RESEARCH ARTICLE OPEN ACCESS

Security and Protection of Enterprise Data in Cloud: Implementation of Deniable CP-ABE algorithm and Performance Considerations

Vijaya Shetty S*, Dr. Sarojadevi H**,Shalini M***, Sanivarapu Mounica***, T S Vinutha***, Sahana S***
(Department of Computer Science and Engineering, NMIT, Bangalore-64 Email: vijayashetty.s@nmit.ac.in)
*** (Department of Computer Science and Engineering, NMIT, Bangalore-64 Email: sarojadevi.h@ nmit.ac.in)*
****(Department of Computer Science and Engineering, NMIT, Bangalore-64 Email: shalinim296@gmail.com;*

ABSTRACT
Enterprise level cloud data storage is gaining importance in the area of consumer level file hostage services. Cloud storage providers are responsible for availability, accessibility and protection of the user data. A number of encrypting schemes have been proposed for encrypting the user data in cloud storage to protect unauthorized access. Most of the Attribute Based Encryption (ABE) schemes that were proposed assume that the data in cloud storage are secure and are never disclosed. However, in reality, some of the authorities may force the cloud storage providers to disclose the cloud user's secrets or personal data. In this paper, a new deniable ABE encryption scheme for cloud storage is proposed to ensure user privacy with minimized unauthorized access. A new ranking algorithm assigns a rank to each user at the time of registration based on their personal information. The rank of the user enhances the privacy and provides access control to the data stored on cloud. Each file uploaded to cloud is assigned with a rank and the file downloads only if the rank of the user matches the rank associated with the file. If rank of the user does not match then a fake file will be downloaded. Since authorities who demand for user secret cannot decide if the information they get about the user are legitimate, the cloud storage providers make sure that the individual user privacy is still protected. The ranking algorithm is also used to provide improved cloud access response time to prioritized users.

Keywords: Cloud Storage Providers, Attribute Based Encryption (ABE), Deniable Encryption, User Rank, Access Control.

I. INTRODUCTION

Cloud storage refers to a cloud computing service model that stores data on remote servers. The data on remote servers is accessed via the Internet or cloud. The servers are built on virtualization techniques. Cloud storage is maintained, backed-up and managed by a cloud storage service provider. Cloud storage providers are responsible for keeping the data available and accessible. Many organizations buy or rent storage from the cloud providers to store their application data. This cloud storage services can be accessed by web application programming interface (API) or by mobile apps. User data on cloud storage is encrypted using different encryption schemes to provide protection from intruders [1]. Attribute-based encryption is a kind of public-key encryption scheme in which the secret key of a user and the generated ciphertext are reliant upon a set of attributes. In such a structure, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. A central security feature of Attribute-Based Encryption is collusion-resistance. A collusion-resistant encryption algorithm is the one in which two inputs do not hash to the same output. These schemes assume that the cloud providers do not disclose the cloud user's data and secrets, which is not the fact always. As an example, in 2010, without notifying its users, Google released user documents to the FBI after receiving a search warrant [2]. In 2014, Edward Snowden disclosed the existence of global surveillance programs that collect such cloud data as emails, texts, and voice messages from some technology companies [3], [4]. Sometimes unauthorized user may also try to access the data illegally. In order to control illegal access to cloud data, there is a need for deniable encryption service that denies illegal access to actual data. This technique was first proposed by R. Canetti et. al[5]. This encryption scheme is based on polynomial deniability and generates a fake user data if the user is found to be unauthorized. The overall idea of this deniable encryption scheme is to convince the unauthorized user by providing the fake data so that the user does not try to access the data again.

Deniable encryption schemes do not model enterprise cloud data access very well in terms of user response time because the scheme does not address response time requirements of users of such systems. Therefore a new rank based deniable encryption scheme is proposed in this research that addresses privacy and response time requirements of users.

