IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education

Vol. 4, Special Issue 8, May 2017

Two Factor Data Security for Cloud Storage System

Naveen H N[1], Praveen M[2]

Department of ISE, BMS College of Engineering, Bangalore

Abstract: Cloud computing provides a cheap and resourceful solution for sharing group resources among cloud users at a low maintenance. In this current world, outsourcing data in multi owner fashion from un trusted cloud is still a tricky issue due to some frequent changes in membership. In this project, we propose a safe and sound data sharing process for vibrant groups in the cloud. By the usage of dynamic techniques, any cloud user can secretly share data with others, but here cloud will secure in an efficient way. The main objective of this project is that the cloud users can share their files such as pdf, txt, doc in a secure way by using the encryption and decryption methods. In this scenario, different Data owner will be in the cloud, those data owners can send the data to their group members in a secured way . Moreover, they will monitor their particular group activities. User will registered with their preferred group and share their files among that particular groups and if they like to share their file with all, there is an option like common sharing method. By using this option other group members can make use of it with proper verifications. Once user registered with valid data and with their preferred group selection. Data owner need to distribute group key to all their registered group members in a secure and authentic manner.

1. INTRODUCTION

Cloud storage is a model of online storage system where data is stored in storage which are generally hosted by third parties. There are many benefits to use cloud storage. The most notable is data access. Data stored in the cloud can be accessed at any time from any place as long as there is network access. The user need not worry about the storage maintenance cost such as buying additional storage as it is completely the task of the storage providers. Another advantage of cloud storage is data sharing between users. If Client A wants to share a piece of data (e.g. a video) to Client B, it may be difficult for her to send it by email due to the size of data. Instead, Client A uploads the file to a cloud storage system so that B can download it at anytime. Despite its advantages, outsourcing data storage also increased the threat for attacks. For example, when data is distributed, due to more locations, it will be vulnerable for physical attacks. By sharing the storage and network to many other user, it will also be prone to unauthorised access. This may be due to mistaken actions, faulty equipment, or sometimes because of criminal intent. The most effective solution is by using Encryption Technique. Encryption can protect data as it is being accessed to and from the cloud service. It can further protect data that is stored at the service provider. Even there is an unauthorized conflicts who has gained access to the cloud, as the data has been encrypted, the intruder cannot gain any information about the plaintext. Asymmetric encryption allows the encryptor to use only the public information (e.g. public key or identity of the receiver) to generate a ciphertext while the receiver uses his/her own secret key to decrypt. This is the most promising mode of encryption for data transition, due to the removal of key management existed in symmetric encryption. With data storage and sharing services (such as Dropbox and Google Drive) provided by the cloud, people can easily work together as a group by sharing data with each other. More specifically, once a user creates shared data in the cloud, every user in the group is able to not only access and modify shared data, but also share the latest version of the shared data with the rest of the group. Although cloud providers promise a more secure and reliable environment to the users, the integrity of data in the cloud may still be compromised, due to the existence of hardware/software failures and human errors . To protect the integrity of data in the cloud, a number of mechanisms have been proposed. In these mechanisms, a signature is attached to each block in data, and the integrity of data relies on the correctness of all the signatures. One of the most significant and common features of these mechanisms is to allow a third party verifier to efficiently maintain data integrity in the cloud without downloading the entire data, referred to as public auditing . For security reasons, when a user leaves the group or misbehaves, this user must be removed from the group. As a result, this removed user should no longer be able to access and modify shared data, and the signatures generated by this cancelled user are no longer valid to the group. Therefore, although the content of shared data is not altered during user removal, the blocks, which were previously signed by the removed user, still need to be re-signed by an existing user in the group. As a result, the integrity of the entire data can still be verified with the public keys of existing users only. An example is e-banking security. Many e-banking applications require a user to use both a password and a security device (two factors) to login system for money transfer. The security device may display a one-time password (OTP) to let the user type it into the system, or it may be needed to connect

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education
Vol. 4, Special Issue 8, May 2017

with the computer (e.g. through USB or NFC). The purpose of using two factors is to enhance the security protection for the access control.

II. RELATED WORK

In [1], B. Wang, B. Li, and H. Li proposed a public auditing mechanism for integrity with efficient user revocation in the cloud. They utilised the idea of proxy re-signatures. Once the user in the group is revoked, the cloud is able to resign the blocks, which were signed by the cancelled user, with a re-signing key. This mechanism is scalable which means its not only able to efficiently support a huge number of user to share data but also able to handle multiple files..

In [2], M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia proposed that cloud computing will grow rapidly. They state that regardless of the cloud providers sells services at a low cost or a high standard like AppEngine, they should focus on continuous scalability rather than single node performance. Application software needs to scale up as well as down and also need to acquire pay-for-use model to use cloud services. They believed hardware systems must be designed at the scale of container.

