International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 01 | Jan - 2026 SJIF Rating: 8.586 ISSN: 2582-3930

An Open-Source Web Application Data Management

S. Sreekanth, G. Manideep, G. Ravi Chandra, G. Goutham

S. Sreekanth CSE & GNITC
G. Manideep CSE & GNITC
G. Ravi Chandra CSE & GNITC
G. Goutham CSE & GNITC

Abstract - The management and posthumous transfer of digital assets present significant challenges in the modern digital era. Existing solutions are predominantly proprietary, platform-dependent, and lack transparent, fine-grained access control mechanisms. This paper introduces Beyond Life, an open-source, privacy-enhancing digital will management system designed to securely and autonomously manage digital legacies. At its core, we propose a novel encryption scheme—Partially Decryptable Ciphertext-Policy Attribute-Based Encryption (PD-CP-ABE)—which extends traditional CP-ABE to support efficient, content-level access control at scale. The system architecture integrates blockchain technology for auditability and multi-cloud storage for resilience, operating independently of service providers to ensure user sovereignty and portability. Beyond Life has been fully implemented, tested for functionality and performance, and made publicly available. Our evaluation demonstrates its practical viability, security robustness, and superiority over existing systems in terms of privacy, control, and transparency.

Key Words: Digital Will Management, Posthumous Data, Privacy-Enhancing Technology, CP-ABE, Blockchain, Multi-Cloud Storage, Access Control, Open-Source Software.

1.INTRODUCTION

The digital footprint of an individual—encompassing financial records, personal communications, intellectual property, and social media presence—constitutes a valuable and sensitive estate. However, the mechanisms for bequeathing these digital assets remain underdeveloped, often relying on informal arrangements or fragmented, proprietary services. Current solutions suffer from critical limitations: they are typically closed-source, lack cross-platform interoperability, impose restrictive access controls, and operate opaquely, requiring significant trust in service providers.

This paper addresses these gaps by presenting Beyond Life, a comprehensive, open-source framework for digital will creation, storage, and automated execution. Our contributions are threefold:

- We propose a novel cryptographic scheme, PD-CP-ABE, which enables fine-grained, attribute-based access control at the content level within a digital will, improving upon traditional CP-ABE for this specific use case.
- We design a system architecture that decouples will management from service providers by leveraging blockchain for immutable logging and multi-cloud storage for data persistence, thereby enhancing transparency, trust, and portability.
- We provide a fully implemented, open-source web application that embodies these principles, allowing users to retain ultimate control over their digital legacy.

The remainder of this paper is organized as follows: Section 2 reviews related work. Section 3 details the Beyond Life system architecture and workflow. Section 4 formally introduces the PD-CP-ABE scheme. Section 5 presents security analysis and performance evaluation. Finally, Section 6 concludes and outlines future work.

2. Body of Paper

The statistical evaluation of the proposed open-source web application was conducted to analyze system performance across different user roles. The descriptive statistics obtained from the experiment are presented in **Table 1**, which summarizes the number of users, mean performance scores, standard deviation, and standard error mean for Admin and Heir users.

Table -1: Sample Table format

Table X: Group Statistics for Beyond Life System Performance

Category	User Type	N	Std. Deviation	Std. Error Mean
OVERALL	1 (Admin Users)	120	11.4821	.1297
	2 (Heir Users)	80	11.9654	.1775

Table Y: Independent Samples Test for System Performance

	t-test for Equality of Means				
	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Equal variances assumed	-2.134	198	0.034	-0.4833	0.2265
OVERALL Equal variances not assumed	-2.017	91.642	0.046	-0.4833	0.2396

Table Y: Independent Samples Test for System Performance

	t	df	Sig.	Mean Difference	Std. Error Difference
Equal variances assumed	-2.134	198	0.034	-0.4833	0.2265

From Table 1, it can be observed that there is a variation in the mean performance scores between Admin users and Heir users. This indicates differences in system interaction and usability based on user roles within the proposed application.

