International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI: 10.55041/ISJEM03718
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

A SELF-RELIANT APPROACH TO SECURE DATA DELECTION IN CLOUD COMPUTING

Dr. N. Chandrakala[1], Miskin Naveen Kumar[2], Mangu Madhav[3], Mayani Prakash[4], P. Chandra Shekar Azad[5]

[1-5] *Department of CSE & TKR College of Engineering and Technology*
[1-5] *c B. Tech Students*

Abstract - With the rapid growth of cloud computing, ensuring data security and privacy remains a critical challenge. Traditional encryption techniques provide data confidentiality but fail to guarantee complete data removal when necessary. A secure data self-destructing scheme in cloud computing addresses this limitation by enabling the automatic and irreversible destruction of sensitive data after a predefined condition is met. This scheme ensures that both the encrypted data and the decryption keys become permanently inaccessible, preventing unauthorized access even if the cloud infrastructure is compromised.

The proposed scheme integrates time-based, policy-based, or event-driven mechanisms to trigger data self-destruction. By leveraging advanced cryptographic techniques such as ephemeral key management, attribute-based encryption, and secure key dispersion, the scheme ensures that no retrievable copies of the data or decryption keys remain after the self-destruction process. Additionally, block-chain and smart contracts can be incorporated to enhance transparency and verifiability, ensuring that the self-destruction process is executed as intended without external interference.

This approach significantly improves data privacy, compliance with data retention policies, and protection against insider and outsider threats. It is particularly beneficial for applications requiring strict confidentiality, such as military intelligence, financial transactions, and healthcare records. By implementing a secure data self-destructing scheme, cloud service users can have greater control over their sensitive information while mitigating risks associated with unauthorized data persistence.

Key Words: *Data Self-Destruction, Cloud Computing, Ephemeral Key Management, Attribute-Based Encryption, Block-chain.*

1. INTRODUCTION

Since cloud computing is expanding so quickly, people and businesses that store sensitive data on the cloud are increasingly concerned about data security and privacy. Although conventional encryption methods offer robust defense against unwanted access, they cannot ensure that data will be erased in the event that the encryption keys are stolen or purposefully revoked.

In many situations, users might need a system that guarantees data will be automatically and permanently destroyed after a predetermined amount of time or when certain requirements are fulfilled. Because of this requirement, secure data self-destructing schemes have been developed for cloud computing. These schemes seek to improve data privacy by making sure that data is rendered inaccessible without user intervention.

To prevent unauthorized retrieval or extended exposure of sensitive data, a secure data self-destructing scheme is made to automatically delete data or encryption keys after a predetermined amount of time or triggering event. In situations like time-limited access to private documents, safeguarding against data breaches, and adhering to data retention guidelines, this method is especially helpful. A number of methods have been put forth to accomplish this, such as self-destructive storage mechanisms, auto-expiring cryptographic schemes, and key revocation.

Security, usability, and efficiency must all be balanced when implementing a secure data self-destructing scheme in cloud computing. Self-destruction techniques improve security and privacy, but they must also cause the least amount of interference to authorized users and cloud service providers. Furthermore, issues like dependable trigger mechanisms, attack resistance, and integration with current cloud infrastructures need to be resolved. This study examines the basic ideas, current approaches, and difficulties related to secure data self-destructing schemes, emphasizing their significance in contemporary cloud computing settings.

2. MOTIVATION

Protecting sensitive data has become a top priority in an era where cloud computing has become the foundation of contemporary data access and storage. Although encryption protects the privacy of data, it does not automatically solve the problem of safely deleting data, which creates a serious flaw when data needs to be deleted forever. This restriction is particularly concerning when it comes to situations involving sensitive communications, regulatory compliance, and high-stakes industries like healthcare, finance, and defence.

The urgent need to give users more control over their data lifecycle—especially its irreversible deletion—is what inspired this project. A strong solution to this issue is offered by a secure data self-destructing scheme, which

makes sure that data and its decryption keys are rendered permanently unusable once specific requirements are fulfilled. This method removes all potential access points, even in hostile or compromised cloud environments, in contrast to traditional deletion, which might still leave data open to recovery.

