|| Volume 3 || Issue 6 || June 2018 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

Secure and Efficient Data Access Control for Public Cloud Storage with Multiple Attribute Authorities

Miss. Manasi Shet[1],Dr. S. N. Kini[2]

Department of Computer Engineering JSPM's Jayawantrao Sawant College of Engineering,Hadapsar ,Pune-28 [1]

Department of Computer Engineering JSPM's Jayawantrao Sawant College of Engineering,Hadapsar ,Pune-28[2]

manasi.shet@gmail.com,snkini@gmail.com

ABSTRACT: ***Protecting the data and controlling its access is a challenging problem for cloud storage which is open for public. Ciphertext Policy Attribute-Based Encryption (CP-ABE) has been embraced as a promising ability to give flexible, fine-grained and secure information access control for public cloud storage with genuine yet inquisitive cloud servers. However various works have been proposed utilizing CP-ABE technique, in which the single attribute authority must execute the tedious client authenticity confirmation and secret key distribution and thus it brings about a single point execution bottleneck when a CP-ABE technique is embraced in a large-scale cloud storage framework. Clients may be stuck in the waiting line for a long stretch to get their secret keys, which results in low-efficiency of the framework. Even though the multiple authority access control plans are proposed, these plans still not able to conquer the disadvantages of the single-point bottleneck problem and low efficiency; because of the way that each of the authority still autonomously deals with a disjoint attribute set. In this work, it has been proposed a novel system to expel the issue of single point execution bottleneck and give a more effective access control scheme with an auditing system. This framework utilizes multiple attribute authorities to share the heap of client authenticity check. In the interim, in this plan, a CA (Central Authority) is acquainted with producing secret keys for authenticity checked clients and each of the AAs (Attribute Authorities) in our scheme manages the whole attribute set individually. This system makes performance improvement in key generation and also guarantees security requirement. To improve the system, it has been proposed to choose one among AAs to act as CA instead of separate CA and have an observer to trace if CA is working properly or not. If observer finds any discrepancy it creates a report and new CA chosen from AAs. This makes the system more secure and efficient and emanates forensic analysis.***

KEYWORDS- Public Cloud storage, Access control, Auditing, CP-ABE, Multiple Authority.

I INTRODUCTION

Cloud computing has drawn substantial recognition from both industry and academic to satisfy the requirement of data storage and high-performance computations. Cloud computing gives major favor as cloud storage which enables data owners to store their data in the cloud through the Internet. Advantages of utilizing cloud storage include greater accessibility, higher reliability, fast deployment and more grounded security are few just to name. Regardless of these mentioned benefits, cloud storage leads to new challenges on data access control, which is the basic issue to guarantee information security. Since cloud storage is operated by cloud service providers, whom data owners cannot trust, the traditional access control methods in the Client/Server model are not suitable for cloud storage environment. The access control of information in cloud storage system thus has turned into a challenging issue. To solve the problem of access control in cloud storage, there have been many schemes proposed, among which Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is best suitable technique. By using CP-ABE scheme data owner can control their data to provide the user with robust, secure and fine-grained data access control for the cloud which is an important characteristic of CP-ABE scheme. In CP-ABE schemes, the access control is accomplished by using cryptography, here an owners data is encrypted with an access policy over attribute set, and a user's secret key is labeled with his/her own attributes. If the attributes related to the user's secret key satisfy the access policy, then only the user can decrypt the corresponding ciphertext to get the plain-text. Till now, the CP-ABE based access control schemes for cloud storage have been developed into two integral classifications, to be specific, single authority scenario and multi-authority scenario. In most existing CP-ABE schemes there is just a single authority in charge of attribute management and distribution of secret keys. This single attribute authority situation can lead to single point bottleneck on performance and security. When the authority behaves maliciously, a foe can without much of his/her efforts can easily acquire the one and only authority's master key, and can create secret keys of required attribute set and then can decrypt the particular ciphertext. Also, when the single authority is damaged, the system totally cannot function admirably. For this reason, the single authority CP-ABE schemes are not broadly used for data access control. Even though there is multi-attribute authority CP-ABE schemes are proposed, they could not solve the problem of the single-point bottleneck on both performance and security specified previously. In proposed multi-authority CP-ABE schemes, the entire characters set is split into numerous disjoint subsets and every characteristic subset is managed by just a single authority. A clear idea to remove the single-point bottleneck is to enable multiple attribute authorities to together deal with the universal attribute set, in such way that each one of them can distribute secret keys to clients independently.

In this work, it has been proposed a novel access control scheme to address the low efficiency and single-point execution bottleneck for public cloud storage. It proposes a robust and efficient system with single CA (Central Authority) and numerous AAs (Attribute Authorities) for public cloud storage. The heap of client authenticity confirmation is shared by multiple AAs, each of which deals with the universal attribute set and can autonomously complete the client authenticity check, while CA is in charge of computational assignments which create secret keys for authenticity confirmed clients. To upgrade security, we additionally propose an auditing system to find which AA (Attribute Authority) has inaccurately or maliciously performed the authenticity confirmation procedure. Along with this auditing mechanism in our work we are proposing to choose one among the AAs to act as CA instead of separate CA and will have an observer computer to trace if CA is working properly or not. If observer finds any discrepancy, it generates a report. This makes the framework more secure and efficient.

