ISSN NO. 2320-5407

Journal homepage:http://www.journalijar.com
Journal DOI:10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

A GROUP SHARING SCHEME BY EFFICIENT SINGLE KEY MANAGEMENT USING CRYPTOGRAPHIC TECHNIQUE.

SanvariyaBhadaniya, Vijay Prakash.
PG Scholar, svits,indore and 452001.

Manuscript Info

Manuscript History:

Received: 18 March 2016
Final Accepted: 29 April 2016
Published Online: May 2016

Key words:
Public Cloud Computing, Encryption, Privacy, Security, Group Sharing.

***Corresponding Author**

Sanvariya Bhadaniya.

Abstract

Cloud computing is a recent paradigm that is creating high expectations about benefits such as the pay per use model and elasticity of resources. However, with this optimism come also concerns about security. In a public cloud, the user's data storage and processing is no longer done inside its premises, but in data centers owned and administrated by the cloud provider. The system is proposed as novel secure group sharing framework for public cloud, which can effectively take advantage of the Cloud Servers' help but have no sensitive data being exposed to attackers and the cloud provider. Extensive security and performance analysis shows that or proposed scheme is highly efficient and satisfies the security requirements for public cloud based secure group sharing.

Introduction:-

With the advancement of technologies the demand of data to outsource is increasing rapidly. For these security of data has become a big issue today. A secure group sharing plays an important role for sharing the resources in a group. To share the useful data in a group is known as group sharing. For example in Whats App the huge and they can share the data in a group. A cloud computing is called public cloud computing if data stored on cloud is open for public use .Services provides by public cloud computing may be free of cost. The difference between the public cloud computing and private cloud computing is openness of data stored into the public cloud computing. There are some advantages of public cloud computing. These are

1. Ultimate Scalability: Public cloud has vast pool of resources so that these resources are available on demand for authorized user. So that applications run on them can respond to seamless to fluctuation in activity.
2. Cost Effective: Public clouds bring together greater levels of resource and so can benefit from the largest economies of scale. Some mass market propositions can even be free to the client, relying on advertising for their revenue.
3. Utility Style Costing: In the utility style costing user pay only for those resources which is useful for user. Therefore it avoiding wasted capacity.
4. Reliability: No single point of failure would make the public cloud service vulnerable means that if one physical component fails the public cloud service still run with unaffected on remaining components.
5. Flexibility: Businesses can even integrate their public cloud services with private clouds, where they need to perform sensitive business functions, to create hybrid clouds.
6. Location Independence: The availability of public cloud services through an internet connection ensures that the services are available wherever the client is located.

Despite of several advantages of public cloud computing there is problem in group sharing. Data stored on public cloud is not secure. If data stored in public cloud then it can be access by any other user, So that the shared data of a group can also be accessed by the users. It will be the great loss of security and privacy of data. For these we propose a new hybrid system of group sharing that eliminates the previous problem of sharing of data in a group on public cloud. In our system we providing the sharing of data in a group in three ways

1. One to one: In one to one sharing one user can share his/her data to any other user in a group. For example user A has some useful data then any user can request to user A for one to one sharing of this data. This data sharing will be more secure in a group.
2. One to many: In this type of sharing if any user A upload some data on cloud then the remaining members can request for that data to user A and they can share this data in one to many form of sharing.
3. Many to one: In this if any user A wants some data so it will request all the group members for this data. If required data is available to any group member then this member will grant the request of user A otherwise it will be refused.

Any user who wants to share the data in a group he/she can easily shares the data in one to one, one to many and many to one form of sharing.

Literature Survey:-

Data privacy can be preserved by two solutions such as encryption of data and then upload the data that is encrypted. It is somehow difficult to design an efficient and secure data sharing between the groups. Literature review is the most important step in software development process. Following is the literature review of some existing technique for data sharing in the cloud.

