GE-International Journal of Engineering Research
Vol. 4, Issue 4, April 2016 IF- 4.721 ISSN: (2321-1717)
© Associated Asia Research Foundation (AARF) Publication
Website: www.aarf.asia Email : editor@aarf.asia , editoraarf@gmail.com

PRIVACY-PRESERVING AUTHENTICATION PROTOCOL IN SHARED AUTHORITY BASED CLOUD COMPUTING USING TRUSTED THIRD PARTY

Mr.Tamboli Sameer Iqbal[1], Prof. Amrit Priyadarshi[2]

[1] Dattakala Group of Institutions Faculty of Engineering Swami-Chincholi, Daund, Pune-413 133

[2] Dattakala Group of Institutions Faculty of Engineering Swami-Chincholi, Daund, Pune-413 133

ABSTRACT

Cloud computing is developing as a prevalent data intelligent worldview to comprehend users' information remotely set inside an on-line cloud machine. Cloud arrangements give awesome comforts expected to the users to savor the experience of the on interest cloud applications without considering the local infrastructure restrictions. Through the data accessing, different users may be in a collaborative relationship, and therefore information sharing becomes significant to achieve productive benefits. The existing protection alternatives mostly give interest to the authentication to appreciate that an customer's private data cannot be not authorized accessed, but disregard a subtle privacy concern during an user challenging the cloud server to request other users intended for information sharing. The challenged gain access to demand itself may uncover the user's privacy no matter whether or certainly not it could obtain the details access permissions. Found in this paper, we offer a shared authority based privacy-preserving authentication protocol to address above privacy issue for cloud storage. In the, 1) shared access authority is achieved by private access request complementing mechanism with security and personal privacy considerations (e. g., authentication, data anonymity, user level of privacy, and forward security); 2) attribute based gain get to control is followed to recognize that the customer can only access the own data fields; 3) proxy re-encryption is definitely utilized by the cloud storage space to provide data sharing between multiple users.. For the same time, general

comparability style is set up to show that the theoretically has the design correctness. What this means is usually that the suggested process knowing privacy-preserving data access authority sharing, is usually attractive for multi-user collaborative cloud applications.

KEYWORDS - CLOUD COMPUTING, PRIVACY PRESERVATION, SHARED AUTHORITY, AES ALGORITHM.

INTRODUCTION

Cloud service provider give magnificent points of interest to the users to appreciate from the on-demand Cloud applications without considering the local infrastructure restrictions. Amid the information getting to, different users might be in a collaborative relationship, and information presenting gets to be critical on accomplish productive advantages [1]. Thus the existing security solutions mainly concentrate on the authentication to know that a users private data are unable to be unauthorized accessed, but neglect a subtle privacy issue throughout a users challenging the cloud machine to request others for data sharing. The pushed access demand itself may expose the user's level of privacy no matter whether or not it can obtain the data access permissions. Different plans utilizing characteristic set up encryption have been proposed for access control of outsourced data in cloud computing [2]. It allows clients with limited computational solutions to outsource their large computation workloads to the cloud, and enjoy the massive computational electricity financially, bandwidth, storage, and also appropriate software that may be shared in a pay-per-use manner. Despite the tremendous benefits, security is the main obstacle that helps prevent the wide adoption of this promising computing model, especially for consumers when their confidential info are developed and consumed during the computation. To combat against unauthorized information access, sensitive data must be encrypted before outsourcing techniques to be able to provide end to- end data confidentiality assurance in the cloud and beyond. However, ordinary information encryption techniques essentially prevent cloud from undertaking any meaningful procedure of the underlying cipher text-insurance policy, producing the computation over encrypted data a very hard difficulty. The proposed scheme not merely achieves scalability because of its hierarchical structure. As a result, there do are present different motivations for cloud server to respond unfaithfully also to return inappropriate outcomes, i. e., they might behave beyond the time-honored semi honest model.

RELATED WORK

In this section, we analyze the related works, Companies are speedily moving onto cloud since they can at this moment utilize the finest capitals accessible available in the market in the blink of a great attention and in addition decrease their very own operations' cost

