Secured Access of Data Using Cloud Computing

Divyabharathi A[1], Divyamira R[2] , Janani V[3],Siva R [4]

[1, 2, 3] UG student, [4] Associate professor, Department of Computer Science and Engineering, KCG College Of Technology
janani1994.7@gmail.com, rdivyamira@yahoo.com, indianbharathi1@gmail.com

ABSTRACT

Security is provided to files uploaded in cloud environment. Cloud is divided into three levels top level, regional and end user. The head can have the control over both regional and end users and can access their files without any permission but the users in the regional level have to send request to the head if they want to access the files in the top level. Similarly the end users have to send request to their respective regional levels to get their files downloaded. If their request are not accepted the file will be in the format of cipher text which is some meaningless information.

I. INTRODUCTION

To provide a security solution based on identity based encryption, signature and proxy re-encryption to address critical security issues of the proposed framework. It has several good properties such a energy saving, cost saving ability, scalability, and flexibility centers to provide different types of computing services for information management and big data analysis.

The main idea of this security solution for the Smart-Frame is to allow all the involved entities, i.e., top and regional cloud computing centers and end- users to be represented by their identities which can be used as encryption keys or signature verification keys. The entities in the lower level can use the identities of higher-level entities to encrypt their data for secure communication with the entities in the higher level. For example, the regional centers use the top cloud's entity to encrypt their messages. By employing an identity-based reencryption scheme, the information storages, which are components of regional clouds, can re-encrypt the received confidential data from the end-user devices so that services requested by the end-users decrypt and process the confidential data without compromising the information storages' private keys. One of the obvious benefits we can gain from applying identity-based cryptography to the Smart- Frame is that through using identities rather than digital certificates which depend on traditional public key infrastructure (PKI), we can save significant amount of resources for computation and communications and resolve scalability issues. The saving gained from the elimination of digital certificate in the big data environment is especially momentous.ID-based encryption, or identity-based encryption (IBE), is an important primitive of ID-based cryptography. As such it is a type of public- key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). Proxy re-encryption schemes are cryptosystems which allow third parties (proxies) to alter a ciphertext which has been encrypted for one party, so that it may be decrypted by another. It has become popular recently due to advantage over traditional computing models Additionally, in order to support security for the framework, we have presented a solution based on identity-based cryptography and identity -based proxy re-encryption. As a result, a proposed framework achieves not only scalability and flexibility but also security features. We have implemented a proof-of-concept for this framework with a simple identity based encryption and proxy re-encryption.

II. RELATED WORK

1. User Authentication

The **Authentication** is a first module in this project.

In this module we will verify the Data owner access permissions and verify the user access permissions. Before that He/she should register first. Then only he/she can be able to do it. For that he needs to fill the details in the registration form. These details are maintained in a database. In this module, any of the above mentioned person have to login, they should login by giving their Name and password.

1. File deployment in cloud

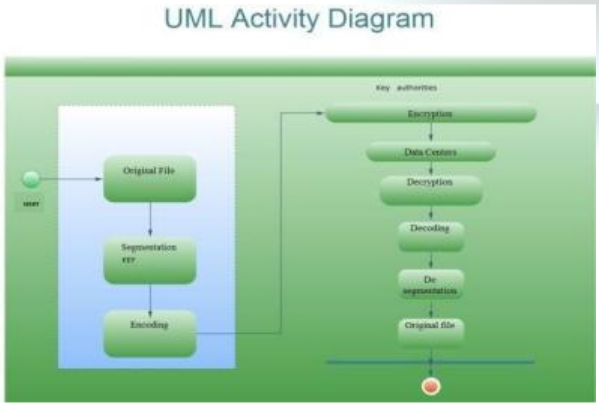
In this module the user can deploy there details in to cloud. For providing security, we use an "**Identity Based Encryption"** to encrypt the details. For the future enhancement segment the details in to several parts, this is stored in different location in cloud. In Segmentation, file size is splits up and save in different location

