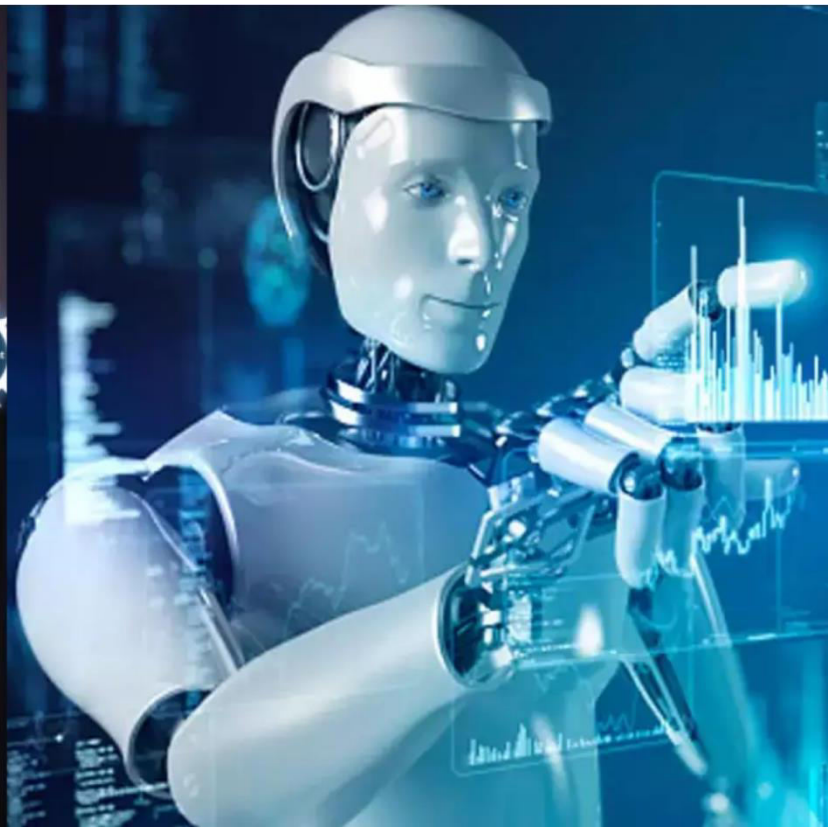
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.935

Volume 15, Issue 5, May 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505200|

HEIRCLOUD: Cloud System for Posthumous Asset Management with Privacy and Authorized Delivery

Mrs. R. Gayathri, MCA ., M.Phil., NET [1], Ms. C. Roshni [2]

Assistant Professor, Department of Master of Computer Application, Vivekanandha Institute of Information and Management Studies Tiruchengode, Namakkal Tamil Nadu, India[1]

PG Scholar, Department of Master of Computer Application, Vivekanandha Institute of Information and Management Studies Tiruchengode, Namakkal, Tamil Nadu, India[2]

ABSTRACT: Posthumous data includes an individual's digital information such as social media accounts, emails, health records, financial data, assets, and last wills or testaments. Disputes over wealth and assets often result in prolonged legal battles, while unexpected deaths leave beneficiaries uncertain about access to critical digital and financial information.

Mishandling or unauthorized access can lead to identity theft, fraud, privacy breaches, or conflicts among heirs. Existing solutions, including static instructions, informal legal arrangements, or platform-specific legacy systems, often lack encrypted storage, fine-grained access control, and verifiable delivery mechanisms. Consequently, sensitive data may be exposed, lost, or mismanaged. To overcome these challenges, this project introduces a secure cloud-based posthumous data management system that employs the Heir Access Code-based Encryption (HACE) scheme and Dynamic Access Control.

The system ensures encrypted storage of sensitive data and controlled delivery to authorized heirs after the data owner's death. It comprises two main modules: a storing module, which securely stores encrypted posthumous data, and a sharing module, which manages authorized access and delivery. By combining encrypted cloud storage, heir-specific access codes, and adaptive access management, this framework ensures that sensitive posthumous data is securely stored, delivered only to intended recipients, and protected against misuse.

