Rajarambapu Institute of Technology, Rajaramnagar

Department of Computer Science and Engineering

Project Synopsis

Area of the Project	Cloud Computing & Cloud Storage Security
Title of the project	CloudVault
Project Guide Name	Prof. Dipali.I.Ghadage
Team Leader's Name	Harshal Prabhakar Gavali
Group Number	*G2*

Members

Sr.	Roll No.	Name	Email	Phone
1	2003040	Harshal Gavali	2003040@ritinida.edu	9890487922
2	2003042	Adharva kumar	2003042@ritinida.edu	8007441617
3	2003044	Gourav Powar	2003044@ritinida.edu	7038686237
4	2003046	Rohan Chinchkar	2003046@ritindia.edu	9527847044

Prof. Dipali.I.Ghadage

Project Guide

Dr. N. V. Dharwadkar

Head of department

Introduction and Motivation

As data generation and storage needs have increased rapidly, cloud storage has become a popular solution for businesses and individuals alike. With cloud storage, data can be stored, accessed, and managed easily and securely, offering many benefits over traditional storage methods. Cloud storage is scalable, cost-effective, and accessible from anywhere with an internet connection. However, storing data remotely also poses several security risks, such as unauthorized access, data breaches, and data loss.

To address these risks, it is essential to implement enhanced security measures to protect user data stored in the cloud. The purpose of this project is to develop a cloud storage platform that is free and provides robust security measures to safeguard user data. The platform will be developed using Java, Spring Framework, Spring Boot, REST API, Apache Tomcat Server, MySQL, and AWS.

The Java programming language is widely used for building cloud-based applications due to its scalability and platform independence. The Spring Framework is an open-source application framework that provides a comprehensive programming and configuration model for modern Java-based enterprise applications. Spring Boot is an extension of the Spring Framework that simplifies the process of building production-ready applications by providing auto-configuration and other useful features out of the box.

REST (Representational State Transfer) is a web-based software architectural style that provides a standard for creating APIs (Application Programming Interfaces). REST APIs allow different software applications to communicate with each other using HTTP (Hypertext Transfer Protocol) requests and responses. This makes it easier to develop, maintain, and scale cloud-based applications.

Apache Tomcat Server is an open-source Java Servlet Container that is used to run Java web applications. It provides a robust and scalable environment for running Java applications in the cloud. MySQL is an open-source relational database management system that is widely used in web applications. It provides a secure and reliable way to store and manage data in the cloud.

AWS (Amazon Web Services) is a cloud computing platform that provides a range of services, including compute, storage, and databases. AWS is widely used by businesses and individuals for hosting and managing web applications, including cloud storage platforms.

The cloud storage platform developed in this project will include several security measures to protect user data. These measures include:

Encryption: All user data stored in the cloud will be encrypted using industry-standard encryption algorithms to prevent unauthorized access.

Access Control: Access to user data will be restricted based on user roles and permissions. Users will only be able to access data that they are authorized to access.

Data Backup: Regular backups of user data will be performed to ensure that data is not lost in the event of a data breach or system failure.

Monitoring and Logging: The cloud storage platform will be monitored and logged to detect any unauthorized access attempts or suspicious activity.

Multi-Factor Authentication: Users will be required to authenticate themselves using multiple factors, such as a password and a security token, to prevent unauthorized access to their data.
Network Security: The cloud storage platform will be hosted on a secure network with firewalls and other security measures to prevent unauthorized access.

The cloud storage platform will be free, making it accessible to individuals and small businesses who may not have the resources to pay for expensive cloud storage solutions. The platform will also be scalable, allowing users to increase their storage capacity as their needs grow.

Literature Survey

In this research paper, the focus is on data security and privacy protection for cloud storage. The research undertaken includes one-to-many encryption, data integrity, data deletion, leakage-resilient, and privacy-preserving solutions. The technologies used in this research include identity-based encryption, attribute-based encryption, homomorphic encryption, and searchable encryption. Solutions are implemented through privacy-preserving and machine learning in the cloud and post-quantum encryption. The results of this research introduce the encryption principles of IBE, ABE, homomorphic encryption, searchable encryption, and the research direction of new encryption models. The future scope of research includes exploring data encryption technologies and protection methods that correspond to the mentioned security requirements.

