The Enhanced Security Systemfor Multi-Owner Data Sharing for Various Groups in Cloud Storage

[1]Laxmi Regadi, [2]S. Seshagiri
[1,2]Dept. of Computer Science Engg., Sri Vaishanavi College of Engineering, Srikakulam, AP, India

Abstract
Cloud Patrons can fulfill a practical and effective viewpoint for information sharing in the cloud with the appeals of low upkeep and little organization cost. Since the code will be outsourced, we give an efforts to establish safety to the sharing information records. Tragically, because of the relentless change of the enlistment, ensuring the sharing information is a testing errand, especially for an untrusted cloud as a result of the connivance ambush. What's more, to exist arranges, they utilize secure correspondence channels to give the secured key dissemination among the gathering, nevertheless, to have such channel is a strong assumption and is troublesome for practice. In this paper, we propose a protected information sharing arrangement for component people. In the first place, we propose a protected way for key appointment with no sheltered correspondence channels, and the customers can securely get their private keys from social occasion boss. Second, our arrangement can fulfill fine-grained get to control, any customer in the social event can use the source in the cloud and disavowed customers can't get to the cloud again after they are denied. Third, we can secure the arrangement from interest strike, which infers that denied customers can't get the main information record paying little mind to the likelihood that they conspire with the untrusted cloud. In our strategy, by using polynomial limit, we can fulfill a secured customer denial arrange. Finally, our arrangement can fulfill fine capability, which suggests past customers require not to redesign their private keys for the situation either another customer participates in the social affair or a customer is denied from the get-together

Keywords
Cloud Computing, Access Control, Data Private Cloud, Security, Secure Data Transmission

I. Introduction

In cloud computing, cloud organization providers offer a pondering of boundless storage space for clients to host information [4]. Cloud processing, with the traits of trademark information sharing and low support, gives a predominant utilization of benefits. It can help clients lessen their cash related overhead of information organizations by moving the area organizations system into cloud servers. As cloud processing gets to be predominant, more delicate information By putting away their information into the cloud, the information proprietors can be eased from the weight of information stockpiling and support, in order to appreciate the on-request great information stockpiling administration cloud server are not in the same trusted area may put the outsourced information at hazard. In this work, a protected information sharing plan, which can accomplish secure key circulation and information sharing for a dynamic gathering in the cloud. The principle commitments of this plan include:

- A path for key dissemination with no safe correspondence channels. The clients secure can safely acquire their private keys from gathering supervisor with no Certificate Authorities because of the check for the general population key of the client.
- This plan can accomplish fine-grained get to control. With the assistance of the gathering client list, any client in the gathering can utilize the source in the cloud and renounced clients can't get to the cloud once more.
- A safe information sharing plan can be shielded from conspiracy assault. The renounced clients can't have the capacity to get unique information documents once they are denied regardless of the possibility that they plot with the untrusted cloud. This plan can accomplish secure client renouncement with the assistance of polynomial capacity.

II. Related Work

Cloud stockpiling a huge administration of cloud registering which gives to its clients a simple, financially savvy and solid approach to deal with the information. It likewise empowers the clients to impart the information to each other by filling in as a gathering. Since shared information can be gotten to and adjusted by different clients and the gathering participation can be changed much of the time, it confronts the test of keeping up the honesty of shared information. A few plans are proposed to guarantee the trustworthiness of the common information. G. Ateniese et al. [3] proposed a model for Provable Data Possession conspire which permits a customer that has put away information at an untrusted server to check that the server has the first information without recovering it. The model creates the evidences of ownership by examining arbitrary arrangements of squares from the server. The customer keeps up the confirmation metadata to check the verification. H. Shacham [4] et al. gives a provably secure confirmation of hopelessness framework. This framework permits conservative verifications with one authenticator esteem. It gives two arrangements; initial one is secretly undeniable and based on pseudorandom capacities; second permits open irrefutable confirmations and in view of the mark plot. B. Wang et al. [6] proposed a novel open reviewing instrument for the respectability of imparted information to effective client disavowal in the cloud. This framework uses the idea of intermediary re-signature, once a client in the gathering is denied; the cloud can leave the squares, which were marked by the repudiated client with leaving key. This technique accept single proprietor information as opposed to multi-proprietor information. T. Jiang et al. [7] made sense of the agreement assault in the current plan and gave a productive open examining plan with secure gathering client disavowal in view of vector duty and verifier-neighborhood renouncement amass signature. This plan considers single proprietor information than a multi-proprietor information. B. Wang et al. [10] proposed a novel open confirmation to review the uprightness of multi-proprietor information in an untrusted cloud by exploiting multi-marks. It proposes a novel multi-signature conspire with blockless unquestionable status and after that uses as a building square to develop the general population check instrument on the uprightness of multi-proprietor information in the cloud. X. Liu et al. [2] exhibited a protected multi-proprietor information sharing plan named Mona. It accomplishes fine grained get to control and

renounced clients won't have the capacity to get to the sharing information again once they are denied. Notwithstanding, the plan will effectively experience the ill effects of conspiracy assault by the renounced client and cloud.

