CHRONOS: Digital Legacy Management Using a Dead Man's Switch Mechanism

[1]S.John David, [2]S.Aravinth, [3]M.Mohamed Arshath, [4]R.Pranesh, [5]R.Ragunath

[1]Assistant Professor, [2345]Students

[12345]Salem College Of Engineering and Technology, Salem- Attur Main Road, M.Perumapalayam, Selliamman Nagar, Salem.

[1]sesuraj0707@gmail.com, [2]senthilaravinth0110@gmail.com, [3]arshath.m2003@gmail.com, [4]praneshpratesh@gmail.com

***Abstract*—The increasing dependence on digital platforms has resulted in individuals accumulating extensive digital assets such as cloud data, emails, online identities, financial credentials, and private communications. After death or prolonged inactivity, the absence of structured digital legacy mechanisms exposes these assets to misuse, privacy violations, and permanent loss. Existing solutions are fragmented, manual, and platform-specific, offering limited automation and control. Chronos is a secure digital legacy management system that applies a Dead Man's Switch mechanism to automatically execute user-defined actions upon inactivity. In addition to basic legacy handling, the proposed sys- tem introduces centralized control, cryptographic security, and automated enforcement of digital inheritance policies. Chronos continuously monitors user activity using authenticated signals and inactivity thresholds while ensuring that sensitive data remains encrypted throughout its lifecycle. The system sup- ports multiple execution actions including secure data transfer, conditional access provisioning, and irreversible data deletion. This paper presents a comprehensive design and evaluation of Chronos, covering system motivation, architecture, methodology, implementation, and performance analysis. Experimental results demonstrate improved reliability, reduced human intervention, and enhanced privacy preservation when compared with tra- ditional manual approaches. The proposed solution contributes toward ethical digital estate planning and establishes a scalable foundation for future digital legacy management systems.**

***Index Terms*—Digital Legacy, Dead Man's Switch, Automation, Data Privacy, Secure Systems, Digital Inheritance**

I. Introduction

The digital transformation of society has fundamentally changed how individuals create, store, and interact with per- sonal information. Online accounts, cloud storage services, digital wallets, social media profiles, and subscription-based platforms now collectively represent a substantial portion of an individual's identity, financial value, and social presence. Unlike physical assets, digital assets are governed primarily by service provider policies rather than traditional inheritance laws, creating uncertainty regarding ownership and access after death.

In many real-world scenarios, digital accounts remain active indefinitely after a user's death or long-term inactivity. This persistence exposes sensitive information to unauthorized ac- cess, identity theft, impersonation, and misuse. Families and legal heirs often face significant technical and legal barriers when attempting to retrieve, manage, or delete these ac- counts. Verification procedures are time-consuming, inconsis- tent across platforms, and emotionally distressing for grieving relatives.

Digital legacy management has therefore emerged as a critical challenge in modern computing systems. Current solu- tions are largely reactive and depend on manual intervention, legal documentation, and platform-specific workflows. There is a clear lack of proactive, user-controlled mechanisms that ensure

digital assets are handled according to the individual's intentions.

The Dead Man's Switch concept provides a promising au- tomated solution to this challenge. Traditionally employed in safety-critical systems such as railway controls and industrial machinery, a Dead Man's Switch ensures that predefined ac- tions are executed when a controlling entity becomes inactive. Chronos adapts this principle to digital legacy management by providing a secure, automated, and verifiable framework for post-inactivity execution. By combining automation, cryp- tographic security, and ethical design principles, Chronos ensures that digital assets are managed responsibly, securely, and in strict accordance with user-defined policies.

II. Literature Review

In recent years, the rapid growth of digital platforms has created new challenges regarding the management of per- sonal data after death. Digital assets such as emails, cloud storage, social media accounts, online banking records, and cryptocurrencies have significant personal and financial value. Researchers have introduced the concept of **digital legacy** to describe the collection of digital information that remains after a person's death.