II REVIEW OF LITERATURE

PRSE (Personalized multi-keyword Ranked Search over Encrypted data) Framework

In Cloud computing searchable encryption is a challenging task. However, most of the existing works follow the model of one size fits all and ignore per-sonalized search over outsourced encrypted data. So PRSE framework solves the problem of personalized multi-keyword ranked search over encrypted data by preserving the security of the system in cloud computing. This framework using semantic ontology WordNet by analyzing users searching history and by adopting a mechanism for producing a score which expresses data consumer interest, builds user interest model for every data consumer. This framework supports both personalized multi-keyword ranking search and query extension. Users interest model is built upon users search history since a long time and it exists on the user side. Using WordNet, the access frequency of both requested keywords and keywords related to them are recorded. Different access frequency of keywords as different priority reflects the different importance of keywords with respect to users interest. The data consumer has to generate a request for search first in order to start with search for interested file. Then user interest model will carry out query reformulation which achieves user keyword priority of query terms. After query using search control mechanism encrypted search will be sent to the cloud server. After receiving a search query from an legal user, the cloud server will conduct some designated search over the index and ranked relevant encrypted documents will be returned by cloud server. Here cloud server is the single authority who does searching, indexing and ranking of relevant documents and sends back to the user[1].

Content aware search over encrypted data

There are many schemes have been proposed to make encrypted data searchable over cloud based on keywords. However, the keyword-based search cannot fulfill the user intention of search as they do not follow semantic representation of information of users retrieval. This work proposes a semantic search scheme which depends on concept hierarchy as well as the semantic re-lationship between them. Here in this scheme documents get indexed first and the trapdoor will be built based on the concept hierarchy and it is further improved for organizing all the documents index vectors by utilizing tree-based index structure. In recent years, the general procedure for searching encrypted data involves five steps: document feature extraction, creating an index which is searchable, creating trapdoor for search, using trapdoor searching the index and return the search results. In this work, using related knowledge of domain concepts of a stored dataset, concept hierarchy tree is constructed. For each document two index vectors are generated, one for matching the request containing the concepts for search and one more is used to decide the attribute value which satisfies the request for the search. The owner of the data constructs a concept hierarchy which is depended on related knowledge of domain concepts of the documents in datasets to be uploaded, then based on the concept hierarchy and key concepts of the document ,two index vectors for each document of the dataset are created and at last index which is used for searching is developed using all the index vectors. Using encrypted trapdoor for search, the legal user is able to search required document from the stored encrypted datasets in the cloud. As soon as the cloud server receives the trapdoor, searchable index will be searched for required document and satisfies the search request by returning the encrypted documents.[2]

Attribute Based Access Control with Efficient Revo-cation

CP-ABE is a most favorable cryptography technique for imposing access control policies defined by the owner on his stored data in the cloud. This leads to several problems with respect to the user and attributes revocation. This work proposes access control policies with the efficient user and attributes revocation capability. Dual encryption mechanism which makes use of the attribute-based encryption and selective group key distribution in each attribute group is used to get fine-grained access control of data.[6]

LABAC Framework

CP-ABE is used for data access control which depended on users unchangeable attributes/properties. However, in some situations, the access policy depends on users both permanent and temporary conditions. In LABAC (Location-aware Attribute Based Access Con-trol) framework data consumers access policy is decided by their properties as well as their changing locations. To get fine-grained access to the data LABAC defines access structure by combining CP-ABE with location trapdoors. LABAC is used for sensitive data encryption under access structure defined and uploading to the cloud. The attributes are handled using CP-ABE and location information is introduced using trapdoor inside access policies. Location servers are used to release the trapdoors for users. Location servers provide tokens with which the trapdoors can be released. To decrypt the ciphertext users attribute set should satisfy the access policies formulated by owner and get the tokens from location servers to release the trapdoors. Users private key is only related to attribute set and not with temporary locations as the trapdoor does not depend on their attribute set. Therefore when the location changes, there is no need of revoking and reassigning of users. Thus trapdoor reduces the burden of revoking and reassigning. In LABAC multiple trapdoors are associated with every ciphertext and location trapdoors are set randomly in the access structure with attribute set. In this system model there six entities: the cloud servers, many data owners, many data users, an attribute authority, and multiple location servers, each with sensors. Under access struc-ture, the owner encrypts his/her data defined by him/her and uploads data to the cloud. Attribute authority is responsible for setting up the system and distributes private keys to users with respect to their attribute keys. The location servers are the servers that are needed to provide location information which in turn needed for providing access privileges are located in particular areas. It helps users to release trapdoors by providing tokens. It states users location by using sensors. To help location servers to authenticate users location, sensors are deployed in the areas around them. The data user can download any interested ciphertext from the cloud server and decrypts it as he/she has private key with respect to his/her attribute set. The platform to store owners data and share data to the user is provided by cloud server. In this framework attribute, authority is a single authority who handles setting up the system, key generation, and distribution due to which it leads to single point bottleneck problem even though it provides location-aware access privilege[8].