2. Retrieval of File

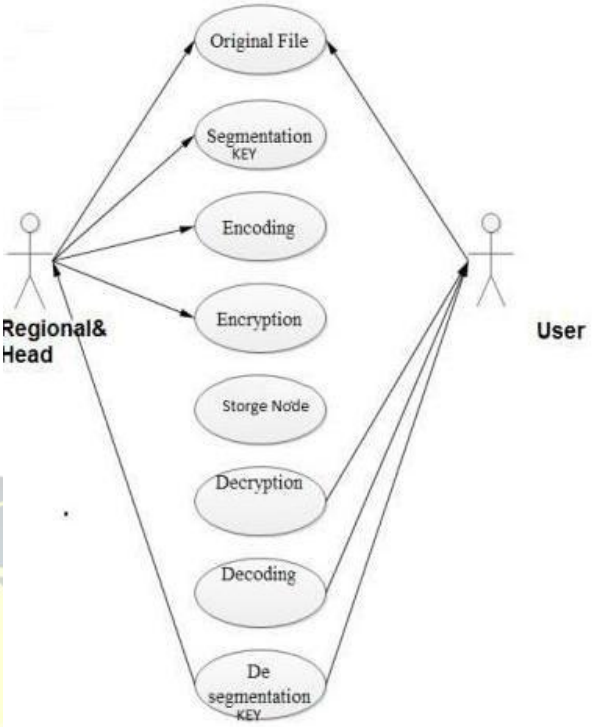
In this module file is download our details in a secure manner.While downloading the uploaded file, cloud server desegment the details which was segmented. We employ the binary tree structure **to** update the secret keys for the client.

3.User Privacy

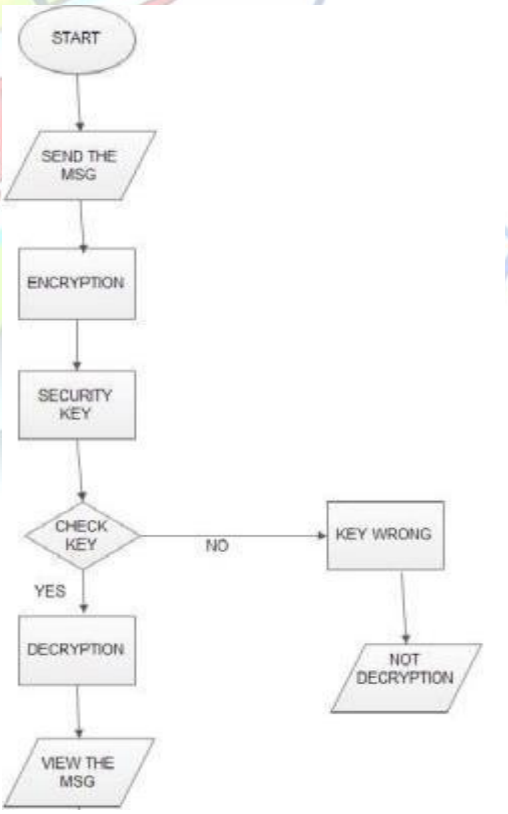
We present our design for a new cloud storage encryption scheme ("**Signature and proxy based Encryption"**) that enables user to create convincing fake files to protect data privacy. If any users want the user details to download the user kindly sent the request to the user. The user have the Access Control .that is if the user want to share the original details with the user , he share the original data and decryption key to the user .Since the provider cannot tell if obtained data are true or not, the cloud storage providers ensure that user privacy is still securely protected. Finally produce the Auditing result.



Use case:



Flow chart:



I. Our Idea

This system proposes a method of downloading the original data or message which is directly uploaded by the authentified end user.It requires a private key from the private key generator to download the original message from the top system.This method makes use of proxy reencyption scheme for uploading and downloading the data.Both identity based encryption and proxy reencryption provides a security information for the data stored in top centers.