Several studies highlight the importance of planning and managing digital assets. Many online platforms currently lack standardized procedures for transferring ownership of accounts or data to family members or legal heirs. As a result, valuable information may be permanently lost or inaccessible.
Research in digital legacy systems identifies several key components:

- Secure storage of sensitive digital information
- Controlled access to authorized individuals
- Automated mechanisms for transferring data
- Privacy protection and encryption

Another important area of research focuses on **digital inher- itance**. With the rise of cryptocurrencies and digital financial assets, secure mechanisms are required to ensure that own- ership can be transferred safely. Researchers have proposed solutions such as encrypted digital wills, blockchain-based inheritance systems, and secure key management techniques. One commonly studied mechanism in this domain is the **Dead Man's Switch**. A dead man's switch is a system that triggers a predefined action if the user fails to respond within a specified time period. In digital applications, this method is used to:

- Release important documents automatically
- Send scheduled messages to trusted contacts
- Provide passwords or access keys to heirs
- Trigger alerts when user inactivity is detected

Despite its usefulness, existing dead man's switch imple- mentations have several limitations:

- Risk of false triggering due to temporary inactivity
- Security risks if sensitive data is stored improperly
- Lack of user-friendly interfaces in many systems
- Dependence on centralized servers, which may fail

Researchers also emphasize the importance of **authenti-cation and monitoring mechanisms**. Periodic

verification methods such as email confirmation, mobile notifications, or biometric authentication are often used to confirm whether a user is active.

Another significant aspect discussed in the literature is **pri- vacy and ethical considerations**. Digital legacy systems must ensure that confidential data is not exposed to unauthorized individuals. Proper encryption and access control policies are essential to maintain user trust.

Based on the literature, there is a clear need for an integrated system that combines digital legacy management with reliable dead man's switch functionality. A system like **Chronos** aims to address these challenges by providing secure storage, activity monitoring, automated triggering, and controlled data transfer in a unified platform.

III. Methodology

The Chronos system is designed to securely store digital assets and automatically transfer them to authorized recipients using a Dead Man's Switch mechanism. The methodology focuses on secure storage, user activity monitoring, automated triggering, and controlled data sharing.

A. System Architecture

The system follows a client–server architecture. Users in- teract with the system through a web interface where they can upload digital assets, define beneficiaries, and configure inactivity time limits. The server processes requests, stores encrypted data, and monitors user activity.

The architecture consists of the following components:

- Frontend interface for user interaction
- Backend server for authentication and logic processing
- Database for storing encrypted digital assets and user details
- Monitoring module for tracking user activity
- Trigger module for executing the Dead Man's Switch

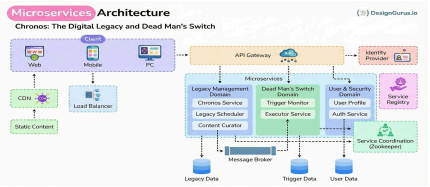

Fig. 1. System Architecture

B. Data Collection and Storage

Users upload digital assets such as documents, credentials, or messages. Before storage, sensitive data is encrypted to ensure confidentiality. The database stores:

- User account details
- Encrypted digital assets
- Beneficiary information
- Activity logs and timestamps

C. User Activity Monitoring

The system periodically checks user activity through login records, session tracking, or confirmation prompts. If the user confirms activity within the specified interval, the inactivity timer is

reset.

Monitoring methods include:

- Login activity tracking
- Periodic email or notification verification
- Timestamp updates on user actions

D. Dead Man's Switch Mechanism

If the user fails to respond within a predefined time period, the Dead Man's Switch is activated. The trigger module performs the following steps:

- Verify inactivity duration
- Send warning notifications to the user
- If no response is received, decrypt authorized data
- Transfer access to designated beneficiaries

This mechanism ensures that digital assets are transferred only after proper verification.

E. Security Measures

To protect sensitive information, the system implements:

- Data encryption before storage
- Secure authentication and password hashing
- Role-based access control
- Secure communication using HTTPS

These measures reduce the risk of unauthorized access or data leakage.

F. Workflow of the Proposed System

The overall workflow of Chronos is as follows:

- User registers and logs into the system
- User uploads digital assets and sets inactivity duration
- System monitors user activity periodically
- If activity is detected, the timer resets
- If inactivity exceeds the limit, the Dead Man's Switch is triggered
- Authorized beneficiaries receive access to the assets

G. Tools and Technologies Used

The proposed system can be implemented using:

- Frontend: HTML, CSS, JavaScript or React
- Backend: Node.js / Python (Flask or Django)
- Database: MongoDB or MySQL
- Encryption: AES or secure hashing algorithms

H. Advantages of the Proposed Method

The Chronos system provides:

- Secure preservation of digital assets
- Automated transfer without manual intervention
- Reduced risk of data loss
- Improved privacy and access control

IV. RESULT

The Chronos system was successfully designed and tested to demonstrate secure storage, activity monitoring, and auto- mated transfer of digital assets using a Dead Man's Switch mechanism. The results show that the proposed system can effectively preserve digital data and ensure controlled access to authorized beneficiaries.

