MJRET

Multidisciplinary Journal of Research in Engineering and Technology

Journal homepage: www.mjret.in

Open Access

ISSN: 2348 - 6953

Rutuja R. Sadul
Dept. of Computer Engineering,
KJCOEMR,Pune, India.

Asawari Rankhambe
Dept. of Computer Engineering,
KJCOEMR,Pune, India.

Neha Subhekar
Dept. of Computer Engineering,
KJCOEMR,Pune, India.

Shaheen Shaikh
Dept. of Computer Engineering,
KJCOEMR,Pune, India

Prof. M.K.Mokashi
Dept. of Computer Engineering,
KJCOEMR,Pune, India

A Survey of Different Encryption Techniques for Secure Cloud Storage

Abstract

Cloud generally relates with a set of hardware, storage of network, services, interfaces which are needed to combine and deliver the service for computing. The role of cloud is to provide the service for delivery of software, and storage of data on internet based on user demand. This paper includes the protocols which provide security with the help of cloud .it includes different properties of protocols along with their features to have a relevant study among different protocols.

Keywords- *FADE(Fine Grain Access Control And Deletion, DHT(Distributed hash table),INS(Index Name Server),RBAC(Role Based Access Control),RBE(Role based Encryption),ABE(Attribute Based Encryption)*

1. INTRODUCTION

Cloud computing [12]is basically computing done over a large communication networks such as internet. It performs the operation like distributed system where many computers can perform operation simultaneously. Cloud is also used as a business solution for storage. It provide a vast amount of storage in all sectors like Government, Enterprise etc. Apart from government and enterprise one can also achieve storage of their personal data on cloud. In future people will use cloud for storing their audio/video files as the storage capacity for smartphone is not more enough. The research area of survey is cloud, why cloud? Cloud is use for following purpose :-

1. It provides infinite storage space for client, to obtain data backup.
2. It reduce financial overhead of data management which is cost due to central repository.(costly than central repository)

This paper is mainly focused on two issues related to cloud:-

1. **Guarantee of access control**: Guarantee of access control implies that only authorized person can access the data.

2. **Assured deletion**: Assured deletion is mainly focused on time based manner.

A particular time is being assigned for the data to be viewed to the authorized user after that particular time the data cannot be accessed by the user. Secondly keeping the data permanently is of no use as data may be unexpectedly disclosed in the future or attack on data can take place or there may be careless management of cloud operators. While surveying we came to know about different approaches like Wang's approach, Jungle disk, cumulus, Perlman ephemerizer, Vanish etc.

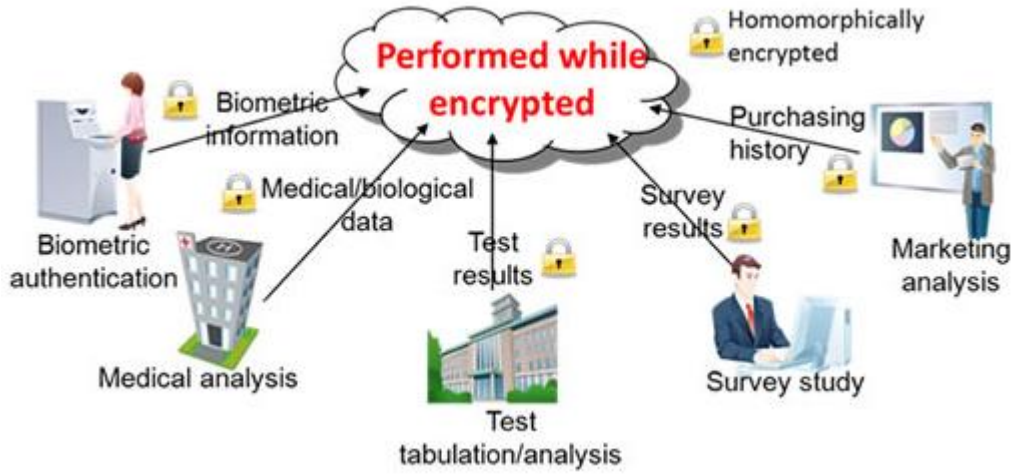

Fig1. Application of Encryption techniques

2. Different Approaches for Encryption:

1. Jungle disk

Jungle disk [3] is used for data encryption with the help of AES-256 encryption algorithm. Jungle disk is an online backup tool that store data on cloud.

