ISSN 2395-1621

Key Distribution and Trust Based Scheme on Big Data Analysis for Group User on Cloud Service

[#1]Mrunal Jagtap, [#2]Prof. A.M.Wade

[1]mrunalsjagtap5@gmail.com,
[2]amwade@sinhgad.edu

[#12]Department of Computer Engineering,

Sou.Kashibai Navale Collage of Engineering, Pune.

ABSTRACT

Now a days cloud computing has become more popular, so more information possessors are actuated to their information to cloud servers for great convenience and less monetary value in data management. In this project the problem of a secure data search with identity based authentication on cloud is solved by using encryption of data before it actually used. Here, we used data secure based ASE algorithm for searching, downloading the file from the cloud. This System presents those models the network behavior of user sessions across both the front-end web server and the back-end database. Implementing system monitoring both web and subsequent database requests. Most of the people do their transaction through web use. So there are chances of personal figures gets hacked then need to be provide more refuge for both web server and database server. For that purpose duel security system is used. The duel security system is used to identify & prevent attacks using Intrusion detection system. Duel security prevents attacks and prevents user account data from unauthorized updating from his/her account.

Keywords:- Encryption Algorithm, Data Privacy, Data Security, Notification System for Alert generation, Message digest.

ARTICLE INFO

Article History

Received: 18th June 2019

Received in revised form :

18th June 2019

Accepted: 21st June 2019

Published online :

22nd June 2019

I. INTRODUCTION

Cloud computing is an developed technology to store data into from number of client. A cloud computing user allows storing their data over cloud. The progressive technique is remote backup system which minimizes the cost of implementing more memory in an organization. It can be helps government agencies and enterprises to reduce the financial overhead of data management. They can extract data backups remotely to third party cloud storage providers than maintaining their own data center. An individual organization does not require purchasing the storage devices. Instead of they store their data to the cloud and archive data to avoid information loss in case of system failure like hardware or software failures.

Cloud storage is flexible, but security and privacy are available for the outsourced data becomes a serious issue. To achieve the secure data transaction in cloud, suitable cryptography method to be used. The data owner must after encryption of the file, store the cloud. If a third person downloads the file, they can view the record and if they had the key which is used to decrypt the encrypted file. To overcome this problem Cloud computing is one of the best technologies, which is contains huge open distributed system. It is an important to protect the data and privacy of user.

Attribute-based Encryption is one of the best most suitable schemes for the data access control in public clouds for it can be ensures data owners direct control over the data and it can be provide a fine -grained access control service. Now, there are many ABE schemes that is proposed in cloud, which can be divided into two types categories; Key Policy Attribute -based Encryption (KP-ABE) and the Cipher text Policy Attribute-based Encryption (CPABE). In KP-ABE schemes, decrypted keys are combined with access structures and in cipher texts it is labeled with special attribute sets, for the attribute management and key distribution an authority is responsible. The authority may be the human resource department in a company, the registration office in a university, etc. The data owner can

be defines the access policies and encrypts the data according to the defined policies. Every user that will be issued a secret key reflecting its attributes. A user can be decrypt the data whenever its attributes match the access policies. Access control methods that can be ensure that authorized user access data of the system.

Access control is a policy or procedure that can be allows, denies or restricts access to system. It also monitors and record all attempts made to access a system. Access Control can also identify the unauthorized users attempting to access a system. It is mechanism which is very much important for protection in computer security. The Cloud storage is a very important service in cloud computing. The Cloud Storage offers services for data owners to host their data over cloud computing environment. A big challenge of the data access control scheme is data hosting and data access services. Because data owners do not completely trust the cloud servers also they can no longer rely on servers to do access control, so the data access control is becomes a challenging issue in cloud storage systems. Therefore the decentralized data access control scheme to be introduced.

II. LITERATURE SURVEY

A. Multi-authority access control system

In this paper [1] they have explained access control systems for the public cloud storage, brings a single-point bottleneck on both side security and performance against the single authority for any specific attribute. Firstly design multi - authority access control architecture to deal with the problem. By introducing the combining of (t, n) threshold value secret sharing and multi-authority CP-ABE scheme, then proposes and realizes a robust and verifiable multi-authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set. Further by efficiently combining the traditional multi-authority scheme with this scheme, construct a hybrid one, which can satisfy the scenario of attributes coming from different authorities and achieving security and system-level robustness.

