2nd International Conference on Current Research Trends in Engineering and Technology
© 2018 IJSRSET | Volume 4 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Data Security in Cloud Computing : A Comprehensive Survey

Nidhi Shah, Digvijay Mahida

[*1] Assistant Professor, Information Technology, Sigma Institute Of Engineering, Vadodara, Gujarat, India
[*2] Assistant Professor, Information Technology, Sigma Institute Of Engineering, Vadodara, Gujarat, India

ABSTRACT

Cloud Computing is evolving as incredible computing model which has been usually used for storing and retrieving large amounts of data over the Internet so data security is one of the major concerns with cloud computing. This paper describes the different techniques along with few security challenges, advantages and drawbacks. It also provides the analysis of data security issues and privacy protection affairs related to cloud by preventing data access from unauthorized users, managing sensitive data, providing accuracy and consistency of data stored. To deal with these security problems, this paper also proposes a novel data sharing mechanism that concurrently achieves data confidentiality and fine-grained access control on encrypted data and user revocation by combining ciphertext policy attribute-based encryption and proxy re-encryption. This paper also delivers security for cloud data storage through a proper key management system with multiple key managers using Shamir's key sharing technique and the policy file encryption is done using Elgamal algorithm for secure data transmission.

Keywords: Cloud Computing, Data Security, Outsourced data, Ciphertext Policy Attribute Based Encryption

I. INTRODUCTION

Cloud storage is a recently developed idea in the field of cloud computation. It can be defined as a system that is composed of cluster, grid and distributed file systems that using application software and it manages a variety of different type storage devices together to provide data storage and access service Even though cloud storage services are offering this number of aids, they are facing many challenges for securing data in public clouds. Data leakage may occur due to internal/external attacks by other users and machines in the cloud. Users' data imported in Dropbox, SpiderOak can face different threats like service operators can copy users' data and credentials because they are authorized and capable to get access to users' data easily, they also can authorize other users to access users' data and even Users' personal data stored in the cloud is accessible from other people's data So attacker can easily hack the cloud storage. . In this paper we survey the solution of different data security issues using virtualization technique and Encryption techniques which provide a solution to ensure privacy and confidentiality of cloud storage data.

II. METHODS

The FADE is a light-weight and scalable technique that guarantee the deletion of files from cloud when requested by the user but still they have some security issues of keys and authentication of participating parties. This is a man-in-the-middle between client and KM. Using this sometimes data may be lost because of adapted policy to KM and client didn't get proper key from KM. This issue can overcome by data security scheme. Shamir's (k, n) threshold scheme is used for the management of keys that uses k shares

out of n to rebuild the key so cryptographic keys must be stored in a robust manner and a single point of failure should not affect the avaibility of data [4]. To avoid man-in-the-middle attack user can use different keys like symmetric key which provides confidentiality and integrity services and asymmetric key for security and their pairs are generated by KM's third party. Except key pair just public key is transmitted to the client. secret key is established between client and KM using STS protocol.

The proposed modules are:
1.Cataloguing of Users & Policy Setting
2.File Upload & Key exchange
3.File Download
4.Policy Revocation and Renewal

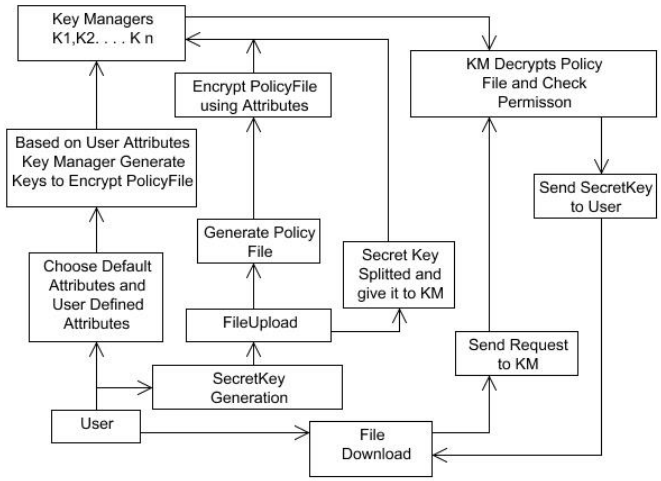

FIGURE 1: System Architecture

1) Cataloguing of Users & Policy Setting

First the user has to register to become a participant in the cloud. After registration the user has to choose some default attributes like name, email, address to create a policy and also user defined attributes to encrypt their policy file which is already created on the time of file uploading process and this Attribute Based encryption using Elgamal algorithm [3].

Elgamal algorithm

ElGamal cryptosystem includes key generation, encryption, and decryption process. This algorithm uses attributes to generate a secret key and it is used for policy file encryption security.

2) File Upload & Key exchange

After above process, the user has to login into the cloud using username and password and authentication process will be performed by user and key manager using Diffie Hellman Key Exchange Algorithm. The encrypted file uploaded into the cloud and Key managers split the secret key and send the key to multiple key managers. Key managers create a public and private key for that own key and key splitting process is done by using Shamir's encryption technique.

Diffie Hellman Key Exchange Algorithm

It is used for authentication between client and KM which construct a shared secret numeric key over an open network with probable observer.

Shamir's Encryption technique

This is an algorithm of cryptography and it's a form of secret sharing where a secret is divided into parts and these are shared to number of participants to reconstruct the tree.