III. End User Security Issues

End Users need to access resources within the cloud and may bear in mind of access agreements like acceptable use or conflict of interest. The client organization have some mechanism to find vulnerable code or protocols at entry points like servers, firewalls, or mobile devices and upload patches on the native systems as soon as they are found. The cloud should secure from any user with malicious intent that will conceive to gain access to information or pack up a service.

A. Security-as-a- Service

In Cloud environment the security provided by customers using cloud services and the Cloud Service Providers (CSPs). Security-as- a-service is a security provided as cloud services and it can provided in two methods: In first method anyone can changing their delivery methods to include cloud services comprises established information security vendors. The second method Cloud Service Providers are providing security only as a cloud service with information security companies. Almost all the security companies, anti-malware vendors involved in the delivery of SaaS with regard to email filtering and so on.

B. Browser Security

In a Cloud environment, remote servers are used for computation. The client nodes are used for input/output operations only, and for authorization and authentication of information to the Cloud. A standard Web browser is platform in-dependent client software useful for all users throughout the world. This can be categorized into different types: Software-as-a-Service (SaaS), Web applications, or Web 2.0. TLS is used for data encryption and host authentication The Legacy Same Origin Policy is the insertion of scripting languages into Web pages for access rights for scripts. In is to allow access read or write operations the same origin on content, to disallow but from the different origin any access on content. Origin means a "the same application", it can be defined with domain name, protocol, port in a web. But some problems with the SOP, but it could be solved with "origin" definition. In the case of WWW it's not working properly. Security requirements for to protect both data during transport, and to authenticate the server's domain name in Web applications is TLS. Attacks on Browser-based Cloud Authentication are one of the security problem with browser-based protocols in Cloud Computing and it is not capable to generate cryptographically valid XML tokens. So, it can possible with a trusted third party. Login is not possible at a server due to the fewer credentials in browser, So HTTP forward it to the Passport login server. After entering username and password from user, then the Passport server convert this authentication into a Kerberos token, it can redirected to the requesting server from other HTTP redirect. Kerberos tokens are not clear to the browser is the security problem with Passport, and it protected by the SOP. But any attacker can access those tokens then he accesses all services of the victim. Secure Browser-based Authentication is the situation is not suggested, but we can perform for better results by combined SOP and TLS for secure FIM protocols. In Cloud Computing by using TLS Browser Enhancements are very limited in an authentication center. It is not possible for XML Signature, the browser can be added many Web Service functionalities by simply loading an appropriate JavaScript library during runtime. So, the browser security API can be adding the enhancements XML Encryption and XML Signature.

C. Authentication

In the cloud environment, the primary basis for access control is user authentication and access control are more important than ever since the cloud and all of its data are accessible to all over the Internet. Trusted Platform Module (TPM) is a widely available and stronger authentication than username and passwords. Trusted Computing Groups (TCG's) is IF -MAP standard about authorized users and other security issue in real-time communication between the cloud provider and the customer. When a user is reassigned or fired, the customer's uniqueness management system can report the cloud provider in real-time so that the user's cloud access can be revoked or modified within seconds. In cloud any fired user is logged, they can be immediately disconnected. Trusted Computing enables authentication of client nodes and other devices for improving the security in cloud computing. The frequently targeted attack is authentication in hosted and virtual services. The secure mechanisms are used to the authentication process for frequent target of attackers by different ways to authenticate users based on different information know by the user.

IV. Design Objectives of Authorized Method

The main design objectives of the schema include:

- A safe key dispersion with no secure communication channel. The user gets the private key from Certificate authorities with the public key.
- The group users can provide fine-grained access control of the group manager.
- The group user can revoke from the dynamic groups safely with the influence of the polynomial function.
- The number of the user revoked is independent of the existing user in dynamic groups getting the private key.

