RESEARCH ARTICLE OPEN ACCESS

Secure Data Sharing In an Untrusted Cloud

Rekha Chandankere*, Masrath Begum**
*(Department of Computer Science, GNDEC, V.T.U University, Bidar)
** (Professor, Department of Computer Science, GNDEC, V.T.U University, Bidar)

ABSTRACT
Cloud computing is a huge area which basically provides many services on the basis of pay as you go. One of the fundamental services provided by cloud is data storage. Cloud provides cost efficiency and an efficient solution for sharing resource among cloud users. A secure and efficient data sharing scheme for groups in cloud is not an easy task. On one hand customers are not ready to share their identity but on other hand want to enjoy the cost efficiency provided by the cloud. It needs to provide identity privacy, multiple owner and dynamic data sharing without getting effected by the number of cloud users revoked. In this paper, any member of a group can completely enjoy the data storing and sharing services by the cloud. A secure data sharing scheme for dynamic cloud users is proposed in this paper. For which it uses group signature and dynamic broadcast encryption techniques such that any user in a group can share the information in a secured manner. Additionally the permission option is proposed for the security reasons. This means the file access permissions are generated by the admin and given to the user using Role Based Access Control (RBA) algorithm. The file access permissions are read, write and delete. In this, owner can provide files with options and accepts the users using that option. The revocation of cloud user is a function generated by the Admin for security purpose. The encryption computational cost and storage overhead is not dependent on the number of users revoked. We analyze the security by proofs and produce the cloud efficiency report using cloudsim.

***Keywords* -** *Cloud computing, data sharing, data-privacy, role based access control and encryption.*

I. INTRODUCTION

Cloud computing has become an interesting topic and has a great deal among users. Yet there is no clear definition. Cloud computing is a pay as you go based service where you can obtain storage space and other required resources. One way to understand cloud computing is to think of your experience with e-mail. Your e-mail client, if it is Gmail, Hotmail and so on, handles all of the resources necessary system software and hardware to support personal email account. To access your email, you open web browser, and then login to the email client. To make this work the most important thing is to have internet access. Your email is not placed on your local system; you always need an internet connection and from anywhere at anytime to access the e-mail. If you are at home or work, or n a trip, you can check your email just by having access to the internet. The working of an email client is similar to cloud computing working, but with more features than just accessing the e-mail**.** The cloud allows you to access information at anytime from anywhere. While a traditional computer requires you as well as the data storage device to be in the same place, this part in excluded in the cloud. The cloud removes the necessity for you to be in the physical location as the storage device. Cloud provider can provide place or house the system resources needed to run your applications. To access cloud one always needs an internet connection. This means that either by using wireless or wired internet connection you can access your data housed in the cloud. By doing this one can enjoy the services of cloud from any place and using any device. This is ubiquity characteristic of cloud. The information placed on the cloud is often considered as a great deal to individuals with malicious intent. Generally people store their personal information and potentially secure data on their systems and the same information is transferred to the cloud. The security measures are provided by the cloud providers, which makes it difficult for you to understand the security measures. So it is equally important for individuals to take personal precautions to secure their data. There are many questions that one can ask, but it is always better to choose a provider that takes into account data security as a major concern. Data security is a critical issue in cloud computing. The fact that users no longer physically possess their data makes it very challenging to protect data confidentiality and secure data sharing in Cloud Computing. In this paper, we will identify the challenges pertaining to the problem of securing data sharing in cloud computing. We will present our preliminary work, an encryption-based fine-grained data access control framework, that is to tackle this challenges in cloud computing. Our solution is based on a recent cryptographic scheme – group signature. Today, large scale data is stored in the cloud in order to save the maintenance cost of in-house storage by many organizations. With cloud storage service, the members of an organization can share data with other members easily by uploading their data to the cloud. Examples of organizations which may profit from this cloud storage and sharing service are numerous, such as international enterprises with many employees around the world, collaborative web application providers with a large user base, or institution deal with big data, health care service provider coordinating data from doctors, researcher's, patient's etc. Cloud computing also has many challenges that, if not taken precaution, may obstruct its fast growth. One of the major challenges faced by cloud applications is data security and is a great concern for the cloud user when they store their sensitive data on the cloud servers. These concerns are basically originated from the fact that cloud servers are operated by commercial providers which are very likely to be outside of the trusted domain of the users. Data confidential against cloud servers is hence frequently desired when users outsource data for storage in the cloud. In some practical application systems, data confidentiality is not only a security/ privacy issue, but also of juristic concerns. Let us consider an example, in healthcare application scenario use, disclosure of protected information system should meet the requirements of health insurance probability and accountability. In order to provide an efficient and secure data storing and sharing by the cloud we need to firstly consider the identity privacy, second, the multiple ownership that is; any member in the group can store and share the data by the cloud and finally, dynamically storing the data without getting effected by the number of users revoked. This is achieved by using group signature and dynamic broadcast encryption technique.