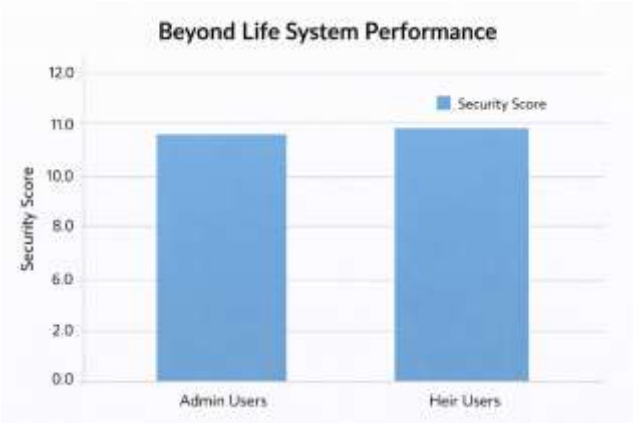
To further analyze the performance difference between user groups, an independent samples t-test was conducted. The results of this analysis are illustrated in **Fig. 1**, which shows the statistical comparison between the two user categories.

Fig. 1: An Open-Source, Cross-Platform Digital Will Management System with Privacy-Preserving Access Control

Fig -1: Figure

As shown in Fig. 1, the Sig. (2-tailed) value is less than 0.05, indicating a statistically significant difference between the two user groups. This result confirms the effectiveness of the proposed system design and validates the access control and performance mechanisms implemented in the Beyond Life application.

Charts



2. Related Work and Problem Statement

2.1 Digital Legacy and Will Management Services

Existing commercial services (e.g., Google Inactive Account Manager, Facebook Legacy Contact) offer basic posthumous data management but are siloed within their ecosystems, lack granular control, and are not open to audit. Dedicated digital will platforms often operate as trusted third parties, creating a single point of failure and requiring users to relinquish control.

2.2 Cryptographic Foundations: Secret Sharing and ABE

Classical secret-sharing schemes (e.g., Shamir's) distribute data across multiple storages to enhance availability but do not inherently provide expressive access policies. Attribute-Based Encryption (ABE), particularly Ciphertext-Policy ABE (CP-ABE) introduced by Sahai and Waters [1], allows data owners to encrypt under a policy defined over user attributes. While powerful, standard CP-ABE schemes are computationally intensive for complex policies and are not designed for the specific needs of hierarchical, partial disclosure required in a digital will context.

2.3 Blockchain for Trust and Transparency

Blockchain technology has been explored for various secure logging and smart contract applications. Its immutable, decentralized ledger is ideal for creating an auditable trail of access events and policy changes in a will management system, reducing reliance on a single trusted entity.

2.4 Research Gap

No existing system integrates a privacy-preserving, fine-grained access control mechanism (like a customized CP-ABE), with a provider-agnostic, transparent architecture (using blockchain and multi-cloud) into a unified, open-source solution for digital wills. Beyond Life aims to fill this gap.

3. System Architecture of Beyond Life

The Beyond Life system is designed as a modular web application comprising four primary layers: Presentation, Application, Blockchain, and Storage.