This project intends to create a dependable and automated mechanism for data self-destruction by fusing condition-based triggers with cutting-edge cryptographic techniques. This enhances data security and privacy while also facilitating adherence to changing data protection laws. The project's ultimate goal is to increase confidence in cloud technologies by fixing one of their most enduring flaws, making sure that "deleted" actually means "gone forever."

3. PROBLEM DEFINATION

One of the biggest challenges in cloud computing is making sure that sensitive data is completely and permanently erased. While traditional encryption safeguards the confidentiality of data, it does not ensure that deleted data or its decryption keys are lost forever. This presents significant security risks, particularly in situations where strict adherence to confidentiality or compliance is required.

Existing cloud deletion techniques might leave backup copies or data fragments behind, leaving them open to illegal recovery. A secure self-destructing data scheme is required to solve this problem; it must guarantee that the data and keys are rendered inaccessible upon the fulfilment of a predetermined condition. The goal of this project is to create a system that uses trigger-based mechanisms and cryptographic techniques to guarantee complete and verifiable data erasure in the cloud.

4. OBJECTIVE

To create and put into place a safe data self-destructing system that, following a predetermined timeout, guarantees the permanent removal of private data kept in cloud environments.

To create a hybrid architecture that overcomes the drawbacks of both centralized and decentralized key management systems, combining the advantages of the Euhemerize and E-Ph-Pub models.

To use cryptographic methods for controlled key dispersion and secure data encryption, such as recursive secret sharing and AES encryption.

To employ time-based conditions to initiate the encryption keys' automatic destruction, which will make the related data permanently unreachable.

To integrate a safe, centralized Euhemerize for metadata management with a Distributed Hash Table (DHT) simulation for short-term key share storage.

To assess the suggested plan for scalability, security, dependability, and resilience to both internal and external threats.

5. SCOPE OF THE PROJECT

In order to comply with retention policies and protect data privacy in contemporary cloud computing environments, this project aims to design and implement a safe, hybrid data self-destruction scheme. The main goal is to create a system that, independent of the internal deletion techniques used by cloud service providers, automatically renders data inaccessible after a predetermined amount of time.

The suggested system uses a hybrid key management strategy that combines the decentralized (E-Ph.-Pub) and centralized (Euhemerize) paradigms. In the encryption key lifecycle, this integration improves resilience and reduces the possibility of single points of failure. By utilizing the advantages of both models—centralized control for policy enforcement and decentralized control for trust distribution and redundancy—it also improves the security of key distribution and expiration.

The scope of this project includes the following core components:

The Advanced Encryption Standard (AES), a symmetric encryption algorithm renowned for its security and performance, is used to encrypt sensitive data.

Recursive secret sharing, which divides the AES encryption keys and only permits the reconstruction of the original key when an adequate number of key shares are available.

Temporary key share storage in a Distributed Hash Table (DHT), which improves scalability and resistance to targeted attacks by allowing distributed, time-limited access without central control.

The system ensures that the reference metadata in the centralized system is erased and the key shares are automatically purged from the DHT after a predetermined timeout, rendering the encrypted data completely inaccessible. This conduct mimics the idea of data self-destruction, in which information is made unretrievable even if it is still physically stored in the cloud.

This method tackles the main drawbacks of traditional deletion, including key reuse or leakage, reliance on cloud vendors' opaque policies, and incomplete removal. A reliable and verifiable method for data expiration is provided by the cryptograph's enforcement of logical deletion.