II. RELATED WORK

The concept of ABE is that the attributes of the user is used to provide file access to the other users. When the user tries to access a file which is encrypted and is stored on cloud, the attributes of that user are checked first, if matches with the attributes associated with the file the user will be able get decrypted file. If attributes do not match, then the user can not decrypt the file [6]. This concept has helped cloud storage providers to maintain privacy of the user data. There are 2 types of ABE; Key Policy ABE (KP-ABE) and Cipher text Policy ABE(CP-ABE). In K P-ABE, user encrypts the data using a set of attributes of the user [7]. The private key is associated with the access policy and cipher text is associated with a set of attributes. The concept of deniability is used along with the ABE, where it helps to deny the unauthorized users. The scheme of deniable encryption can be a deniable shared key scheme or a public key scheme. For cloud storage scenario, we focus on public key scheme. In this scheme, the dispatcher gets a data which seems to be intended plain text that was actually stored in cloud storage[8]. This scheme can be applied on both sender and receiver side to make it a bi-deniable scheme. Bi-deniable scheme increases the computational overhead of the overall encryption scheme and not used much in practice. The CP-ABE scheme is an enhancement of KP-ABE in which cloud providers provide convincing fake user information to the outside coercer [9]. As the coercer does not know the data accessed about the user is original or fake, he never tries again to disturb the cloud providers to obtain the users data. By using this CP-ABE in cloud storage the user privacy is still confined and his information is not disclosed to anyone by assigning the access control.

III. ARCHITECTURAL MODEL OF THE SYSTEM

The Architectural model of the system is shown in fig. 3.1. The subsystems of the model include process of encryption and decryption of the file. A key is generated by using the rank (attribute) of the user. This Attribute key is used to encrypt the data and uploaded to the cloud. When a user with different rank tries to access this data his rank and key is checked. If matches the user is authorized user and the decrypted ciphertext is downloaded to the user, otherwise user is treated as unauthorized user and gets a fake data from which user is convinced and do not try again to access the data. Here rank of the user plays an important role to protect the privacy of the user and sets an access control mechanism for multiple user data sharing.