KEYWORDS: Heir Access Code-based Encryption (HACE), Dynamic Access Control (DAC), Adaptive Access Management**.**

I. INTRODUCTION

An antiquated term that refers to the document written by a testator that details what is to happen to property owned by that testator upon death. This term is still frequently used in an interchangeable way to mean a will, though to be precise a last will and testament refer to the most recent version of a will. [1] A will can confer rights or ownership over real property or personal property and can also be used to appoint legal guardians, but only takes effect once the testator dies.

A will or testament is a legal document that expresses a person's (testator) wishes as to how their property (estate) is to be distributed after their death and as to which person (executor) is to manage the property until its final distribution. For the distribution (devolution) of property not determined by a will, see inheritance and intestacy.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505200|

Figure: 1.1. Will or Testament

Types of Wills
There are multiple types of Wills that are valid and legal, and the type you choose will depend on several factors, including how large or complicated your estate is.

Simple Wills
A Simple Will allows you to state your basic wishes without the inclusion of multiple stipulations or clauses. And you can also designate a guardian for any minor children or dependents.

Testamentary Trust Wills
A Testamentary Trust, also known as a "Trust Under Will" or a "Will Trust," is written inside a Will. Similar to other Trusts, a Testamentary Trust distributes assets after you pass. Testamentary Trusts will go through probate, [2] and are often used in cases when beneficiaries will need to be cared for over an extended time period – examples are a dependent with special needs or young minors.

Joint Wills
A Joint Will is similar to a Mutual Will, but a Joint Will only has one document, whereas a Mutual Will has two. Joint Wills can be useful in cases where you want your spouse to be the initial Beneficiary of your whole estate, with the final Beneficiaries being your children after you both pass As long as both parties are living, changes can be made.

Online Wills
An Online Will is exactly what it sounds like. When done properly, it can absolutely offer adequate protection, and with a significantly reduced cost compared to going the more traditional Estate Planning route, face-to-face with attorneys.[1] Just like you would make sure you trust and have confidence in your attorney before hiring him or her, you want to know that you're working with an online company that's preparing solid, legal documents that will hold up when it counts the most.

Deathbed Wills
Perhaps the least effective and most problematic type of Will, a Deathbed Will is written when you are in a die state, near death. problems that result, from forgotten assets to questions about mental states[1].

Holographic Wills
A Holographic Will is a Will that's written and signed by hand. While not all that common, this type of Will does still exist, generally resulting from extreme, unexpected, often life-threatening situations. Though they do occasionally surface, they're not recognized in all states[1].

Nuncupative Wills
A Nuncupative Will is spoken. Like Holographic Wills, Nuncupative Wills aren't always recognized the same way (or at all) in every state. You may need to have a certain number of witnesses, or need to have wishes written down after being spoken, or there may be other nuances [1] .

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505200|

Oral Wills
Least widely recognized are oral wills, in which the testator speaks their wishes before witnesses. Lacking a written record, or at least one prepared by the testator, courts do not widely recognize oral wills.

Pour-over Wills
Another type of will, a pour-over will, is used in conjunction with creating a trust into which your assets flow. (See "Wills and Trusts" below.)

Mutual Wills
A married or committed couple usually executes this type of will. After one party dies, the remaining party is bound by the terms of the mutual will. Mutual wills can be used to ensure that property passes to the deceased's children rather than to a new spouse. Because of state differences in contract law, a mutual will should be established with a legal professional's help. Though the terms sound similar, a mutual will should not be confused with a joint will.

II. LITERATURE REVIEW (SURVEY)

Privacy Aware Authentication Scheme for Distributed Mobile Cloud Computing (Mrs. Chaitali P. Kathar, Prof. Vidya Dhamdhere, Li, M., Chow, S. S. M., & Guo, M (May 2016)
As mobile users generally access different types of mobile cloud computing services from a variety of service providers, it is extremely tedious for users to register different user accounts on each service provider and maintain corresponding private keys or passwords for authentication usage [1]. In this paper, I propose a encryption method call Attribute encryption method.

Cloud computing is a revolutionary computing paradigm, which enables flexible, on-demand, and low-cost usage of required resources, but the data is outsourced or stored to some cloud servers, and various privacy concerns emerge from it. This paper focuses on data privacy, anonymity, access control. Attribute based encryption technique attached attributes along with the data and only attributes are encrypted the data is kept as it is. Attribute based encryption technique increased the security, performance and reduce the time of proposed system **[2].**

Managing Distributed Machine Learning Lifecycle for Healthcare Data in the Cloud (ENGIN ZEYDAN AND MADHUSANKA LIYANAGE (2019)
The main objective of this paper is to highlight the research directions and explain the main roles of current Artificial Intelligence (AI)/Machine Learning (ML) frameworks and available cloud infrastructures in building end-to-end ML lifecycle management for healthcare systems and sensitive biomedical data. **Wang, Q., Zhang, Y., & Zhang, Z. (2016)** [3].

