File Store Splitting

Kunal P. Gaikwad[1], Shreyash B. Patil[2], Rutuja R. Sahane[3], Yash N. Tilay[4], Prof. J Y. Kapadnis[5]

[1,2,3,4]Students, [5]Guide
Pune Vidyarthi Griha's College of Engineering & S S. Dhamankar Institute of Management, Nashik

Abstract: In cloud computing, outsourcing data to third-party services raises security concerns, as data can be compromised by attacks from other users or systems in the cloud. To address this, we need strong security measures, but these must also ensure fast data retrieval. This paper presents a method called DROPS (Division and Replication of Data in the Cloud for Optimal Performance and Security) that tackles both security and performance issues. In DROPS, we break a file into smaller pieces and store these pieces across different cloud nodes. Each node holds only one piece of a file, so even if a node is attacked, the attacker can't get the full information. We also spread these nodes far apart using a graph coloring technique, making it difficult for attackers to guess where the pieces are stored. DROPS does not rely on traditional encryption methods, which can be slow, making it faster. We show that it's very unlikely for an attacker to find and compromise all the nodes holding a file. Compared to other methods, DROPS provides better security with only a small performance impact.

***Keywords*: Data Security, Cloud Computing, Data Replication, Performance Optimization, Data Division, Graph Coloring, Distributed Storage, Attack Resistance**

INTRODUCTION

In today's world, many businesses store their data in the cloud, which means they rely on third-party services to keep their information safe. However, this comes with risks, as hackers can try to access sensitive data stored in these systems. To tackle these security concerns, we need effective methods that also ensure quick access to data. This paper introduces a new approach called DROPS (Division and Replication of Data in the Cloud for Optimal Performance and Security). DROPS works by breaking files into smaller pieces and storing these pieces across various cloud locations. Since each location only holds a part of the file, even if one is attacked, the attacker cannot access the entire file. Additionally, DROPS uses a technique called graph coloring to spread the storage locations far apart, making it harder for attackers to guess where the pieces are kept. Unlike traditional encryption methods that can slow down access, DROPS provides faster performance while significantly improving security. Overall, this method offers a reliable way to protect data in the cloud without compromising on speed.

LITERATURE SURVEY

Sr no	Title	Author	IEEE/ journal / conference years
1	Enhancing Mobile Cloud Security Using Audio Steganography	Younis A., Kifayat K., Merabti M,	International Journal of Engineering Research and Technology (IJERT) 2021
2	A Data Security In Cloud Computing Using Three-Factor Authentication	Nalajala S	International Conference on Communication, Computing and Electronics Systems 2020

3	Improving Cloud Security with Blockchain	Singh S., Jeong Y., Park JH	Advanced in Artificial Intelligence and Cloud Computing 2021.
4	Cybersecurity In Cloud Computing for Higher Education Institutions	Grance W.J.	IEEE ACCESS 2017

METHODOLOGY

The algorithm in which every operation is uniquely defined is called deterministic algorithms.The algorithm in which every operation may not have unique result, rather there can be specified set of possibilities for every operation, such algorithms are called Non deterministic algorithms. Non deterministic means no particular rule is followed to make guess

- **P Class:-**This group consists of all algorithms whose computing times are polynomial time that is there computing time is bounded by polynomials of small degree. Eg. insertion sort, merge sort, quick sort have polynomial computing time.
- **NP Class:-**This group consists of all algorithms whose computing time are non- deterministic polynomial time. Eg. Traveling salesman problem.

The NP class problem can be classified into two groups:

(a) **NP Hard Problems:**

Normally optimization problems are NP-Hard problems. All NP complete prob-lems are NP hard but some NP hard are not NP complete. A problem is NP hard if and only if its at least as hard as NP complete problem.

(b) **NP complete problems::**

Normally decision problems are NP-Complete problems. Non deterministic poly-nomial time complete problems. Decision Problems: Any problem having the answer either zero or one is called decision problem.