A. Scheme Representation

The System model consists of the Group Manager, Group user, and the Cloud [6]. The Group member or group users can divide as creator, reader and writer. The system setup is as follows

Step 1: Set up the Cloud Server
Step 2: Confirm the Group Manager
Step 3: Select Group Member with privileges
Step 4: Group Member Registration
Step 5: Key Distribution for Group Member & Group Manager
Step 6: Data Read/Write/Create
Step 7: Revocation procedures

The work flow of the system model is

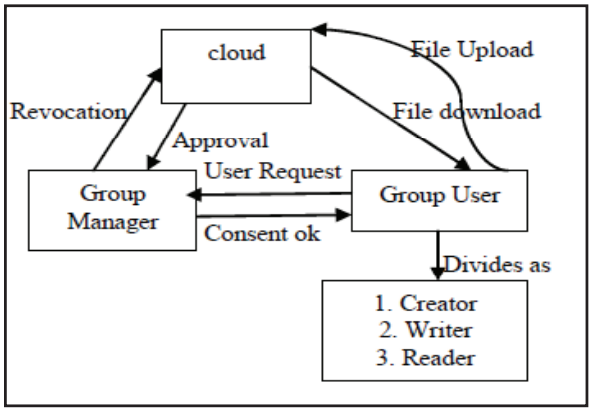

Fig. 1:

B. Methodology

Preliminaries:

[1] Bilinear Maps: Let G1 and G2 be additive cyclic groups of the same prime order q. Let e: G1 x G2 →G2 denote a bilinear map constructed with the following properties:

1. Bilinear: ∀ a, b ∈ Z*q and P,Q ∈G1, e(aP,bQ) = e(P,Q)ah
• 2. Non generate: There exists a point Q such that e(Q.Q)≠ 1.
• 3. Computable: There is an efficient algorithm to compute e(P,Q) for any P,Q ∈ G1.

C. Asymmetric Encryption Algorithm

Step 1: Select two Prime Numbers P and Q
Step 2: Compute N=p*q Compute φ(N)=(p-1)*(q-1)
Step 3: Choose e such that 1<e<φ(N) and e and N are Co prime
Step 4: Computer a value for d such that (d *e) % φ(N)=1
Step 5: Public key is (e, N) Private Key is (d, N)
The asymmetric Encryption techniques enable the group manager to dynamically increase fresh user and at the same time reserves the earlier calculated information. So, newly joined users can straightly decrypt data files withoutcontacting with the owners. So that there will be no need to change user decryption keys.

D. System Entities Work

1. User Registration For user registration of user member has an ID. The group manager adds the user ID into the group user list, which will be used in tracking. After registration, user obtains a private key, with will be used for group signature and file decryption. While during registration itself, the user differentiates themselves as a creator or a writer or a reader.

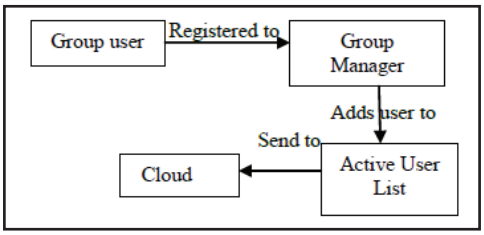

Fig. 2:

2. Upload Files the File upload is done only by the group Manager or an admin.
3. Files Update Moreover, the creator and writer only can do editing of the data with the consent of the group manager. The reader can only use the data content with authorization.
4. File Deletion The file or data stored in the cloud are deleted by either the group manager or the member who uploaded the file into the server.
5. Revoke user from the group User revocation is performed by group manager by executing a polynomial function done by group manager alone. Once the user is revoked from the group, then the group member r cannot be able access the cloud resources and its data.

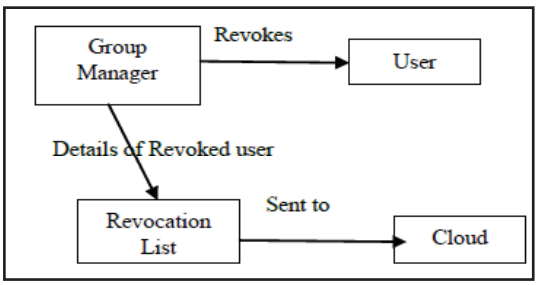

Fig. 3:

V. Proposed System

The group manager will maintain the revocation list of the members. If any of the member leave the group then the member detail is added to that list and the user will not be able to further login to that group. When the new member is added to the group then group key is provided to the member. To remove identity privacy problem, the group manager will have the list of the uploaded files along with the memberID from which the file is uploaded. By this privacy is kept secure and no one will misuse as it is traceable by the group manager. And as it is multi-owner then any member can not only read data but also modify their own data along with the group manager. The files which are uploaded present in encrypted form, and the files can be viewed by group member as they have the group key on which he or she belongs.

