International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04| Apr -2016 www.irjet.net p-ISSN: 2395-0072

PRESERVING SECURITY IN CLOUD COMPUTING USING IDENTITY BASED ENCRYPTION WITH KEY REVOCATION PROCESS

R.Priyanka[1], R.Balapriya[2], S.Santhiya Devi[3], R.Sanjana[4], Mrs.G.Sumalatha[5]

B.Tech (IT)-Final Year Students[1234], V.R.S college of engineering &technology,

Guide[5], Assistant professor, Information technology,

Arasur-607 107, Villupuram Dt TN,

Abstract: The main aim of the project is to provide utility to maintain day to day operations of cloud computing security. This project helps them to store files in cloud and revoke them in a secure manner. Cloud Computing security is the major concept of cloud server. Files are stored in a cloud with encryption. The existing system based on identity based encryption with decryption. To propose the system for identity based encryption with outsourced revocation in cloud computing. Identity based Encryption means with use of some identity value to store and retrieve files from the cloud server. This system fully focuses on the encryption with outsourced revocation. User can get the service from the service provider after that can upload the files to the corresponding cloud server. PKG (Private Key Generator) is the process to generate private key to the user and cloud server. Cloud server having KU-CSP (Key Update - Cloud Service Provider). PKG to send the outsource key to the CSP. CSP can provide the updated key to the user. When the file revocation process the private key and updated key to be combined and verify to the user after that the file can be downloaded from the cloud server. File Revocation is the process to outsource the data from one server to another server. When the revocation process the revocation request can be send to the server and after that the private key and updated key combine with matching and revocation the file. After the completion of file revocation it can be downloaded from the corresponding server. Key Update cloud service provider can update the key for the outsource the date to the user to cloud service provider. Before store the files into the server it can be verify, encrypt and re encrypt the file after that stored into cloud server.

1. INTRODUCTION

The main objective of this project to provide the better service to the cloud user with file security. Mainly used to develop a better communication between the user and the cloud service provider. User can get the cloud request and upload the files with encryption and re encryption format. When the outsourcing process the particular user can send the file revocation request to the cloud server. After the completion of revocation request it should be combine the process with private key and updated key. PKG (private key generator) can generate the private key and send to the user and KU-CSP (key update cloud service provider). Cloud can send the updated Key to the user when the file revocation process. Finally the files are downloaded from the server with combine key process.

2. EXISTING SYSTEM

In Existing system the cloud server files are not having security. Because files are stored into the server with identity based encryption techniques.

While the file retrieves process it can be make the Decryption with public key and private key to download the files from the cloud. Nowadays The cloud computing files security is the major problem to manage and secure the files. To solve this problem now they are looking for better alternative solution.

Disadvantages

Very difficult to maintain all the data in a secure manner. Public key can know any other person easily. Many files are missing because unauthorized person can retrieve the files from the server. Existing System Files are corrupted in some time. User cannot outsource the files from one server to another cloud server in a secure manner.