In [3], G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song focused on the checking if an untrusted serves stores a clients data. They proposed a model for provable data possession, in which it is better to minimise the file block access, the calculation on the sever and user server communication. The advantages of the proposed model are: they process in a low overhead at the server and require a small, constant amount of communication per transfer. The main components of the scheme is the key verifiable. They allow to verify data possession without having access to actual data file. Experiments proved that sampling of the server storage, make it feasible to verify possession of large data sets. In [4], HovavShacham and Brent Waters provide a proof-of-retrievability system. A data storage provider convinces the user that they store the entire data of the client. They provide schemes with full proofs of security against disputes in the huge model. They built a first scheme using BLS signatures and secure in the oracle model, has the shortest query and response of any proof-of-retrievability and verifiability. Their second scheme was built on pseudorandom functions (PRFs) which is more secure and has longer queries. In [5], C. Wang, Q. Wang, K. Ren, and W. Lou focus on the problem of data storage in cloud, Security. Cloud storage is a distributed data storage system. They provided an efficient scheme to promise the correctness of clients data in the cloud storage. If this is too much resource consuming on the client side, the task can be given to Third Party Auditor (TPA) and the tokens can be stored in users local device or the cloud storage in the encrypted format. Analysis showed that the scheme was highly efficient during bursty data losses.

3. PROPOSED WORK

Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error with the help of cryptographic techniques.Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and save.Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against load balance failure, malicious data modification attack, and even server colluding attacks.

ADVANTAGES

We motivate the public auditing system of data storage security in Cloud Computing, and propose a protocol supporting for fully dynamic data operations, especially to support block insertion, which is missing in most existing schemesWe extend our scheme to support scalable and efficient public auditing in Cloud Computing. In particular, our scheme achieves auditing tasks from different users can be performed simultaneously by the TPA.

Highly secured by using cryptographic techniques

1.Authentication module

Authentication is a function where a user presents some credentials to the Mobile. The user needs to be authorized to request services from the system. The New user, he has to get registered with a system and then authenticated before he can request Services. In a basic authentication process, a user presents some credentials like user ID and some more information to prove that the user is the true owner of the user ID. An example of this type of authentication process is the use of user ID and password.Users register their token to obtain secrets in order to later decrypt the data they are allowed to access. Users register their tokens related to the attribute conditions in ACC with the Owner, and the rest of the identity tokens related to the attribute conditions in ACB/ACC with the Cloud. When Users register with the Owner, the Owner issues them two sets of secrets for the attribute conditions in ACC that are also present in the sub ACPs in ACPB Cloud. The Owner keeps one set and gives the other set to the Cloud. Two different sets are used in order to prevent the Cloud from decrypting the Owner encrypted data.

2. Data owner

When data are highly sensitive, the data need to be encrypted before outsourcing to the cloud. However, when data are encrypted, irrespective of the underlying encryption scheme, performing any data mining tasks becomes very challenging without ever decrypting the data. Over time, either ACPs or user credentials may change. Further, already encrypted data may go through frequent updates. In such situations, data already encrypted must be re-encrypted with a new key. As the

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education
Vol. 4, Special Issue 8, May 2017

Cloud performs the access control enforcing encryption, it simply re-encrypts the affected data without the intervention of the Owner.

3.Security module

Data encryption:

The Owner first encrypts the data based on the Owner's sub ACPs in order to hide the content from the Cloud and then uploads them along with the public information generated by the AES algorithm and the remaining sub ACPs to the Cloud. The Cloud in turn encrypts the data based on the keys generated using its AES algorithm. Cloud takes the secrets issued to Users and the sub ACPs given by the Owner into consideration to generate keys.

Data decryption

Users download encrypted data from the Cloud and decrypt twice to access the data. First, the Cloud generated public information tuple is used to derive the encrypt key and then the Owner generated public information tuple is used to derive the key using DES algorithm. These two keys allow a User to decrypt a data item only if the User satisfies the original ACP applied to the data item.

4. User module

The Cloud User who have a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data. the User's Data is converted into data blocks . The data blocks are uploaded to the cloud. The TPA view the data blocks and Uploaded in cloud. The user can update the uploaded data. If the user wants to download their files, the data's in cloud is integrated and downloaded. In this module, the client sends the query to the server. Based on the query the server sends the corresponding file to the client. Before this process, the client authorization step is involved. In the server side, it checks the client name and its password for security process. If it is satisfied and then received the queries form the client and search the corresponding files in the database. Finally, find that file and send to the client. If the server finds the intruder means, it set the alternative Path to those intruder.

5.Cloud Service Provider (CSP)

A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems. Cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data..users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies.

6. Third Party Auditor (TPA)

An optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request. Security threats faced by cloud data storage can come from two different sources. As cloud servers may concurrently handle multiple verification sessions from different clients, given K signatures on K distinct data files from K clients, it is more advantageous to aggregate all these signatures into a single short one and verify it at one time. To achieve this goal, we extend our scheme to allow for provable data updates and verification in a multi-client system. The signature scheme allows the creation of signatures on arbitrary distinct messages. Moreover, it supports the aggregation of multiple signatures by distinct signers on distinct messages into a single short signature, and thus greatly reduces the communication cost while providing efficient verification for the authenticity of all messages.