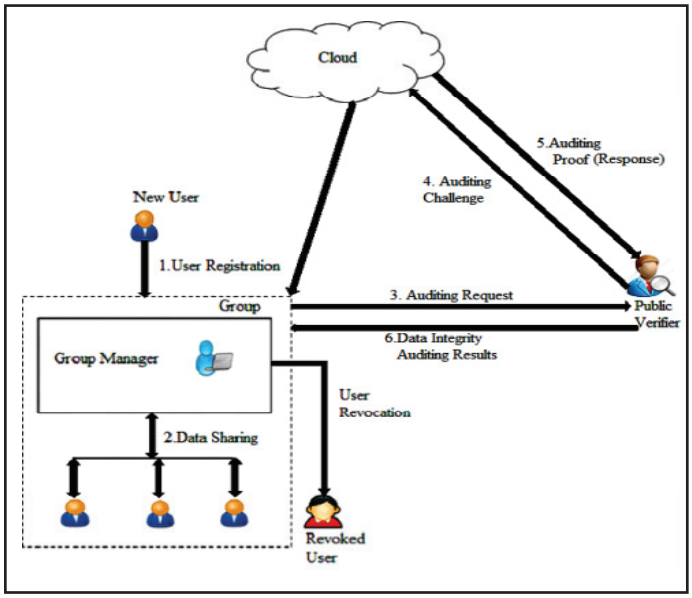

Fig. 4: Proposed system Architecture

A. AES Encryption

The input 16 byte Plain text can be converted into 4×4 square matrix.
The AES Encryption consists of four different stages they are
Substitute Bytes: Uses an S-box to perform a byte-by-byte substitution of the block
Shift Rows: A Simple Permutation
Mix Columns: A substitution that makes use of arithmetic overGF(9)
Add Round Key: A Simple Bitwise XOR of the current block with the portion of the expanded key

B. AES Decryption

The Decryption algorithm makes use of the key in the reverse order. However, the decryption algorithm is not identical to the encryption algorithm

VI. Conclusion

In this paper, we investigated the problem of data security in cloud data storage and data transmission, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, we proposed an effective and flexible distributed scheme. Our scheme achieves the integration of storage correctness insurance and data error localization. Through detailed security and performance analysis, we show that our scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks. We believe

that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. Adding secure cloud storage using the proposed cryptographic solution and with a searchable encryption technique for the files to be accessed, it will work as a better approach to the user to ensure security of data. The cloud security using cryptography is already in use for secure data storage which can be enhanced for secure data transmission and storage. An interesting question in this model is if we can construct a scheme to achieve both public verifiability and storage correctness assurance of dynamic data.

References

[1] Zhongma Zhu, Rui Jiang,"A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", 10.1109/TPDS.2015.2388446, IEEE Transactions on Parallel and Distributed Systems

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. 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] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] Shucheng Yu, Cong Wang, Kui Ren, Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[5] R. Lu, X. Lin, X. Liang, 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.

[6] Xuefeng Liu, Yuqing Zhang, Boyang Wang, Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 6, pp. 1182-1191, June 2013.

[7] D. Boneh, X. Boyen, E. Goh,"Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[8] Lan Zhou, Vijay Varadharajan, Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," IEEE Transactions on Information Forensics and Security, Vol. 8, No. 12, pp. 1947-1960, December 2013.

[9] M. Nabeel, N. Shang, E. Bertino,"Privacy preserving policy based content".

[10] Boyang Wang, Hui Li, Xuefeng Liu, Fenghua Li, Xiaoqing Li,"Efficient Public Verification on the Integrity of Multi-Owner Data in the Cloud", IEEE Jour. of Comm. and Netw., Vol. 16, No. 6, Dec 2014

Laxmi Regadi Holds a B.Tech certificate in Computer Science & Engineering from Sana Engineering College Affiliated to the JNTU HYDERABAD .She presently Pursuing M.Tech (CSE) department of computer science engineering from Sri Vaishnavi college of engineering at srikakulam Affiliated to JNTU KAKINADA.

S. Seshagiri, M.TECH (CS) Assistant Professor in CSE department Sri Vaishnavi College of Engineering, Srikakulam, AP, India.

He believes in the wordings of Swami Vivekananda:
You have to grow from the inside out. None can teach you, none can make you spiritual. There is no other teacher but your own soul.