B. Attribute Revocation

In this paper [2] they proposed demonstrated that, with the component CUK a revoked user can be transform the new encrypted cipher text to a previous version, which can be further data decrypted with his/her revoked old-version secret keys.

C. Data access privilege and anonymity

In this paper [3] they proposed a semi-anonymous attribute-based privilege scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. In this proposed scheme was able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. The scheme was tolerant against authority compromise, and compromising of up to (N −2) authorities did not bring the whole system down. Author provides detailed about security and the feasibility of the scheme. Also it can be implements the real toolkit of a multi-authority based encryption scheme AnonyControl and AnonyControl-F.

D. Efficient and revocable data access

In this paper [4] they proposed a revocable multi -authority CP-ABE scheme, where efficient and secures revocation technique introduced to solve the attribute revocation problem in the system. Attribute revocation method is an efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security and the forward security. This scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semi-trusted in some scenarios, this scheme can still guarantee the backward security. At that time, apply proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for the multi-authority cloud storage systems.

E. Secure multi-owner data sharing for dynamic groups

In this paper [5] they proposed to achieve secure source of data sharing for dynamic groups in the cloud, combined the group signature and dynamic broadcast encryption techniques. This scheme describes the details of Mona including system initialization, user revocation ,user registration, file generation, file deletion, file access and the traceability. Also this scheme can be provides security to Mona in terms of access control, data confidentiality, anonymity and traceability.

F. Provably secure scheme under keyword guessing attack

In this paper [6] they proposed allows a third party knowing the search trapdoor ofa keyword to search encrypted documents containing that keyword without decrypting the documents .However, it is shown that the keyword will be compromised by a malicious third party under a keyword guess attack (KGA) if the keyword space is in a polynomial size. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. Cloud service providers are separate administrative entities, moving to the commercial public cloud deprives users of direct control over the systems that manage their data and applications. To enable ranked searchable symmetric encryption for the effective utilization of the outsourced cloud data under the different model. Exploitring the signatures to compute verification metadata needed to audit the correctness of shared data.

III. PROPOSED METHODOLOGY

A. Architecture

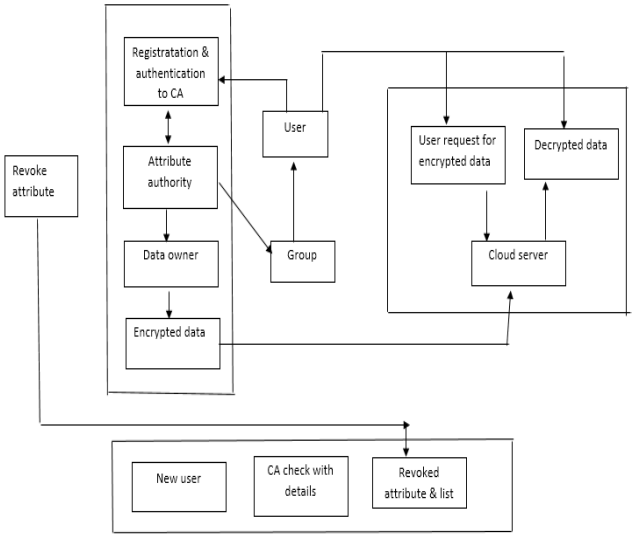


Fig1. System Architecture

1. Registration :

Each user registers to the CA by providing their details. CA provides a global unique ID and certificate for each user who entering into the system. AA should also be registered to the CA. For each AA, CA provides Global unique ID and submits the certificates provided for each user in the system. The user details, AA details are stored in database.

2. Authentication :

Users provide the id obtained from CA, while login for the data access in CSP. CSP validates the id using the details stored in database. If the id is valid, users are allowed for the data access in cloud, Otherwise access is denied for the user.

3. Data Processing and Encryption by owner:

Data processing includes the data owners first split the data into multiple components according to logical granularity. Data owner collects the attributes generated by the AA and design the access policy for each attributes.

4. Encryption by Owner:

The data owner encrypts the data with content keys using symmetric encryption algorithm. Then the content keys are encrypted based on access policies of each attribute and send the encrypted data together with Cipher texts to the cloud.

5. Decryption by user

The user requests for the data to the cloud. If the users attribute and access control rights are satisfied, user can download the data from the cloud. User first decrypts the data for the content keys using their secret keys. Using the content keys user decrypts the original data.