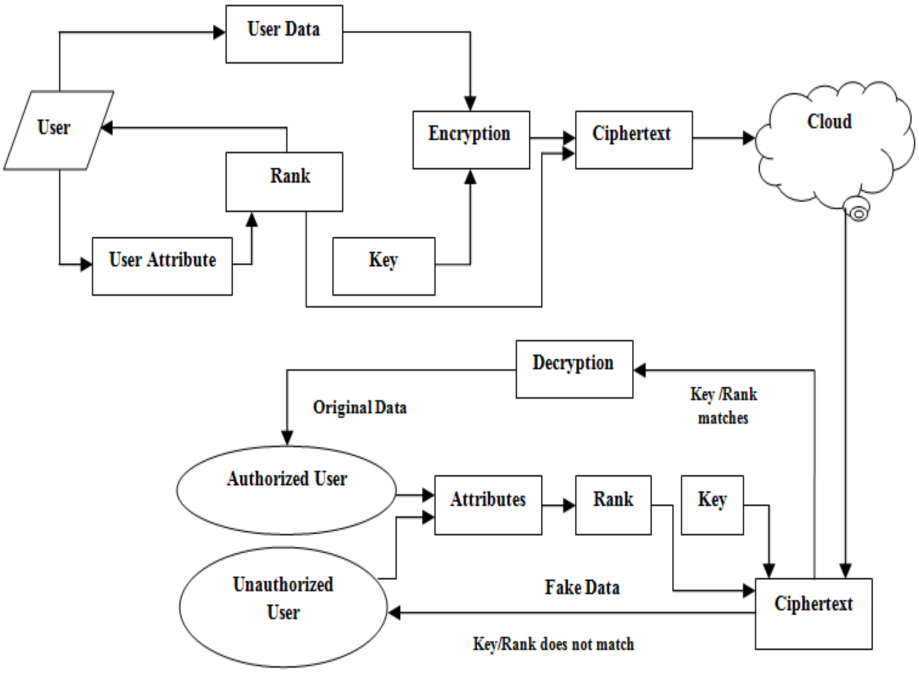

Fig 3.1: System Architectural Model

IV. MODULAR DESCRIPTION OF THE SYSTEM

Deniable encryption involves both senders and receivers. Senders encrypt the data and transmit it to the receivers who decrypt it. Senders upload the encrypted file and receivers download the encrypted file from cloud [10]. Deniable encryption ensures that a fake cipher text is created and transmitted to unauthorized user to disrupt his future data access attempts. This approach tries to make the efforts of the unauthorized users useless but gives the pleasure of worth full efforts. This scheme also ensures that the legitimate users access the actual data. We make use of this technique such that cloud storage providers can ensure the audit-free storage services for the cloud users. In this research the characteristics of ABE is used for securing stored data and deniable encryption to prevent outside auditing.

A. Ranking Algorithm

Rank is an attribute of a user generated using Joindate and designation. It is an important parameter used to upload file to cloud and download file from cloud. Joindate is passed to a function where it is compared with a threshold value, if it is equal or less than the threshold value then value of Rank1 variable is 1 else it is the difference between joindate and threshold value. Designation of a person is compared with an array containing list of designations. If this matches it returns an index value and this is a second variable known as Rank2.One more function is created to calculate the average of Rank1 and Rank2 variables and the final value is assigned to a variable called Rank.

Admin creates the user by entering all his information including join date and designation. Using this 2 parameter admin creates a rank and sends a mail to user with user id, user password and user rank. User uses this information to login, upload and download the file which is shown in Fig 4.1 and the ranking algorithm is shown below.

Jdate(): this function takes a input of user joining date compares with threshold date and generates a number called num1.

Desgn(): the function takes users designation as input and produce a number called num2.

RankGen(): The input for this algorithm is from the above 2 functions, using this two parameter a algorithm generates a rank for each user.

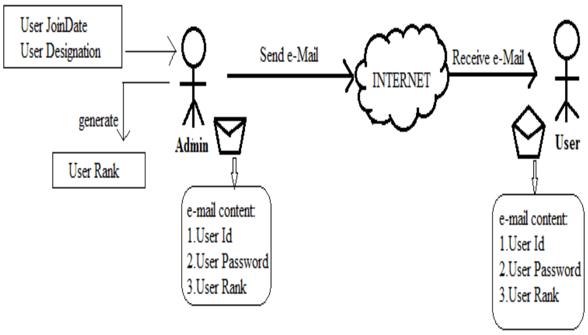

Fig 4.1: The process of Rank generation

B. Rank based Deniable CP-ABE Algorithm

A cloud storage service has been used widely by everyone all over the world for storing their application file. User can store their data on the cloud and access it anywhere and anytime. A cryptography technique is used to give more security to the cloud storage [11]. To preserve user privacy, the data stored on the cloud is encrypted and protected from access by other users. However, in reality entities like some authorities or coercer intercept communications between user and cloud storage providers where they request to leak out the user secrets by using government or other means of power [12]. In this research the ABE uses the rank of the user to generate a key and this key is used in encryption scheme. Each user is assigned a rank based on his/her emp-id and joining date. Rank based ABE is regarded as one of the most suitable encryption scheme for public cloud storage where response time is uncertain. The rank of the user is verified before the data access. The data access request of the user with lower rank is given priority. If this has access permission to the file requested then it is downloaded otherwise he is denied by the deniability scheme and a fake file downloads [13] [14].

The Deniable Rank based CP-ABE algorithm steps are shown in table 4.1

Table 4.1: Deniable Rank based CP-ABE algorithm

Setup(1) → (P,MK): This algorithm takes security parameter as input and returns public parameter P and master key MK.

RankGen(Num1,Num2) →Rank: This algorithm takes input from Jdate() and Desgn() functiond and generates a rank for the user.

KeyGen(MK, Rank) → PK: Given Rank of the user and MK, the algorithm outputs private key PK.