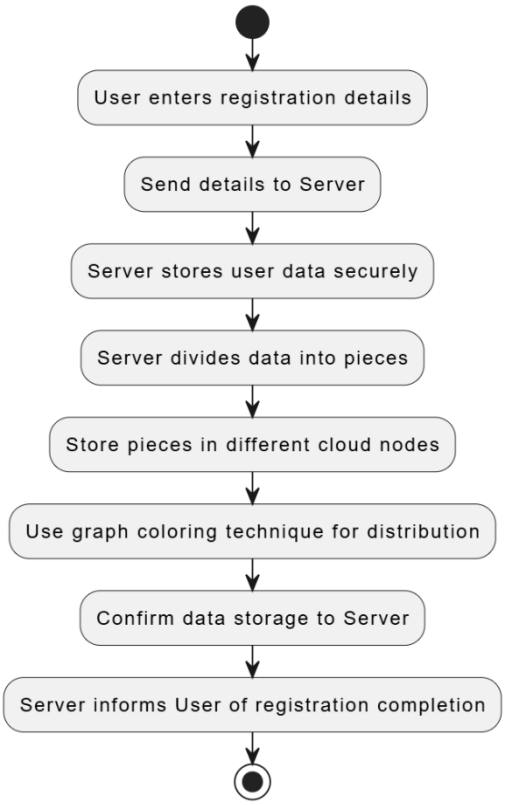
PROBLEM STATEMENT

As businesses increasingly move their data to cloud services, they face significant security risks. Storing sensitive information with third-party providers can make it vulnerable to cyberattacks, where hackers might try to access and steal this data. Traditional security measures, such as encryption, often slow down data retrieval, leading to performance issues for users who need quick access to their files. There is a pressing need for a solution that not only protects data from unauthorized access but also ensures that users can retrieve their information quickly and efficiently. The challenge lies in finding a way to securely store data in the cloud without compromising on performance, making it essential to develop innovative methods that effectively address both of these concerns.

OBJECTIVE

1. To enhance data security by breaking files into smaller pieces and distributing them across multiple cloud nodes, reducing the risk of unauthorized access.
2. To improve performance by enabling faster data retrieval without relying solely on traditional encryption methods that can slow down access.
3. To utilize graph coloring techniques for strategically placing data pieces far apart, making it difficult for attackers to locate and compromise all parts of a file.
4. To provide a reliable solution for organizations that need to protect sensitive information in the cloud while ensuring seamless access for authorized users.