Kaipingxue et al. [1] proposed a dynamic secure group sharing framework in public cloud computing. In spite of several advantages of cloud storage of data there are some challenges like the privacy and security of users' data. In generally the data owner stores his data to fully trusted server so there is requirement of fully trusted administrator which can control the access of data. So that the traditional schemes are not more beneficial for cloud storage because the cloud service provider is the semi-trusted. If the data owner share his/her private data with intended recipient then there is a possibility that anyone can get the information from the encrypted data stored on cloud but this data should be decrypted by only the intended recipient, So that in existing system problems are that.

1. To distribute and update this session key is an issue.
2. If there are N specific authorized users shares a file then N digital envelopes are required.
3. For any single file the communication and computation overhead of digital envelope is O(N).
4. If there is M share files and N intended recipient are exist then overall overhead O(MN).

In this proposed system they are using proxy re-encryption which decreases the overhead of cloud while securing the users' information and Tree based Group Diffie-Hellman(TGDH) to update group key dynamically. All the sharing files are stored in the cloud securely and session key protected by using the digital envelope, by the security and performance analysis system highly efficient and secured. Some of advantages of our proposed system are:-

(1)Proposed scheme [1] update the group key whenever any group member join or leave so that overhead of communication and computation transferred to cloud server without leaking the privacy of data.

(2)Enhance the Tree based Group Diffie-Hellman(TGDH); so the group key update automatically and there is no need to online all the group member together.

Mohamed Nabeel et al. [2] proposed privacy preserving policy based content sharing in clouds. The main problem in existing system is that how to share the document which is stored in public cloud. This approach uses different policies and different keys to encrypt the document. Problem exist in this system is that the policy changes results in the multiple copies of same encrypted data on cloud so high computational overhead. So that this approach cannot efficiently work to add or revoke the users or the identity attribute. If the number of users are increases and multiple keys are required to distribute to multiple users so identity attributes cannot be protected by this approach. To improve the performance of existing system new key management scheme known as broadcast group key management (BGKM) is used in [2]. This approach is an efficient approach for fine grained encryption control for data stored in an un-trusted public cloud. The advantage of our proposed system is that if the user will add or revoke or updating the access control policy so our scheme perform well compare to existing once. By BGKM approach we design an attribute based access control method in which user can only be decrypt the content if its identity attributes satisfy the policies of content providers. In this the cloud provider and content provider has no idea about users' identity attributes. Our approach support attribute based access control policy preserving the privacy and confidentiality of users' identity attributes for sharing in a un-trusted cloud storage.

Hong Liu et al. [3] proposed shared authority based privacy preserving authentication protocol in cloud computing. As the increasing popularity of cloud services security and privacy of data become need of today. The existing approach based on only the authentication so that the users' private data cannot be accessed by the unauthorized user. If one user want to share the data with other users with help of cloud server then the privacy of data is also required. This problem exists in existing system. Conventional schemes are attention only the strong authentication so that the user can access his data on demand. To get the benefit if user want share each other's data then security and privacy of data is biggest challenges for the cloud storage server. To preserve the privacy issue for cloud storage new scheme shared authority based privacy preserving authentication protocol(SAPA) is proposed in [3]. In this protocol attribute based access control is used so that user can access its own data and to share the data among multiple authorized users proxy re-encryption is used by the cloud server. This proposed approach mainly focuses on:-

1. It provide an authentication protocol which enhance a user's access request related privacy and get the authority access by anonymous access request comparing methods.
2. It uses cipher text policy attribute based access control so that a user can access its own data and authorized data can be shared among multiple users by proxy re-encryption.
3. It insures data confidentiality and data integrity by authentication establishment.