radically. Nevertheless as more and extra data is relocated to the cloud the security concerns have keeping on developing. Information breaking is the greatest security issue. A skilled programmer might effectively enter a customer part application and get into the customer's close information [2]. Clumsy and defective APIs and interfaces turn into the objective. IT organizations which give cloud provider allow third get together companies to alter the APIs and familiarize their own personal functionality which often allows these companies to know the internal workings of the cloud [2]. Denial of Service (DoS) is additionally danger in which the client is acknowledged incomplete or not in each entrance to their own special information. Organizations now utilize disable always says all times and DoS might effectively primary enormous increase in cost both for the shopper and administration supplier. Interconnection snooping is that in which a hacker can look at your online activities and duplicate/replay a specific private data. It may also cause the user to unlawful or unwanted sites. Loss of data is also another issue. A destructive hacker can get eliminate of the information or any type of natural/manmade catastrophe can ruin your data. In such instances having an high street copy is a major benefit. Carelessness of the business can also cause data loss [3]. Suitability between different cloud providers is additionally a worry. On the off chance that a client moves starting with one cloud then onto the next the similarity ensures that there is absolutely no loss of data. Foreign can be utilized intended for wrong purposes i. at the. cloud abuse. Because of the of latest innovations on the foreign it works extremely well for top of the line estimations which should not be possible on a standard computer[2],[3]. Insufficient comprehension of impede innovations can prompt obscure degrees of danger. Organizations move to cloud since it gives generous bringing down of expense however in the event that reinforcement is performed without appropriate background taking in; the issues that happen can be even greater. Internal gatecrashers can utilize the information for harming purposes. Safe-keeping of encryption keys is also an issue. Regardless of the fact that you are working with encryption for increased insurance, keeping a key a secure point of interest turns into a worry. Whom ought to be the Data Owner of the key? Client seems to complete up being the answer however how tenacious and careful can surely he/she be will settle on a choice the security in the data. Suitability between different cloud providers is likewise a worry. On the off chance that a client moves starting with one cloud then onto the next the similarity ensures that there is unquestionably no loss of data. Cloud can be utilized planned for wrong purposes. at the. Cloud misuse. Because of the accessibility of latest advancements on the remote access it works extremely well for top of the line figuring's which is impossible on a standard computer [2],[3]. Insufficient

understanding of cloud technologies can bring about unknown degrees of risk. Cloud computing offers a new scheme to supplement the current usage. The users might not know the machines which process and distribute their data. During their very own convenience brought by this new technology, users are anxious about losing control of their own data. The data processed on

Confuses are often utilized, leading to several issues related to accountability, including the handling of information. Such drawbacks are becoming a hurdle to the large adoption of cloud service. Cloud computing allows highly scalable services to become easily consumed on the internet about an as-needed basis. A significant characteristic of the cloud services is that users' data are often processed slightly in unknown machines that users do not own or perhaps operate. A drawback the existing system does not have the choice of granting/revoking data gain access to. It has very much less security where hacking takes on a fantastic role.

Liu et al. [12], proposed a multi-Data Owner information sharing defended plan for variable gatherings in the weaken applications. It means to realize that a client can securely share the information with different users by means of the untreated foreign server, and can productively bolster dynamic gathering associations. Inside the plan, another allowed shopper can basically directly decoded information records without per-reaching with data owners, and client reversal, toppling; invalidation is accomplished by a reversal, upsetting, dissolution list without modernizing the secret keys of the remaining users. Access control is connected to verify that any client in an association can namelessly use the cloud resources, in addition to the information proprietors' real individual can without much of a stretch be uncovered by gathering chief for contention intervention. It shows the capacity overhead and security calculation expense is really autonomous with the amount of teasers.

Grzonkowski ou al. [13] recommended a zero-learning proof based authentication structure for sharing cloud arrangements. Contingent upon the amiable home frameworks, a shopper driven methodology is put on permit the sharing of customized substance and propelled system based provider through TCP/IP infrastructures, in which a respected option gathering is acquainted with get decentralized communications.

Nabeel ou al.[14] proposed a broadcast group key management to boost the weakness of symmetrical key cryptosystem in open public clouds, plus the broadcast group key management realizes that an user want not use open public crucial cryptography, and can

effectively derive the symmetric keys during decryption. Appropriately, attribute based access control mechanism is built to achieve that a great user can decrypt the contents if and just if its identity characteristics fulfil this content provider's policies. The fine-grained algorithm applies access control vector for determining 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 broadcast group key management has an evident advantage during adding/revoking users and updating access control plans.

Wang et 's. [15] proposed a distributed storage integrity auditing mechanism, which features the homomorphic token and allocated erasure-coded data to improve secure and trusted safe-keeping services in impair computing. The scheme allows users to audit the cloud storage with light communication overloads and calculation cost, and the auditing effect ensures strong cloud safe-keeping correctness and fast data error localization. Toward the dynamic cloud data, the scheme helps active outsourced data operations. It indicates that the structure is resilient against failure, malicious data changes attack, and server colluding attacks

PROBLEM STATEMENT AND IMPLEMENTATION

We propose a structure for security issue to recommend protection preserving authentication convention for the cloud information stockpiling, based about cloud storage which gives authentication and approval without surrendering a client's private data. The primary thought will be as comes after: 1) another protection issue in cloud safe-keeping is to be situated and additionally distinguish an indirect individual level of security for information sharing, when the tested request itself can't get the wearer's close to home security 2) Design an authentication convention which upgrades a great client's entrance request, which more often than not is connected to the security. The shared access power is accomplished by unidentified access request planning system. 3) Cipher content arrangement is used and a client can just get to their own special information areas and proxy re-encryption is acknowledged to give confirmed data sharing among different users [10]. In the proposed and examined stage, through record encryption getting of documents is expert. The document present about the gadget will get to be encoded utilizing pass word structured Advance encryption standard calculation. For all intents and purposes any of the transferred archives which as a rule are secured can complete up being downloaded by client and read it on the framework. Advance encryption standard (AES) is unquestionably not responsible to be impacted by some other strike however Brute Force ambush. Advance encryption standard is

a great deal more rapidly than the Rivest-Shamir-Adleman algorithm (RSA). Along these lines, it settles on a considerable decision for security of data on the cloud [11]. It is to be noticed that the proposed framework works just if a steady web association is generally accessible. Here, the specific framework and information proprietor can choose whether or maybe not the client might

