ISSN 2395-1621

Secure Data Sharing In Cloud: A Review

[#1]Prof. Shital B. Jadhav, [#2]Neetal A. Revankar, [#3]Sanjli S. Raorane, [#4]Payal B. Oswal, [#5]Vaishnavi D. Sagale

[1]jadhavshital81@gmail.com
[2]neetalrevankar@gmail.com
[3]sanjliraorane2524@gmail.com
[4]oswal.payal7@gmail.com
[5]vdsagale111@gmail.com

[#12345]Department of Computer Engineering
BVCOEW, Dhankawadi, Pune

ABSTRACT

Cloud Computing is the future generation internet based computing system which provides easy and customizable services to the users for accessing their data or to work with various cloud applications. One of the major services provided by cloud is data storage. Cloud Computing provides a way for storing and accessing the cloud data from anywhere by connecting the cloud application using internet. Cloud Computing security is the major issue rising nowadays. If proper and efficient security measures are not provided for data operations and transmissions then data is at high risk. Since Cloud computing provides facility for a group of users to share and access the stored data, there is a possibility of having high data risk. A secure and efficient data sharing scheme needs to provide identity privacy, access control, multiple owner and dynamic data sharing without getting affected by number of cloud users revoked. In this paper, we have reviewed various security data sharing schemes in cloud. This paper presents comparative analysis of the various techniques used for secure data sharing and the system architecture of the proposed system for secure data sharing in cloud.

ARTICLE INFO

Article History

Received: 24th November 2016

Received in revised form :

24th November 2016

Accepted: 26th November 2016

Published online :

30th November 2016

Keywords: Cloud Computing, Cryptographic Server, Access Control

I. INTRODUCTION

Cloud computing is a type of online network based computing that delivers shared computer handling resources and data to personal computers and other devices on demand. It is a unique way for enabling universal, on-interest access to shared computing assets (like servers, storage, computer network, applications and services), which can be quickly planned and released with reduced management effort. Cloud computing and storage solutions provide users and IT firms with potential to store and process their data in third-force data centers that may be located anywhere worldwide. Cloud computing relies on sharing of resources to get consistency and scale in economy.

Cloud computing is the result of the development and acquisition of existing technologies and paradigms. The goal of cloud computing is to let users make profit from all of the cloud technologies, without the actual need of deep knowledge and comprehension of cloud. The cloud intents to reduce or optimize costs, and helps the users focus on their main business instead of being blocked by IT barriers. The main enabling technology for cloud computing is virtualization. It sets apart a physical computing device into one or more virtual i.e. not physically existing devices which can be easily managed to perform computing tasks. With OS-level virtualization essentially creating a flexible system of multiple non-dependent computing devices, idle computing resources can be distributed and used in more organized way. Virtualization provides the alertness required to speed up operations and reduces cost by increasing infrastructure totalisation. Self-governing computing automates the process through which the user can supply resources on-demand. By reducing user involvement, automation speeds up the process, minimizes labour costs and reduces the possibility of user errors. Customers routinely face difficult business problems.

Cloud model possesses five important characteristics:

- **Rapid flexibility :**
  You can go from 10 servers to 100 or from 100 servers to 10.
- **Measured service :**
  You have to pay for what you use.
- **On-demand self-service :**
  You get flexibility impulsively.
- **Ubiquitous network access :**
  Cloud can be accessed from anywhere.
- **Position-independent resource pooling :**
  You can work with virtual machines that could be hosted anywhere.

The cloud model provides three service models:

- **Software as a Service (SaaS) :**

The facility provided to the user is to use the owner's applications running on a cloud framework. The applications can be accessed from various client devices through a client interface such as a web browser like web-based email.

- **Platform as a Service (PaaS) :**

The amenity provided to the customer is to set up onto the cloud infrastructure his own applications without installing any platform, tools on their local machines. PaaS means providing platform layer resources, including support for operating system and software development schema that can be used for building higher-level services.