Boyang Wang et al. [4] proposed storing shared data on the cloud via security mediator. For the security of data in the cloud the users and data owner should insure the integrity of cloud data before sharing this data among multiple users with provable data possession (PDP). Previous approaches are not able to give identity of data owner to un-trusted cloud and there exist overheads for preserve anonymity. Operations on data in the cloud are not visible to user so that security of data like data integrity is big issue on cloud. Size of the cloud data can be huge so that if verifier checks the data integrity it requires to download entire data stored on cloud. In this situation the benefit of cloud storage may lost and amount of computation and communication resources is waste. To ensure the integrity of cloud data and anonymity of data owners and remove the overheads a simple approach is used in [4]. Our proposed method uses the security-mediator (SEM) which verifies the metadata. In our system identity of data owner is not revealed to cloud and extra overhead is removed which is present in previous approach. To achieve anonymity to store the data on cloud with ensuring verifiable integrity of data our (SEM) approach is secure and efficient compare to existing approach. Our approach not only minimizes the computation overheads but it provides data privacy and identity privacy.

Xin Dong et al. [5] proposed achieving an effective, scalable and privacy preserving data sharing service in cloud computing. The number of customers and enterprises are grooving who stores the data on cloud so there is requirement of privacy and security of data. There are some challenges to achieve effective, scalable and privacy-preserving data sharing service in cloud. These are.

1. The data owner should give permission to different users so that they can access this data.
2. The cloud server must support dynamic request of data so that data owner can add or revoke and access permission give to other user to delete or create and update data.

Proposed scheme [5] provides several benefits if we compare to previous scheme. The advantages are:

1. Proposed scheme [5] provides effective and scalable encryption for cloud data. So that data sharing services achieves full privacy preserving and data confidentiality.
2. Proposed scheme [5] mainly enforces fine grandness, backward secrecy and access privilege confidentiality.
3. Proposed scheme [5] takes small overheads compare to existing scheme.

In 2010 Lan Zhou et al. [6] proposed a scalable and fine-grained data access control scheme by defining access polices based on data attributes and KP-ABE technique. The combination of attribute-based encryption (ABE), proxy re-encryption and lazy re encryption permit the data owner to assign the computation tasks to un trusted server without revealing the necessary contents of data. Data files are encrypted using random key by data owner. Using key policy attribute-based encryption (KP-ABE), the random key is further encrypted with a set of attributes. Then the authorized users are assigned an access structure and corresponding secret key by the Group Admin. Thus, only the user with data file attributes that satisfy the access structure can decrypt a cipher text. This system has some limitation such as multiple owner manner is not supported by this system so that those single owner manners make it less flexible as only Group Admin are responsible for modifying the data file shared. And user secret key needed to be updated after each revocation.

In 2012 B. Wang et al. [7] focused on cloud computing and storage services, data is not only stored in the cloud, but routinely shared among a large number of users in a group. In this paper, they propose Knox, a privacy-preserving auditing mechanism for data stored in the cloud and shared among a large number of users in a group. In particular, the utilize group signatures to construct holomorphic authenticators, so that a third party auditor (TPA) is able to verify the integrity of shared data. Meanwhile, the identity of the signer on each block in shared data is kept private from the TPA. The original user can efficiently add new users to the group and disclose the identities of signers on all blocks. With Knox, the amount of information used for verification, as well as the time it takes to audit with it, are not affected by the number of users in the group.

In 2013 Xuefeng Liu et al [8] proposed new method “MONA”. This method presents the design of secure data sharing scheme for dynamic groups in an untrusted cloud which involve integration of group signature and broadcast encryption techniques. This method support dynamic group i.e. User can be revoked easily through revocation list without updating remaining users as well as new user can decrypt data file without contacting to the data owner. Therefore size and computation costs of encryption are independent with the number of revoked users. This system identified some limitations in terms of efficiency and security. Also in revocation list the time given for each user is fixed after time expire user cannot access the data until Group Admin update the revocation list and give it to the cloud.

Problem Statement:-

There aresome problems exist in existing system. These are

1. In existing system computation cost and communication cost are very high in a group sharing.
2. There exists a problem of key management when the number of users increases in a group.
3. We are storing data on the public cloud so in existing system there is a problem of the privacy and security of data on public cloud.
4. Existing methods are not fined grained.
5. Existing algorithm mainly focus on authentication of data but the privacy and security of data are very big issue in public cloud computing.