The Key-Aggregate Cryptosystem is a crucial framework for scalable data sharing in cloud storage, providing efficient and flexible key delegation for different ciphertext classes. This research involves the implementation of cryptographic keys for a predefined hierarchy and a compact key in symmetric-key and identity-based encryption, including the frameworks of KeyGen, Encrypt, Extract, and Decrypt, and sharing encrypted data. The Public-Key Extension technique is used to compress secret keys in public-key cryptosystems, enabling delegation of secret keys for various ciphertext classes. The results of this study demonstrate how to compress secret keys efficiently while supporting key delegation in cloud storage. The future scope of this research involves designing a leakage-resilient cryptosystem that allows efficient and flexible key delegation, further enhancing the security and scalability of cloud storage.

Achieving secure role-based access control on encrypted data in cloud storage is crucial for ensuring data confidentiality and integrity. To achieve this, the research involves role-based encryption systems and the use of bilinear pairings. The construction of the role-based encryption schema is carried out using setup, extract, manage role, add user, encrypt, decrypt, and revoke user operations. The implementation involves architectural components and system operations. The results of this research demonstrate that encryption and decryption computations are efficient on the client-side, and decryption time at the cloud can be reduced by having multiple processors, which is common in a cloud environment. This research has significant future scope in commercial situations as it captures practical access policies based on roles in a flexible manner and provides secure data storage in the cloud.

The cost-effective dynamic replication management scheme is crucial for improving the performance of cloud storage clusters while maintaining availability, load balance, and stability. The research involves Cloud Storage, Data Replication, Replica Placement, Cost-Effectiveness, and Dynamic Replication Management. The technology used includes the system model, availability, blocking probability, and implementation in HDFS, with control strategies to achieve load balance. The results of this research demonstrate that CDRM places replicas among cloud nodes to minimize blocking probability, improving load balance and overall performance. The future scope of this research involves maintaining a rational number of replicas that not only satisfy availability but also improve access latency, load balance, and keep the entire storage system stable, making it a cost-effective solution for cloud storage clusters.

Privacy-preserving public auditing is crucial for ensuring secure cloud storage. The research involves the system and threat model, design goals, and technology used, including a MAC-based solution, privacy-preserving public auditing scheme, security guarantee for batch auditing, and the cost of privacy-preserving protocol. The implementation involves support for batch auditing, TPA, cloud server, storage correctness guarantee, and generalization. The results of this research demonstrate that privacy-preserving public auditing not only eliminates the burden of cloud users from the tedious and possibly expensive auditing task but also alleviates users' fear of their outsourced data leakage. The future scope of this research is to extend the privacy-preserving public auditing protocol into a multi-user setting where the TPA can perform multiple auditing tasks in a batch manner for better efficiency, making it more effective in ensuring secure cloud storage.

The research involves combining data owner-side and cloud-side access control for encrypted cloud storage using various technologies such as ciphertext-policy attribute-based encryption, authenticated encryption with associated data, digital signature, hybrid encryption for CP-ABE, bloom filter, and building systems against covert adversaries. The implementation involves partially outsourced protocol (POP), fully outsourced protocol (FOP), and security against EDoS attacks. The results show that Bloom filter and probabilistic check in the resource consumption accounting help to reduce overhead. Performance analysis indicates that the overhead of this construction is small over existing systems. The future scope of this research is to further improve the efficiency of the proposed approach and explore other security measures to enhance the security of encrypted cloud storage.

The research focuses on enabling cloud storage auditing with key-exposure resistance and involves defining the system model and security model. The technology used includes the naive approach and cloud storage auditing with key-exposure resilience. Implementation involves supporting the TPA, lazy update, and multiple sectors. The proposed protocol is designed to provide key-exposure resistance, and the security proof and asymptotic performance evaluation show that it is secure and efficient.

The research paper focuses on developing a dual-server public-key encryption with keyword search (DS-PEKS) for secure cloud storage. The study includes the implementation of various key generation, encryption and security models such as SPHFSetup, HashKG, ProjKG, Hash, ProjHash, and linear and homomorphic SPHFs. The goal is to prevent the inside keyword guessing attack, which is an inherent vulnerability of the traditional PEKS framework. The proposed DS-PEKS scheme is designed to offer semantic security against chosen keyword attack and indistinguishability against keyword guessing attack. The study presents a smooth projective hash function (SPHF), which enables efficient DS-PEKS without pairings. The future scope of the research is to develop an efficient instantiation of the new SPHF based on the Diffie-Hellman problem.

Cloud storage has become an increasingly popular solution for storing and managing data. Cloud storage providers offer various benefits, such as easy accessibility, scalability, and cost-effectiveness. However, data security concerns remain a significant challenge for cloud storage solutions. Several studies have investigated various security issues associated with cloud storage, such as data privacy, data integrity, data availability, and data confidentiality.

