Towards Achieving Efficient and Secure way to Share the Data

Sreevathsa C.V[1], Rajeshwari R[2], Meghana B[3]

[1,2,3] *Bachelor of Engineering, Department of ISE, SKIT, Bengaluru, Karnataka, India*

Abstract - *The impact of the cloud computing technique made users to store and share their data easily and accessible anywhere and at any point of time. The cloud can handle huge amount of data where the data is stored in datacenter which is placed in a remote place. The users can use the service of cloud for personal or the professional use depending on the purpose. The continuous use of the cloud is prone to number of security attacks because users now store and share the data using cloud rather than any other means. There are number of cloud service providers and the third-party platforms where the users store their data and those stored data will be shared to other users or to the group. The data may be accessed for the public or the private use. When the data is kept for sharing certain security measures should be taken such that the data of the users is secure in the cloud. There may be major security attacks in the cloud so when the data is shared certain cryptographic and authentication techniques should be given in order to protect the data of the users. The security measures must be strong enough and have to be updated frequently as the cloud service updates its settings. Also the efficiency of the cloud service which handles the data must be good and it must use the resources well. The resources must be idle when the data is not in use which saves the energy. The mechanism must be very efficient even when the data is shared among multiple users.*

Key Words*:* **Cloud Computing, security, efficiency**

1. INTRODUCTION

Cloud services have been used by the users for its flexibility and ability to store huge amount of data. Using the services of the cloud the stored data can be shared among individuals or the group of users. It is one of the major aspect in which the users stick on this service. The small scale users or the major organizations have been into data sharing because it increases their productivity. Also the data sharing facility reduces the amount of time to spend on sharing on the huge amount of data irrespective of the physical devices which may take more time to share. Multiple users can access the same data at the same time on the same platform. The Fig.-1 shows the structure of the multiple users' access the same cloud service in which data is shared. This leads to the less usage of time and the cost to build and maintain the storage structure. The storage can be set up once and the data can be stored and shared among multiple users at a time using the same storage. The datacenter should be maintained such that it is efficient to handle the multiple requests from the users and the resources allocated to them. However, the cloud services have to meet the confidentiality, integrity and privacy of the user's data which is stored. There may be anonymous users over the internet where the send fake request for the resources in which authentication must be set up [5] for the cloud service to its storage and the shared data. To provide security some identity based signatures have to be used have been proposed. Authentication is very much important for the organizations in order to share data on a large scale even if there is single or multiple users to maintain its confidentiality. Security in the public cloud is most important [10] because in order to protect the shared data and resources of the users from the possible attacks. The best solution provided is to add a two step authentication technique by using a private key to share and encrypt using the session keys. Even though it may prevent attacks such as key escrow and reduces computational cost it is limited to the image based authentication and the private key which is used for once for sharing purpose it uses Hash functions to generate the keys which can be unlocked easily. The users can store and share the data in cloud but unable to control the data which is stored in the remote datacenters [11]. Thus, controlling the data in the remote site and maintaining its integrity is the major task. In order to overcome these problems the technique using function proxy re-encryption is used. Here the change is in the decryption process where the entire process depends on the user's secret key in which a string has been linked. In turn the string is linked with the cipher text which holds a string if its matches decryption will be made. This method will provide some means of security but it consumes lot of time in re-encryption process where a delay can be introduced. There may be other aspects in cloud such as there may be multi-owner for the same shared data and the groups may be dynamically formed in the cloud [12] which uses One-Time Password [OTP] which is the easiest way and the most popular mechanism which is being used. The OTP is the authentication technique for securing the account which may be used in different machines. It provides three levels of security using mixture of image and password generation technique. The level 1 and 2 are based on the captcha and after successful solving the captcha the user gets the OTP. This technique is very basic and the image related grid can be easily solved. Thus, it moves a little step down in terms of providing a strong security to the cloud to handle the shared data. There must be some strong mechanisms to handle data especially when it is shared among multiple users and an efficient approach needed to be used.