We identify and explore the versatility of many genuine techniques from distributed computing and current state-of-the-art ML research, such as building cognition-inspired learning pipelines and federated learning (FL) ecosystem. Additionally, we outline the advantages and highlight the main obstacles of our methodology utilizing contemporary distributed secure ML techniques, such as FL, and tools designed for managing data throughout its lifecycle [6]. For a robust system design, we present key architectural decisions essential for optimal healthcare data management, focusing on security, privacy and interoperability. Finally, we discuss ongoing efforts and future research directions to overcome existing challenges and improve the effectiveness of AI/ML applications in the healthcare domain

Sahai, A., & Waters, B. (2005) [1].
NumPy, Pandas, Scikit-learn, Matplotlib – "Python Data Science Handbook" by Jake VanderPlas, O'Reilly, 2016.
MySQL – "Learning MySQL" by Seyed Haghighi & Hugh Williams, O'Reilly, 2012.
Flask – "Flask Web Development: Developing Web Applications with Python" by Miguel Grinberg, O'Reilly, 2018.
Python – "Learning Python" by Mark Lutz, O'Reilly, 2013.
HTML – "HTML and CSS: Design and Build Websites" by Jon Duckett.
CSS – "HTML and CSS: Design and Build Websites" by Jon Duckett.
JavaScript – "JavaScript and jQuery: Interactive Front-End Web Development" by Jon Duckett**. Lai, X., Zeng, Y.,**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505200|

Zhao, X., & Tian, J. (2018) [8].
The project has successfully addressed key challenges in managing posthumous digital and financial assets. However, there are several areas for future enhancement to further improve security, usability, and transparency.

Advanced Biometric Authentication –
Integrate fingerprint, facial recognition, or voice-based authentication to strengthen identity verification for both data owners and heirs, ensuring higher security and trust.

Blockchain-Based Audit Trail –
Implement a blockchain-based logging mechanism to provide immutable, tamper-proof records of all data access, policy updates, and sharing events, enhancing transparency and accountability.

Mobile Application Support
Develop a dedicated mobile application to deliver real-time notifications, enable easier access management, and improve user convenience for data owners and heirs.

Multi-Factor Authentication (MFA) –
Introduce MFA to add an additional layer of security during login and data access, reducing the risk of unauthorized entry.

Cloud Interoperability –
Expand support for multiple cloud providers to enhance data redundancy, availability, and scalability.
The results of the proposed secure cloud-based posthumous data management system show that it effectively addresses the major challenges associated with handling digital assets after an individual's death. The implementation of the Heir Access Code-based Encryption (HACE) scheme ensures that all sensitive data is securely encrypted before being stored in the cloud. This guarantees that personal information such as financial records, emails, and legal documents remains confidential and protected from unauthorized access.

The system also demonstrates strong performance in controlled data sharing through its dedicated sharing module. Only authorized heirs with valid access credentials are able to retrieve the stored data, ensuring that information is delivered strictly to intended recipients.

The verification-based access mechanism ensures that data is released only after confirming specific conditions, such as the death of the data owner. This reduces the chances of premature or unauthorized disclosure and ensures a reliable and timely transfer of critical information to beneficiaries.

Discussion perspective, the integration of dynamic access control plays a crucial role in improving flexibility and usability. Users can modify access permissions, update their details, and revoke or grant access rights at any time, allowing the system to adapt to real-life changes such as evolving relationships or asset updates.

This dynamic nature overcomes the limitations of traditional static inheritance systems, which often fail to reflect changes once established. As a result, the system provides a more practical and user-centric approach to posthumous data management.

The system helps in reducing legal disputes, fraud, and confusion among heirs by clearly defining and enforcing access policies. Since all data is securely stored and systematically shared based on predefined rules, there is greater transparency and trust in the process.