Proposed Solution:-

Description of terms:-

Registration: -To check the identity of any user registration is required. In registration process user gives his/her details like username or email id and password. In our proposed system username, email id, password and mobile number are used for registration of any user.

Login: -As the username and password are matched user identifying and authenticating themselves. In our proposed system username and password are used for Login process. Now user can access the computer system after the login.

Authentication: -Authentication is a principle of security which identified a user or computer system so that it can be trusted. To confirm the identity of a user is authentication. It might involve confirming the identity of a person by validating their identity documents. In our proposed system only authorized group user can access the data stored on cloud.

Encryption: -The process of encoding plaintext into cipher text is known as encryption. In other word encryption is the process in which original data converted into cipher text after adding some other data known as cipher to original data. To encrypt the data we apply some encryption algorithms on data vice versa for decryption process at receiver end we apply some decryption algorithm on cipher text to get original data. To protect the confidentiality of data encryption is used.

Cloud storage: -Cloud storage is generally a model of data storage. By storing the data on cloud user need not to purchase device for storage and also there is no need to hire server management engineer for the managing purpose. As the data is stored on the cloud it is easier to share the data with intended receiver for the data owner. In our proposed system we are uploading and downloading the data on cloud then we providing sharing facility to user in a group.

Upload: -Putting something on internet is known as uploading. In our proposed system we are uploading the data on cloud in encrypted form. As the data is uploaded a key is generated and this key is updated automatically when sharing is performed. By using this key only the data can be decrypted and downloaded.

Download: - Downloading generally transferred the data for local storage and later use. To receive the data from server is downloading. In our proposed system we download any file which store on cloud using the key only.

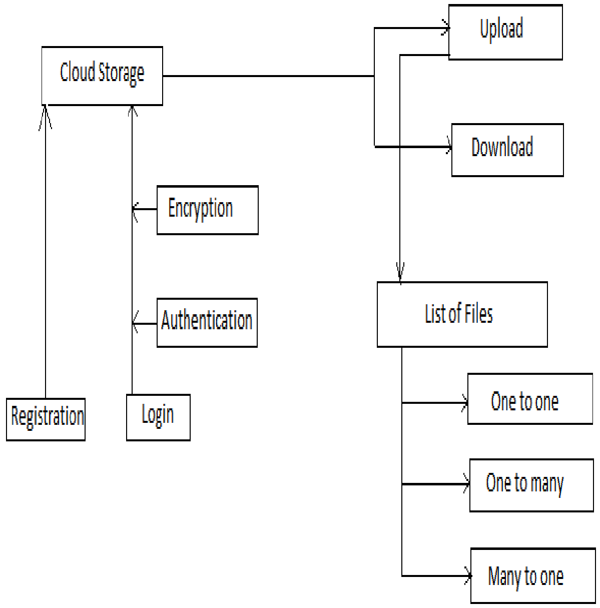

Figure 1:-Work flow of proposed system.

Cryptographic Model:-

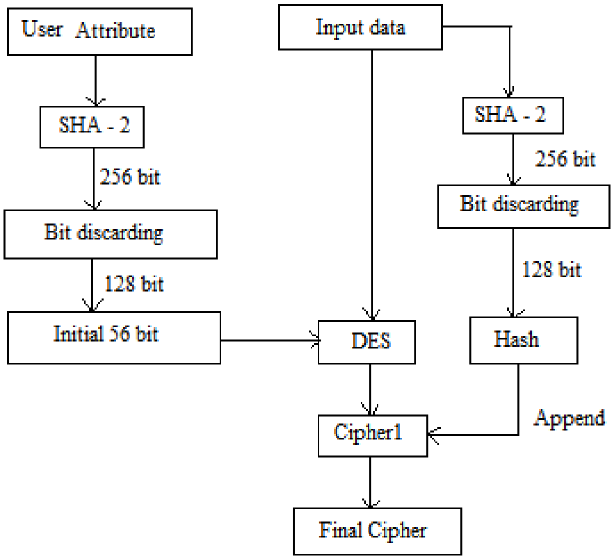

Figure 2:- EncryptionModel.