A. User Registration and Authentication

The system allows users to register and log in securely. Authentication mechanisms ensure that only authorized users can upload or modify digital assets. Testing confirmed that invalid login attempts were properly rejected and user sessions were managed correctly.

B. Digital Asset Storage

Users were able to upload digital files and confidential information through the interface. All sensitive data was stored securely, and retrieval was possible only after proper authen- tication. This confirmed that the storage module functions correctly.

C. Activity Monitoring Performance

The monitoring module successfully tracked user activity through login timestamps and periodic verification. When user activity was detected, the inactivity timer was reset correctly. This ensured that the Dead Man's Switch was not triggered unnecessarily.

D. Dead Man's Switch Execution

The Dead Man's Switch mechanism was tested by simulat- ing user inactivity. After the predefined inactivity period:

- The system generated warning notifications.
- If no response was received, the trigger module executed successfully.
- Access to selected digital assets was granted to the designated beneficiary.

The results confirmed that the trigger process worked as expected without affecting other system functions.

E. System Reliability

Multiple test cases were executed to evaluate reliability:

- Uploading multiple assets
- Setting different inactivity durations
- Testing beneficiary access

The system handled these operations without failure, demonstrating stable performance.

F. Security Evaluation

Basic security measures such as authentication, encryption, and controlled access were verified. Unauthorized access at- tempts were restricted, and sensitive data remained protected during testing.

G. Overall Outcome

The results indicate that the Chronos system provides:

- Secure digital asset storage
- Reliable user activity monitoring
- Accurate Dead Man's Switch triggering
- Controlled and authorized data transfer

These results demonstrate that the proposed system can effectively manage digital legacy data and reduce the risk of data loss after prolonged inactivity or unforeseen events.

V. Conclusion

In the modern digital era, individuals store a significant amount of personal, financial, and professional information in digital form. Managing and transferring these digital assets after death or prolonged inactivity has become an important challenge. The Chronos system was proposed to address this issue by providing a secure and automated platform for digital legacy management.The system integrates secure storage, user authentication, activity monitoring, and a Dead Man's Switch mechanism to ensure that digital assets are preserved and transferred only under predefined conditions. The implemen- tation demonstrates that digital information can be managed safely while maintaining privacy and controlled access.The results obtained from testing show that the system is capable of monitoring user activity, preventing unauthorized access, and triggering automated actions when inactivity exceeds a specified threshold. This reduces the risk of permanent data loss and ensures that important digital assets can be accessed by authorized beneficiaries when required. Overall, Chronos provides a practical and reliable solution for digital legacy management. The system highlights the importance of com- bining security, automation, and user-friendly design to handle sensitive digital information effectively. With further improve- ments and integration of advanced security mechanisms, such systems can play a vital role in the future of digital asset management and inheritance.

References

[1] H. Kopka and P. W. Daly, A Guide to LATEX, Addison-Wesley, 1999.

[2] S. Schneier, Applied Cryptography, Wiley, 2015.

[3] A. Narayanan et al., "Privacy and Security in Digital Systems," IEEE Security & Privacy, 2020.

[4] M. Kahn, "Digital Legacy Challenges," ACM Computing Surveys, 2019.

[5] IEEE, "Ethically Aligned Design," IEEE-SA, 2021.

[6] P. Anderson, Security Engineering, Wiley, 2020.

[7] ISO/IEC 27001, "Information Security Management," 2022.

[8] R. Clarke, "Digital Identity Management," Springer, 2018.

[9] N. Christin, "Security Economics," IEEE Computer, 2019.

[10] E. Bertino, "Data Protection Techniques," IEEE Computer Society, 2019.

[11] J. Smith, "Automated Trust Systems," Springer, 2020.

[12] A. Greenberg, "Cloud Privacy," Wired, 2020.

[13] K. Laudon, Management Information Systems, Pearson, 2021.

[14] T. Berners-Lee, "Information Management," IEEE Internet Computing, 2017.

[15] R. Rivest, "Cryptographic Protocols," MIT Press, 2018.