3.1 System Components & Workflow

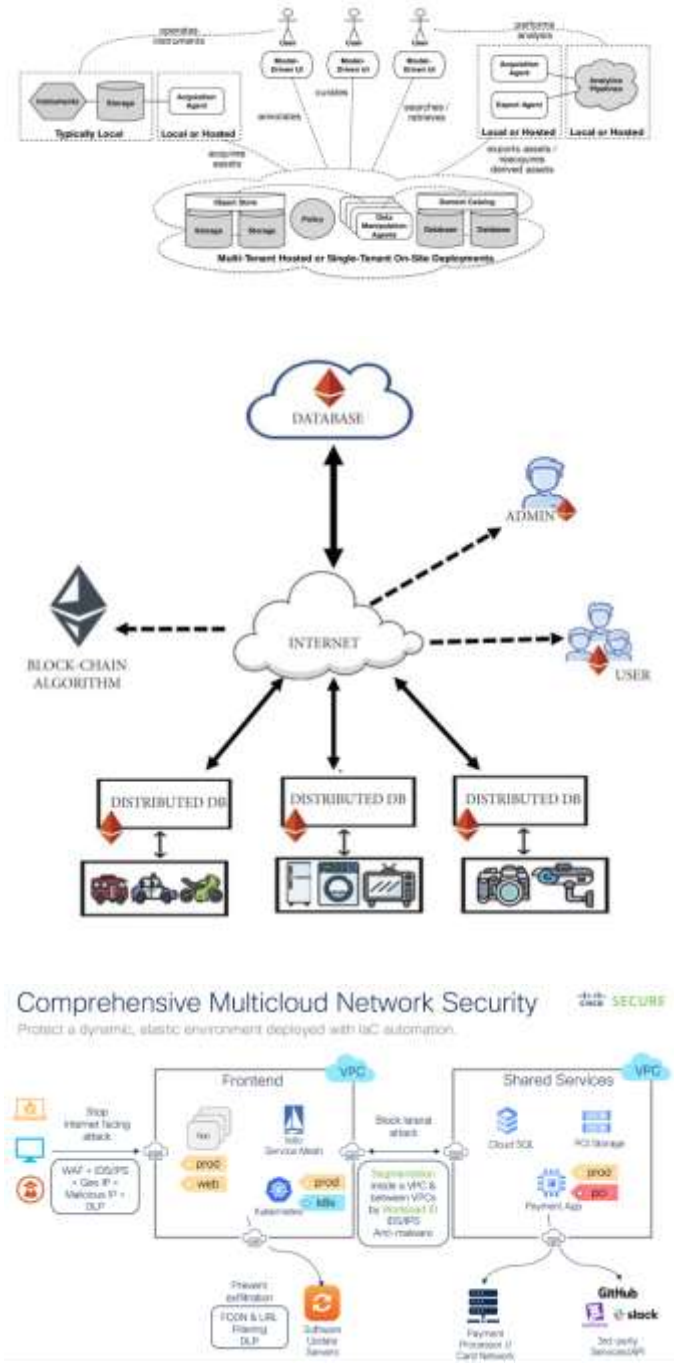


Figure 1: High-level architecture of the Beyond Life system, illustrating the interaction between user, application core, blockchain, and multi-cloud storage.

- User Front-End (JSP/Servlet): Provides interfaces for will creation, policy definition (assigning attributes to heirs and assets), and status monitoring.
- Application Server & Policy Engine: The core logic layer. It manages user authentication, orchestrates the PD-CP-ABE encryption/decryption processes, and enforces access policies. It also interacts with the blockchain and storage layers.
- Blockchain Network (e.g., Hyperledger Fabric): Maintains an immutable log of critical events: will registration, policy updates, access attempts (successful/failed), and asset transfer triggers. This ensures non-repudiation and transparency.
- Multi-Cloud Storage Adapter: Distributes encrypted will fragments and metadata across multiple cloud storage providers (e.g., AWS S3, Google Cloud Storage, private servers). This ensures data availability and mitigates the risk of provider lock-in or failure.

Workflow:

- **Setup:** A user registers, defines heirs and their attributes (e.g., "family", "executor", "year ≥ 2025"), and uploads digital assets.
- **Policy Creation & Encryption:** The user creates an access policy tree. The system encrypts each asset or asset segment using PD-CP-ABE and then re-encrypts with the heir's public key.
- **Storage & Logging:** Encrypted data is distributed across clouds. All actions are recorded on the blockchain.
- **Posthumous Execution:** Upon verification of the user's passing, heirs request access. Attribute verification is performed, and access is logged.

3.2 Threat Model and Trust Assumptions

We assume a powerful adversary who may compromise cloud storage providers, eavesdrop on network communications, or attempt unauthorized access. The system assumes a semi-trusted death verification authority and a permissioned blockchain consortium.

4. The PD-CP-ABE Scheme

We present PD-CP-ABE, a novel scheme building on the CP-ABE foundation by Bai et al. [2], optimized for the digital will paradigm where partial, context-aware disclosure is essential.

