RESEARCHERID
THOMSON REUTERS

[Khalid, 4(9): September 2017]
DOI- 10.5281/zenodo.928915

ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A STUDY ON SECURE CLOUD DATA SHARING SCHEMA USING DYNAMIC TECHNIQUES

Syeda Tahira Khalid[*1] & Dr. G. Sambasiva Rao[2]

[*1]Dept. Of Computer Science Engineering, Nawab Shah Alam Khan College of Engg & Tech, New Malakpet, Hyderabad,Telangana

[2]Professor & HOD, Dept of CSE, Nawab Shah Alam Khan College of Engg & Tech, New Malakpet,Hyderabad,Telangana

ABSTRACT

Information sharing among clients of a cloud is greatly benefited due to cloud computing, low support and small cost of administration. Although security certification is required for sharing the out sourced information documents. Due to the continuous change in participation, sharing of information with protection safeguarding is difficult particularly for an untrusted cloud. Under the existing arrangements, the safe keeping of key transmission is totally done with the help of communication channel. In this project work weare proposing a safe and trustworthy information sharing plan for dynamic clients. We plan a path which is safe for the distribution of the keys without using a single communication channel, the group manager hands over the keys safely to the clients. The aim of our schema is to get control over fine-grained access, that means any of the users can use the cloud and the revoked users cannot use it after getting revoked. We can also safeguard the schema from collusion attack that means the users which are revoked cannot use the cloud once after getting revoked even if they indulge in conspiring with the untrusted cloud. In our approach we can accomplish a safe client repudiation plot by utilizing polynomial capacity. Our plan can fulfill fine adequacy, a fully protected revocation schema for the user can be attained. At last, this schema attain proficiency that means there is no need to update the old keys in the case when either a new user joins or an old user revokes.

Keywords*:* Fine-grained access, privacy-preserving, key transmission, clients of a cloud

I. INTRODUCTION

What is cloud computing

The application of figuring out the assets like programming and also equipment which can be conveyed over a system i.e. internet is called Cloud Computing. The origin of the name is taken from the usage of a regular cloud-formed image for the intricate structure it contains in structural graphs. It commends services which are remote for the software, computation and data of the user. The Cloud computing also have resources (both software and hardware) which are made available and managed by the third-party service area. The access to these highly advanced and innovative software applications and networks of server systems (that are high-end) is provided by these services generally.

II. HOW CLOUD COMPUTING WORKS

The main aim of the cloud computing is to provide customary ultimate form of computing or highly efficient computing capacity which is generally used by scientific researchers or military, to do tens of billions of computations and processing per second, in massive computer games, consumer-based applications like financial groups, to personalize the information, to provide storage of data. The networks of huge clusters of servers that normally have less rate PC technology of the consumer with particular networks for spreading data handling tasks

across them. This public IT substructure comprises of a number of pools of computers that are connected to one another. Virtualization methods are mostly used to increase the computation power of the cloud.

The process of converting user oriented explanation of the input into a workstation is called Input Design. The most important thing in this is design and it used to avoid unnecessary mistakes and errors in this process and to guide the management for extracting right knowledge from the workstation.

Vast capacity of data is handled by generating user friendly screens for the entry data. Its objective is to make entry of data very easy and free from inaccuracies. Manipulations of data is made easy due to the design of data entry screen. It does offers record viewing conveniences.

Validity of data is checked upon its entry. By taking the advantage of the screens the data can be easily entered. To avoid the maize of a moment, apt messages are given. Hence, the goal of input design is to build an input layout that is very easy to keep track.

III. PRIVACY-PRESERVING PUBLIC AUDITING FOR DATA STORAGE SECURITY IN CLOUD COMPUTING

Cloud Computing is the envisaged revelation of computing as a utility, where the users can store their data tenuously into the cloud in order to enjoy the on-demand applications of extraordinary quality and services from a common pool of computing resources which are configurable. The users can be free from the liability of storage of data locally and its maintenance by the use of data outsourcing. On the other hand, the point that the users don't have physical possession of the huge amount of data makes the protection of data integrity in Cloud Computing a very perplexing and theoretically intimidating job, exclusively for the users with unnatural computing resources and competencies. Hence, enabling the public auditability for the data storage in the cloud, security is of serious prominence so that the consumers can be able to choose an external audit party to verify the integrity of the subcontracted information whenever required. For the secure introduction of an efficient third party auditor (TPA), the following two necessary necessities are to be fulfilled. The TPA should not introduce an extra online overhead to the user of the cloud and should be capable of proficiently auditing the data storage of the cloud without keeping a local copy of the data The third party auditing process should not fetch new liabilities towards the privacy of user data. In this project work, we make use of and distinctively associate the public key centered homomorphic authenticator with unsystematic screening to accomplish the privacy-preserving public cloud data auditing system that can meet all the above mentioned necessities. To back the effectual management of several auditing jobs, we moreover discover the practice of bilinear aggregate signature to outspread our focal outcome into a multi-user setting, where TPA can be able to implement multiple auditing responsibilities at the same time. Extensive security and performance analysis displays the schemes that are proposed are provably secure and exceedingly competent.

