Privacy Preserving of Information Sharing for Authenticated users in Cloud Computing

Pradeep Kumar Regeti [1], BeharaVineela [2]
[1]*Final M.Tech Student, Asst.professo*[2]
[1,2]*Dept of CSE, Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh, India*

Abstract: *Cloud computing is a promising information technology architecture for both enterprises and individuals. The cloud is most attractive by storage of data and also interactive paradigm of data consumers, network access and independent resource pooling. By implementing cloud architecture is very difficult for provide security and data access policy. So that in this paper we are proposed concepts of authentication of data consumers, generation of group and secure forward, data anonymity and security of transferring data. By performing those operations we can implement following concepts. In this paper we are proposed concepts for authentication of data consumers using group digital signature algorithm, data anonymity using block corruption protocol, group key generation using prime order group key generation and security of transferring data using triple data encryption standard. By implementing those techniques we can improve the efficiency, more data access authority sharing and privacy of forward data.*

Keywords: *Cloud computing, authentication protocol, privacy preservation, shared authority.*

I. Introduction

Today's technologies cloud computing place an important role for sharing of information through network. By implementing this architecture we can provide information sharing both enterprise and individual applications. So that by implementing this architecture we can improve advantages, including on-demand self-service, information access and location of independent resource pooling [1]. By providing cloud architecture we can perform the functionalities of anything as a service to inter connection of networks. Recently most of the cloud computing architecture can be implemented internet oriented service. So that by performing the functionalities of cloud through the internet we can be consider mainly of security and privacy of sharing information. Those two concepts will face key issue in a cloud computing in fracture. By implementing those two concepts we can improve popularity of cloud service.

In the cloud computing architecture contains so many approach for performing the authentication and privacy cloud data. One of the approach is conventional approach by implementing this approach we can provide strongly authentication process to realize that users can remotely access its own data in on demand mode. By providing diversity of the application requirements users may want to access and share each authorized data. By implementing this approach we can provide new security and privacy challenge of the cloud computing. By implementing cloud storage architecture it will follow the chain management architecture. The cloud storage architecture contains various groups for sharing of information in a network. In the each group contains its own group member and those users contains independent access control policies. So that in group any user can access data fields and also store the data into cloud. Before performing those access authorities of users, those users are verified by cloud server. After performing authentication users we can give access request can be performed for the getting information from the cloud.

By implementing cloud environments some of the reasonable authentication protocol should achieve the following requirement. i.e. authentication of user. By providing the authenticated user can access its own data fields, so that the authorized can access data from the cloud. Another process authentication is data anonymity is an irrelevant entity cannot exchanged data and communication can be done by open channel. Other concepts of cloud computing is user privacy for the authentication users can be done by cloud service. After performing authentication users can access data files from the cloud storage. If any unauthorized user cannot get data from the cloud storage. So that if any user share the information through clouds it will contain access permission. In the cloud architecture one of most important concepts is provide security of forwarding message. So that if any user transferring messages it will provide privacy of that message. So that to provide privacy of that data we can implement one of cryptography concepts.

II. RELATED WORK

Grzonkowski *et al.* [2] proposed a zero-knowledge Proof (ZKP) based authentication scheme for sharing of information in cloud services. By implementing these concepts we provide the centric approach for sharing of information in human networks. So that each user will enable the personalized and sophisticated network based approach which enable cloud services. By implementing this process we can provide trusted third party for decentralized interaction between the users. Wang et al[3] proposed concepts distributed storage auditing mechanism for introducing homomorphic token and dependable storage in a cloud service. By implementing this concept each user will auditing cloud service for sharing of information. The user performing auditing mechanism is light weight communication over heads and also provides strong correctness storage of data. By implementing this concept we can also overcome malicious data modification attack.

Nabeel et al[4] is proposed the concepts broadcast group key management schema for improving weakness of symmetric key cryptography in a public clouds. By implementing symmetric key cryptography technique user need not utilize public key cryptography and dynamically derive the symmetric for decryption process. Accordingly, attribute based access control mechanism is designed to achieve that a user can decrypt the contents if and only if its identity attributes satisfy the content provider's policies. The fine-grained algorithm applies access control vector (ACV) for assigning secrets to users based on the identity attributes, and allowing the users to derive actual symmetric keys based on their secrets and other public information. The BGKM has an obvious advantage during adding/revoking users and updating access control policies. Sundareswaran *et al*. [5] established a decentralized information accountability framework to track the users' actual data usage in the cloud, and proposed an object-centered approach to enable enclosing the logging mechanism with the users' data and policies. The Java Archives (JAR) programmable capability is leveraged to create a dynamic and mobile object, and to ensure that the users' data access will launch authentication. Additionally, distributed auditing mechanisms are also provided to strengthen user's data control, and experiments demonstrate the approach efficiency and effectiveness.