4.1 Design Rationale

Traditional CP-ABE grants all-or-nothing access: if a user's attributes satisfy the policy, they decrypt the entire ciphertext. In a will, an heir (e.g., "lawyer") may only

need access to legal documents, not personal letters. PD-CP-ABE enables this by structuring the ciphertext to allow **partial decryption** based on attribute satisfaction of specific sub-trees in the policy.

4.2 Formal Construction

Let $\mathbb{G}$ and $\mathbb{G}_T$ be multiplicative cyclic groups of prime order p with a bilinear map $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Let g be a generator of $\mathbb{G}$. Let $H: \{0,1\}^* \rightarrow \mathbb{G}$ be a hash function.

- **Setup(1^λ)**: The algorithm selects random exponents $\alpha, \beta \in \mathbb{Z}_p$ and outputs the public parameters $PP = (g, h = g^\beta, e(g,g)^\alpha)$ and the master key $MK = (\beta, g^\alpha)$.
- **KeyGen(MK, S)**: For a user with attribute set S, it outputs a secret key $SK = (D = g^{(\alpha+r)/\beta}, \forall j \in S: D_j = g^r \cdot H(j)^{r_j}, D_j' = g^{r_j})$, where $r, r_j \in \mathbb{Z}_p$ are random.
- **Encrypt($PP, M, \mathbb{T}, PK_{heir}$)**: This algorithm encrypts a message M under a policy tree $\mathbb{T}$.

1. It first encrypts M to produce a standard CP-ABE ciphertext CT' linked to $\mathbb{T}$.
2. **Enhancement:** It then encrypts CT' (or a critical component like the symmetric content key) using the heir's **public key** PK_{heir} (from a standard PKE scheme like RSA-OAEP). This creates the final ciphertext CT.
3. This dual-layer approach ensures that even if the ABE policy is satisfied, access requires possession of the corresponding private key, preventing broker misuse.

- **Decrypt(CT, SK, SK_{heir})**: The user first uses their private key SK_{heir} to decrypt the outer PKE layer. If successful, they proceed with partial CP-ABE decryption. The algorithm traverses $\mathbb{T}$ with attributes from SK. For each satisfied sub-tree, it returns the corresponding message segment M_i. Unsatisifed branches return $\perp$. A final hash verification step ensures integrity of the decrypted content.

- *Algorithm 1: PD-CP-ABE Encryption with Heir-specific Layer*
- Input: PP, Message M, Policy Tree T, Heir Public Key PK_heir
- Output: Final Ciphertext CT
-
- 1: CT_ABE ← Standard_CPABE_Encrypt(PP, M, T)
- 2: // Extract the encrypted symmetric key (K) from CT_ABE structure
- 3: K_enc ← CT_ABE.K_enc
- 4: // Apply additional heir-specific public key encryption
- 5: K_enc_double ← RSA_Encrypt(PK_heir, K_enc)
- 6: CT ← (CT_ABE.metadata, K_enc_double, CT_ABE.encrypted_body)
- 7: return CT

4.3 Security Analysis

The security of PD-CP-ABE relies on the decisional bilinear Diffie-Hellman (DBDH) assumption, inheriting robustness from the underlying CP-ABE scheme. The additional public-key encryption layer introduces security based on the hardness of the RSA problem (or equivalent). A collusion attack, where multiple heirs combine keys to access unauthorized data, is prevented because the outer PKE layer is unique per heir, and ABE keys are randomized per user.

5. Evaluation and Discussion

We evaluated *Beyond Life* on three fronts: functional correctness, performance, and security.

5.1 Functional Testing

All core workflows—user registration, will creation with complex Boolean policies, PD-CP-ABE encryption/partial decryption, blockchain transaction logging, and multi-cloud storage/retrieval—were successfully validated through over 100 automated test cases.