DAC-MACS Framework

In DAC-MACS(Data Access Control For Multiple Attribute Authority Cloud Storage) framework a multi-authority CP-ABE scheme is used where each attribute authority maintains disjoint attribute set which is proposed to provide efficient attribute revocation technique and efficient decryption for it, which is applied to get robust data access control with multiple attribute authorities in cloud storage system.The CA is a reliable Certificate Authority in the system who initializes re-quired parameters and registering of AAs and users. For every authenticated user, CA allocates a globally unique uid.CA creates a global secret and public key pair for the data consumer. AA is an attribute authority who in-dependently issues, revokes and updates users attributes with respect to their identity in the discipline.Each at-tribute is related to single AA and every AA maintains a random number of attributes. Each AA generates public attribute key for every attribute associated with it and also generates a secret key for the user who possesses same attribute set. The cloud server stores the ciphertext of the owner and authenticated data consumer can access it. It creates ciphertext token using secret keys generated by AAs for the users to decrypt the ciphertext.The exact decryption token can be generated if and only if attribute set fulfills the access structure in the ciphertext. To get ciphertext decryption token user has to submit global secret key and the public key generated by some AAs to the server. After server generates decryption token, using this token along with global secret key user the ci-phertext can be decrypted by the user.When there occurs attribute revocation the server does ciphertext update. Every owner splits his/her data into several components depending on logical granularities and using symmetric key algorithms every component will be encrypted with content keys. These content keys are encrypted by the access structure defined by the owner with respect to attributes from different attribute authorities. Then the owner sends the ciphertext along with the encrypted content keys to the server. Thus it provides efficient decryption method using token based decryption. It also provides efficient attribute revocation techniques which facilitates both backward security and forward security. It is efficient means it occurs with less interaction and less calculation cost.The new data consumer is able to decrypt the earlier broadcasted data encrypted with earlier public keys if it possesses sufficient attributes. This is called forward security.The revoked users cant decrypt the new ciphertext as it needs already revoked at-tributes for decryption. This is called backward security. Even though it provides efficient decryption method and efficient attribute revocation method it leads to single point bottleneck problem as multiple attribute authorities act a single authority since each AA maintain disjoint attribute set[9].

TMACS Framework

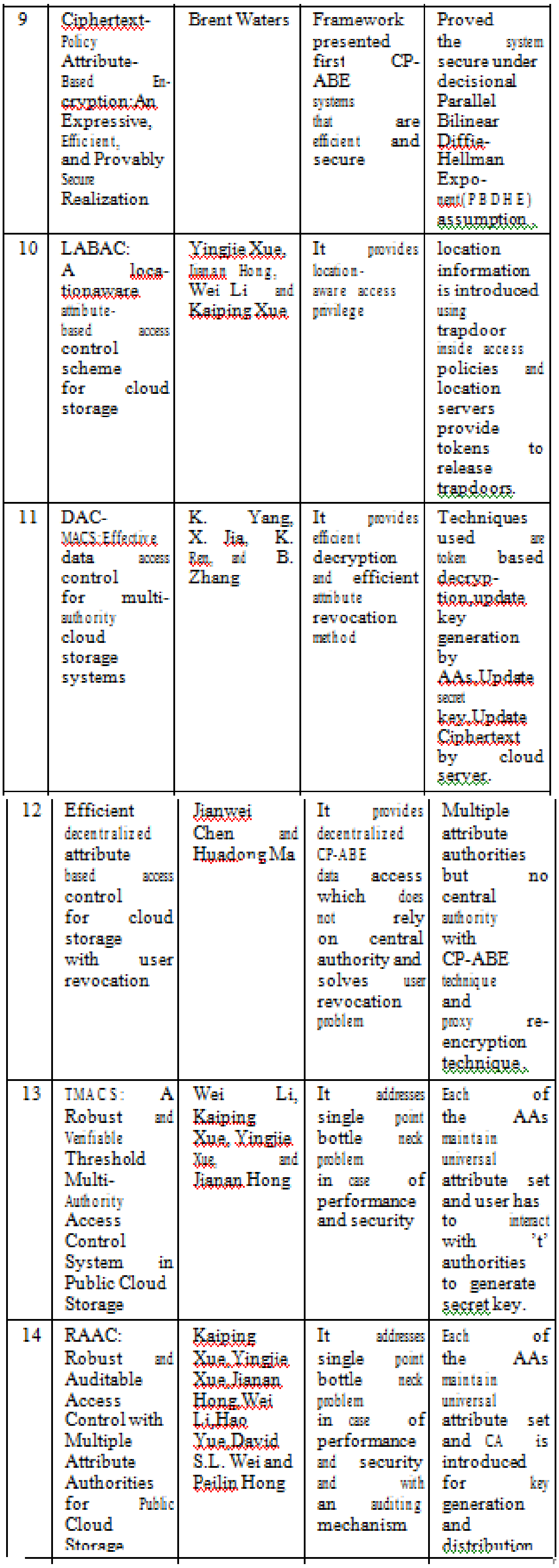
In TMACS(Threshold Multi-Authority Access Control System) with multiple authorities for public cloud storage system, CP-ABE scheme is used which guarantees owner to get full control over his/her data. In previous multi-authority schemes like DAC-MACS, multiple attribute authorities maintain disjoint attribute subsets; however, it results in single point bottleneck problem. In order to solve this, TMACS is proposed where multiple authorities jointly manage a uniform attribute set. In this framework, the master key is shared among multiple attribute authorities by making use of (t,n) secret sharing threshold and any authenticated data consumer is able to generate a secret key by interacting with any t attribute authorities among n authorities. In this framework, the CA is the globally trusted entity responsible for setting up the system and initializing required parameters. It assigns unique user identity for the authenticated data consumer and aid for every