Enc(P,M,A) → C: This encryption algorithm takes as input public parameter P, message M, and access structure A = (M, P) over the Rank. This algorithm encrypts message, M and outputs the ciphertext C,

which can be decrypted by those who has an attribute set that satisfies access structure A.
Dec(P, PK,C) → {M,⊥}: This decryption algorithm takes as input public parameter P, private key PK with its Rank, and ciphertext C with its access structure A. If Rank satisfies A, then this algorithm returns M(message); otherwise, this algorithm returns ⊥(fake message)[15].

C. CLOUD STORAGE:

Cloud storage has become a social phenomenon used by everyone to store their organizational data and files. User may lose their control on their data stored on cloud, because the data is stored on someone else storage device. The different authority (coercer) may force the storage providers to disclose the user secrets to avoid, their many schemes proposed but they assume cloud storage providers are trusted and no one hack their data [16]. We propose a scheme in which a rank is assigned to each user and they use this rank when they upload the data to cloud. The user who try to access this file should satisfy the rank only then he gets an original file else a convincing fake data is provide. So the authority does not try again to access the file [17].

V. RESULTS

The results of the proposed system and different test **scenarios** are given below.

Scenario 1: Admin Login
Admin enters admin id and password. System checks for correctness of admin id and password.
If match then home page is displayed else an error message to re-enter the admin id and password is shown

Scenario 2: User is created
Admin can create user by providing his personal information like user id, name, password, e-mail id etc. The system check the user id already exists or not. If the user id doesn't exists user is successfully created and the user id, password, and the rank is mailed to the users e-mail id else user id should be changed to create a new user.

Scenario 3: User Login
Users login to the system using his user id and password. System checks for match of user id and password. If match is correct then user home page is displayed else a error message to re-enter the user id and password is shown.

Scenario 4: File Upload
User selects a file to upload it to cloud storage. The system checks whether file already exists, if exists it checks the rank and if it is higher than the previous rank the file is replaced else error message is displayed saying you don't have right to replace the file. If file doesn't exist then the user is asked to enter a rank to give file access permission.

Scenario 5: File Download
User chooses a file to download. System checks the access permission of the file; if he has permission then he can download else he will get a fake file.

A. EVALUATION RESULTS OF ACCESS CONTROL OF THE USERS:

Table 5.1 shows the results of accessing the file from the cloud. When the users try to download the file and if his rank does not match with the rank that is associated with the file then he is an unauthorized user and he is denied otherwise he is authorized user and Access is granted to download the original file. The table also shows that every time when unauthorized users try to download they are denied.

Table 5.1 Access rights of the user

User Name	User Rank	File Name	Rank Associated with the File	Download Results
Chaithra	9	Ch.txt	4	Access Denied
Mamatha	6	Th.png	7	Access Denied
Rashmi	4	mi.doc	4	Access Granted
Bhavya	3	Ya.jpg	5	Access Denied
Manjula	5	La.doc	6	Access Denied
Bindiya	8	di.txt	9	Access Denied
Ramya	13	My.doc	13	Access Granted
Reshma	17	Sh.png	15	Access Denied
Rakshitha	4	Rak.txt	14	Access Denied
Deepika	15	De.txt	16	Access Denied
Pragathi	19	Ga.doc	3	Access Denied
Preethi	2	Pro.jpg	2	Access Granted

B. PERFORMANCE EVALUATION:

Table 5.2 shows the processing time for the request from the users for uploading the file. The admin processes the request from the users based on the rank and the higher rank person is served first and the lower rank. The processing time in the above table shows that time taken to process the request and it is clear the time taken for the higher rank user less when compared to the lower rank user. We can derive a conclusion that the prioratized use**r** request is not delayed.

VI. CONCLUSIONS

In our work, we proposed a Rank based deniable ABE scheme to build an audit-free cloud storage service. The deniability feature makes unauthorized users invalid, and the property of ABE ensures secure cloud with access control. Rank is an attribute derived from several attributes of a user. The scheme also provides a possible way to fight against unauthorized interference with the right of privacy by providing the fake data while decryption of the cipher text, If rank do not match and these schemes can be created to protect cloud user privacy. The idea of the proposed replication technique is to provide data security by giving set of privileges to the users to perform duplicate check of the files that are outsourced on the cloud and make a copy of it in another cloud for backup from which a user can store his data in cloud without any auditing on the storage frequently.