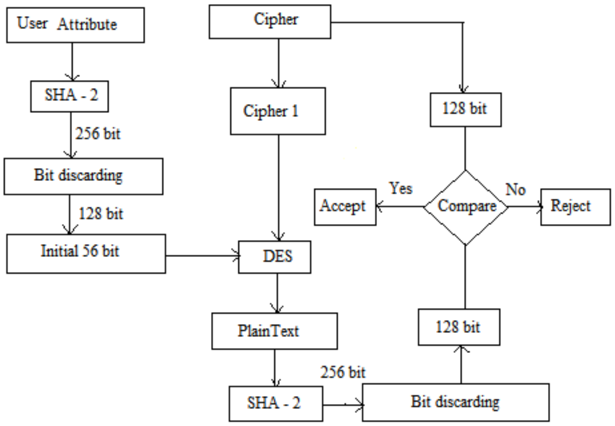

Figure 3:- DecryptionModel.

In our proposed work we are applying the encryption on data in Fig 2 and decryption on cipher in Fig 3. In encryption we are passing data as a input to SHA-2 algorithm and DES algorithm. The main task of SHA-2 algorithm is to converts the data into 256- bit. Then we apply bit discarding process on this 256-bit. By this process every alternative bit is discarded and it results in 128-bit. On other hand we use some user attribute to generate the key. This key is also passed to the SHA-2 algorithm for generate the unique key. This unique key is further use for encryption and decryption of data. The DES algorithm will encrypt the data by using this key and generate the cipher. Now both the cipher and 128-bit are append and send to the network.

On the decryption end both cipher and 128-bit are separated. Now this cipher is passing to DES for getting the plaintext and this 128-bit reserve for comparison. Again user attribute key is given to SHA-2 algorithm it will generate the hash key. The DES algorithm will decrypt the cipher by using this key. The original plaintext is given to SHA-2 algorithm will results in 256-bit of data. Now bit discarding process is applied on this256-bit will produce the 128-bit. Finally this 128-bit is compared with separated reserve 128-bit. If both the bits are equal then accept otherwise reject.

Acknowledgements:-

This research work is self-financed but recommended from the SVITS so as to enhance the sharing of data in a group using single key management by cryptographic techniques. Thus, the authors thank the anonymous reviewers for their valuable comments, which strengthened the paper. The authors also wish to acknowledge institute administration for their support & motivation during this research. They also like to give thanks to VIJAY PRAKASH for discussion regarding the approach adapted for this paper.

References:-

1. KaipingXue, and Peilin Hong, “A Dynamic Secure Group Sharing Framework in Public Cloud Computing”, IEEE TRANSACTION ON CLOUD COMPUTING, YEAR 2014.
2. Mohamed Nabeel, Ning Shang, Elisa Bertino “Privacy Preserving Policy Based Content Sharing in Public Clouds”IEEE Transaction on knowledge and data engineering, Volume 25..
3. Hong Liu andHuanshengNing, ,QingxuXiong, and T. Yang “Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing”, IEEE Transaction on Parallel and Distributed System.
4. Boyang Wang, Sherman S.M. Chow, Ming Li, and Hui Li, “Storing Shared Data on Cloud via Security Mediator”IEEE 33rd International Conference on Distributed Computing System (ICDCS),2013.
5. Xin Dong, Jiadi Yu, Yuan Luo, Yingying Chen, GuangtaoXue, and Minglu Li “Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing” computers and security (2014) ,
6. S. 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.
7. B. Wang, B. Li, and H. Li, “Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud,” Proc. 10th Int’l Conf. Applied Cryptography and Network Security, PP. 507-525, 2012.
8. Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud”, IEEE Transactions on Parallel and Distributed Systems, Vol.24, No. 6, June 2013
9. M. Kavitha Margret, “Secure Policy Based Data Sharing for Dynamic Groups in the Cloud”, International Journal of Advanced Research in Computer Engineering and Technology ((IJARCET), PP. 2073 – 2076, Volume 2, June2013