It determines the threshold value for AAs who are included in the secret key creation at every time. The AAs do attribute management and key generation. Unlike previous multiple attribute authority schemes, AAs together maintain the entire attribute set.Every AA gets its share of mater key as its private key due to the cooperation of AAs among themselves for sharing the master key. In secret key generation phase, AA independently generates the corresponding secret key and there is no communication between AAs. Now the owner sends the ciphertext along with the encrypted symmetric key which is encrypted using access structure to the cloud. The legal data consumer can obtain the interested ciphertext from the cloud server, however, the data consumer can decrypt the ciphertext if and only if the access policy formulated by owner satisfies, the attribute set possessed by the user. The cloud server provides the owner platform for storing and sharing their data. Performance and forensic analysis show that TMACS is reliable when less than t attribute authori-ties are incorrectly behaved and also robust when all the attribute authorities are active in the system. This framework solves the issue of single point bottleneck in both execution and security; however, it is not efficient because the user has to interact with 't' authorities and thus adds higher interaction overhead[11].

TABLE I

LITERATURE ANALYSIS

Sr. No.	Paper Name	Author	Advantages	Techniques
1	Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improve-ment	Zhangjie Fu,Kui Ren,Jiangang Shu,Xingming Sun	It provides personalized multiple keyword search over outsourced encrypted information	Using semantic ontology wordnet user interest model is built.
2	Towards efficient content-aware search over encrypted outsourced data in cloud	Zhangjie Fu,Xingming Sun,Sai Ji,Guowu Xie	The primary advantage is semantic search is made more successful	Tree based index structure for indexing and trapdoor based on concept hierarchy Is used.
3	A dynamic secure group sharing framework in public cloud computing	Kaiping Xue,Peilin Hong	It enables group members to share data through cloud by preserving security	This Framework uses Proxy signature, enhanced TGDH And proxy re-Encryption techniques.
4	Attribute-based access to scalable media in cloud-assisted content sharing Networks	Yongdong Wu Zhuo H. Deng	The primary advantage is access to scalable media content	Multi message CP-ABE technique using access privilege tree with tree hierarchy is used.
5	Improving security and efficiency in attribute based data sharing	Junbeom Hur	It solves key-escrow problem and supports fine grained user revocation	Escrow-free key issuing protocol and proxy re-encryption is used.
6	Attribute-based access control with efficient revocation in data outsourcing systems	Junbeom Hur, Dong Kun Noh	Along with access control capability provides efficient user and attribute revocation capability	Technique used is dual encryption mechanism which uses ABE and selective group key distribution.
7	TAFC: Time and attribute factors combined access control on time sensitive data in public cloud	Jianan Hong, Kaiping Xue, Yingjie Xue, Weikeng Chen, David S.L. Wei, Nenghai Yu and Peilin Hong	Access Control is provided for time sensitive data	In CP-ABE algorithm trapdoor is used for time release function.
8	Improving Privacy and Security in Multi-Authority Attribute-Based Encryption	Melissa Chase,Sherman S.M. Chow	Attribute based encryption without trusted central authority which avoids con-fidentiality depending on security of CA	PRFs (pseu-dorandom functions) used to make the key user specific.



9	Ciphertext-Policy Attribute-Based Encryption:An Expressive, Efficient, and Provably Secure Realization	Brent Waters	Framework presented first CP-ABE systems that are efficient and secure	Proved the system secure under decisional Parallel Bilinear Diffie-Hellman Expo-nent(PBDHE) assumption.
10	LABAC: A loca-tionaware attribute-based access control scheme for cloud storage	Yingjie Xue, Jianan Hong, Wei Li and Kaiping Xue	It provides location-aware access privilege	location information is introduced using trapdoor inside access policies and location servers provide tokens to release trapdoors.
11	DAC-MACS:Effective data access control for multi-authority cloud storage systems	K. Yang, X. Jia, K. Ren, and B. Zhang	It provides efficient decryption and efficient attribute revocation method	Techniques used are token based decryp-tion,update key generation by AAs,Update secret key,Update Ciphertext by cloud server.
12	Efficient decentralized attribute based access control for cloud storage with user revocation	Jianwei Chen and Huadong Ma	It provides decentralized CP-ABE data access which does not rely on central authority and solves user revocation problem	Multiple attribute authorities but no central authority with CP-ABE technique and proxy re-encryption technique.
13	TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage	Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong	It addresses single point bottle neck problem in case of performance and security	Each of the AAs maintain universal attribute set and user has to interact with 't' authorities to generate secret key.
14	RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage	Kaiping Xue,Yingjie Xue,Jianan Hong,Wei Li,Hao Yue,David S.L. Wei and Peilin Hong	It addresses single point bottle neck problem in case of performance and security and with an auditing mechanism	Each of the AAs maintain universal attribute set and CA is introduced for key generation and distribution

III. EXISTING SYSTEM

In the existing system, it has been proposed a framework to remove the problem of single-point performance bottleneck and provide a more efficient access control scheme with an auditing mechanism with single CA for key generation and distribution ,who is assumed to be trust worthy and multiple attribute authorities for client authenticity verification.

IV. PROPOSED SYSTEM

In the proposed system, it has been proposed a novel framework to improve the security of the system along with single CA and multiple AAs and auditing mechanism, an observer machine is added in the system which monitors CA for its behavior.It checks whether CA is doing anything else other than what it has claimed to do.If observer finds any discrepancy then it generates a report regarding it.Then a new CA has chosen among AAs.In this system there is no separate CA, instead, CA is chosen among AAs and CA is not assumed to be trustworthy. This system along with solving the problem of single point bottleneck in case of performance and efficiency makes the system more secure.