To address these challenges, several security measures have been proposed, including data encryption, access control mechanisms, and authentication mechanisms. Data encryption is a common technique used to protect data in transit and at rest. Access control mechanisms are used to ensure that only authorized users can access data. Authentication mechanisms are used to verify the identity of users before granting access to data.

Problem Statement

❖ Develop a high storage cloud platform that provides enhanced security measures to protect user data while maintaining the confidentiality, integrity, and availability of their data.

Objectives

❖Develop a high storage cloud architecture.

❖Implement effective authentication mechanisms.

❖Implement robust data encryption techniques to protect user data both in transit and at rest.

❖Ensure the confidentiality, integrity, and availability of user data.

Scope

❖ The scope of this project includes developing a cloud storage platform using Java, Spring Framework, Spring Boot, REST API, Apache Tomcat Server, MySQL, and AWS.

❖ The platform will be designed to store data and provide users with easy access to their data.

❖ The platform will also include enhanced security measures, such as data encryption, access control mechanisms, and authentication mechanisms.

Limitations

❖The project will not include redundancy and failover mechanisms to ensure business continuity in case of hardware or software failures.

Proposed Methodology

Define the requirements and specifications of the cloud architecture, including the amount of storage needed, the expected volume of user data, and the scalability of the system. Choose a cloud service provider, such as AWS, and set up an account and environment. Set up and configure the necessary infrastructure components, such as virtual machines, storage solutions, and network architecture. Develop and deploy the cloud-based application using Java, Spring Framework, and Spring Boot, which provide a scalable and flexible architecture that can handle large volumes of user data.

Implement user authentication using REST API and Spring Security, which provides a robust and secure authentication framework. Configure access controls to restrict access to sensitive data and resources, using role-based access control (RBAC) or attribute-based access control (ABAC). Set up SSL/TLS encryption to secure data in transit, ensuring that sensitive information remains secure from eavesdropping and man-in-the-middle attacks. Implement two-factor authentication (2FA) for additional security, requiring users to provide a second form of authentication, such as a one-time password (OTP), in addition to their login credentials.

Use industry-standard encryption algorithms, such as AES and RSA, to encrypt user data both in transit and at rest, ensuring that sensitive information is protected from unauthorized access. Implement encryption key management solutions to securely store and manage encryption keys, ensuring that only authorized users can access sensitive data. Use secure protocols, such as HTTPS, to encrypt data in transit, protecting against eavesdropping and man-in-the-middle attacks. Use data masking techniques to protect sensitive data, such as credit card numbers and social security numbers, from unauthorized access.

Implement backup and disaster recovery procedures to ensure that user data is backed up and can be restored in case of an outage or data loss. Use automated security testing tools, such as OWASP ZAP, to identify vulnerabilities in the system and take remedial action to address any issues found. Monitor the system logs and alerts to detect and respond to security incidents promptly. Implement security policies and procedures to ensure that all users are aware of the security requirements and follow best practices for securing their data.

Time Frame of Schedule

The development of the cloud storage and cloud security project will take approximately six months. The following is a tentative schedule for the project:
Month 1: Planning phase
Month 2: Designing phase
Month 3-4: Developing phase
Month 5: Testing phase
Month 6: Deployment and maintenance

References & Bibliography

1. Yang, Pan, Naixue Xiong, and Jingli Ren. "Data security and privacy protection for cloud storage: A survey." IEEE Access 8 (2020): 131723-131740.

2. Chu, Cheng-Kang, et al. "Key-aggregate cryptosystem for scalable data sharing in cloud storage." IEEE transactions on parallel and distributed systems 25.2 (2013): 468-477.

3. Zhou, Lan, Vijay Varadharajan, and Michael Hitchens. "Achieving secure role-based access control on encrypted data in cloud storage." IEEE transactions on information forensics and security 8.12 (2013): 1947-1960.

4. Wei, Qingsong, et al. "CDRM: A cost-effective dynamic replication management scheme for cloud storage cluster." 2010 IEEE international conference on cluster computing. IEEE, 2010.

5. Wang, Cong, et al. "Privacy-preserving public auditing for secure cloud storage." IEEE transactions on computers 62.2 (2011): 362-375.

6. Xue, Kaiping, et al. "Combining data owner-side and cloud-side access control for encrypted cloud storage." IEEE Transactions on Information Forensics and Security 13.8 (2018): 2062-2074.

7. Yu, Jia, et al. "Enabling cloud storage auditing with key-exposure resistance." IEEE Transactions on Information forensics and security 10.6 (2015): 1167-1179.

8. Chen, Rongmao, et al. "Dual-server public-key encryption with keyword search for secure cloud storage." IEEE transactions on information forensics and security 11.4 (2015): 789-798.