Disadvantages:

1. Jungle disk does not meet most of market standard criteria's.

2. It does not offers feature like file sharing capabilities.

2. Perlman ephemerizer

This approach [4]is also used for encrypting the file with the help of data key. Data key is further encrypted with the help of time based control key. The control key is deleted when the expiration time is being reached. The control key is managed by a separate key manager.

Disadvantage of this approach are:

1. It target only time based assured deletion.
2. No fine grained control of different file access policies.
3. No implementation is done.

3. Wang's approach

Wang's approach deals with the use of security issues in cloud. It provides data access procedure which is based on owner write user read scenario. in this approach end user sends a request to access the data to the data owner then the data owner sends a encryption key and access certificate to user, user sends the access certificate to storage provider and the storage provider sends the encrypted detail to the end user.

Advantages of Wang's approach are:-

1. Low clients' responsibilities
2. Low storage overhead
3. Block insertion, update, deletion and appending.

Disadvantages of Wang's approach:-

1. Requires support from the cloud side
2. No multiple policies combination

4. Vanish Protocol

The focus to implement this paper is on the use of multiple policies which is not being supported by Wang's approach so hence we are focusing on the new approach named as Fade Roxana Geambasu, Tadayoshi Kohno, Amit A levy, Henry M levy in their study they introduce a protocol named Vanish which is used for providing data privacy and self-destructing data. Their study mainly focused on the data should be able to access for limited period of time. After that time access to the data should be revoked for everyone including

the user who prepares the data as well as the known and unknown entries holding the copies of data.

Vanish protocol application is applicable for sensitive data only. To achieve self-deleting, following activities takes place, Vanish encrypts the user's data locally with the help of encryption key which is no known to the user also, destroy the local copies of key and then sprinkles bits in the DHT randomly. The authors mainly concentrated on DHT because it supports three main properties which are as follows:-

1. DHT consists of many nodes which are distributed across many countries, these nodes are powerful.

2. It provides the facility of protected reliable storage that is the data is available for a desired interval of time.

3. DHT is constantly changing that means the information which is sprinkled will be deleted/disappear naturally after a certain time.

They developed vanish protocol by considering two systems:

1. Bittorrent'sVuze Based System supports 8 hour timeouts and the open DHT based system can support timeouts up to one week.
2. On the top of vanish core, a Firefox for Gmail and other websites and a self destructing file management application are build.

DHT's possess some unique properties which are suitable for achieving data destruction. Properties of DHT's are:

1) There is large scale geographical distribution of nodes across many countries and complete decentralization makes them powerful and legally influential adversaries.

2) They provide reliable distributed storage: This property is useful for ensuring that the sensitive data remain available for specified time only.

3) DHT's are constantly changing. Thus the information gets automatically vanish as the DHT's node internally clean themselves.

To support this application, one notion is introduce called as vanishing data objects. A VOD encapsulate user's data and prevent it from persisting indefinitely and fall into wrong hands. Regardless of whether the VOD is copied, stored or transmitted on the internet it becomes unreadable after predefined period of time

There are two prototype applications that uses vanish:

1) Fire vanish: It is a Firefox plug-in for Gmail services that allow to send and receive the self-destructing mails. This plug-in uses vanish daemon to transform an email into VOD before sending it to Gmail and vice versa…

2) Vanishing files: it is another application that can be used directly or by other application as a self-destructing trash bins. User can stored all the files containing sensitive data into these self destructing VOD which expires after specified time

Disadvantages:

Major drawback of this system is it only provide the time based assured deletion of data. It allow the legitimate user to access to the data for specified time and after the expiration of that time the original and all the copies get automatically deleted from all storage sites but it does not provide any access control mechanism. This system is beneficial for preventing the unauthorized access to the data by third party. But because of its mechanism even the authorized user do not get access to the data as it deletes the sensitive data permanently. Switching from one cloud two another clouds. In this case a user working in a company stores data on cloud X and is associated with a policy P. if the user switches to new company then all the data is being deleted on cloud X by revoking the policy.

5.Cumulus

Michael Vrable, Stefon Savage and Geoffrey M .Voelkar in their study of cumulus backup file system backup in cloud their introduced about the protocol cumulus [6] which is used for storing data backup in cloud. The concept of thin cloud is used because of the property of get and put of the complete file it doesn't require any special software at a server storing backup , only ability to store and retrieve entire file, making it well suited for sending backups to service.

Disadvantage of cumulus:

1. Seeding data and full recovery.
2. Size limitations.
3. Discontinuation of service.
4. Nonexistent service level agreement.
5. Does not offer coordination between multiple backup client.