A. System Architecture

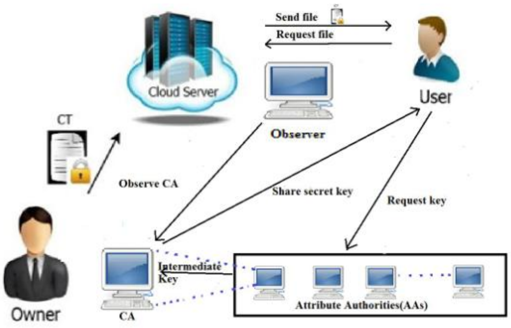


Figure. 1. System Architecture

B. Data Owner

Data owner uses the symmetric key algorithm to encrypt the information. He/She formulates the access structure using an attribute set and then the symmetric key will be encrypted under the access structure with respect to the public keys obtained by CA.

C. User

The data user (consumer) is allocated with a global identity Uid by CA. It can get any interested encrypted data from the cloud and the user can decrypt the encrypted data if and only if its attribute set satisfy the access policy.

D. Central Authority (CA)

It is the administrator of the entire system. It helps in system construction, initializing required parameters and generating public keys for attributes from the universal attribute set. It generates unique ids for AAs and users after registration.

It generates secret keys for legitimacy verified users. It has the capacity to trace which AA has maliciously verified a user.

E. Attribute Authorities (AAs)

The attribute authorities (AAs) manages the whole attribute set individually so it can perform legitimacy verification of any user independently. AAs verify users legitimate attributes and generates an intermediate key to assist CA to generate secret keys.

F. Cloud Server

Cloud servers provide the public platform with which own-ers can store and share encrypted information. Encrypted data can be freely downloaded by any user.

G. Observer

An observer is a system or a protocol in a system which monitors the CA for its behavior. It checks whether CA is doing anything else other than what it has claimed to do. If observer finds any discrepancy then it generates a report regarding it. Then the current CA leaves its position and becomes AA and a new CA has chosen among AAs.

V.SYSTEM REQUIREMENTS

A. Software Requirement

1) Operating System : Windows7/XP
2) Application Server : Tomcat5.0/6.X, Glassfish
3) Front End : HTML, Java, Jsp
4) Scripts : JavaScript
5) Server side Script : Java Server Pages.
6) Database : Mysql 5.5
7) Database Connectivity : JDBC.
8) IDE : Netbeans 7.4

B. Hardware Requirement

1) Processor : Intel 4
2) CPU Speed : 1.1 GHz or Higher
3) RAM : 2 GB or Higher
4) Hard Disk : 100 GB or Higher

VI. MATHMATICAL

MODEL Let, S be the whole System,

S = fI, P,

Og......................(1) I = Input

P =

Procedure O

= Output

I = f I0, I1, I2, I3, I4, I5 g.....(2)

I0 = Owner Logins f O0, O1, O2, ..., On g

I1 = Encryption Keys f Sk1, Sk2, ..., Skn g

I2 = Files to be Uploaded f F0, F1, ..., Fn g

I3 = Cloud Setup f , U g

I4 = User Logins f U0, U1, U2, ..., Un g

I5 = Key request By data Users f R0, R1, R2, ..., Rn g

P = f P0, P1, P2, P3, P4, P5, P6, P7, P8, P9, P10, P11, P12 g........................(3)

P0 = Owner Verification By CA

P1 = File Verification By CA

P2 = User and AA Registration

At the time of system initialization every AA and user sends registeration request to CA

P3 = Generation of UID by CA

Every legal user gets unique identity U id Z_p, randomly chosen private key k_{Uid} Z_p and computed corresponding public key P K_{Uid} = g^kUid . Legal user also gets certificate $Cert_{Uid}$ which contains P K_{Uid} from CA.

P4 = Generation of AID by CA

Every legal AA gets Aid, private key k_{Aid}, public key P K_{Aid} and certificate $Cert_{Aid}$ from CA

P5 = Formulation of Access Policy

The owner to define the access policy A, defines monotonic boolean formula and converts it into LSSS access structure, which can be expressed as (M,),where M is l x n matrix,l represents specific attribute set of particular access policy and n value depends on monotonic boolean formula.The function maps each row of matrix M to particular attribute, that is (i) fAtt_1,Att_2,.....,Att_U g[14]

P6 = Encryption of the file to be uploaded

The owner selects a random number k G_T as sym-metric key and using symmetric key algorithm, encrypts the plain text message M with k.The encrypted data can be represented as E_k(M).Then the owner encrypts the symmetric key k using CP-ABE under access policy defined ,in which random secret parameter 's' is used to encrypt symmetric key k

P7 = Uploading the file to the cloud

The owner along with encrypted data ,encrypted symmetric key using Access policy A will upload to the cloud.