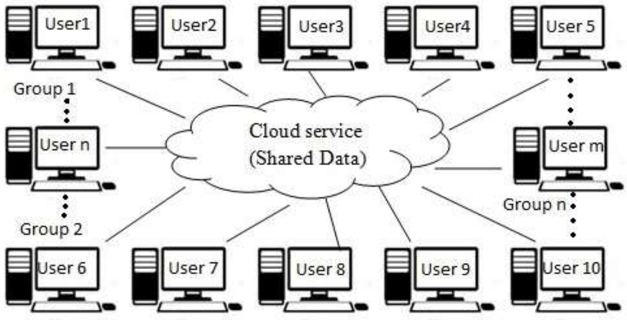

Fig -1: Multiple users trying to access the same shared data in cloud service.

1.1 Related Work

Whenever there is a term cloud service there always exists some common term that is security. Security is an important aspect which has to be taken care by the users who use the cloud service and the vendor who provide the cloud service to the user. The vendors may provide storage to the users from the various datacenters which is located in the remote places. The datacenters may not be secured enough and prone to some of the security attacks. The storage from the datacenters may be scalable in use but the quality of the service provided by the third-party sources [4] must be highly important in order to use the cloud service. As the cloud service has become one of the on-demand services which are used in day-to-day life some intelligent way of authentication is required to safeguard the resources and data of the users when both stored and shared. A third-party authentication is kept to audit and detect any intrusion or the attack in the cloud. The third-party authenticator may provide some sort of security by providing some generalized authentication methods and safeguard the data. The shared data may be divided into number of blocks and then it may be shared. There are chances that few blocks may not be transmitted and there may be few errors in auditing results which declines the authentication mechanism. The audit record may contain some redundant data in which it may fail few mechanisms which affects the security of the system. The Log records [7] may be used by the several organizations in which they maintain a log file which may contain some of the important data of services which may provide security to the data stored in the datacenters. The log file must be maintained as long as data is kept for sharing it requires some of the additional cost because for the maintenance purpose. The new algorithms or the methods should be found out to eliminate the use of the log records and reduce its expenses for the organization. Integrity of the data cannot be maintained by the use of the log files because multiple auditing techniques are required for the purpose. The cloud service has a drawback in the de-centralized auditing and the information from the audit must be properly accounted [6] which can be built into a framework called Cloud Information Accountability [CIA]. The CIA will monitor the flow of the shared data in the cloud and protects the user data from the attacks by using some of the object-oriented mechanisms which performs actions based on the automated logging system which ensures the authentication of the users' login and protects the data. The technique may in the form of the image which is uses as the encryption technique named as chaos image. It is a scramble image consists of the jumbled pixels which are randomly distributed. Due to high randomness of the scattered chaos image it is very difficult to decrypt and to find the correct position of the scramble image thus providing a bit of enhanced security. In [9] a new approach called the log and log harmonizer is used in which it takes help of the JAR file to provide additional layer of security to the cloud service. As soon as the user request any data in the cloud it generates the JAR file upon its creation the authentication request and response will be obtained through the help of the service provider and the JAR file is decrypted if the authentication is matched the data logs are sent to the users else the data will not be shared or can't be accessed by the user. As this technique a light-weight approach it could be stated that it is efficient. Yet it is not applicable for the multi-cloud environment. There may be some modifications to the data in the cloud when the data is shared among the group members who are authorized for the access of the shared data. Integrity has to maintain for the modifications in the groups [8] who have the authorization. The data may have been divided into number of blocks and may be accessed by the users. A technique of digital signature is added to the block of data and the signature has to be made while modifying the data. The data has to been signed by all of the users in the group and have to access by the signatures and have to re-sign the data when it is modified for the security purpose. If any of the users exit from the group re-sign has to be done by all the users. Thus, hereby maintaining the integrity of the data and providing some sort of protection to data of the users. Making into further move for the security and efficiency of the data higher level signatures may be required where there is large numbers of anonymous users in the cloud. Ring-Signature [3] is used for this purpose where the cloud storage and its analysis can be made. As the Public-key infrastructure (PKI) requires various steps including certificate verification and aspect it becomes a cumbersome approach. So, the idea of Identity-based (ID-based) ring signature may be proposed by providing forward security. If the secret keys have been generated previously even those keys become valid thus it saves the time generating keys. Thus, generating and maintaining the keys will be reduced and it will be very effective to implement to use. As the smart-grid approach will be used in which all the keys will be stored and those are valid keys used by the users to authenticate the energy consumption will be less and thus its efficiency may increase. [2] Ring-signatures try to build a trust among the users by sharing the accurate information to the users. When the clusters have been made to share data among the group the ID-based signatures has to be applied and it uses RSA algorithm to provide security and increase its efficiency. [1] The ID-based Ring signature is efficient which doesn't require any pairing operation. The size of its secret key is very small may be just a size of a single integer. It may be implemented in a multi-cloud system because of its efficiency as it's requires less space and time for its operations to take place. Thus, an attempt is made to move a step forward of these approaches to provide security and increase the efficiency when data is shared in cloud.