- **Infrastructure as a Service (IaaS) :**

The amenity provided to the customer is the provision of storage, processing, networks and other primary computing resources where the customer is able to set up and run arbitrary software, which includes operating systems and applications.
A cloud model provides three deployment models:

- **Public Cloud :**

A cloud is named a "public cloud" when the services are rendered over a network that is open for anyone to use. Public cloud services can be free.

- **Private Cloud :**

Private cloud is cloud infrastructure operated completely for a single organization, whether governed internally or by a third-party, and organized either internally or externally.

- **Hybrid Cloud :**

Hybrid cloud is a composed of two or more clouds (private or public) that remain definite entities but are bounded together.

II. NEED OF THE SYSTEM

Data sharing is becoming increasingly important for many users. For businesses and organizations data sharing has become the most important requirement. People love to share information with one another. Whether it is with friends, family, companions or the world, many people benefit greatly through sharing data.
Some of the benefits are:

- **Higher Productivity :**

Hospitals benefit from data sharing which leads to lowering of healthcare costs. Students can also get benefit from data sharing while working on group projects due to which they can easily interact with each other and get their work done efficiently with collaboration. Businesses can gain profit by working together. Employees also get benefit as they can share work and collaborate with other employees and can also pursue working at home or any other place such as the library.

- **More Enjoyment :**

Many people of any age, gender or ethnicity can connect with one another and share their life experiences, achievements, photos etc. As well as catch up with other people from various different regions via social networking sites like Facebook, Twitter, Instagram, Orkut etc.

Requirements of Data Sharing in the Cloud:

To enable sharing of data in the Cloud, it is important that only authenticated users can access data stored in the Cloud. Following are the ideal requirements of data sharing in cloud:

- The data owner should be able to define a group of users that are authorized to view his/her data.
- Any member of the group should be able to access the data anytime without the data owner's interposition.

- No other user, other than an owner of the data and the members of the group, should gain the access to the data, including the Third Party Auditor (TPA).
- The data owner should be able to abrogate access to data for any user of the group.
- The data owner should be able to add users to the group.
- No member of the group should be allowed to abrogate the rights of other members of the group or join new members to the group.
- The data owner should be able to define who has read/write permissions on the data owner's files.

III. LITERATURE SURVEY

T. Jiang, X. Chen, and J. Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation," [1], 2015, This paper proposes an efficient use of vector commitment and verifier local revocation group signature to provide efficient public integrity auditing scheme.

M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, and A. Y. Zomaya, "SeDaSC: Secure Data Sharing in Clouds,"[2], 2015, This paper proposes a methodology that provides data confidentiality, secure data sharing without re-encryption, access control for malicious insiders, and forward and backward access control.

S. Seo, M. Nabeel, X. Ding, and E. Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," [3], 2014, This paper proposes the mCL-PKE (Mediated certificate-less public key encryption) scheme without pairing operations that solves the key escrow problem and revocation problem.

S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," [4], 2012, This paper proposes innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism.

C. Chu, S. S. M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage," [5], 2013, This paper proposes a new public key cryptosystem that produces a constant size cipher text with private keys to decrypt.

C. Yang and J. Lai, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing," [6], 2013, This paper proposes the idea of adding symmetric property in secret sharing to successfully minimize the cost to share the shares between the client and the server. Also extended SSC (Secure Cloud Computing) to MSCC (Multi server SCC) fitting the multi-server environment by using a homomorphism property of secret sharing.

Z. Zhu and R. Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud," [7], 2016, This paper proposes a scheme, in which users can securely obtain their private keys from group manager certificate authorities and secure communication channels.

J. Wei, W. Liu and X. Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption," [8], 2015, This paper proposes a notion called RS-IBE (revocable-storage identity-based encryption), that supports identity revocation and cipher text update simultaneously such that a revoked user is blocked from accessing previously shared data, as well as eventually shared data.

