Revolutionizing Cloud Data Security with Elliptic Curve Cryptography

ABSTRACT:

In the era of cloud computing, ensuring data security and efficient data retrieval is paramount. "Efficient Traceable Authorization Search System Cloud Storage" addresses these concerns by implementing a robust authorization mechanism that allows only authorized users to perform searches on cloud-stored data. Authorized users are distinguished into two categories: role-based users, such as data owners and their delegates and attribute-based users, such as specific departments within an organization. The project emphasizes the use of advanced cryptographic techniques to enhance data security within cloud storage environments. Existing systems primarily use RSA cryptography, which has notable limitations in security and efficiency. To overcome these challenges, we propose the integration of Elliptic Curve Cryptography (ECC). ECC stands out due to its superior security features and efficiency in data search operations. ECC not only provides higher security with smaller key sizes compared to RSA algorithm but also supports automatic updating of audit logs, enhancing overall system integrity. By employing ECC, system ensures heightened security for cloud-stored data without compromising confidentiality. This approach facilitates security, efficiency, and authorized data searches, addressing current security gaps and advancing the field of cloud data management.

Keywords: Authorization Search, Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Cryptography, Elliptic Curve Cryptography (ECC).

STATEMENT ABOUT THE PROBLEM

In the era of cloud computing, ensuring data security and efficient data retrieval is critical, yet current systems relying on RSA cryptography face significant challenges due to its large key sizes and inefficiencies in handling encrypted data. This results in compromised security and sluggish performance, particularly in data search operations. To address these issues, the **" Revolutionizing Cloud Data Security with Elliptic Curve Cryptography"** proposes integrating **Elliptic Curve Cryptography (ECC)**, which offers enhanced security with smaller key sizes and superior efficiency. This system will implement advanced role-based and attribute-based authorization

mechanisms to ensure only authorized users can access and search data. Additionally, it will support automatic updating of audit logs to bolster system integrity and traceability, thus advancing cloud data management by addressing current security and performance gaps.

WHY IS THE PARTICULAR TOPIC CHOSEN?

The topic **" Revolutionizing Cloud Data Security with Elliptic Curve Cryptography "** was chosen due to the pressing need to enhance data security and retrieval efficiency in cloud computing environments, where traditional RSA cryptography's limitations in scalability and performance are increasingly problematic. As cloud systems evolve and handle vast amounts of sensitive data, RSA's larger key sizes and slower operations can hinder effective data management and security. By integrating **Elliptic Curve Cryptography (ECC)**, known for its superior security with smaller key sizes and better performance, this topic addresses both the inefficiencies and security concerns of existing systems. The focus on implementing advanced authorization mechanisms and automatic audit log updates aims to offer a more robust, scalable, and traceable solution, ultimately advancing cloud data management practices.

SCOPE:

The scope of the **" Revolutionizing Cloud Data Security with Elliptic Curve Cryptography "** encompasses the development and implementation of a secure cloud storage system that integrates **Elliptic Curve Cryptography (ECC)** to overcome the limitations of traditional RSA cryptography. This system will focus on enhancing data security and efficiency through advanced role-based and attribute-based authorization mechanisms, ensuring that only authorized users can perform searches and access data. Additionally, it will incorporate automatic audit log updates to maintain comprehensive traceability and system integrity. By addressing both the cryptographic and authorization challenges in current cloud storage solutions, this project aims to provide a more secure, efficient, and reliable framework for managing and retrieving cloud-stored data.

OBJECTIVE OF THE PROJECT:

The objective of the **" Revolutionizing Cloud Data Security with Elliptic Curve Cryptography "** is to develop a cutting-edge cloud storage solution that leverages **Elliptic Curve Cryptography (ECC)** to enhance data security and operational efficiency. This system aims to implement

advanced role-based and attribute-based authorization mechanisms to ensure precise access control and secure search capabilities for authorized users. Additionally, it seeks to integrate automatic audit log updates to provide robust traceability and maintain system integrity. By addressing the limitations of traditional RSA cryptography, this project intends to deliver a more scalable, efficient, and secure cloud storage framework, advancing the state of cloud data management.

EXISTING METHOD

Existing methods in cloud storage primarily rely on **RSA cryptography** for securing data and managing access. RSA, while historically significant, is characterized by its large key sizes and computationally intensive operations, which can lead to inefficiencies, particularly in handling encrypted data and performing search operations. Traditional cloud storage systems often utilize basic role-based and attribute-based access control mechanisms but lack advanced features for managing fine-grained permissions and secure, efficient searches. Additionally, these systems may not support automatic audit log updates, resulting in less effective traceability and system integrity. As a result, there is a growing need for more efficient and secure cryptographic solutions that address these limitations and enhance overall cloud data management.