2. PROPOSED SYSTEM

The various types of security measures have been described such as using session keys and ID-based Ring signatures mechanisms. When these types of systems are used considerable amount of protection is given to the cloud services and secure the data which is being stored and shared among various users. Though this kind of mechanism is found to be efficient way to secure the shared data it is having its own drawbacks as mentioned. An attempt is made to propose a system which provides a better security to the shared data which is being shared among multiple users and could be accessed efficiently which lesser amount of time and the cost to implement it. In this system a cloud system is setup such that it holds huge amount of data in which its services are scalable.

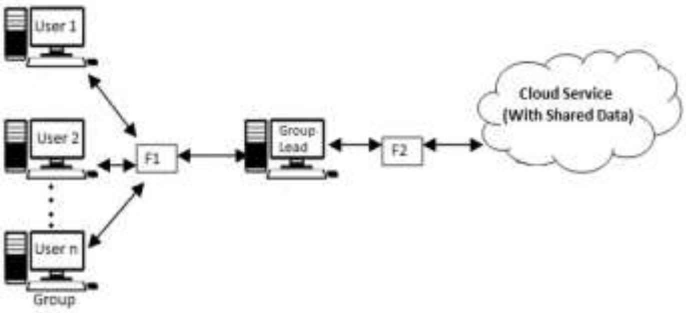

Fig -2: A Set-up for Secure Sharing of Data in Cloud.

In this system certain groups are made in which data has to be shared among multiple users in the cloud. As in Fig -2, the data which has to be shared is placed in the cloud. Some credentials are kept at the interface of the cloud such that no other users can access the data. In the group the numbers of members have to be fixed and the particular members of the group have to be assigned a user-id and key should be generated when a request is made in order to access the shared data which should be dynamic. Here the database is very small and it contains the list of group members and the key. The key will be generated as soon as the request is being made and stored in the database which is temporary. As soon as the requested work is complete the generated key will be disposed. Thus, the amount of data in the database will be reduced. This is taken care by the F1 functional block in which in which it has all the details of the group and its members. It consists of all the group members' id(s) and the data which is requested. AES technique is used to generate the key dynamically which is one of the most secure encryption techniques. In turn the generated key is Hashed and stored and then sent to the Group lead. The Group lead consists of the key and the user-id of the particular member of the group and request to the cloud for the data which has to be shared. The group member and its key is decrypted and checked for its validity by the F2 functional block. If the key and the user-id are matched then the data will be shared else the data will not be shared. While transmitting the data from the cloud to the users the data will be encrypted and sent using the same AES technique and the key will be generated dynamically again. While data is shared the key and the user-id will be checked if it matches the users can access the data. This is done because to prevent any attack in the cloud. As the amount of the data in the database which is used to store member-id, key and the hash value is very less as the key and the hash value is dynamic it can be accessed at a faster rate. More the data in the database, lesser will be the performance of the system. Thus, reducing the database will increase the performance of the system. The keying using the AES technique will be of 192 or 256 independent bits for extreme encryption and which in turn the key is hashed and it is sent to the Group lead and stored. Thus this prevents the attack from external source which may be of man-in-middle attack, or the denial of service.

