isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

A NEW IDENTITY BASED SCHEME THAT PROVIDE SECURED CLOUD SERVER

Nagarajan.R[1], Yoganand.S[2],

Student, Dept. of Computer Science and Engineering, Agni College of Technology, India.[1,]
Asst. Professor, Dept. of Computer Science and Engineering, Agni College of Technology, India. [2]

ABSTRACT-*The main aim of the project is to provide utility to maintain day to day operations of cloud computing security. This project help 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 focus 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.*

Keywords— Identity-based encryption, Revocation, Outsourcing, Cloud Computing.

1. INTRODUCTION

THE GREEK MYTHS tell of creatures plucked from the surface of the Earth and enshrined as constellations in the night sky. Something similar is happening today in the world of computing. Data and programs are being swept up from desktop PCs and corporate server rooms and installed in "the compute cloud." Whether it's called cloud computing or on-demand computing, software as a service, or the Internet as platform, the common element is a shift in the geography of computation. When you create a spreadsheet with the Google Docs service, major components of the software reside on unseen computers, whereabouts unknown, possibly scattered across continents. The shift from locally installed programs to cloud computing is just getting under way in earnest. Shrink-wrap software still dominates the market and is not about to disappear, but the focus of innovation indeed seems to be ascending into the clouds. Some substantial fraction of computing activity is migrating away from the desktop and the corporate server room. The change will affect all levels of the computational ecosystem, from casual user to software developer, IT manager, even hardware manufacturer.

In a sense, what we're seeing now is the second coming of cloud computing.

Almost 50 years ago a similar transformation came with the creation of service bureaus and time-sharing systems that provided access to computing machinery for users who lacked a mainframe in a glass-walled room down the hall. A typical time-sharing service had a hub-and-spoke configuration. Individual users at terminals communicated over telephone lines with a central site where all the computing was done.

2. 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.

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

3. SYSTEM ANALYSIS

EXISTING SYSTEM

In Existing system the cloud server files are not having security. Because files are stored into the server with identity based encryption. When the file retrieve process it can be make 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.

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.

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

ADVANTAGES

- Easy to make file revocation .
- Easy to usage and time saving.
- Cloud user needs to be solved by a better manner and better compatibility.
- Combine key process help to retrieve files from the server.
- Proposed system used to enhance file security.

