USER REVOCATION OF SHARED DATA THROUGH CLOUD

Mr.N.Devender[1], Ms.M.Jahnavi [2], Ms.T.Swetha [3]
Asst.profeesor[1], Student [2, 3]
CSE Department
Balaji Institute of Technology & Science, Telangana, India

Abstract: By using cloud services the sharing of data and other services related to cloud can be done easily. Where ever sharing of data with single are multiple entity's a group can be done efficiently to provide secure data integrity the data is verified in the group. The sum of authentications is been verified in the blocks of cloud the data modifications can be possible only by the authorized user. Once the user exit from a group. Then the user must re-signed with the existing user in the group, the existing user have to download the shared data and re-signed in the user revocation. So it requires more space for revocation of data in the cloud. To overcome this problem we use new mechanism called public auditing mechanism. This is used to share the data with efficient users and for data integrity. By this the existing user need not sign in the group and also the user any need to download the previously shared data. The public verifier is used to audit the integrity of shared data without accessing the data from the cloud. Even though some part of shared data is re-signed by the cloud this mechanism is able to verify the integrity of shared data and multiple auditing task simultaneously. By this the user efficiency and revocation is improved.

KEYWORDS: *Integrity, shared data, revocation, efficiency, auditing.*

I. INTRODUCTION:

The services provided by the cloud like data sharing and storage services like (drop box)where people can easily access either individually or group .here the user can access or share the data which must be secured because data which is been shared or modified must be authenticated reliable existence without human or software errors. Many mechanisms are been enabled by the cloud to secure the data like signature authentication and common features like accessing the data through the cloud with third party .the main mechanism that must be enabled is that the client who like to utilize the cloud must be authenticated with a digital signature (denoted as provable data profession) which provides data integrity and security. In the shared data, the user can modifies a block and must compute a new signature to the modified block. The different users can modifies different block so that they can be signed by different users, by the security reasons the user must follow the rules which are assigned in group if the user does not follow the rules the n the user revoked from the group. AS a result when the user revoked from the group the user cannot access the shared data and also user cannot be able to modify the data after a longer time. Even though the content of the data cannot be changed And also the signatures which can be generated by the revoked user is not valid for longer period in the group. If the revoked user want to sign in then the existing user in the group must be re-signed by this the integrity of data can be verified with the public key of existing user. The existing user must be re-signed, verify and download the content of the block. For this the existing user may cost huge amount of communication and computation resources. By uploading the re-signed signature it quite large amount changes. The cloud provides the private key for every user then it is easy to re-signing to the existing user. it providing private key but the cloud cannot trust each user by some security issues. By the user revocation re-computing the signatures it doesn't effect to public auditing. Hence significant burden to the existing user is efficiently reduce by introduced by user revocation and also the public verifies is used to check the integrity of shared data . In this paper we propose a mechanism where the integrity for the shared data with proxy signature where the user can easily accuses the data with security mechanism and integrity thus it enables the re signatures to accesses the data.

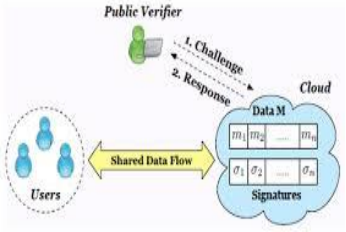

Fig: 1 Mechanism for data sharing through authentication.

II. PUBLIC AUDITING FOR SHARED DATA WITH EFFICIENT USER REVOCATION IN THE CLOUD:

By the cloud the user can easily share, store modifies the data in a group. The shared data integrity can be verified publicly; generally in shared data different users can modify the different data. By security reasons if the user revoked once from the group then the existing user must be resigned by the previously revoked user and need to download the shared data.

In this paper we proposed knowledge public auditing mechanism for integrity of shared data with efficient user revocation. By the proxy re-signature, during user revocation the cloud re-sign blocks on behalf of existing user. Hence the public verifier is always checking the integrity of shared data from the cloud. By providing all this security services even though there is some integrity of shared data is not retried .the public verifier always checks the task simultaneously. By this the efficiency of user revocation is improved.

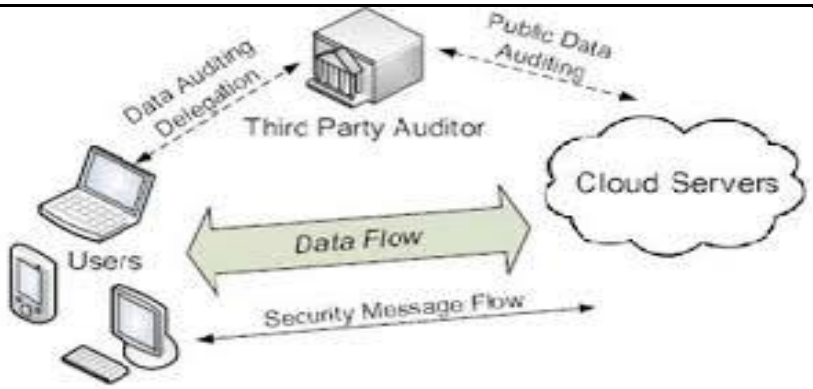

Fig 2: Public Auditing Sharing Data

III. A VIEW OF CLOUD COMPUTING, COMMUNICATIONS OF THE ACM

Cloud computing dream to provide computing as a utility. It has high potential to share large amount of data, IT industry, designing the software with more attractive mechanisms and software's which are related to the storage and sharing. Most of the developers are innovating the great ideas in software field with prediction and provisioning programs that result in better enabling resources.