II. LITERATURE SURVEY

In [2], Armbrust et al. propose a cryptographic primitive, Proxy Reencryption with Private Searching (PRPS). This scheme allows the owner and the users to access and query the data in an untrusted cloud, while maintaining the privacy of the query as well as the data from the cloud providers. This is constructed on proxy re-encryption; that is public key encryption with the keyword search and the dual receiver cryptosystem.

In[3], a virtual private storage service based on cryptographic techniques is proposed which aims to provide security of private cloud and the functionality and cost savings of public cloud.

S.Yu et al. [4] presents a fine-grained, scalable and data confident system called as key policy Attribute Based Encryption (ABE) where the cipher text can be decrypted by a constant number of pairing. In this technique the data owner used a random key to encrypt the data file. Using a set of attributes this random key is again encrypted. And a group manager assigns an access structure and its corresponding secret key to authorized user, such that if the data file attributes satisfy the access structure provided by the manager then only the user can decrypt the ciphertext.

In [6] Lu et al. introduces a secure provenance scheme based on the bilinear pairing techniques. The proposal is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents. This scheme is based on group signatures and ciphertext policy attribute based encryption. In which each user is provided with two keys group signature key and attribute key.

Waters et al.[7] presents a new methodology for realizing Cipher text-Policy Attribute Encryption (CP-ABE) under concrete and non interactive cryptographic assumptions in the standard model. This solution allows any encryption to specify access control in terms of any access formula over the attributes in the system.

In[8], Kallahalla et al. introduced a secure file sharing on untrusted server. In which the network integrity is protected with file-sign/file-verify keys. Generally, the files are divided into file groups and each group is encrypted with an exclusive file block key. Due to which there is heavy key distribution and more over the file block key needs to be updated and distributed again each time the user is revoked.

Goyal et al.[9] developed a cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.

In[12], Wang et al. utilize and uniquely combine the public key based homo morphed authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements.

From the above study we can find that the data sharing among the dynamic user in an untrusted cloud remains a challenging issue. In this paper we present a novel protocol to secure the data sharing in the cloud computing. Compared to above work, this proposal provides following features:

- It provide secret key to each user so it has high security file transmission.
- User is able to share data with others in the group without revealing identity privacy.

It supports efficient user revocation and new user joining.

III. METHODOLOGY

To fulfill the requirement two methods are used group signature and dynamic broadcast encryption technique.

3.1 Group Signature:

This method is first introduced by Chaum and Heyst [11]. In general this scheme allows to preserve the identity of any member of a group while sign up. Also allows admin to disclose the identity when dispute occurs. In this paper, Digital signature with RSA will be used to achieve anonymous access control which supports user revocation efficiently.

3.2 Dynamic Broadcast Encryption:

This technique allows the broadcaster to transmit encrypted data to the members of a group. Also allows the admin to add users dynamically while preserving previously computed information. This means to decrypt the data user need can use the same key. The file sharing in dynamic groups is based on the bilinear pairing technique [10].

IV. PROPOSED SYSTEM

To overcome the problems presented in our existing system we propose a secure data sharing system in an untrusted cloud. It supports effectively dynamic groups. Specifically, any new registered users can decrypt data files uploaded in the cloud without taking permission of the data owners. User revocation can be easily achieved without changing the secret keys of the other users in a group. The computation and size overhead of encryption remains the same and independent of the number of users revoked. In this method we use secure provenance scheme, this is built upon group signatures and cipher text-policy attribute-based encryption techniques.

In our scheme, the keys are generated with the help of the group signature and these keys are sent to the each user via the e-mails. After receiving this keys and password the user enter into the cloud system. Admin can generate these keys and send to the each user involved in the group. Also the admin can generate the file access permission and the revoke function for security purpose. The file access permissions are provided to the user using RBA based algorithm. The access permissions are read, write and delete permission. The revoke function is enabling the user to access the file which means the authorized person can only access the file. Finally, in our proposed scheme the files are been shared between the dynamic users by the cloud in an efficient and secure manner as shown in the system model where GK is group key and SK is secret key.