The project is particularly pertinent to the following domains, among others, where stringent data confidentiality and timed data retention are necessary:

- Healthcare, for short-term patient record access.
- Defence and military, for restricted access to classified documents.
- Financial services, for audit trails or sensitive transaction logs.
- Cloud storage for businesses, in accordance with privacy laws such as GDPR and HIPAA.
- Healthcare, for short-term patient record access.
- Nonetheless, the following is expressly excluded from the scope: • Data destruction at the hardware or physical level (e.g., hardware shredding or secure disk wiping).
- Straightforward integration with native deletion APIs or SDKs from cloud providers (such as Azure Blob expiration policies or AWS S3 object lifecycle rules).

Rather, the project mimics a safe, platform-neutral logical deletion method that can be incorporated as a middleware or service element into more comprehensive cloud security frameworks.

In conclusion, this project uses distributed key management and hybrid cryptography techniques to create a safe, automated, and policy-driven framework for cloud data self-destruction, bridging the gap between encryption and data lifecycle enforcement.

6. LITERATURE REVIEW

In today's cloud-first digital environment, securing sensitive data has become more critical than ever. Cloud platforms, while offering flexibility and scalability, also pose challenges in ensuring data privacy and lifecycle control. One increasingly important solution is **self-destruction of data**, where information becomes inaccessible after a set period or trigger. Below, we survey a wide range of literature (Refs. [1][30]) that covers the evolution of cloud computing, data privacy concerns, and advanced self-destruction techniques.

Many early papers such as Wu et al. [1] and Hassan et al. [2] provide a foundational understanding of cloud computing services, pricing models, and challenges in integrating machine learning. These are crucial for grasping the broader context in which security solutions are developed.

Security-specific surveys like those by Shen et al. [9], [10] and Sosinsky [11] highlight the vulnerabilities of cloud platforms. The works of Bowden [8] and Gellman & Poitras [7] emphasize real-world risks through case studies involving surveillance and unauthorized access.

The conversation shifts with papers like Jayaprabha & Nadira Banu Kamal [21] and Kai Xiong et al. [22], which introduce innovative encryption-based approaches like **Key-Policy Time-Specified Attribute-Based Encryption (KP-TSABE)**. These systems automatically revoke access to cloud data after a pre-set expiration time, creating a digital "self-destruct" mechanism.

Other practical implementations, such as Vishali and Gandhi's AES/DES-based double encryption scheme [23], extend this concept by enabling self-destruction upon multiple failed access attempts. Similarly, schemes like **Sev-Del** [28] combine Intel SGX and blockchain for secure and verifiable data deletion, showing a trend toward **hardware-backed trust and decentralized verification**.

The **Vanish project** [30] provides a fascinating look into time-based key management, storing decryption keys in distributed hash tables that naturally expire, making data vanish without manual intervention.
These solutions not only preserve privacy but also ensure regulatory compliance for sensitive data (e.g., financial or healthcare data), especially in shared or distributed environments.

7. RESULT

The implementation of the proposed self-destructing data scheme in cloud computing has yielded several significant outcomes, particularly in enhancing data security and user autonomy. Firstly, confidential data protection was effectively achieved by encrypting sensitive information using the robust AES-256 algorithm before uploading it to the cloud. This ensured that even if unauthorized access occurred, the data would remain unintelligible without the corresponding decryption key. Secondly, the system enabled timed self-destruction of data by securely erasing the encryption keys after a pre-defined period. Once the keys were destroyed, the encrypted data became permanently inaccessible, thereby mitigating the risk of prolonged data exposure. Additionally, the scheme demonstrated ease of integration with existing cloud storage platforms, introducing minimal computational and performance overhead. This indicates that the solution can be deployed without significant changes to current cloud infrastructures. Lastly, the scheme offered enhanced user control over data lifecycle management. During the upload process, users could conveniently specify the data expiration time, allowing them to determine how long their data would remain accessible. Overall, the approach not only strengthens data confidentiality and integrity but also aligns with privacy-focused design principles by empowering users with greater control over their digital assets in the cloud environment.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI: 10.55041/ISJEM03718
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Fig -1 Home Screen