P8 = Verification of user by AA

P9 = Generation of Intermediate Key

After successful verification AA_i obtains current time stamp value TS,computes t1=H(U id_jjjTSjj0) and t2=H(U id_jjjTSjj1)where U id_j is the Uid of user U_j and generates intermediate key $IC_{Aidi;Uidj}$ which is given as[14]:

$$IC_{Aidi;Uidj} = fK_x = h^{k\ Aidi\ t1}_x\ ,\ J_x = h^{t\ 2}_x\ g_{8x\ Sj}$$

where S_j is the verified legitimate attribute set for the user with identity U id_j.Finally this AA securely sends the following message CA:

$$fU\ id_j,Aid_i,S_j,IC_{Aidi;Uidj}\ ,TSg$$

P10 = Secret Key Generation by CA

CA uses intermediate key and its MSK to generate secret key SK_j for the user as follows:

K=g (P K_{Aidi} $)^{a\ t}$1 $g^{a\ t}$2 = g ($g_{Aid}{}^{k}{}_{i}$ $)^{a\ t}$1 $g^{a\ t}$2 , L=(P K_{Aidi}) ^{t}1 g ^{t}2 = (g^kAidi) ^{t}1 g ^{t}2 ,

$8x\ Sj;\ Kx^{0} = Kx\ :g^{b(t}1^{+t}2^{)} = h^{k}_{x}{}^{Aid}i \qquad {}^{t1}\ :g^{b(t}1^{+t}2^{)}$

$Kx^{00} = Jx\ :g^{b(t}1^{+t}2^{)} = hx^{t}2\ :g^{b(t}1^{+t}2^{)}$

where Master secret key, MSK = ; ,a,b public key, PK=G_T ,G,H,g,g_a,e(g; g) ,h_1,....h_U

randomly chosen by CA from the system, where G, G_T are multiplicative cyclic groups with same prime order p and g be generator of G,let H:(0; 1) ! Z_p be a hash function[14]. Thus CA sends SK_j and TS to the user.

P11 = User decrypt the file using secret key

User first finds the secret parameter s using which symmetric key k will be found.With the computed k,user can decrypt the ciphertext CT to find the plaintext M.

P12 = Selecting CA among AA

O = f O0, O1, O2 g..........................(4) O0 = Report Generation for AA

O1 = Report Generation for CA

O2 = Decrypted File

VII. ALGORITHM

The CP-ABE scheme is composed of four algorithms.[6-12]

1) Setup(,U) ! (PK,MSK). This algorithm accepts security parameter and the universal attribute set U as the input. It gives public parameters PK and a master secret key MSK as output.
2) Encrypt(PK,M,A) ! CT. This algorithm accepts the public parameters PK, a plain message M, and an access policy A as input. The encryption algorithm will encrypt M and outputs a ciphertext CT such that only a user whose attributes set satisfies the access policy will be able to decrypt the ciphertext. Assume that access structure A implicitly present in ciphertext.
3) Key Gen(MSK, S) ! SK. This is a key generation algorithm which accepts the master secret key MSK and attributes set S as input. It gives a secret key SK as output.
4) Decrypt(PK,CT, SK) ! M. This is a decryption algorithm which accepts the public parameters PK, a ciphertext CT which has an access structure A, and a secret key SK as input, where SK is a secret key for a set of attributes S. This decryption algorithm decrypts the ciphertext only if the set of attributes S satisfies the access policy A and return a message M.

A. AES Algorithm

Key Expansions

For each round AES algorithm needs a distinct 128-bit round key block and one additional bit.

Beginning Round

Add Round Key - Using a block of the round key, every byte of the state is integrated using bitwise xor.

Different rounds

Sub Bytes - In this sub bytes step, every byte is substi-tuted with another byte.

Shift Rows - for a few number of steps, the last three rows are shifted repeatedly in cyclic fashion.

Mix Columns - In this step,a mixing operation is per-formed on the columns of the state, integrating the four bytes in each column.

Add Round Key

Last Round (no Mix Columns)

Sub Bytes

Shift Rows Add Round Key.

VIII. ADVANTAGES

- The Proposed System is scalable and efficient.
- Provides Data confidentiality.
- Provides Data Security.

IX. EXPERIMENTAL RESULTS

The system has been developed in java. Each entity is tested by deploying them on individual machines. The cloud, Owner, AA, CA and Observer deployed on core i-3 processor with 4 gb RAM. Client system uses i3 processor with 2 gb ram. JRE-1.7 is installed on each system. Thesystem used jdk 1.7, IDE:Netbeans 7.4 and Adrive cloud for development. Mysql 5.3 database is used for database storage. For implementation of the system users business structure has been followed. The system user's structure along with designation given below.

Consider a situation, where a user wants to share his/her data with manager and developer of branch 1 and 2 and to generate keys following attributes will be required. branch1-manager branch1-developer branch2-manager branch2-developer

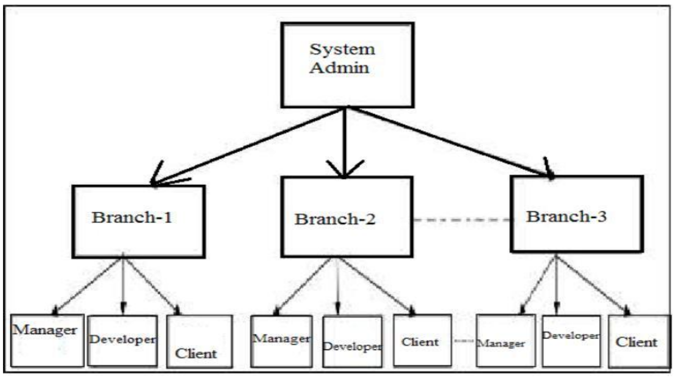


Figure 2. Work Break-Down Structure

The system uses ABE algorithm for implementation and its performance is evaluated.