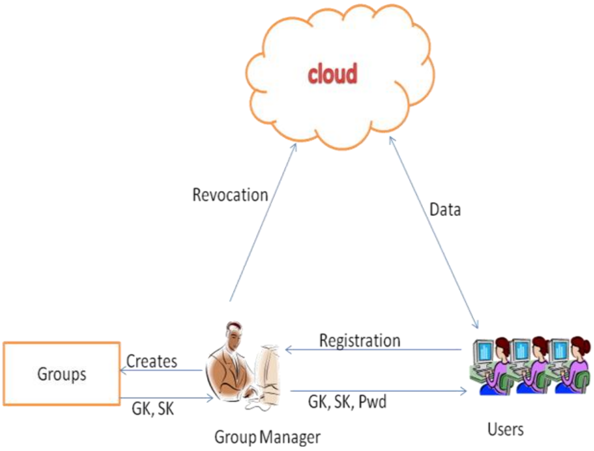


Fig. 1: system model

V. MODULES

The proposed system has following modules:

5.1 Admin Process:

The admin can create a group and add some users to its group. This module will create unique signature for each users. The admin also creates the file access permission using RBA based algorithm and the revoke functions. The Admin can only allow the authorized persons to access the file in the cloud. If the Admin find any one person can perform misbehave for the file access. The admin will have full permission to block the user.

5.2 User Process

In this module authorized user can enter into the cloud system for accessing files. By using the password provided by the admin via e-mail and a group key to the user in order to enter into the group. The group key is same for all members in a particular group. The file access permission is also given to the user. The user can upload or download the data from the cloud server.

5.3 Signature Verification

Here, the signature is in the form of key. At the registration process the signature is sent to the user’s e-mail. This signature verification is mainly used to restrict the file access from unauthorized users. If the outside group member supposed to download the file of other group it will display the message of signature verification false.

5.4 Access Permission

The File Access Permission is given to the user with the help of RBA algorithm. This algorithm will generate the File access Permission based upon the Role of user. The File access permission contains three types of permissions. There are Read permission, Write permission, and delete permission. In this File Access Scheme the user able to delete the file from the cloud storage.

5.5 Revocation

The revocation process is performed by the admin. Here, the admin can provide permission for every file access in the group. The file access permission can be displayed for every user in the group. According to the permission's they will be able to use the data. With the help of revocation function we can easily identify whether the file access user is authorized or not. If the user is unauthorized user the Admin will block the user from accessing the data in the cloud.

5.6 File Sharing

File sharing is the main module. While uploading data this process asks whether to share e-mail address or not. If shared, the process will show the shared file details with their e-mail address. If the admin want to remove the shared list they can delete the particular shared file list. The file can be shared between the multiple users in the same group effectively.

VI. Feasibility Study

6.1 Data Sharing

When the data is shared in file sharing module the e-mail address details are shown. If the admin want to remove the shared list he/she can delete the particular shared file list. The file can be shared between the multiple users in the same group effectively.

Whether cloud-based file sharing is used as an alternative to backup solutions or traditional file sharing, it's clear the technology is obtaining grip as a business tool. Cloud computing may offer risk due to its nature of being impalpable. Many businesses who wish to utilize cloud resources take a chance by hosting their entire network on something that is remotely monitored. This added ease also lessen virtual private network (VPN) costs.

In our proposed concept the file are shared between the more numbers of users in the same group. First the admin give the file access permission and then perform the revocation function to allow the user to share the file across the cloud for security purpose. If the admin identify that the user is not an authorized person. She/he will have the rights to block the user and then delete the file shared list present in our cloud storage system.

5.2 File Access Permission

The file access permission is our additional feature of our concept. The file access permission was generated by the Admin and given to the user to access the file present in the cloud storage system. First the Admin perform the signature verification function on the user side for security purpose. In this verification, the Admin first give the password and key to the user when the user creates the account in the cloud via the mobile phones. After that with the help of that password and key the admin perform signature verification. The signature is first created for the user by Admin after that verification is performed.

The signature can be created with the help of the Group signature algorithm. The signature may be in the form of the keys. This is used for a security purpose whether the file accessed person is authorized or not. After that perform the signature verification the revocation function is performed. The revocation function is generated by the Admin. This function is used for the privacy and then the authorization purpose. After performing these two functions, the admin provide the file access permission with the help of the RBA algorithm.