B. FLOW CHART

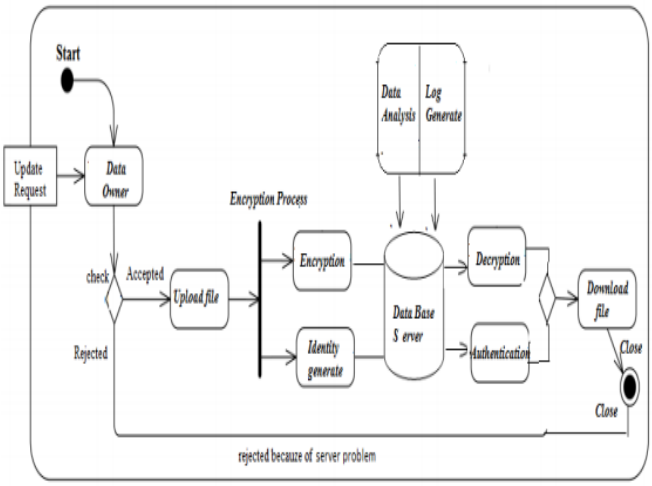


Fig2: Flowchart

1) **Data Owner:** They are responsible for uploading the files and granting access permission to the users of the respective group user. Admin has the main access permission for maintaining the files over cloud. Admin can navigate through the group as well. Admin can view the log details of the activities carried on the cloud file storage.

2) **User:** Every user needs to register with the corresponding group for getting access permission and signature key from the same. Using the signature key they can get the access permission. They can upload the files to cloud. User from same group can view the content of the file from cloud and make changes over it and can save them. Simultaneously they can download the files as well.

3) **Third Party Auditor (TPA)**: TPA has the rights to validate the files which are available in the cloud. TPA is the respective authority for performing the verification of files which are uploaded by any user who are registered under a single group.

4) **User Operations:** User can revoke their account at any cost. The file key will be generated while upload each file into the cloud. Every member can view the files which are available for the download access through the group. This is the list of files available in the cloud for members.

5) **Temper analysis server:** Admin is the authorized person, he check all the user activity records as well as profile. He also manage the tempering on changing the values from data base. Here we use the algorithm for analysis the unauthorized changes made on the databases server.

IV. ALGORITHM USED

Algorithm:

AES Algorithm:
For encryption of data:-

START
Step 1- U=Upload (file), he input is consider as Text, is being converted to 128 bit plain text.
Step 2- R= Read (input file),

Step 3- K=Key generation (file)
e.g= key=123456;
Step 4- E=Encrypt(file, key), encode the upcoming file
Step 5- C=Convert (file),
If(encrypt), then file convert plain to cipher text
Split (file1, file2);
Stored (file)
Else, file not encrypted
Step 6- D=Decrypt (file), decode the file
if (decode), then file convert cipher text to plain
Combine (file1, file2);
Else, file not decoded
Step 7- Download file
END.

MD5 Algorithm:

The main MD5 process consist of five steps that is used to analysis database modification result which are as follows:

Step 1: Append padding bits
The message is padded so that its length is congruent to 448, modulo 512. The message is extended so that it is just 64-bit shy of being a multiple of 512 bits long. So, "1" bit is appended to the message and then 0 is appended so that the length is congruent to 448.

Step 2: Append length
A 64-bit representation of length of message before padding bits were added is appended to the result of the previous step.

Step 3: Initialize MD buffer
A four-word buffer is used to compute the message digest where each of the 32-bit register is initialized in hexadecimal, low-order bytes.

Step 4: Process message in 16-word bits
The four auxiliary function is then processed with various steps to produce the desired output.

Step 5: Output
The message digest is produced as an output. The hashed values is changed then log will generated.

V. RESULT AND DISCUSSIONS

To provide secure and efficient system for securing the file from unauthorized access AES and MD5 algorithm is used .MD5 algorithm is used for the hash key generation and authentication of registered users. And AES algorithm is used for encryption and decryption purpose and new concept is added i.e. key distribution. The file is stored in splited form.