Table 5.2 Processing time based on the rank

User Name	User Rank	File Name	Processing Time (nsecs)
Priyanka	1	pch.txt	57356
Swathi	2	ith.png	118335
Pavvithra	3	hmi.doc	174484
Divya	4	fya.jpg	233047
Tanu	5	lta.doc	287988
bindu	6	dei.txt	2095608
Santha	7	smy.doc	2185566
lakshmi	8	wsh.png	2271902
Leka	9	wrak.txt	2333484
Gayithri	10	tde.txt	2396877
Pavan	11	gffa.doc	2460271
manju	12	prso.jpg	25905344

REFERENCES

[1] Chi PW, Lei CL. Audit-Free Cloud Storage via Deniable Attribute-based Encryption. *IEEE Transactions on Cloud Computing.* 2015 Apr 21.

[2] Aparna, P. and Murthy, K.S.N., 2016. A Deniable Cp-Abe Scheme For An Audit-Free Cloud Storage Service. *IJSEAT*, *4*(10), pp.602-604.

[3] Greenwald, G. and MacAskill, E., Boundless Informant: the NSA’s secret tool to track global surveillance data. *The Guardian*, *11*. 2013.

[4] Edward snowden. [Online]. Available:http://en.wikipedia.org/wiki/Edward Snowden (2014)

[5] Canetti, R., Dwork, C., Naor, M. and Ostrovsky, R., 1997, August. Deniable encryption. In *Annual International Cryptology Conference* (pp. 90-104). Springer Berlin Heidelberg.

[6] Chi, Po-Wen, and Chin-Laung Lei. "Audit-Free Cloud Storage via Deniable Attribute-based Encryption." *IEEE Transactions on Cloud Computing* (2015).

[7] Sahai, A., Seyalioglu, H. and Waters, B., 2012. Dynamic credentials and ciphertext delegation for attribute-based encryption. In *Advances in Cryptology–CRYPTO 2012* (pp. 199-217). Springer Berlin Heidelberg.

[8] Dr. T Ramaprahu, S priya. An Auditing-free Cloud Storage Using Control Attribute Based Encryption, in © IJIRCCE 2016, DOI: 10,15680/IJIRCCE.2016.0407141.

[9] Cheng-Chi Lee, Pei-Shan Chung and Min-Shiang Hwang, A Survey on Attribute Based Encryption Scheme of Access Control in Cloud Environment, in international journal of Network Security, 2013, pp. 231-240.

[10] P. Lokesh Kumar Reddy, B. Rama Bhupal Reddy, S. Rama Krishna, Deniable Encryption key, IOSR-JCE, 2013, pp. 08-12.

[11] By Stefan Rass, Daniel Slamanig Cryptography for Security and Privacy in Cloud Computing, Boston : Artech House, [2014].

[12] S. Hohenberger and B. Waters, Attribute-based encryption with fast decryption, Public Key Cryptography, 2014, pp. 162–179.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, ACM Conference on Computer and Communications Security, 2006, pp. 89–98.

[14] Minu George, Dr. C. Suresh Gnanadhas, Saranya .K, A Survey on Attribute Based Encryption Scheme in Cloud Computing, *IJARCCE*, 2013.

[15] Salini K, Sruthy Manmadhan, CP-ABE Secure Data Retrieval, *IJRASET* 2015, IC Value: 13.98.

[16] “Cloud Storage” [online]. Available: https://www.lifewire.com/what-is-cloud-storage-2438541

[17] Rehman, M.S. and Sakr, M.F., 2011, April. Teaching the cloud-experiences in designing and teaching an undergraduate-level course in cloud computing at the Carnegie Mellon University in Qatar. In *Global Engineering Education Conference (EDUCON), 2011 IEEE* (pp. 875-879). IEEE.