The RBA stands for Role Based Access control mechanism. This algorithm allows the user to access the file based upon the role of the user. The role may be in the form of business man, user, etc. Based upon the role of user we can access the file. The file access permission contains the three different kinds of permissions. They are read file access, Write file access and then the delete file access. These different file access permissions are generated by the admin.

VII. System Implementation

7.1 Privacy Preserving

Cloud computing utilizes virtual computing technology, where in the cloud users data may be scattered over various datacenter. The cloud service makes it easier for users to access their personal information from the datacenters, and is also distributed and available over Internet. The availability of such information housed in the cloud is critical to provide better services to users and is difficult to authenticate users in case of services sensitive with respect to privacy and security. Users have to provide their identity each time they use different cloud service, this is carried usually by filling an online form and supply delicate personal information (e.g., name, home address, credit card number, phone number, etc.). This leaves a trail of personal information that, if not properly protected, may be misused. Thus, the development of digital identity management (IdM for short) systems suitable for cloud computing is crucial. An important requirement is that customers of cloud services must have control and transparency on which personal information is revealed and how this information is used in order to reduce the risk of identity theft and fraud.

Two main security and privacy concerns of Cloud Computing are:

- Loss of data control and
- Dependence on the Cloud provider.

These two fears can lead to legal and security concerns related to infrastructure, identity management, access control, risk management, auditing and logging, integrity control as well as Cloud Computing provider dependent risks. Most of the customers know the danger of providing data control from their hands to outside provider. This information could be compromised by the Cloud provider themselves or by other competitive enterprises who are customers with the same service provider. There is a potential lack of control and transparency for users on how, when, why and where their data is processed. Data protection requirement are not clearly understood by the customers. The user is unaware of the processing of their data.

Considering the security and privacy issues in cloud computing and then developing efficient and effective solutions are critical concerns. Although clouds allow customers to avoid monetary costs, and expanding their agility by instantly acquiring services and structural resources as and when needed, their unique architectural characteristics also uplift varying security and privacy worries. Both Cloud providers and customers must divide the level of security and privacy in cloud computing environments, but dividing responsibility will vary for various delivery models, this in turn influence cloud extensibility.

Providers on one hand are typically more responsible for the security and privacy of the application services when related to the public cloud. On the other hand the customer organization may be more responsible for providing stringent security needed for the services in the private cloud. The ultimate goal is to allow developers to construct their own applications on some policies. Therefore, clients are basically responsible for securing the applications they build and execute on the plan. Cloud providers are later accountable for alienating the client's applications and workplace from one another. This is implemented at the client side by using group signature and data encryption before it is uploaded into the cloud. Unauthorized users and the revoked are not able to know the content stored in the cloud. This preserves the data confidentiality. Identity privacy is maintained by hiding the actual identity of the user. Anonymity and the traceability is applied by allowing only the authorized users of the group to enter into the cloud and access the data, and the conflict for the ownership is dealt by the admin respectively.

7.2 Access Control

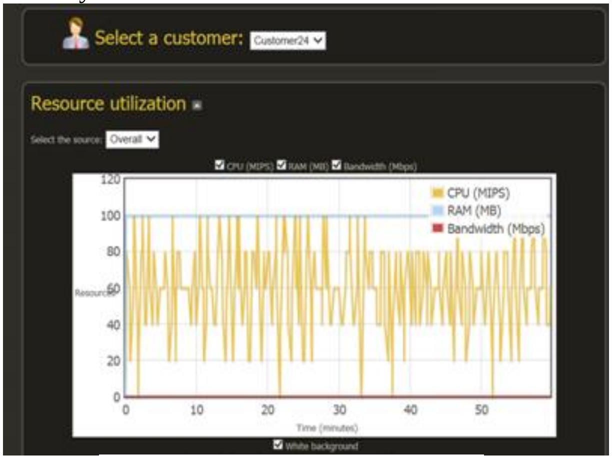
Access control in general term is a procedure that permits, denies or limits access to a system. It may also monitor and log all attempts done to access a system. It is a technique which is important for shielding in computer security. Various models of access control are in use, such as Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). These models are known as identity based access control. In all these access control methods, unique names used to identify the users and resources. Identification can be done either directly or by roles assigned to the cloud users. System provides security by controlling access to its data and resources. However, in access control systems different steps such as identification, authentication, authorization and accountability are taken before actually accessing the resources.

Role based Access Control (RBAC) is used in the proposed system to access the files in our cloud environment which determines user's access based on the Job role. The Access control mechanism is generated by the Admin and then the control is provided to the user to access the file stored or upload in our cloud environment. Three different types of access controls are given to the user. There are read the file, write the file and then the delete the file. Thus, for the data operation all the group members are able to access the cloud resources.