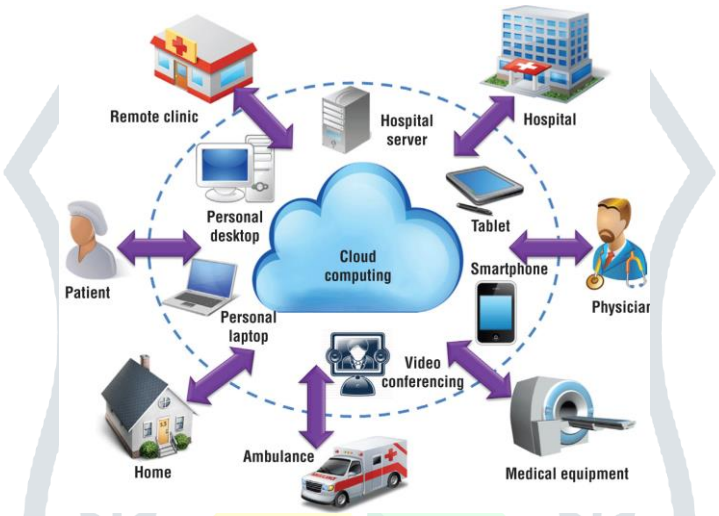

Fig: 3 cloud computing communication

IV. COMPACT PROOFS OF IRRETRIEVABILITY:

The data storage must provide an authentication that client's data is been secured with authentication and efficient. The scheme with proof of retrievably with proofs against the model must be strong and the protocols and the signatures must be feasible with client server response the scheme also provides the authentication value with proofs with aggregate values with the properties along the scheme.

In existing system the data uploaded in cloud which n is not signed by user authentication in each time of upload. So that the data integrity of shared data is not possible in the existing system. However, the cloud is not trusted in the same domain with each user in the group, every user have an individual private key with their security issue.

V. FUTURE ORGANIZATION

In this Proposal we verify about the impropriety of shared content in order to accumulate the reputation of avoid losing money and data services. In addition, we also assume there is no complicity between the cloud and user design of our mechanism. Usually, the inappropriateness of data under the beyond semi trusted model is been introduced by hardware/software failures or human errors happened in the obscure. In view of these factors, users do not fully trust the cloud with the integrity of shared data. It provide the Blocking User account, Security question, Login with encryption format data for the user access.

Some common policy's while creating DFDs:

- Processes should modify the incoming content, producing outgoing data.
- Data store must be involved with at least one or more data flow.
- The external entity must involve with one data flow process

VI. CONCLUSION

In this paper, we projected a latest public auditing mechanism for shared data with well-organized user revocation in the cloud. In the group the user is revoked, the cloud allows the semi-trusted user to re-sign blocks that were signed by the revoked user with proxy re-signatures. As results it shows that the cloud can improve the integrity of shared data by user revocation, during user revocation an existing users in the group must accumulate a large amount of computation and communication possessions.

VII. REFERENCES

[1] Ahamed, B. B., & Hariharan, S. (2012). Implementation of Network Level Security Process through Stepping Stones by Watermarking Methodology. International Journal of Future Generation Communication and Networking, 5(4), 123-130

[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," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[3] Sundravadivel,P., & Yuvaraj, D.(2018).An Effective Document Category Prediction System Using Support Vector Machines, Mann-Whitney Techniques. International Journal of Pure and Applied Mathematics, V118,No.22,PP 895-900.

[4 BazeerAhamed, B., & Mohamed, S. S. S. (2011). Implementation of Trusted Computing Technologies in Cloud Computing. International Journal of Research and Reviews in Information Sciences (IJRRIS), 1(1), 7-9..

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in the Proceedings of ACM/IEEE IWQoS 2009, 2009, pp. 1–9.

[6] Mahalakshmi,K., Sivaram, M., & Yuvaraj, D.(2018). Healthcare Visible Light Communication. International Journal of Pure and Applied Mathematics, Volume 118 No.11 ,PP 345-348.

[7] Ahamed, B. B., & Ramkumar, T. (2018). Proficient Information Method for Inconsistency Detection in Multiple Data Sources..

[8] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in the Proceedings of ACM SAC 2011, 2011, pp. 1550–1557

AUTHORS:

Mr. Nayini Devender has 3+ years experience as Assistant Professor in the Department of Computer Science & Engineering, BITS, Warangal, India and he is a life member of ISTE. He has published more than 3 research papers. His area of research includes Internet of Things (IoT), image processing etc.

MANGA.JAHNAVI
I'm pursuing B.Tech 2nd year in Balaji Institute of Technology & Science Narsampet, Dept of CSE

THOTA.SWETHA
I'm pursuing B.Tech 2nd year in Balaji Institute of Technology & Science Narsampet, Dept of CSE