The system calculated time needed for key generation. For

TABLE II
PERFORMANCE ANALYSIS

File size in MB	Key generation Time in milliseconds	Encryption Time in milliseconds	Decryption Time in milliseconds
1	219	5342	7949
2	213	8970	14321
3	214	14307	23579
4	212	17423	27357
5	229	20342	32572

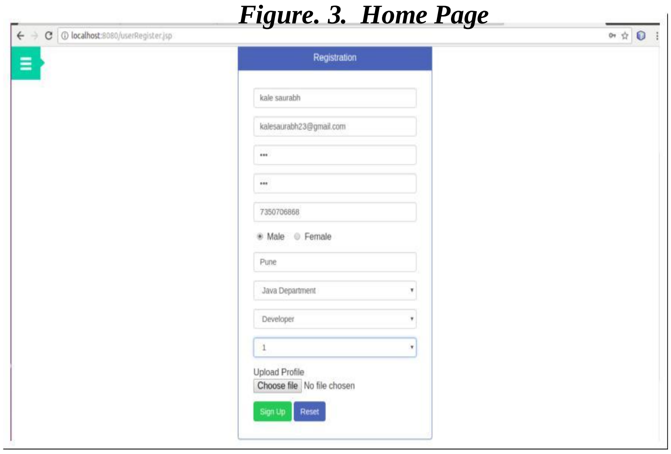
10 users the average time needed is 30 mili Seconds. The system is working on secret key distribution and its management. Finishing the complete system implementation, the system will evaluate its performance with

- Uploading and downloading time for different sizes of files.
- Key distribution and file sharing times.

X. RESULTS

Secure and Efficient Data Access Control For Public Cloud Storage With Multiple AA

Figure. 3. Home Page



localhost:8080/userRegister.jsp

Registration

kale saurabh

kalesaurabh23@gmail.com

•••

•••

7350706868

● Male ○ Female

Pune

Java Department

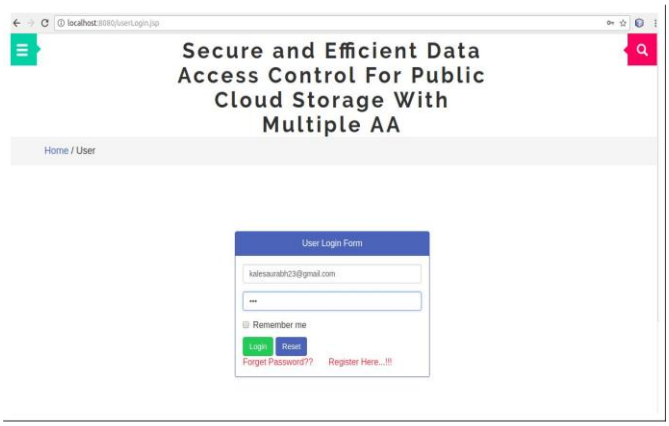
Developer

1

Upload Profile

Choose file No file chosen

Figure. 4. User Registration



localhost:8080/userLogin.jsp

Secure and Efficient Data Access Control For Public Cloud Storage With Multiple AA

Home / User

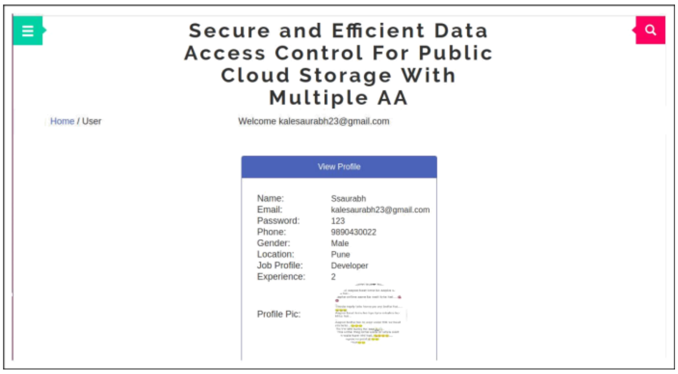
User Login Form

kalesaurabh23@gmail.com

•••

□ Remember me

Figure. 5. user login



Secure and Efficient Data Access Control For Public Cloud Storage With Multiple AA

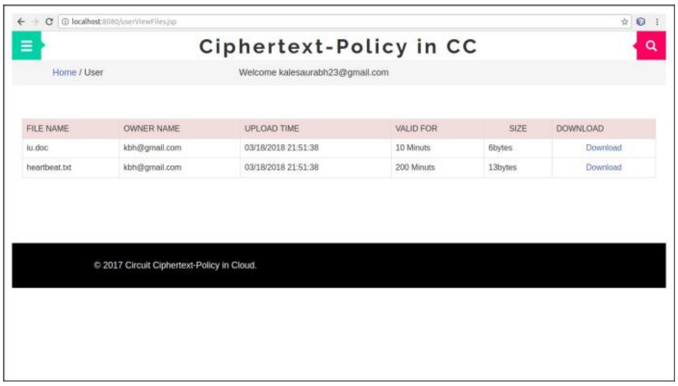
Home / User

Welcome kalesaurabh23@gmail.com

View Profile

Name: Ssaurabh
Email: kalesaurabh23@gmail.com
Password: 123
Phone: 9890430022
Gender: Male
Location: Pune
Job Profile: Developer
Experience: 2
Profile Pic:

Figure. 6. View Profile



localhost:8080/userViewFiles.jsp

Ciphertext-Policy in CC

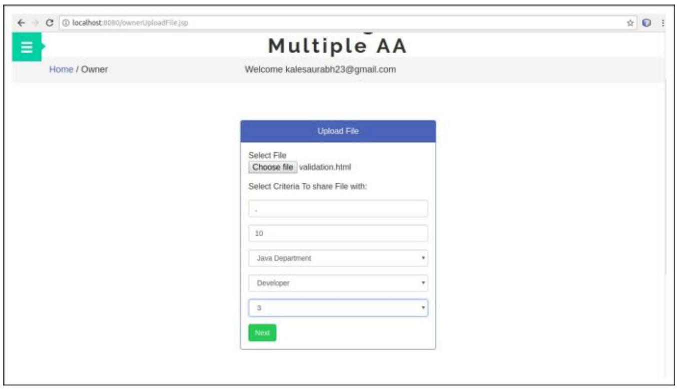
Home / User

Welcome kalesaurabh23@gmail.com

FILE NAME	OWNER NAME	UPLOAD TIME	VALID FOR	SIZE	DOWNLOAD
iu.doc	kbh@gmail.com	03/18/2018 21:51:38	10 Minuts	6bytes	Download
heartbeat.txt	kbh@gmail.com	03/18/2018 21:51:38	200 Minuts	13bytes	Download

© 2017 Circuit Ciphertext-Policy in Cloud.

Figure. 7. Download File



localhost:8080/ownerUploadFile.jsp

Multiple AA

Home / Owner

Welcome kalesaurabh23@gmail.com

Upload File

Select File

Choose file validation.html

Select Criteria To share File with:

10

Java Department

Developer

3

Figure. 8. share file

XI. CONCLUSION

It has been proposed another novel system to remove the single point execution bottleneck and increment the efficiency of the current CP-ABE scheme. By successfully reformulating CP-ABE cryptographic system into this novel structure, the proposed system gives a fine-grained, robust and secure access control with one-CA chosen among multi-AAs for public cloud storage. This plan utilizes various AAs to share the heap of the tedious authenticity check and standby for serving subsequent client demands. It has been proposed an auditing technique to trace the AAs for their potential incorrect behavior. An observer is introduced to monitor CA and if there is any malicious behavior then new CA has chosen among AAs which increases the security. It has been conducted detailed performance and forensic analysis to verify that this scheme is efficient and secure. The security analysis shows that the scheme could effectively resist individual and colluded malicious users, as well as the honest-but-curious cloud servers.

ACKNOWLEDGMENT

It is matter of great pleasure for me to submit this Paper on Secure and Efficient Data Access Control for Public Cloud Storage With Multiple Attribute Authorities as a part of curriculum for award of Master in Computer Engineering degree of Savitribai Phule Pune University. Firstly I would like to thank to my guide Dr. S. N. Kini, for his agile and skillful guidance, continuous inspiration, supervision and discussion while working on this project and writing of this paper. I would also want to thank all the authors of various research papers referred while preparing this paper. My guide and college very much helped and inspired for knowledge gaining to continue my work in future.

REFERENCES

[1]Zhangjie Fu, Kui Ren, Enabling personalized search over encrypted outsourced data with efficiency improvement 2015 IEEE.

[2]Zhangjie Fu, Xingming Sun and Sai Ji, Towards efficient content-aware search over encrypted outsourced data in cloud IEEE INFOCOM 2016

[3]Kaiping Xue, A dynamic secure group sharing framework in public cloud computing 2013 IEEE.

[4]Yongdong Wu,Zhuo Wei,Robert H. Deng,” Attribute-based access to scalable media in cloud-assisted content sharing Networks”

[5]Junbeom Hur Improving security and efficiency in attribute based data sharing 2013 IEEE.

[6]J. Hur and D. K. Noh, Attribute-based access control with efficient revocation in data outsourcing systems, IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 12141221, 2011.

[7]Jianan Hong, Kaiping Xue TAFC: Time and attribute factors combined access control on time sensitive data in public cloud 2015 IEEE

[8]M. Chase and S. S. Chow, ”Improving Privacy and Security in Multi-Authority Attribute-Based Encryption” ACM, 2009

[9]B. Waters, Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, Springer, 2011

[10]Yingjie Xue, Jianan Hong, Wei Li and Kaiping Xue, LABAC: A location-aware attribute-based access control scheme for cloud storage 2016 IEEE

[11]K. Yang, X. Jia, K. Ren, and B. Zhang, DAC-MACS:Effective data access control for multi-authority cloud storage systems 2013 IEEE

[12]Jianwei Chen and Huadong Ma Efficient decentralized attribute based access control for cloud storage with user revocation 2014 IEEE

[13]Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage 2015 IEEE.

[14]Kaiping Xue,Yingjie Xue,Jianan Hong,Wei Li,Hao Yue,David S.L. Wei and Peilin Hong RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage 2016 IEEE.

[15]Guofeng Lin,Hanshu Hong,Zhixin Sun, A Collaborative Key Manage-ment Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing 2017 IEEE.

[16]Xiaotu li,Shaohua Tang,Lingling Xu, Two-Factor Data access Control With Efficient Revocation for Multi-Authority Cloud Storage Systems 2017 IEEE.