3) File Download

If users need to download their files then they will send a request to Key-Manager with proper attributes and KM will check their attributes for authentication process and provide decrypted share for the user. After getting the key from KM, users will receive their secret key and download their file and decrypt their secret key using RSA algorithm [3].

4) *Policy Revocation and Renewal*

Revocation is defined as user will remove all polices before user set and policy request is sent to KM to delete all user polices. In renewal process KM will allow user to renew the policy after authorization from KM.

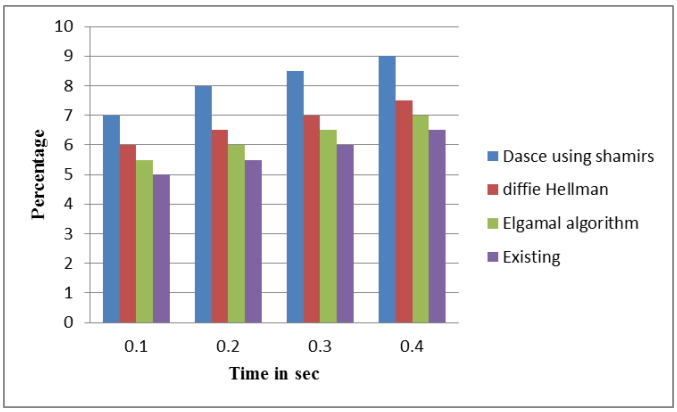

FIGURE 2: Result of Different System [1]

SOA is used for security purpose in cloud computing. Virtualization allows multiple users to share physical layer and it enables data sharing, data accuracy and performance optimization. Generally traditional symmetric encryption algorithms DES and AES provide relatively low security and encrypted data are susceptible to attacks so for that data splitting algorithm is used for data reliability. To achieve efficient data sharing, owner's level encryption and access control's level encryption are used.

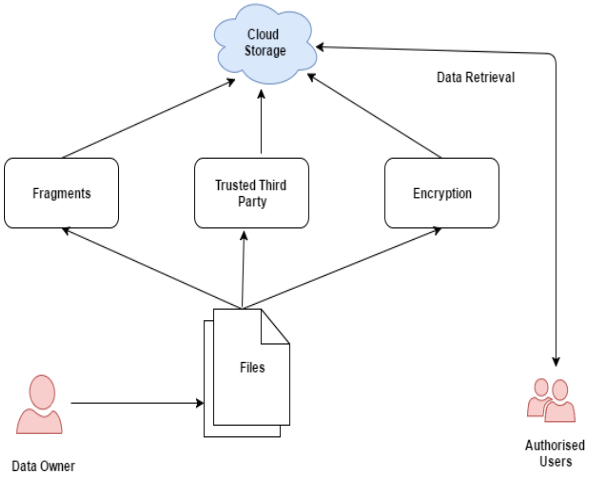

FIGURE 3 : Architecture of Data Storing Security and Privacy [4]

The different data access techniques are used for different purpose. Fragment placement and Fragment replication technique improves Retrieval Time but Time and Resource consumption is more. Searchable Attribute based proxy reencryption system enables data owner to well-organizedly share his data to a specified group of users matching a sharing policy. CIBPRE allows a sender to encrypt a message by identifying the receiver's identity. DaSCE is based on the time consumption during file upload and download. And for data confidentiality also different techniques are used. Public Auditing Scheme, Dynamic Hash Table used 2-dimensional data structure to verify the data property information for dynamic auditing. It reduces the computational cost and communication overhead. Data integrity is a main concept of data security. It refers correctness and consistency of stored data in a database. Data Vaporizer have many techniques of secret sharing of the keys to improve the security level and consistency. ID-PUIC checks data integrity of both private and public authorization. Data privacy is achieved from Attribute based data sharing scheme. From different techniques we can achieve data security and privacy in cloud computing.

III. CONCLUSION

In this paper, we defined different techniques for data security, data access, data confidentiality in cloud computing. Through this paper, we were also able to achieve knowledge about fine grained access control and flexible revocation that enables holders to cancel users with less computational requirements and avoids involvement between the proxy and the users. This paper mainly focus on security and privacy issues and also discusses about the different techniques used in existing cloud storage. Additionally, these different techniques are used in improving the security of the stored data.

IV. REFERENCES

[1]. Dr. Santhi Baskaran, A. Isaiarasi, "Secure data transmission with multiple key management in cloud environment," International Conference on Emerging Innovation in Engineering and Technology ICEIET-2017, Vol 2, ISSN NO: 2456-1983.

[2]. Mai Mansour Dahshan, Sherif ElKassass .2014, "Data Security in Cloud Storage Services", The Fifth International Conference on Cloud Computing, GRIDs, and Virtualization. (2014), ISBN: 978-1-61208-338-4.

[3]. Karthik Selvakumar, Alwin KoilRaj.A, Mrs. Beena Godbin, "Dasce-Data Security for Cloud Environment with Semi-Trusted Third Party Key Managers", International Journal of Advanced Research in Computer Science Engineering and Information Technology. (Apr 2016), Volume: 4, Issue: 3,Special Issue: 2 , ISSN_NO: 2321-3337.

[4]. Jeevitha B. K., Thriveni J, Venugopal K. R," Data Storage Security and Privacy in Cloud Computing: A Comprehensive Survey", International Journal of Computer Applications.(Dec 2016 0975 – 8887) Volume 156 – No 12, December 2016.