENCES

- [1] R. Gulotta, A. Kelliher, and J. Forlizzi, “Digital systems and the experience of legacy,” in *Proceedings of the 2017 Conference on Designing Interactive Systems*, Edinburgh, United Kingdom, 2017, pp. 663–674.
- [2] A. Shaghaghi, P. Scolyer-Gray, and D. Ashenden, “Digging your own digital grave: How should you manage the data you leave behind,” *The Conversation*, Aug. 2020.
- [3] A. Reeves, A. Shaghaghi, S. Krebs, and D. Ashenden, “Data after death: Australian user preferences and future solutions to protect posthumous user data,” *arXiv*, 2024.
- [4] J. Jargon, “A plan for your digital life after death,” *The Wall Street Journal*, Apr. 2023.
- [5] M. E. Locasto, M. Massimi, and P. J. DePasquale, “Security and privacy considerations in digital death,” in *Proceedings of the 2011 New Security Paradigms Workshop*, 2011, pp. 1–10.
- [6] J. Connor, “Digital life after death: The issue of planning for a person’s digital assets after death,” SSRN, 2010.
- [7] J. C. Shah et al., “Crypto-wills: Transferring digital assets by maintaining wills on the blockchain,” in *Communication and Intelligent Systems (ICCIS 2019)*, Springer, 2020.
- [8] W. Entriken et al., “Ethereum improvement proposals,” 2018.
- [9] N. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
- [10] M. Solomon, “What is a digital will?” Jul. 2023.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 8.152