Tin-Yu Wu, Jeng-ShyangPan ,Chia-Fan Lin [9] in their study their focused on the storage related issues on cloud. As data on cloud is stored so different files are stored, in these case the workload increases and a lot of hardware resources is wasted. To overcome above drawbacks they proposed INS. the main use of INS is that it manage storage of different file the data which is duplicated, compression of file is done, the load on server, Internet Protocol information and all real time feedback is given. In INS al nodes are arranged in elicit optimal performance so that desired resources can be accessed by client. In these way the overcome of file storage and other related issues are solved to some extent by INS. Lan Zhou, Vijay Varadharanjan, MichaelHitchene[10] in their study they focused on how user can access the data in these paper according to the role of user the data can be accessed. To develop this type of access control they focused on a protocol RBAC which is based on RBE the introduced two type of cloud:

1. Public Cloud:-A public cloud is available to all people.

2. Private Cloud:-A private cloud is a cloud available to only authorized person.

While the private cloud is operated only by a single organization and single organization is responsible for building the cloud. According to the survey 43% people are using private cloud whereas 34 % people are going to use it in future. The studied of above researchers were to provide security of data and give access of data according to the role.

To provide security of data the concept of cryptographic technique is used where data is encrypted and after verifying whether the user is authorized then and then only data can decrypt with the help of private key. This helps to avoid unauthorized access of data of users.

VipulGoyal, OmkantPandey , AmitSahai Brent Waters[8] in their study the focused on providing fine grained access control .As we know that third party stores the sensitive data on the internet e.g. Gmail, Yahoo etc. storing data at different site will lead to different attacks and legal pressure faced by services. To solve above problem we can store data in encrypted form and decrypt the data with the help of private keys but the condition arises when more than one user need to access data than the owner has to give the entire user the private key. To avoid this problem we are using attribute based encryption.

3. FUTUREAND RESEARCH WORK

The modern generations of the cloud storage infrastructures does not provide any security against untrusted cloud workers making them unfitting for storing sensitive information such as financial records, medical records or high impact business data. So storing sensitive information on cloud in secure manner is the research work in future on cloud storage. Designing a secure cloud storage system for storage of information which provides the protection for sensitive data is also a research work.

4. CONCLUSION

In this paper we have surveyed and studied about various protocols which are used in cloud for providing secure access as well as deletion operation. Protocols were presented in this paper gives the current state of it along with the broad spectrum of characteristics, which include advantages as well as disadvantages.

ACKNOWLEGEMENT

We would like to thanks our guide Prof. M.K.Mokashi for the guidance and support. We will forever remain grateful for the constant support and guidance extended by guide, for the completion of paper. We also thank to editor and referees for their comments.

REFERENCES

[1] G.Gayatri ,S.Soumya. FADE: A Secure Overlay Cloud Storage System.

[2] R. Geambasu, T. Kohno, A. Levy, and H.M. Levy, "Vanish:Increasing Data Privacy with Self-Destructing Data," Proc. 18th Conf. USENIX Security Symp, Aug. 2009.
[3] JungleDisk, http://www.jungledisk.com/, 2010.
[4] S. Nair, M.T. Dashti, B. Crispo, and A.S. Tanenbaum, "A Hybrid PKI-IBC Based Ephemerizer System," Int'l Federation for Information Processing, vol. 232, pp. 241-252, 2007.
[5] R. Perlman, "File System Design with Assured Delete," Proc. Network and Distributed System Security Symp. ISOC (NDSS), 2007.

[6] "Cumulus: Filesystem Backup to the Cloud" Michael Vrable, Stefan Savage, and Geoffrey M. Voelker

[7] "File System Design with Assured Delete"Radia Perlman.

[8] "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data" byVipulGoyal¤ OmkantPandeyyAmitSahaizBrent Waters.

[9] "Improving Accessing Efficiency of Cloud Storage Using De-Duplication and Feedback Schemes"
[10] Tin-Yu Wu, *Member, IEEE,* Jeng-Shyang Pan, *Member, IEEE,* and Chia-Fan Lin.
[11] "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage" Lan Zhou, Vijay Varadharajan, and Michael Hitchens.
[12] "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems"
[13] AyadBarsoum and Anwar Hasan, Senior Member, IEEE.
[14] "A View of Cloud Computing" by Michael Armbrust, Armando Fox, ReanGriffith,Anthony D. Joseph, Randy Katz, Andy Konwinski,Gunho Lee, Dav id Patterson, Ariel Rabkin, Ion Stoica,andMateiZaharia.