Table 1 Log table

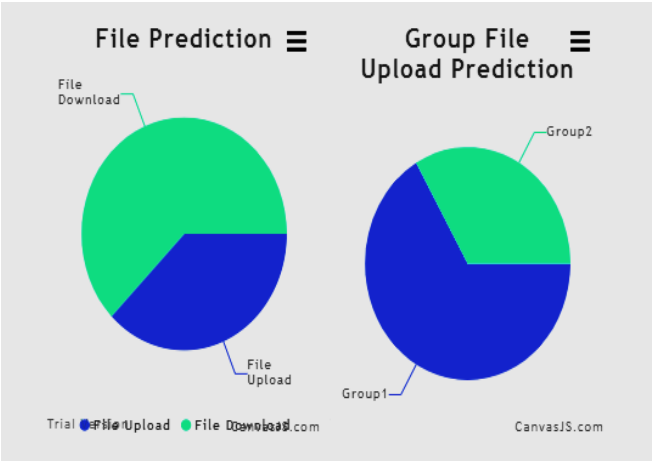
Input File	Group User	Log Status	Date and Time
Abc.txt	Group 1	Upload	2019/Jan/10 13:52:45
Pqr.txt	Group 2	Upload	2019/Jan/06 11:08:26
Xyz.txt	Group 2	Download	2019/Jan/20 16:33:25
Abc.txt	Group 1	Deleted	2019/Jan/09 10:55:05

In table 1, describes the details about file i.e. log status, date and time of that file. Table 1,gives the result to the server which file is under which group and any unwanted activity is happen from the user with data and time. Here show the file log detail for future analysis.log status describes the file related operations like encryption, decryption and modification.

Table 2 File description table

Input File	Data	Key	User
Abc.txt	4Al1qf3cDLDiV3VS84WgAmJSwTZDLamXQS/8j+O/WVOeff41+	RhXJuxk1sqI=	mayuri
Pqr.txt	qL47Dw99tF5xF7j0apw4ZBBnoA4rN4/aSJTp1x8jyW/Ffn8b5LfeosjxwFAGhZRL0UT536hq5UazPKu92HPumrFg/96ZoXFJBckohTW6J0	o0nxR1fFy6049JEXW4a8ng==	nadan
Xyz.txt	m2n5/KHUesBGZ7L4xAh6srJxNzEIzm7bDglfc50awArxC31T0jlWpKYp06QLccojJcf0GukyO0RzUEm0bvGwUZ2Vn/ddlXBKMYfe12pUY4KPIZ7cRV/gc6mknEX0pCBsuq	nq+tfIXyTR1gkCCaOzFKaQ==	Shiva

In table 2, data includes the encrypted data and there key .the key is generated using AES algorithm. The AES algorithm is very efficient for the encryption and decryption of file.



In graph 1, the computational speed of encryption and decryption and the complexity analysis of the reported and proposed algorithm have been mentioned.in above graph ,the group file prediction indicates the how many users are in groups.it describes the how many users are registered in which group.

VI. CONCLUSION

Our propose technique provides data security using data encryption in cloud environment. We introduce a relative addressing method in which data will check at entry level when user uploading phases. Data privacy has become extremely important in the Cloud environment. The object interface offers storage that is secure and easy to share across platforms.

REFERENCES

[1] Wei Li, and JiananHong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL.24, NO. 06, October 2015.

[2] Jianan Hong, and Wei Li, "Comments on "DAC-MACS: Effective Data Access Control for Multi-authority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multi-authority Data Access Control for the Cloud Storage Systems", IEEE transactions on information forensics and security, VOL. 10, NO. 06, June 2015.

[3] Taeho Jung, Xiang-Yang Li, "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption", IEEE transactions on information forensics and security, VOL. 10, NO. 01, January 2015.

[4] Kan Yang and XiaohuaJia, " Efficient, and Revocable Data Access Control for Multi-Authority in Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2014.

[5] Hideaki Ishii, and Er-Wei Bai, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Transactions on parallel and distributed systems, VOL. 24, NO. 06, June 2013.

[6] Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute-based encryption," in SP'07.IEEE Computer Society, 2007, pp. 321{334.

[7] BhartiRatan Madnani,Sreedevi N, Attribute Based Encryption for Scalable and the Secure Sharing of the Medical Records in Cloud Computing Design and Implementation" Interrnational Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 3May 2013.

[8] B.Waters, Ciphertext-policy attribute-based encryption: An expressive, efficient, and proxy-ably secure realization," in PKC'11. Springer, 2011,pp. 53.

[9] Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, B Waters - Public Key Cryptography{PKC 2011, 2011.

[10] D. Boneh and M.K. Franklin, Identity-Based Encryption from the Weil Pairing," in Proc. 21st Ann. Int'l Cryptology Conf.Advances in Cryptology - CRYPTO'01, 2001, pp. 213-229.

[11] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-Policy Attribute-Based Encryption," in Proc. IEEE Symp.Security and privacy (SP'07), 2007, pp. 321-334.

[12] J. Hur and D.K. Noh, Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