IV. PROPOSED SYSTEM

In this project work, we are proposing a secure schema for data sharing, thatwhich aims at the achieving of secure data sharing and secure key distribution for the dynamic group.

Here we try to provide a way for secure key distribution with not using any of the secure communication channels. The group managers provide the private keys to the users without using any Certificate Authorities because of the public key verification of the given user. This schema can accomplish fine-grained access control, by taking the help of the group user list, the resource in the cloud can be used by any user in the group and revoked users are not allowed to access the cloud again after getting revoked.In this project work we aim at proposing a data sharing schema that is secured and which can be safeguarded against the collusion attack. The revoked users cannot get access to the original data files after getting revoked even if they try to conspire with the untrusted cloud. Our schema aims at achieving secure user revocation by using the polynomial function. Our schema is capable to give support to the dynamic groups very efficiently, on the entry of a new user or revocation of a user from the group, the

private keys of the other users of the group need not to be updated and recomputed. In order to prove the security of our schema we provide security analysis.

Data Flow Diagram Use Case Diagram

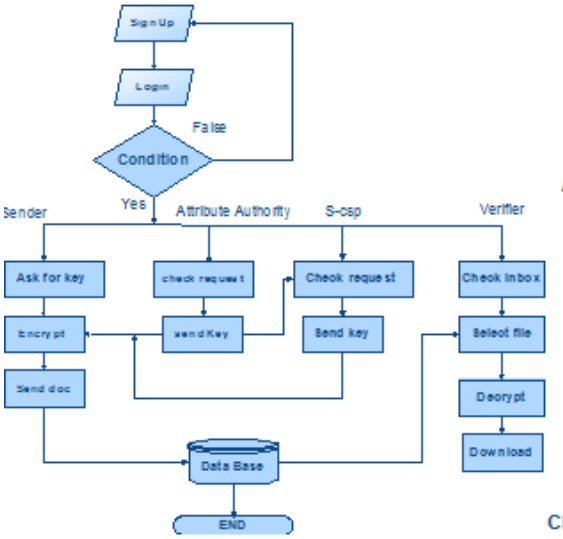

Fig 1: Data Flow Diagram

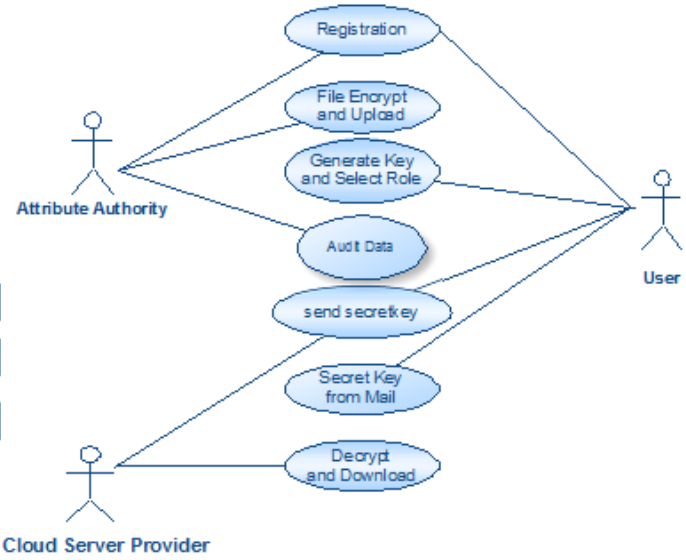

Fig 2: Use Case Diagram

V. INPUT DESIGN

The linkage between the two, i.e. user and information system is the input design. It encompasses the procedures and developing specification for data ground work and to set transaction data in to a serviceable form for process handling those steps are obligatory and these steps can be reached by scrutinizing the workstation to read data from a printed document or written or it can occur easily by having people keyboarding the data straight into the workstation. The main focus of the design of input is on eluding delay controlling the inaccuracies, monitoring the amount of input required, avoiding unnecessary steps and keeping the process without confusion. The design of the input is done in such a way that it gives comfort in usage along with preserving the privacy and it also provides security. The Input Design measures these items. What should be the data that is given as input. What should be the arrangement of data and how the Coding of data should be done. What should be the dialog to give directions to the operating personnel in the given input. Input Validation Preparation Methods and the steps need to be taken when an error occurs.

VI. OUTPUT DESIGN

To portray the information without doubts and to meet all the needs of the end user the output design is used. The outcomes of process handling in computer systems are transferred to the users and to different computer systems via outputs. It is to be determined that how the information is to be evacuated for instantaneous want and the hard copy output also in the output design. It is the right source of information to the end user. The computer system's link can be improved for making better user decisions by the output design. The design of the system's output should be well organized and well thought; Designing computer output should proceed in an organized, well thought out manner; the accurate output should be developed along with making sure that each of the output elements are well designed so that the people can make use of the system efficiently and without any difficulty. When the analysis of design computer output is done, the precised output should be recognized to meet all the necessities. Methods for portraying the information should be chosen.Generate a document, give a report, or some other different formats that enclose information formed by the computer system.The arrangement of output of the information system should at

least undertake one or more aims of the following. Past activities information, projections of the future and current status information is conveyed. Signaling of the important events, prospects, complications, or cautions. Action should be triggered. Confirmation of an action.