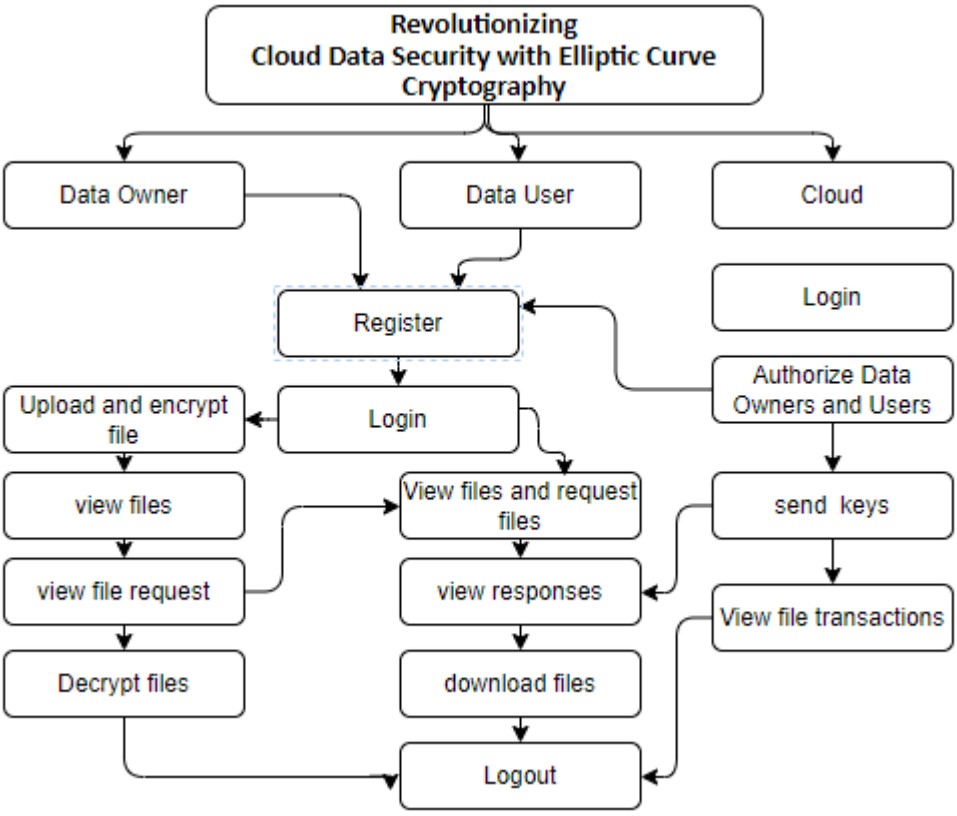
DISADVANTAGES

1. **Large Key Sizes:** RSA requires long keys, which make encryption and decryption slower and more resource-intensive.
2. **Performance Issues:** The large key sizes lead to slower data retrieval and search operations.
3. **Scalability Problems:** As data grows, RSA's performance issues become more pronounced, affecting system efficiency.
4. **Lower Security Efficiency:** RSA's security relies on larger keys, which can be less efficient compared to newer cryptographic methods.
5. **Limited Access Control:** Traditional systems may lack advanced features for fine-grained access control and efficient search capabilities.
6. **Manual Audit Logging:** Existing systems may not automatically update audit logs, reducing traceability and integrity.

PROPOSED SYSTEM:

The proposed system, **" Revolutionizing Cloud Data Security with Elliptic Curve Cryptography, "** aims to enhance cloud data security and efficiency by integrating **Elliptic Curve Cryptography (ECC)**. ECC offers superior security with smaller key sizes compared to RSA, resulting in faster encryption and decryption processes. This system will implement advanced role-based and attribute-based authorization mechanisms to ensure precise and secure access control for different user types. Additionally, it will incorporate automatic audit log updates to improve traceability and maintain system integrity. By addressing the limitations of traditional RSA-based systems, the proposed solution will deliver a more scalable, efficient, and secure cloud storage framework, optimizing both data security and retrieval performance.

PROJECT FLOW:



ADVANTAGES:

1. **Smaller Key Sizes:** Elliptic Curve Cryptography (ECC) uses smaller keys for the same level of security, which enhances performance and reduces the computational load during encryption and decryption.
2. **Improved Performance:** The efficiency of ECC results in faster data retrieval and search operations, addressing RSA's performance issues.
3. **Better Scalability:** ECC's smaller key sizes and efficient processing support better scalability, allowing the system to handle large volumes of data more effectively.
4. **Enhanced Security Efficiency:** ECC provides superior security with smaller keys, improving both the speed and security of cryptographic operations compared to RSA.
5. **Advanced Access Control:** The proposed system includes advanced role-based and attribute-based access controls, offering more precise and secure management of user permissions.

SOFTWARE FRONT END REQUIREMENTS

H/W CONFIGURATION:

Processor	- I3/Intel Processor
Hard Disk	- 160GB
Key Board	- Standard Windows Keyboard
Mouse	- Two or Three Button Mouse
Monitor	- SVGA
RAM	- 8GB

S/W CONFIGURATION:

- Operating System : Windows 7/8/10
- Server side Script : HTML, CSS, Bootstrap & JS
- Programming Language : Python
- Libraries : Flask/Django, Pandas, Mysql, Smtplib, Numpy
- IDE/Workbench : PyCharm/VSCode
- Technology : Python 3.6+

MODULES/IMPLEMENTATION

Modules:

Data Owner:

Register: Data owner can register into website by entering details.

Login: He can login into website by entering their credentials.(after admin authorized)

upload files: Here he can upload their files into website and he can encrypt that file using ECC.

view files: here he can view their files.

view file request: Here Owner can view his file requests and decrypt the file.

Data User:

Register: Data user can register into website by entering details.

Login: He can login into website by entering their credentials.(after admin authorized)

view files : He can view the file and send a file request to data owner.

view response: here he can view the requested file response.

download file: he can download the file by using the key.

Cloud:

Login: He can login into website by entering their credentials.

view and authorize data owners: here admin can view the registered data owners and he can authorize and unauthorize the data owners.

view and authorize data users: here admin can view the registered data users and he can authorize and unauthorize the data users.

send key: Here admin can send a key through email for downloading the file.

view file transactions: here user can view the file transactions.

Logout: All can logout after completion of their operations.