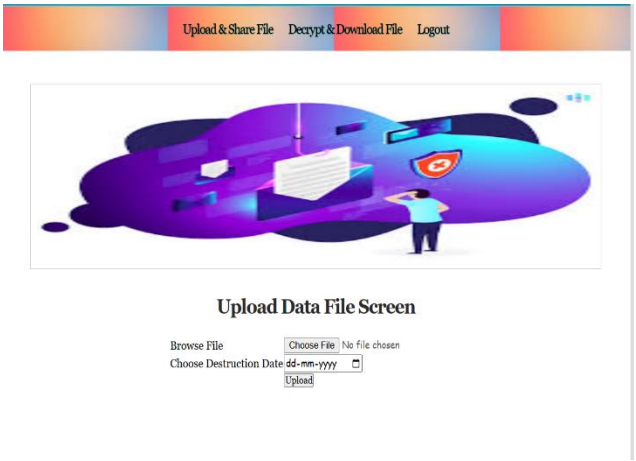

Fig -2 File Upload for Sharing and Deletion

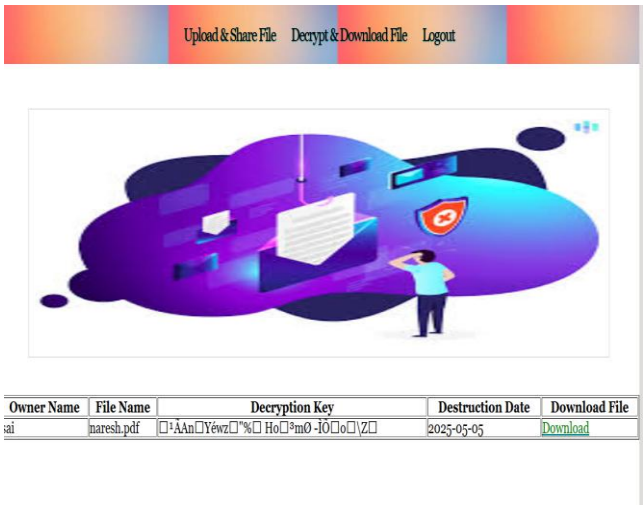

Fig -3 Decryption key and Deletion Time

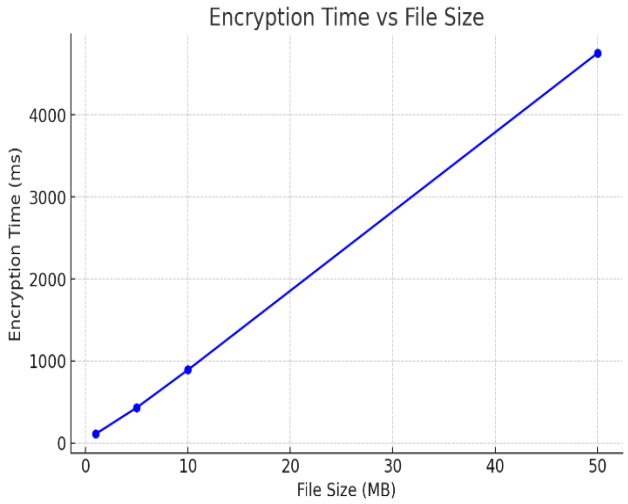

Fig -4 Encryption / Decryption Time

8. CONCLUSIONS

In cloud computing, a secure data self-destructing scheme is essential for guaranteeing data security, privacy, and regulatory compliance. Such a system gives data owners more control over their sensitive data by combining cryptographic techniques, time-based access control, and secure key management. The data and its encryption keys are automatically erased, making it unrecoverable, when the preset criteria are satisfied, such as time running out or unwanted access attempts. This strategy is especially helpful for sectors that handle sensitive data, like government, healthcare, and finance, where privacy laws and data retention guidelines must be closely followed.