3. RESULTS

The various techniques such as OTP and the captcha techniques used for the security purpose which are prone to man-in middle attack or the time- delay. So those methods are not secure to use to share the data. The smart-grid technique which is based on the Id-based Ring signature mechanism is very time consuming and it relay on the clusters which is not dynamic. So, using the proposed system the keys can be generated dynamically for the dynamic group in which data is shared in the cloud. This system uses AES technique which is proven to be very efficient and vey secure as it provides a lengthy key of 192 or 256-bits which in turn padded and hashed. The AES is faster in both hardware and the software environment in which it is widely used. As the encryption and decryption is done while requesting and transmitting this system will be powerful as the authentication is checked twice as there is no delay and faster in accessing the data from the cloud.

4. CONCLUSIONS

The proposed system will use lesser database to store the keys which is generated dynamically and will be recycled after the request is being processed completely. And then generates the key for each request is being made. Thus, the security is provided to the system and authentication is made both by the group members and the group lead so security issues have been resolved by this technique. As the AES encryption technique is used for this system it is less prone to attack, the key and the data transmission rate will be faster. As the double protection is given between group members and the cloud it is very efficient and less prone to attack. So, implementing this system will provide better security while sharing and transmitting the data in the cloud. If the data is stored in any datacenter which is located in remote places the users need not worry. As the efficient encryption technique of AES is used by the system and the key size is bigger and dynamically generated at the time of use, in the remaining time the system will be idle so the performance will be increased as the energy utilization will be less.

ACKNOWLEDGEMENT

This work is made with the author's interest, with regard to the cloud services and its data sharing facility. The author's made an attempt to propose a solution for the efficiency and security of the cloud service through this paper.

REFERENCES

[1] Bindumol V S,Dr.Varghese Paul, "Forward Secure Identity Based Ring Signature for Data Sharing in the Cloud",IJSTE, Volume 2, Issue 02,August 2015.

[2]Mrs.S.ArogyaSwarna, Ms.Shirin, AyishaMaryam.M, "Increasing Security Level in Data Sharing Using Ring Signature in Cloud Environment",IJERA,Vol. 6, Issue 2, (Part - 6) February 2016, pp.01-06.

[3] Xinyi Huang, Joseph K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security",IEEE TRANSACTIONS ON COMPUTERS, VOL.64 , NO.6, 2015.

[4]G.Ranjith,J.Vijayachandra,P.Sagarika and B.Prathusha, "Intellingence based Authentication- Authorization and Auditing for Secured Data Storage" ,International Journal of Advances in Engineering &Technology, August, 2015.

[5] M.Manipriya, C.Yalini, "Authenticate Data Distribution BasedOn User Identity",International Journal on Applications in Information and Communication Engineering, Volume 2, Issue 5,May 2016, pp 25-28.

[6] Swapnil Dattatraya Taru, Prof. Vikas B. Maral"Secure Data Sharing in Cloud for Distributed Accountability using Patchy Image Encryption",IJIRCSMS,Volume 2, Issue 12, December 2014.

[7]Vikram.J ,M.Kalimuthu,"A Comparative Study on Privacy-Preserving Public Auditing for Secure Cloud Storage",IJIRCCE,Vol. 2, Issue 11, November 2014.

[8]Elayaraja.D, J.Caroline EL Fiorenza, "An Efficient Approach for Data Sharing in Cloud Computing Using Digital Signature", International Journal of Computer Techniques, Volume 2 Issue 2, 2015.

[9] Nilutpal Bose, Mrs. G. Manimala, "Secure Frameworkfor Data Sharing in Cloud Computing Environment", IJETAE,Volume 3, Special Issue 1, January 2013.

[10]Roshni Sharma,Prof. AmitSaxena,Dr. Manish Manoria,"An Efficient Data Sharing in Public Cloud using two way Authentication &Encryption", International Journal of Computer Science and Information Technologies(IJCSIT), Vol.6(5),2015,4807-4811.

[11]S.I.ShaikHussain,V.Yuvaraj, K. Vishnu, "An Assessmenton Various Secure Data Sharing Methods in Public Cloud", IJAICT, Volume 1, Issue8, December 2014, Doi:01.0401/ijaict.2014.08.06.

[12] P Lavanya, S Komala and N Vikram, "Anonymous Data Sharing Scheme for Dynamic Groups in an Untrusted Cloud",IIJCS,Volume 2, Issue 8, August 2014.