IV. PROPOSED SYSTEM

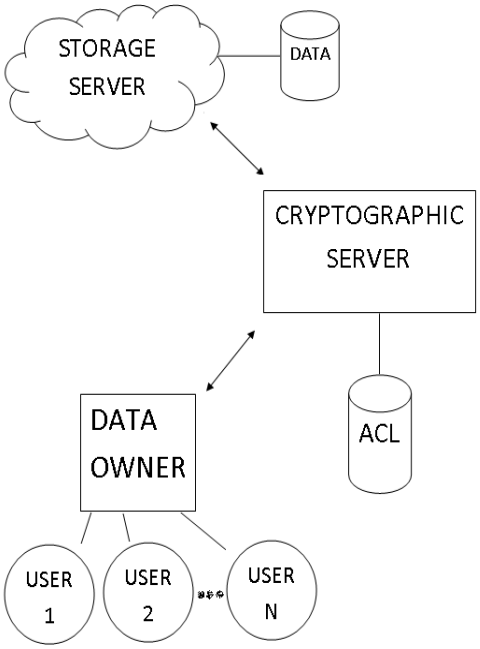

Fig. 1 Proposed system architecture

Basically our system consists of three main entities: -1) Data Owner 2) A Cryptographic Server (CS) and 3) A Storage Sever. Firstly, the data owner sends the data, the list of the users among whom he wants to share the data, and permissions for each user to the CS. The CS here is a trusted third party (TTP) that is responsible for management of keys, encryption, decryption, and access control. On receiving the data from the data owner, the CS generates an Access Control List (ACL). For key management a random number is generated and its hash value is calculated. This becomes the symmetric key for encryption and decryption. The CS encrypts the data with the generated key and then for each member in the group, the CS splits the key into two parts such that a single part alone cannot regenerate the key. Gradually, the main key is deleted through secure overwriting. One part of the key

is given to the corresponding user in the group, whereas the other part is preserved by the CS within the access control list related to the data file. After this hash value is calculated of the encrypted file to detect the tempering of the data and then it is uploaded onto the storage server i.e., Cloud. The user who wishes to access the data sends a download request to the Cryptographic Server. The CS, after authenticating the user, receives the part of the key from the user and afterwards downloads the data file from the storage server. The key is regenerated by operating on the user's part of the key, and the corresponding part of the key for that particular user maintained by the CS. Before decryption hash value is calculated to detect the tempering. After detecting the data file is decrypted and sent to the user. For a new member, the two parts of the key are generated, and the member is added to the ACL. For a departing user, the record of the user is deleted from the ACL. The departing user cannot decrypt the data on its own as he/she only possesses a part of the key not the whole key.

V. CONCLUSION

The security and efficiency of the data stored in cloud are the most challenging issues in the data sharing systems. The cryptographic techniques in the cloud must provide data protection, availability of the data and secure sharing of the data among group of users. This paper has aimed at giving a general overview and comparative analysis of the various cryptographic techniques that are being employed for use in the cloud computing environment and also the system architecture of the proposed system for secure data sharing in cloud.

REFERENCES

[1] T. Jiang, X. Chen, and J. Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation," IEEE Transactions on Computers vol: pp no: 99 year 2015.

[2] M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, and A. Y. Zomaya, "SeDaSC: Secure Data Sharing in Clouds," IEEE Systems Journal year 2015.

[3] S. Seo, M. Nabeel, X. Ding, and E. Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," IEEE Trans. Knowl. Data Eng., vol. 26, no. 9, Sep. 2014.

[4] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transactions on Dependable And Secure Computing vol.9 no.4 year 2012.

[5] C. Chu, S. S. M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage," IEEE Transactions on Parallel And Distributed Systems year 2013.

[6] C. Yang and J. Lai, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing," International Symposium on Biometrics and Security Technologies year 2013.

[7] Z. Zhu and R. Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud," IEEE Transactions on Parallel And Distributed Systems, vol. 27, no. 1, Jan. 2016.

[8] J. Wei, W. Liu and X. Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption," IEEE Transactions on Cloud Computing vol. 14, no. 8, Aug. 2015.