However, certain limitations exist, such as the dependency on accurate death verification mechanisms and the need for users to securely manage their access codes. Despite these challenges, the system proves to be a reliable and secure solution[10].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505200|

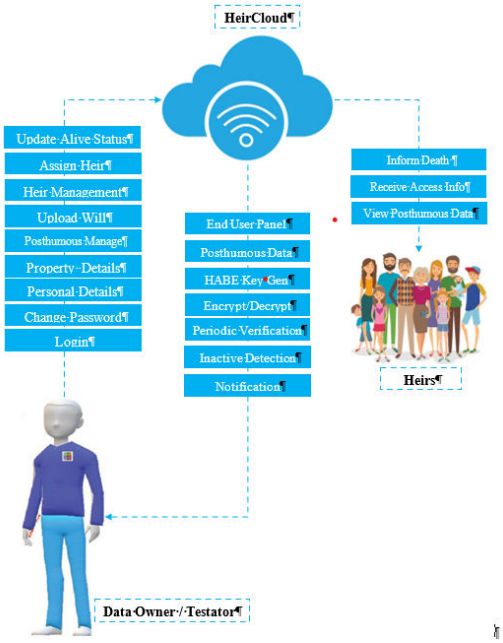


Figure 1.2 Architecture

III. METHODOLOGIES

The methodology of the project explains the steps and processes used to securely store posthumous digital assets and deliver them to authorized heirs. The system follows a structured approach to ensure data privacy, encryption, and controlled access.

User Registration and Authentication
Users first create an account in the system by providing basic details and login credentials. Authentication mechanisms ensure that only authorized users can access their accounts and manage their stored information.

Secure Data Storage
The data owner uploads digital assets such as documents, credentials, or important information to the system. All data is encrypted using secure encryption techniques before being stored in the cloud database to ensure privacy and protection.

Heir Access Code Generation
The system generates a unique Heir Access Code (HACE) that is assigned to authorized heirs. This code acts as a secure key that allows heirs to access specific data after verification.

Dynamic Access Policy Management
The data owner can define, modify, or revoke access policies at any time. This dynamic access control ensures that only selected heirs receive permission to view or retrieve specific information.

Death Verification and Access Activation
After verification of the data owner's death through predefined conditions or confirmation mechanisms, the system activates the inheritance process and allows authorized heirs to request access.

Authorized Data Delivery
Once the heir enters the correct access code and passes authentication checks, the system decrypts and securely delivers the permitted information to the authorized recipient.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505200|

The proposed system introduces a secure cloud-based posthumous asset management framework designed to store, protect, and deliver digital and financial assets automatically to authorized heirs. By integrating Heir Access Code-based Encryption (HACE), Dynamic Access Control, and multi-stage death verification mechanisms, the system ensures secure, selective, and auditable inheritance while minimizing disputes, unauthorized access, and reliance on third parties.

Secure Posthumous Data Storage

This module is responsible for storing all sensitive digital and financial assets securely in the cloud. Data is encrypted using the HACE algorithm, generating heir-specific cryptographic keys to ensure that only designated heirs can decrypt their assigned assets. Redundant cloud storage ensures data availability and integrity, preventing accidental loss or tampering[5].

Authorized Access & Controlled Delivery

The system manages inheritance policies, access rights, and selective delivery of posthumous data using Dynamic Access Control. The data owner defines which heirs can access specific data and under what conditions. After death confirmation through inactivity detection and alert verification, authorized heirs are verified and granted access using their unique access codes. [6]This ensures controlled, auditable, and secure delivery of sensitive assets.

Audit Logging and Verification

To maintain accountability and transparency, the system logs all activities, including data uploads, access requests, decryption events, and policy changes. Periodic activity verification and inactivity detection prevent premature data release. Multi-stage alert notifications confirm the data owner's inactivity before activating posthumous data sharing.

IV. ALGORITHM

1. Protects sensitive digital and financial data after the data owner's death.
2. Ensures secure, heir-specific access to assigned assets.
3. Enables controlled, selective, and auditable data sharing.
4. Reduces disputes among heirs by enforcing transparent inheritance policies.
5. Minimizes reliance on legal procedures and third-party custodians.
6. Supports dynamic updates to permissions and access rules.
7. Provides timely and verified access for heirs after death confirmation.
8. Maintains comprehensive audit logs for accountability and dispute resolution.
9. Enhances privacy, trust, and integrity in posthumous asset management.