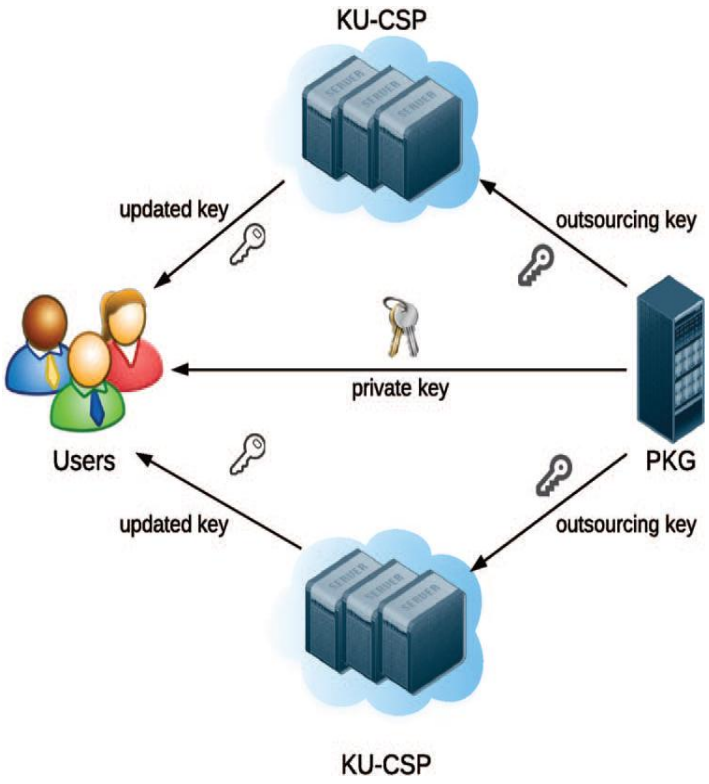

Fig 1: Existing Architecture diagram

3. PROPOSED SYSTEM:

To propose the system can using key update cloud service provider with private key generator and combine key process. User can upload the files to the server with encryption and re encryption. When the file revocation process the private key and updated key send to the user. With use combine key process to match the keys and retrieve the files from the server. The proposed system provide the better solution to the file security

Advantages:

1. Easy to make file revocation.

2. Easy to usage and time saving.

3. Cloud user needs to be solved by a better manner and better compatibility.

4. Combine key process help to retrieve files from the server.

5. Proposed system used to enhance file security.

4. SCOPE OF THE PROJECT:

The scope of the project is to solve the user needs and provide the service to the cloud user. And also secure the cloud files with use of combine key process. User files are retrieve from the cloud in a secure manner.

Proposed architecture diagram:

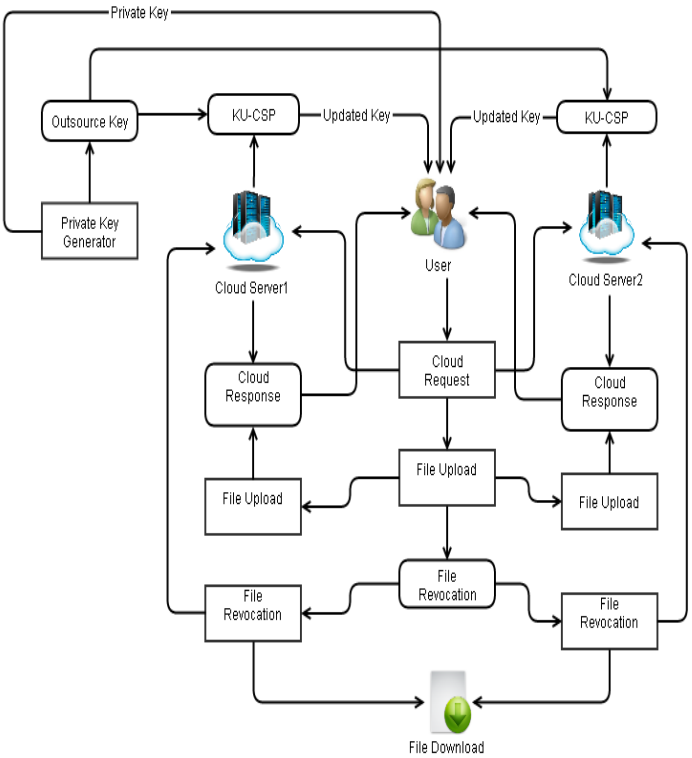

Fig 2: Proposed system architecture diagram

5. TECHNIQUES OR ALGORITHMS:

Proposed Technique:

Identity Based Encryption Scheme: AES-Advanced Encryption Standard

Real time example:

Nowadays the cloud environment provides multiple security mechanisms. But the real cloud environment the server persons also make some illegal process in the form of getting customer data without him or his permission. To avoid this problem they are focusing identity based encryption technique.

- Cloud service user
- Cloud service provider
- Private key generator
- Revocation process
- File approval process
- Key update-CSP
- Combine key process

6. FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

7.ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

8.TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available

technical resources. This will lead to high demands being placed on the client. request

9.SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

10. CONCLUSION:

This project can be very help full to the user and the cloud service provider. The PKG can generate private key and the KU_CSP can generate updated key to the cloud user. With use of private key and updated key the combine key process can compare these keys and make a file retrieve process. But the existing concept only based on the identity based encryption in a single cloud service provider. With of this concept the cloud server can store and retrieve files in a better manner. Finally this is to be concluded in an efficient file security mechanism and file outsource process for an Identity based encryption with outsource revocation in cloud computing system