It allows only particular users to access the data from the top centers in which it restricts the other users from accessing it.In this case, security is maintained between the particular users who need the data from the top centers and top centers who is having the collection of data the user wants.

II. Block Diagram:

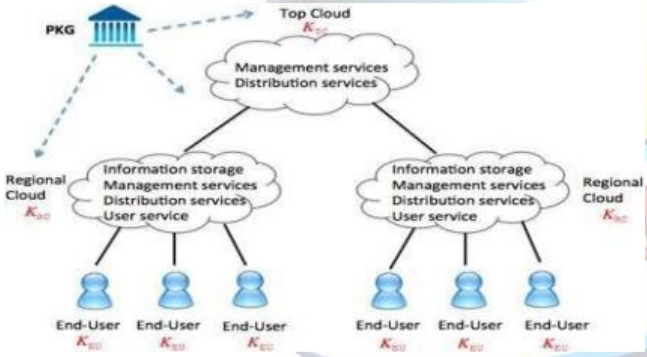


Diagram Description:

The basic idea of the project is to set up cloud computing centers at three hierarchical levels to manage information: top, regional, and end-user levels. While each regional cloud center is in charge of processing and managing regional data, the top cloud level provides a global view of the framework. Additionally, in order to support security for the framework, a solution is provided based on identity-based encryption and proxy re-encryption. The main idea of the framework is to build a hierarchical structure of cloud computing centers to provide different types of computing services for information management and big data analysis.

The entities in the lower level can use the identities of higher-level entities to encrypt their data for secure communication with the entities in the higher level. For example, the regional centers use the top cloud's entity to encrypt their messages.

I. Algorithm Explanation

Identity based encryption:

ID-based encryption, or identity-based encryption (IBE), is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). This means that a sender who has access to the public parameters of the system can encrypt a message using e.g. the text-value of the receiver's name or email address as a key. The receiver obtains its decryption key from a central authority, which needs to be trusted as it generates secret keys for every user.

PROXY REENCRYPTION:

Proxy reencryption is an algorithm where the original meaning of the text is revealed only when the first party gives acceptance to the request given by the other parties,if the request is not accepted it appears in the form of cipher text that is some meaningless information even though after downloading it!

V1. CONCLUSION

This structural framework provides security in data management between the end user and the cloud systems by using proxies.data are transfered and maintained with security solution using algorithms such as identity based encryption(IBE), and proxy re-encryption(PRE). This system proposes a new concept by using proxy re-encryption algorithm on uploading and downloading the data.

On uploading data ,the message is customized and is

split into respective fields and only the customized recipients only can download the specialized message from the top system.Otherwise it will be appearing in the form of cipher text that is some useless information

The file distribution in cloud is provided with at most security. Here the Cloud is divided into top, regional and end users which is easy to access the files. security is provided using identity-based and proxy reencrytion method where the files can never be misused since it appears only as the meaningless information if it is downloaded without the permission of the top cloud.

III. REFERENCE PAPER

[1]Gregory M .coates , Kenneth M . kopkinson , Scott R . Graham and Stuart kurkowskimembers,IEEE(2010) A trusted system architecture for SCADA network security,IEEE,vol.25,no.1,January,pg,no.158

[2]XiFang,SatyajayantMisra,Guoliangxue,Dejungyan,members IEEE(2012), Managing smart grid information in the cloud:opportunities,model,andapplications,IEEE,vol.26, July-August,pg,no.32

[3] Christo Ananth, H.Anusuya Baby, "Encryption and Decryption in Complex Parallelism", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3, Issue 3, March 2014,pp 790-795

[4]H.Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in Proc. 1st Int. Conf. Cloud Comput., 2009, vol. 5931, pp. 157–166.

[5] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol., 2001, vol. 2139, pp. 213–229.

[6] X. Boyen, "A tapestry of identity-based encryption: practical frameworks compared," Int. J. Appl. Cryptograph., vol. 1, no. 1, pp. 3–21, 2008