4. IMPLEMENTATION

The implementation is divided into 3 levels

1. The first level shows the common functionalities of the User and Admin.
2. The second level shows the detailed functionalities of the Admin.
3. The third level shows the detailed functionalities of the User

The level 1 design consists of the basic functionality of the Admin and the User. The Admin logs in to the website and has the authority to manage and verify the files in the file list. The file in the file list can be accessed by the user only if the admin verifies the file. The basic functionality of the user is to first register using the personal credentials and logging in to the website. If the user wishes to share a file, he has to upload the file either in the doc, pdf or txt format. The file will be saved in the file list.

The level 2 design consists of the detailed functionalities of the Admin. The Admin handles all the files and data of the webpage. The Admin also acts as a Third Party Auditor (TPA). The purpose of an Admin is to develop an auditing scheme which is secure, efficient to use and possess the capabilities such as privacy preserving, public auditing, maintaining the data integrity along with confidentiality. The admin can also upload the files and add it to the file list. The basic functionality is to handle the files by verifying them. The files uploaded by the users will be saved to the file list only if the admin approves orverifies it. Admin can also delete the files if he finds the file harmful. Since the Admin is the main entity in the project, he is responsible for the encryption and storage of the files. This allows the admin to maintain the data security and privacy of the files and the users. The Admin stores and maintains the details of all the users and their private data.

The most important entity of the project is the end user. The end user is any person who is using the services provided by the cloud service providers. The user first has to register to the cloud by entering the registration page and entering the required personal details. Once the registration is done, the user can login to the webpage where his/her profile will be created. The user is allowed

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education
Vol. 4, Special Issue 8, May 2017

to share his files only to his group. The files uploaded by the user will be shared only with the users belonging to that group. If the user does not wish to share his files and use the cloud only for storage purpose, he has an option to make the files private. The files uploaded must be in doc, pdf or txt format. The user can view the files uploaded by him/her and the files uploaded by the users of the same group. The files will be displayed in a list format along withFileID, File name, File Size, Type of the file and the accessibility such as public or private. The user can download the files in the file list uploaded by the users of the same group. The files uploaded by the same group users will be stored as an encrypted file. The encrypted storage of these files ensures security to the files.

Fig 1. System Architecture

1. The details of the users are stored in a table as a database. 2. The files which are uploaded by the users are encrypted before storing.

3. The Encrypted files are stored locally in a system server. 4. The details of the users are privately protected as a database in the cloud.

5. The data about the users are stored using RDBMS in the cloud.

5. CONCLUSION

The project presents a two-factor data security protection mechanism for cloud storage system, in which a file uploader is allowed to encrypt the file with knowledge of the identity of a receiver only, while the receiver is required to use both his/her secret key and a security device to gain access to the file. The solution not only enhances the confidentiality of the data, but also offers the cancellation of the device so that once the device is lost, the corresponding cipher text will be updated automatically by the cloud server without any notice of the data owner. The project protects the file shared on the cloud in two ways; by encrypting the file and second is by sharing the file only with the user who has the generated key and the security device. This is twice the enhanced security than the ordinary security featured provided by the cloud service providers.

ACKNOWLEDGEMENT

We express our deep sense of gratitude to our respected and learned guide, Asst. Prof. Sowmya K. S., for her invaluable help and guidance. We are thankful to her, for her constant encouragement and support during the difficulties we faced in the making of our project. Her kindness instilled a sense of courage and a greater drive to accomplish our project. We are also grateful to our project coordinators who set us time frames to complete various phases of our project, which helped us approach our project Implementation, in a well-organized manner. And, it goes without saying, their encouragement and positive reinforcement when it was much needed was a great boost. We are also thankful to our HOD, Dr. Radhika K. R. and our Principal Dr. MallikharjunaBabu K, for providing us with such a wonderful opportunity to explore and experience the real application of our knowledge, acquired in Information Science Engineering. We are very grateful to our entire faculty and staff. We truly feel we are in the best department, with the entire faculty being absolutely down to earth and helpful at every possible time, when we, as students have approached them. They have been supportive from the beginning and never stopped at anything. They made us feel at home and have truly made our experience in college as if it was our second home. Lastly, our classmates, who are brilliant, openminded, always supportive and loving, and our amazing parents who have been there with us through everything, trusting in our future, in us, even when we could not.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revoation in the Cloud" in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing" Communications of the ACM, vol. 53, no. 4, pp. 50–58, April 2010.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores" in the Proceedings of ACM CCS 2007, 2007, pp. 598–610.

[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability" in the Proceedings of ASIA CRYPT 2008. Springer-Verlag, 2008,pp. 90–107.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing" in the Proceedings of ACM/IEEE IWQoS 2009, 2009, pp. 1–9