The proposed system is a secure cloud-based solution designed to manage an individual's digital and financial data after their death in a safe and controlled manner. Posthumous data, which includes social media accounts, emails, financial records, health information, and legal documents, often becomes difficult to access or manage due to lack of proper security mechanisms and clear access policies. [9] This system addresses these challenges by providing a structured and secure platform where users can store their sensitive information and define how it should be accessed by their heirs.

The core idea of the system is to ensure that all data is encrypted before being stored in the cloud, thereby maintaining confidentiality and preventing unauthorized access. It uses a specialized encryption approach called Heir Access Code-based Encryption (HACE), where only designated heirs with valid access codes can decrypt and retrieve the data. This ensures that sensitive information is shared only with intended recipients and remains protected from misuse or cyber threats.

The system is divided into two main modules: the storing module and the sharing module. The storing module is responsible for securely uploading and maintaining encrypted data, while the sharing module manages the controlled distribution of this data to authorized heirs. A key feature of the system is Dynamic Access Control, which allows users to update their details, modify access permissions, and revoke or grant access at any time. This flexibility ensures that the system adapts to real-life changes and user preferences[10].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505200|

The concept provides a reliable and secure framework for posthumous data management by combining encryption, controlled access, and cloud storage. It minimizes risks such as data loss, unauthorized access, fraud, and inheritance disputes, while ensuring that important information is delivered safely and efficiently to the rightful beneficiaries

V. CONCLUSION

In conclusion, the project successfully implements a secure and technology-driven system for managing posthumous digital and financial assets. By integrating Heir Access Code-based Encryption (HACE), dynamic access control, inactivity detection, and automated heir notifications, the system ensures that sensitive data is stored securely, shared only with authorized beneficiaries, and protected from unauthorized access.

The project provides a flexible framework for defining and updating inheritance policies, maintaining audit logs, and enforcing controlled data delivery after death confirmation. While the system effectively addresses challenges related to privacy, legal disputes, and data mismanagement, future enhancements can focus on optimizing alert mechanisms, integrating advanced multi-factor authentication, and supporting seamless cloud interoperability. Overall, project improves transparency, security, and reliability in posthumous asset management, providing peace of mind to users and ensuring orderly digital inheritance for heirs.

REFERENCES

1) Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In Advances in Cryptology - EUROCRYPT 2005 (pp. 457-473). Springer.
2) Li, M., Chow, S. S. M., & Guo, M. (2013). Attribute-based encryption with efficient verifiable outsourced decryption. IEEE Transactions on Information Forensics and Security, 8(12), 1970-1980.
3) Wang, Q., Zhang, Y., & Zhang, Z. (2016). A secure and efficient attribute-based encryption scheme with verifiable outsourced decryption for cloud storage. Security and Communication Networks, 9(7), 568-578.
4) Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Attribute based data sharing with attribute revocation. In 2010 Proceedings IEEE INFOCOM (pp. 1-9). IEEE.
5) Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.
6) Boldyreva, A., Goyal, V., & Kumar, V. (2011). Identity-based encryption with efficient revocation. In Proceedings of the 15th international conference on the theory and application of cryptographic techniques (pp. 417-436). Springer.
7) Jin, H., & Deng, R. H. (2012). Efficient and secure sharing of personal health records in cloud storage using attribute-based encryption. Journal of medical systems, 36(6), 3779-3791.
8) Lai, X., Zeng, Y., Zhao, X., & Tian, J. (2018). Secure data sharing scheme for cloud storage based on attribute-based encryption. Security and Communication Networks, 2018, 1-8.
9) Chen, Q., Liu, X., Guan, C., & Zhang, Z. (2017). A cloud-based e-health system with verifiable privacy-preserving attribute-based keyword search. IEEE Transactions on Cloud Computing, 6(3), 835-847.
10) Chen, X., Ma, J., & Liu, W. (2019). A cloud-based secure data sharing scheme for IoT using attribute-based encryption. Future Generation Computer Systems, 95, 363-374.M.Egger,R.Urbanke,andR.Bitar “Federate done-shot learning with data privacy and objective-hiding,“in Proc .IEEE Int .Symp. Inf .Theory (ISIT), Jun.2025.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details