Liu *et al.* [6] proposed a multi-owner data sharing secure scheme (Mona) for dynamic groups in the cloud applications. The Mona aims to realize that a user can securely share its data with other users via the untrusted cloud server, and can efficiently support dynamic group interactions. In the scheme, a new granted user can directly decrypt data files without pre-contacting with data owners, and user revocation is achieved by a revocation list without updating the secret keys of the remaining users. Access control is applied to ensure that any user in a group can anonymously utilize the cloud resources, and the data owners' real identities can only be revealed by the group manager for dispute arbitration. It indicates the storage overhead and encryption computation cost are independent with the amount of the users. Dunning *et al.* [7] proposed an anonymous ID assignment based data sharing algorithm (AIDA) for multiparty oriented cloud and distributed computing systems. In the AIDA, an integer data sharing algorithm is designed on top of secure sum data mining operation, and adopts a variable and unbounded number of iterations for anonymous assignment. Specifically, Newton's identities and Sturm's theorem are used for the data mining, a distributed solution of certain polynomials over finite fields enhances the algorithm scalability, and Markov chain representations are used to determine statistics on the required number of iterations.

III. EXISTING SYSTEM

Researches have been worked to strengthen security protection and privacy preservation in cloud applications, and there are various cryptographic algorithms to address potential security and privacy problems, including security architectures data possession protocols, data public auditing protocols, secure data storage and data sharing protocols, access control mechanisms, privacy preserving protocols, and key management. However, most previous researches focus on the authentication to realize that only a legal user can access its authorized data, which ignores the case that different users may want to access and share each other's authorized data fields to achieve productive benefits. When a user challenges the cloud server to request other users for data sharing, the access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this work, we aim to address a user's sensitive access desire related privacy during data sharing in the cloud environments, and it is significant to design a humanistic security scheme to simultaneously achieve data access control, access authority sharing, and privacy preservation.

IV. PROPOSED SYSTEM

The cloud torage system includes data consumers or users and cloud servers. The cloud storage system more efficient for storing and retrieve the data, also

provide the shared authority of data access. In this paper we are proposed concepts for providing authentication, data anonymity, group key generation and privacy of transferring data. By implementing those concepts we can provide more shared authority of data access and also perform the authentication of data consumers. In this paper the proposed concepts will be explained as follows.

Authentication of data consumers:

In this module perform the operation of authentication of each user in a group. The authentication process will perform by trusted center. Before perform the authentication process each group member will register into cloud service and get username and password. The authentication process will perform by using group digital signature algorithm. The process of group digital signature algorithm as follows.

1. Each group member will choose a large prime number P with the range of 512 to 1024 bits and is multiple of 64.

2. Each group member will choose q with the range of 160 bits prime divisor of p-1.

3. After choosing those values each group member will calculate g by using following formula

$g=h^{(p-1)/q}$ where $1<h<p-1$ and $h^{(p-1)/q} \bmod p > 1$

4. Each group member choose private key $x < q$

5. After choose the private key each group member will calculate public key by using following formula

$$Y= g^x \bmod p$$

6. After calculate public key each group member will generate signature and send to trusted center. The generation signature can be done by using following formulas.

$$r = (g^k \bmod p) \bmod q$$

$s = [k^{-1}(H(M)+ xr)] \bmod q$ where M is username of each group member

After generation of signature each group member will sent global public values (p, q, g, r, s, and y) to trusted center. The Trusted center will retrieve global public values and again generate signature for individual users. After generating signature of each user the trusted center will verify that the signature is equal authenticated user else not authenticated. The generation signature will be done by using following equation.

$$w = s^{-1} \bmod q$$

$u1= [H(M)w] \bmod q$

$u2= (rw) \bmod q$

$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$

After completion of authentication users the trusted center will generate group key and sent to individual users. The generation of group key is as follows

Group key generation:

In this module the trusted center will generate group key for the data consumers. The trusted center will use prime order group key generation technique for generation of group key. The procedure of prime order group key generation is as follows.