Unit Testing
It checks whether the schema of test cases that which is needed to corroborate the program logic which is internal for the proper operation and to see that the inputs of the program yield acceptable or desirable outputs. Validation of internal code flow and decision branches is to be endorsed. Each discrete units of software of the application needs testing and it is performed only after each distinct unit completes its execution before integration. The structural testing is intrusive and solely depends upon the information of production. Whereas, Unit tests do simple and plain tests at the component-level and also helps in testing a precised application, system configuration and a financial plan or procedure. It ensures that commercial procedure paths which are on of a kind works correctly according to the given requirements and it has rightly described inputs and desirable outputs.

Integration Testing
The purpose of Integration tests is to design and devise a test to determine whether the components of software that are integrated execute as one program or not. It is more worried about the result of fields or screens and is also event-driven. Even after the unit testing shows that the components are satisfied individually, the integration testing proves that the component combination is valid and reliable. Integration testing reveals the problems and aims specially at this.

Functional Test
The functions tested by Functional tests gives us logical explanation of how the functions tested are provided as prescribed by the technical and financial requisite, user manuals and the documentation of the system. Requirements, special or unique test cases, key functions etc. is the main focus of the preparation and the organization of the functional testing. The additional tests are found out and the truthfulassessment of the recent tests is also found out and all these things are done just before the Functional testing gets completed.

System Test
It goals at meeting the wants of the software that is integrated of the system. It also tests a configuration to confirm acknowledged and expectable outputs. The configuration oriented system integration test can be taken as an example of it. The basis of System testing is emphasized pre-driven links of processes, integration points and flows and descriptions.

White Box Testing
It is a kind of testing that involves the criteria that the person which is testing the given software has an inside understanding or information of the configuration, processes, working and the language of the given software, or at minimum its goal. White Box Testing aims at testing the regions that fails to be reached at the black box level.

Black Box Testing
It is a kind of testing in which the given software is tested with not having any prior inside information or statistics of the structure, the workings, or the language of the section that which is under the test. It is just identical toany of the other test but this ought to be transcribed from the source of the tentative document, like requirement or description document. This is a type of testing that in which the given software that is being tested is considered as a black box because it doesn't allow you to "see" into the system. This test gives inputs and then returns outputs without taking the given software into consideration.

Acceptance Testing
It is a very important segment of a given project work and it needs a substantial membership by the user at the end. It also certifies that the given computer system encounters all the needed practical necessities.

ISSN 2348 – 8034
Impact Factor- 4.022

VII. CONCLUSION

The primitive of certifiable database with proficient updates is a significant means to give a solution to the problem of certifiable subcontracting of storage. We plan a schema to comprehend secure and competent data integrity auditing to share the vigorous data with multiple user variation. The Asymmetric Group Key Agreement (AGKA), scheme vector commitment and group signs with revocation of user are adopted to attain the integrity of data auditing of the currently used data which is remote. Alongside the data auditing done publicly, the merging of the primordial which are three allow our schema to subcontract database of cipher text to the cloud which is remote and to provision revocation of group users securely to the already shared vigorous data. In this schema we like to offer analysis of security, and that this demonstrates that this schema offer confidentiality of data for the users of the group, and also it is safeguarded against the attack called collusion attack of the storage server of the cloud and users which are revoked. And also the analysis of performance demonstrates, equated with all its appropriate schemas, this schema is found to be real effective in various segments

REFERENCES

1. *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," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.*
2. *S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Int.Conf.FinancialCryptographyDataSecurity,Jan.2010,pp.136–149.*
3. *M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.*
4. *E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.*
5. *G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 29–43.*
6. *S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.*
7. *V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.*
8. *R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.*
   Fig. 10. Comparison on computation cost of the cloud for file download among RBAC, Mona and our scheme.
   ZHU AND JIANG: A SECURE ANTI-COLLUSION DATA SHARING SCHEME FOR DYNAMIC GROUPS IN THE CLOUD 49
9. *B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.*
10. *X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.*
11. *D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 440–456.*
12. *C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size Ci-phertexts or decryption keys," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 39–59.*
13. *Z. Zhu, Z. Jiang, and R. Jiang, "The attack on mona: Secure multiowner data sharing for dynamic groups in the cloud," in Proc. Int. Conf. Inf. Sci. Cloud Comput., Dec. 7, 2013, pp. 185–189.*
14. *L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.*
15. *X. Zou, Y.-S. Dai, and E. Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," in Proc. IEEE Conf. Comput. Commun., 2008, pp. 1211–1219.*