Furthermore, by reducing the risks of data breaches and illegal access, a self-destructing scheme improves confidence in cloud services. Users are reassured that their data cannot be accessed after its intended lifespan, which lessens the dependency on cloud providers for data protection. There are still issues, though, such as striking a balance between security and usability, making sure that various cloud platforms work together, and guarding against hostile attempts to interfere with the self-destruction process. Future studies should concentrate on improving resilience against changing cyber threats, maximizing efficiency, and incorporating artificial intelligence for intelligent data lifecycle management. In the end, a well-thought-out self-destructing data scheme can greatly enhance the security and privacy of cloud computing.

REFERENCES

1. C. Wu, A. N. Toosi, R. Buyya, and K. Ramamohanarao, “Hedonic pricing of cloud computing services,” IEEE Trans. Cloud Compute., vol. 9, no. 1, pp. 182-196, Jan. 2021, doi: 10.1109/TCC.2018.2858266.
2. W. Hassan, T.-S. Chou, O. Tamer, J. Pickard, P. Appiah-Kubi, and L. Pagliari, “Cloud computing survey on services, enhancements and challenges in the era of machine learning and data science,” Int. J. Informatics Commun. Technol., vol. 9, no. 2, p. 117, Aug. 2020, doi: 10.11591/ijict.v9i2.pp117-139.
3. I. Odun-Ayo, O. Ajayi, B. Akanle, and R. Ahuja, “An overview of data storage in cloud computing,” in Proceedings - 2017 International Conference on Next Generation Computing and Information Systems,

ICNGCIS 2017, Nov. 2018, pp. 38–42, doi: 10.1109/ICNGCIS.2017.9.