4.Architecture Diagram

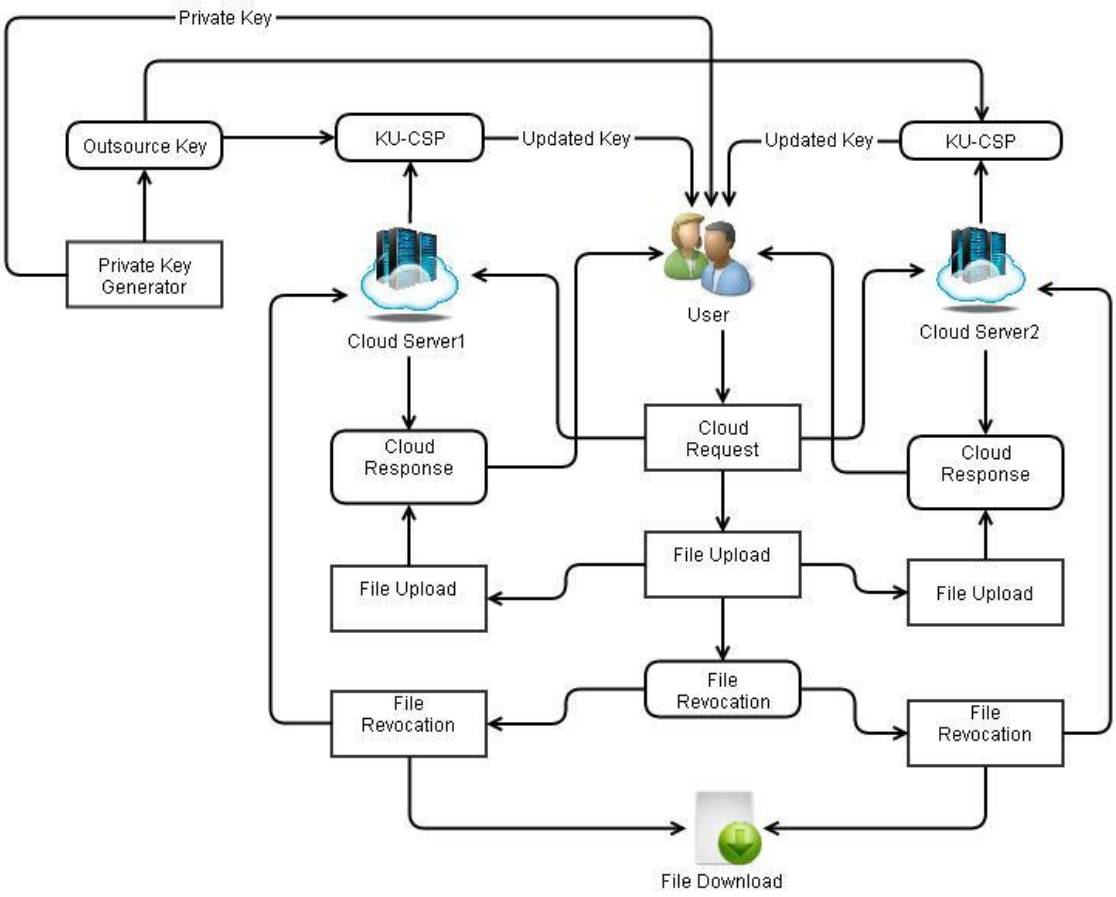

FIGURE:1 SYSTEM ARCHITECTURE

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

5. ALGORITHM

Setup(λ) : The setup algorithm takes as input a security parameter λ and outputs the public key PK and the master key MK. Note that the master key is kept secret at PKG.

KeyGen(MK, ID) : The private key generation algorithm is run by PKG, which takes as input the master key MK and user's identity ID ∈ {0, 1}∗. It returns a private key SKID corresponding to the identity ID.

Encrypt(M,ID) : The encryption algorithm is run by sender, which takes as input the receiver's identity ID and a message M to be encrypted. It outputs the ciphertext CT.

Decrypt(CT,SKID) : The decryption algorithm is run by receiver, which takes as input the ciphertext CT and his/her private key SKID . It returns a message M or an error ⊥.

KU-CSP:

Revoke(RL, TL, {IDi1, . . . , IDik }) : The revocation algorithm run by PKG takes as input – a revocation list RL, a time list TL and the set of identities to be revoked

{IDi1 , IDi2, . . . , IDik }. It outputs an updated time period Ti+1 as well as the updated revocation list RL and time list TL .

KeyUpdate(RL, ID, Ti+1,OKID) : The key update algorithm run by KU-CSP takes as input – a revocation list RL, an identity ID, a time period Ti+1 and the outsourcing key OKID for identity ID. It outputs user's updated time component in private key TK[ID]Ti+1 if his identity ID does not belong to RL, otherwise, outputs ⊥.

KEY REVOCATION:

This module fully based on the file revocation process during the key update cloud service provider. The user can send the file revocation request to the cloud service provide. After the confirmation of file revocation it should be move to the process of keying process. When the file revocation the PKG can send the private key and KU-CSP can send the updated key to the cloud

user. With use of these keys and combining the process the file to be revocation in a particular cloud service provider.

6. CONCLUSION AND FUTURE ENHANCEMENT

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.

FUTURE ENHANCEMENT

Our IEEE concept has to be keep on information in a large number of cloud computing environments by adding extra features like listed below,

- Data Retrieve from the various clouds in a effective manner.
- The large number of cloud the particular user can retrieve the files in a secure way of processing.
- Key Revocation Process very helpful to secure the user files.

All these process can be give as update to our project users throughout the world via Using this Application.

7.REFERENCES

[1] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology – CRYPTO'98. Springer, 1998.

[2] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security, ser. Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds. Springer Berlin / Heidelberg, 2007, vol. 4886, pp. 247–259.

[3] F. Elwailly, C. Gentry, and Z. Ramzan, "Quasimodo: Efficient certificate validation and revocation," in Public Key Cryptography PKC 2004, ser. Lecture Notes in Computer Science, F. Bao, R. Deng, and J. Zhou, Eds. Springer Berlin / Heidelberg, 2004, vol. 2947, pp. 375–388.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology – CRYPTO 2001, ser. Lecture Notes in Computer Science, J. Kilian, Ed. Springer Berlin / Heidelberg, 2001, vol. 2139, pp. 213–229.

[5] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security, ser. CCS '08. New York, NY, USA:
ACM, 2008, pp. 417–426.

[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 2005, vol. 3494, pp. 557–557.

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337