1. The trusted center will generate random number and also choose one prime number.

2. After that the trusted center will xor with those value and convert into binary format.

3. After conversion binary format the trusted center will perform once complement and convert into ascii value.

4. After that each user contain shared values, the trusted center will send those values to individual user.

5. Each user will retrieve shared value and perform the reverse process get same secret of individual users.

File Encryption and generation of signature:

In this module each user will encrypt the upload file and stored into cloud. In the encryption process we are using triple data encryption standard algorithm. After completion of encryption the each user will generate signature for that cipher data and stored into cloud. The generation signature we are using block corruption protocol. The implementation procedure of block corruption protocol as follows.

1. Calculate length of m in upload cipher file.

2. Choose the length of block n is any one of 128 or 256 or 512 or 1024.

3. Select 16 bit as reserved bit i.e. res
4. Calculate P= m mod n it will get last block length then Q=n-(P+res)

If(Q>0)

Then append Q zero to file F

Else if(Q<0)

R=n+Q
Then append R zero to file F

5. Append res for end of file

6. After appending zero to file again calculate length of file L

7. After calculating length file we can find number blocks using count =L/n.

For j=1 to count
S=0;
S= reversΣ $_{A=1}^{n}$ ((A®B)□(A□B))
Where B=Integer(to Char(A))
Sig=sig+to_binary(B)

F=sig+File

After generating signature of file each user will stored data into cloud and also store signature.

File Decryption process:

In this module each user will retrieve file from the cloud service and again generate signature by using block corruption protocol. The user also retrieves the previous signature and compares both signatures. If both signatures are equal the upload file will not corrupt and decrypt the file. The decryption process will be done by using triple data encryption algorithm. By performing signature verification process we can provide sharing data anonymity. After decryption process each user will get original plain data. Here we can also provide more privacy of shared data by using cryptography technique.

V. CONCLUSION

In this work we have identify new privacy challenge of sharing authority of data access and also provide authentication of data consumers. In this paper we can also implement of generation of group key for encryption and decryption of sharing data in the cloud. By implementing this technique all group members will get same secret key and performing sharing of data. Here we can also performing data anonymity for that shared data will be corrupted or not. By implementing those techniques we can improve the more efficiency of data anonymity and also provide more security of sharing data in the cloud service.

VI. REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," National Institute of Standards and Technology, USA, 2009.
[2] S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 3, pp. 1424-1432, 2011.
[3] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220-232, 2012.
[4] M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," *IEEE Transactions on Knowledge and Data Engineering*, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, 2012.
[5]. S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp.556-568, 2012.
[6]. X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud," *IEEE Transactions on Parallel and Distributed Systems*, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, 2012.
[7]. L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 402-413, 2013.
[8]. Y. Xiao, C. Lin, Y. Jiang, X. Chu, and F. Liu, "An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing," in *Proceedings of Global Telecommunications Conference (GLOBECOM 2010)*, December 6-10, 2010.
[9]. H. Zhuo, S. Zhong, and N. Yu, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability," *IEEE Transactions on Knowledge and Data Engineering*,
vol. 23, no. 9, pp. 1432-1437, 2011.
[10]. S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds,"
IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6463404, 2013.
[11]. J. Yu, P. Lu, G. Xue, and M. Li, "Towards Secure Multi-Keyword Top-k Retrieval over Encrypted Cloud Data," *IEEE Transactions on Dependable and Secure Computing*, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6425381, 2013.
[12]. I. T. Lien, Y. H. Lin, J. R. Shieh, and J. L. Wu, "A Novel Privacy Preserving Location-Based Service Protocol with Secret Circular Shift for K-nn Search," *IEEE Transactions on Information Forensics and Security*, [online] ieeexplore.
ieee.org/stamp/stamp.jsp?tp=&arnumber=6476681, 2013.
[13]. K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, [online] ieeexplore.
ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398, 2012.

BIOGRAPHIES:

Pradeep Kumar Regeti is student in .Tech(CSE) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his B.tech (C.S.E) from R.R.S College of engineering and technology, muthangi , Hyderabad. His interesting areas are network security and cloud computing.

BeharaVineela is working as Asst.professorin Sarada Institute of Science, Technology And Management, Srikakulam, Andhra Pradesh. He received his M.Tech (CSE)from AITAM ,Tekkali, Srikakulam, AndhraPradesh. JNTU Kakinada Andhra Pradesh.His research areas include Network Security