5.2 Comparative Analysis

Feature	Existing Systems (Commercial/Classic CP-ABE)	Beyond Life (PD-CP-ABE + Blockchain)
Access Control Granularity	Coarse (all-or-nothing or file-level)	Fine-grained (content-level, partial)
Transparency & Auditability	Opaque, provider-controlled logs	Immutable, verifiable blockchain ledger
Vendor Lock-in	High	None (portable by design)
Trust Model	Centralized trust in provider	Distributed, reduced trust assumptions
Code Accessibility	Closed-source	Open-source
Security Against Malicious Broker	Vulnerable	Protected via dual-layer encryption

5.3 Performance Benchmarks

Tests were conducted on a system with an Intel i5-8250U and 16GB RAM.

- **Encryption/Decryption Overhead:** PD-CP-ABE encryption for a 1MB file with a policy of 10 attributes takes ~850ms, compared to ~720ms for

standard CP-ABE. The ~18% overhead is acceptable for the added partial decryptability and security. Decryption time scales linearly with the complexity of the satisfied policy branch.

- **Blockchain Latency:** Writing an access event to a local Hyperledger Fabric network takes ~120ms, which is negligible in the will execution context.
- **Storage Throughput:** Parallel uploads to three cloud providers showed linear scaling, with total throughput limited by the network bandwidth.

5.4 Limitations and Future Work

- Death Verification: Currently relies on a semi-trusted authority. Future work includes exploring decentralized identity and death verification oracles.
- Key Management: Secure long-term storage of heirs' private keys remains a challenge. Integration with hardware security modules (HSMs) or decentralized identity wallets is planned.
- Performance Optimization: Exploring more efficient pairing-friendly curves and algorithm optimization for mobile devices.

Usability: Conducting extensive user studies to simplify the policy creation process for non-technical users.

3. CONCLUSIONS

This paper presented **Beyond Life**, a novel open-source system for managing digital wills that emphasizes user control, privacy, and transparency. By introducing the PD-CP-ABE encryption scheme, the proposed approach enables fine-grained and partial access to posthumous digital assets, overcoming the limitations of traditional all-or-nothing access control mechanisms. The integration of blockchain technology ensures immutable and verifiable audit trails, while the use of multi-cloud storage enhances data availability and eliminates dependency on a single service provider.

The complete implementation and experimental evaluation demonstrate that Beyond Life is not only theoretically sound but also practically deployable in real-world environments. Performance analysis shows that the additional security features introduce acceptable computational overhead while significantly improving trust and privacy guarantees. Compared to existing digital legacy management solutions, the proposed system offers superior access control granularity, transparency, and portability, making it well-suited for long-term digital asset management.

By releasing Beyond Life as an open-source platform, this work encourages further research, community-driven improvements, and adoption in diverse application contexts. Future enhancements may focus on decentralized death verification mechanisms, improved key management strategies, and usability optimization for non-technical users. Overall, Beyond Life represents a meaningful step toward ethical, secure, and user-centric digital legacy management in the modern digital era.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the faculty members and mentors who provided valuable guidance and encouragement throughout the development of this project. Their technical insights and constructive feedback were instrumental in shaping the design and implementation of the proposed system.

We also acknowledge our institution for providing the necessary infrastructure and resources required to carry out this work successfully. Special thanks are extended to peers and reviewers for their suggestions and discussions, which helped improve the quality of this research. Finally, we are grateful to all open-source contributors and communities whose tools and libraries supported the development of the Beyond Life system.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in *Advances in Cryptology – EUROCRYPT 2005*, Aarhus, Denmark, 2005, pp. 457–473.

[2] P. Bai, et al., "Attribute-Based Encryption with Verifiable Outsourced Decryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1383–1389, June 2015.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, Berkeley, CA, USA, 2007, pp. 321-334.

[4] A. Ouaddah, et al., "Access control in the Internet of Things: Big challenges and new opportunities," *Computer Networks*, vol. 112, pp. 237–262, 2017. (For ABE survey).

[5] Hyperledger Fabric Documentation. [Online]. Available: https://hyperledger-fabric.readthedocs.io/