VIII. SIMULATION

To study the performance we use cloudsim as a simulator and use its extension cloudreports to produce html reports. The simulation consists of two components: client side and cloud side. The performance parameters are cost, reliability, network bandwidth, resource provisioning, interoperability, energy and latency.

8.1 Client Computation Cost in terms of above mentioned metrics: Consider two customers (Customer24 and Coustomer1) with 5 and 6 virtual machines (VM) for each user. The fig. 2 shows the resource utilization of all the VMs for Customer24. And the fig. 3 shows the execution time of the user Customer24 in the cloud. This shows that we can securely store the data in the cloud.



Select a customer: Customer24

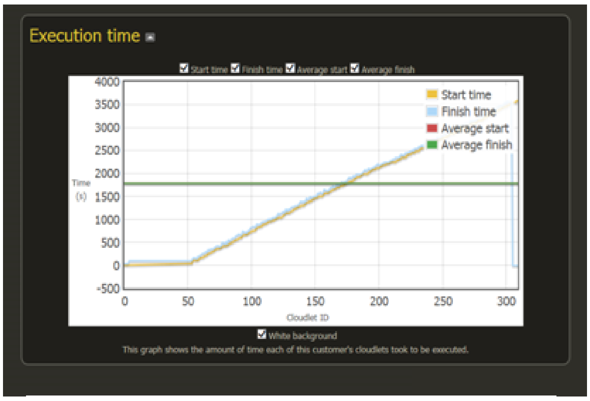
Resource utilization

Select the source: Overall

☑ CPU (MIPS) ☑ RAM (MB) ☑ Bandwidth (Mbps)

☑ White background

Fig. 2: resource utilization by a user



This graph shows the amount of time each of this customer's cloudlets took to be executed.

Fig. 3: execution time for the cloudlet of the user.

8.2 Cloud Computation Cost: To evaluate the performance of cloud in our proposed system, we test its cost to respond to the client operation which includes file sharing, storing.

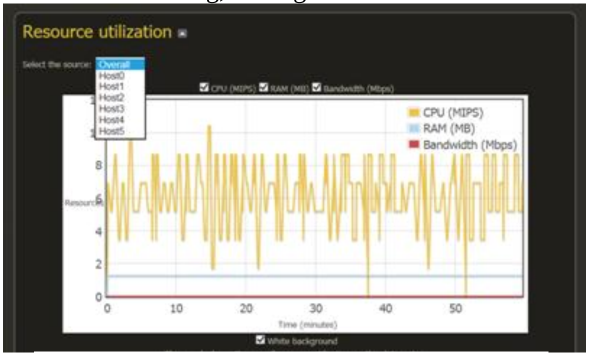
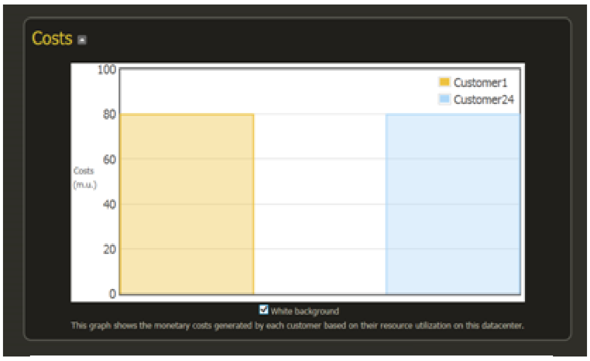


Fig. 4: resource utilization at the cloud by users.



This graph shows the monetary costs generated by each customer based on their resource utilization on this datacenter.

Fig. 6: Monetary costs of the user's utilization of resource on the cloud.

IX. CONCLUSION

In cloud computing, the multiple users are sharing the file in cloud environment in secure manner. But, the user having the fear about loss of their data and then they need more privacy about our data. In this scheme, multiple user in a same group can store and sharing the data in secure manner. This system first creates the groups for users. After that, generate signature for each user. Once users login into the cloud environment, the signature verification process is performed for each user. The signature may be in the form of keys.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Trans. On parallel and distributed systems, vol. 24, no. 6, June 2013.

[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," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

[4] Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[6] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[7] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[10] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[11] D. Chaum and Van Heyst, "Group Signatures", Proc. Int'l Conf. Theory and Applications Of Cryptographic Techniques, pp. 257-265, 1995.