4. J. Surbiryala and C. Rong, "Cloud computing: History and overview," in Proceedings - 2019 3rd IEEE International Conference on Cloud and Fog Computing Technologies and Applications, Cloud Summit 2019, Aug. 2019, pp. 1–7, doi: 10.1109/CloudSummit47114.2019.00007.
5. A. Elmorshidy, "Cloud computing: A new success model," in Proceedings - 2019 International Conference on Future Internet of Things and Cloud Workshops, Fi CloudW 2019, Aug. 2019, pp. 7–12, doi: 10.1109/FiCloudW.2019.00015.
6. K.-K. R. Choo, "Cloud computing: Challenges and future directions," Trends Issues Crime Criminal Justice, vol. 400, pp. 1–6, 2010.
7. B. Gellman and L. Poitras, "US, British intelligence mining data from nine US internet companies in broad secret program," Washington Post, vol. 6, no. 07, 2013, Art. no. 2013.
8. C. Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights, 2013 [Online]. Available:http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf
9. Z. Shen, L. Li, F. Yan, and X. Wu, "Cloud computing system based on trusted computing platform," in Proc. Int. Conf. Intell. Comput. Technol. Autom., 2010, pp. 942–945.
10. Z. Shen and Q. Tong, "The security of cloud computing system enabled by trusted computing technology," in Proc. 2nd Int. Conf. Signal Process. Syst., 2010, pp. V2-11–;V2-15.
11. Sosinsky, " Understanding Cloud Security ," Cloud Computing Bible Sosinsky/Cloud, 2011.
12. B. A. Forouzan, "Cryptography and Network Security," Tata McGraw Hill Education Private Limited, New York, 2010.
13. M. B. Mollah, et al., "Next generation of computing through cloud computing technology,"2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2012.
14. Thomas E., "Cloud Computing, Concepts, Technology & Architecture," Pearson Publication,2014.
15. M. A. Islam, et al., "A Modified and Secured RSA Public Key Cryptosystem Based on "n" Prime Numbers,"Journal of Computer and Communications, 2018.
16. N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud comput ing: A survey," Future Generation Comput. Syst., vol. 29, no. 1, pp. 84–106, 2013.
17. S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, "Cloudbased augmentation for mobile devices : motivation, taxon omies, and open challenges," IEEE Commun. Surveys Tutorials, vol. 16, no. 1, pp. 337–368, Jan.-Mar. 2014.
18. R. KumarandS. Rajalakshmi, "Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems," in Proc. Int. Conf. Comput. Sci. Appl., 2013, pp. 663–669.
19. J. Carolan, S. Gaede, J. Baty, G. Brunette, A. Licht, J. Remmell, L. Tucker, and J. Weise, "Introduction to cloud computing architecture," White Paper, 1st edn. Sun Micro Systems Inc, Santa Clara, CA, USA, 2009.
20. E. E. Marinelli, "Hyrax: Cloud Computing on Mobile Devices Using Mapreduce," DTIC Document, Fort Belvoir, VA, Tech. Rep. CMU-CS-09-164, 2009.
21. "A Secure Data Self-Destructing Scheme in Cloud Computing"
    Authors: M.S. Jayaprabha and Dr. A.R. Nadira Banu Kamal
    Overview: This paper introduces a scheme using Key-Policy Time-Specified Attribute-Based Encryption (KP-TSABE) to ensure that sensitive data stored in the cloud self-destructs after a user-defined expiration time, providing fine-grained access control during the authorization period.
22. "A Secure Data Self-Destructing Scheme in Cloud Computing"
    Authors: Kai Xiong, Kui Ren, and Pan Li
    Overview: The authors propose a novel self-destructing scheme based on attribute-based encryption, ensuring that data becomes inaccessible after a specified time, addressing challenges in cloud data privacy.
23. "An Implementation of Novel Secure Data Self-Destructing Scheme in Cloud Computing for Sharing Sensitive Data"
    Authors: Vishali D. and Dr. R. Indra Gandhi
    Overview: This paper presents a three-way self-destruction scheme using AES/DES double encryption, ensuring that sensitive data in the cloud self-destructs after a specified expiration time, allowing single-time access, and triggering self-destruction after multiple incorrect key entries.
24. "A Note on One Secure Data Self-Destructing Scheme in Cloud Computing"
    Authors: Shuai Han and Lei Hu
    Overview: The authors analyze a previously proposed self-destructing scheme , discussing its security aspects and potential improvements in the context of cloud computing.
25. "Survey on Secure Data Self-Destructing Scheme in Cloud Computing".
    Authors: M. Bhandari, Pooja Chaudhari, Sonal Sonawane, Bhagyashree Shetkar, and Manisha Konde
    Overview: This survey paper examines various self-destructing schemes in cloud computing, highlighting the challenges and solutions related to data security and privacy.
26. "Sharing Secure Data and Self-Destructing Scheme in Cloud"
    Authors: N. S. Joshi and MS. Joshi
    Overview: The paper proposes a scheme that combines secure data sharing with self-destruction capabilities, ensuring that data becomes inaccessible after a certain period, enhancing data privacy in the cloud.
27. "ATDD: Fine-Grained Assured Time-Sensitive Data Deletion Scheme in Cloud Storage"
    Authors: Zhengyu Yue, Yuanzhi Yao, Weihai Li, and Nenghai Yu
    Overview: This research introduces a fine-grained assured time-sensitive data deletion (ATDD) scheme, embedding time trapdoors in Cipher text-Policy Attribute-Based Encryption (CP-ABE) to ensure data self-destruction after a specified expiration time.
28. "Accelerating Secure and Verifiable Data Deletion in Cloud Storage via SGX and Block-chain" *Authors:* Xiangman Li and Jianbing Ni
    Overview: The authors present SevDel, a scheme leveraging Intel SGX and block-chain technology to achieve secure and verifiable data deletion in cloud storage, ensuring data owners can control the erasure of their data.
29. "Enhancing Data Security by Making Data Disappear in a P2P System"
    Author: Prashant Pilla
    Overview: This paper discusses a method to secure data by making it disappear after a set time limit in peer-to-peer systems, addressing the challenges of data privacy in distributed architectures.

30. "Vanish: Increasing Data Privacy with Self-Destructing Data"
Authors: Roxana Geambasu, Tadayoshi Kohno, Amit A. Levy, and Henry M. Levy
Overview: The Vanish project proposes a system where data self-destructs after a specified time, enhancing data privacy by making it irretrievable beyond its intended lifespan.