FLOW CHART



DESIGNS

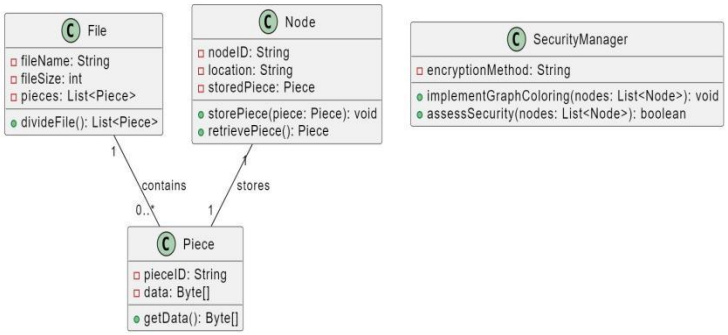


Fig: Class diagram

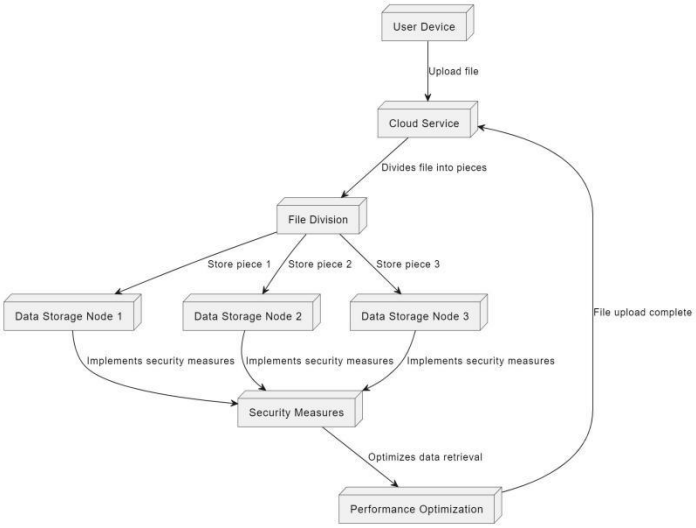


Fig: Development diagram

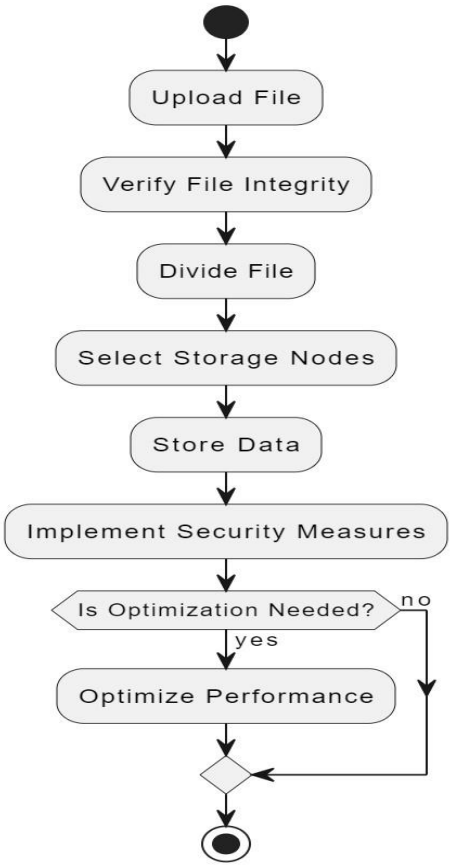


Fig: Activity diagram

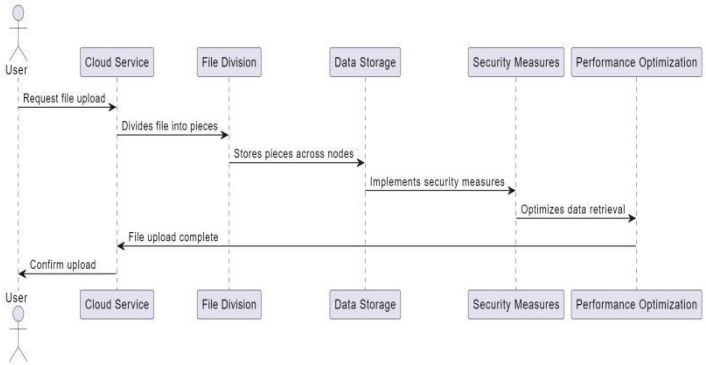


Fig: Sequence diagram

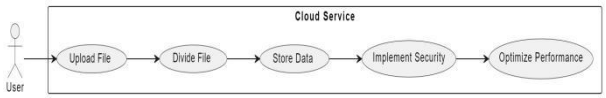


Fig: Use case diagram

FUCTIONAL REQUIREMENTS

- File Division: The system should divide files into smaller, manageable pieces before storing them in the cloud.
- Data Distribution: The system must distribute file pieces across different cloud nodes using graph coloring to ensure security.
- Replication Management: The system should manage data replication for each piece to ensure data availability and fault tolerance.

- Data Retrieval: The system should quickly retrieve and reassemble data pieces to reconstruct the original file when a user requests it.
- User Authentication: Only authorized users should be able to upload, retrieve, and manage files in the system.
- Monitoring and Logging: The system should log access events and monitor for potential security threats.
- Integrity Verification: The system should verify the integrity of data pieces during retrieval to ensure accuracy.

NON FUCTIONAL REQUIREMENTS

- Performance: The system should provide fast data retrieval, with minimal delays compared to traditional encryption methods.
- Scalability: The system should be scalable to handle large volumes of data and many users.
- Reliability: The system should ensure high reliability, with minimal downtime, and should manage data redundancy to prevent loss.
- Security: The system should ensure strong data security by effectively distributing and isolating data pieces across nodes.
- Availability: The system should guarantee high availability, allowing users to access their data at any time.
- Usability: The system interface should be user-friendly to ensure that users can easily upload, retrieve, and manage their files.
- Fault Tolerance: The system should maintain functionality even if one or more nodes fail or are attacked.
- Compliance: The system should comply with data security and privacy regulations, such as GDPR or CCPA, as required.
- Maintainability: The system should be designed for easy maintenance and updates.

CONCLUSION

In conclusion, the DROPS system offers a promising solution for enhancing both data security and retrieval speed in cloud computing. By dividing files into smaller pieces and storing them across different locations, DROPS protects sensitive information from unauthorized access while ensuring that users can quickly access their data when needed. The use of graph coloring techniques makes it difficult for attackers to locate all parts of a file, adding an extra layer of security. Additionally, with realtime monitoring of potential threats, the system ensures that data remains safe and secure. Overall, DROPS addresses the critical challenges of cloud storage, providing a balanced approach that prioritizes security without sacrificing performance.

REFERENCES

[1] A. Younis, K. Kifayat, and M. Merabti, ”Enhancing Mobile Cloud Security Using Audio Steganography,” International Journal of Information Security and Privacy (IJISP), vol. 5, no. 2, pp. 78-89, 2021.

[2] S. Nalajala, A. Kaleem, P. Kumar, and R. Ramesh, ”Data Security in Cloud Computing Using Three-Factor Authentication,” in Proceedings of the 2015 International Conference on Cloud Computing and Virtualization (CCV), Chennai, India, 2020, pp. 115-120.

[3] S. Singh, Y. Jeong, and J. H. Park, ”Improving Cloud Security with Blockchain,” Future Generation Computer Systems, vol. 86, pp. 527538, Sept. 2021.

[4] W. J. Grance, R. Dempsey, and K. Kent, ”Cybersecurity in Cloud Computing for Higher Education Institutions,” in Proceedings of the 2014 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Singapore, 2017, pp. 211-218.