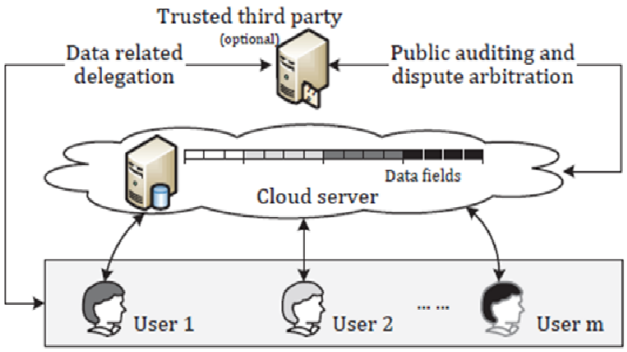

FIGURE 1: SYSTEM MODEL

get to the framework. The effectiveness check must be taking after the usage of the given recommended model. After the response timings has recently been measured then genuine computations will bolster the very truth that this sort of work has a huge quality. Utilization of the Reliable Third Party shows up the testing part and the absolute best segment. In the event that it manages all the call from the client to get to information from cloud to begin with, it ought to: 1) Validate and an individual user2) Guarantee the information for which the user is asking, approved to that specific user. 3) If not by any stretch of the imagination it ought to return the inadmissible access report to user. As it were as opposed to calling the cloud provider or maybe strategies there should be a middle person observing each of the authentication and assent. Every one of us propose a system for the aforementioned level of protection issue to recommend security preserving authentication convention for the cloud information stockpiling, based about cloud storage which gives authentication and approval without surrendering a user's private data.

IMPLEMENTATION

In this segment, the execution subtle elements of the proposed framework including different modules are talked about

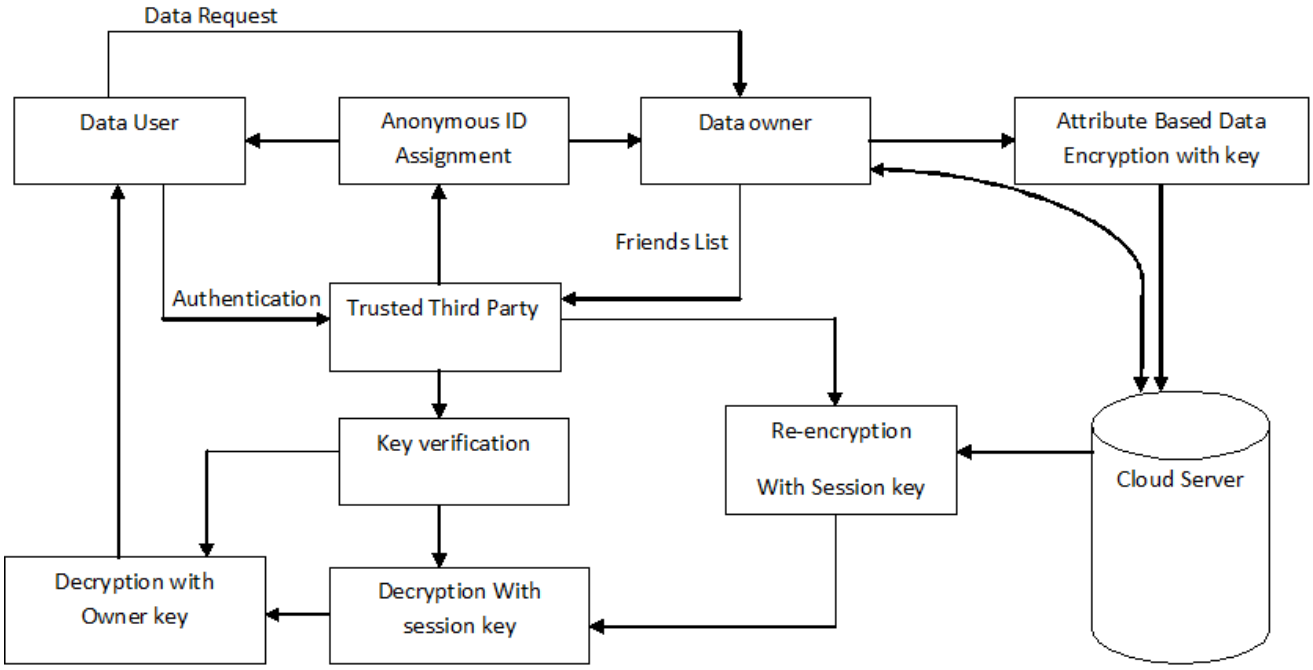

FIGURE 2: SYSTEM ARCHITECTURE

MODULE DESCRIPTION

- Data Owner Registration:

A Data Owner needs to transfer its documents in a cloud server, and afterward client ought to register first. After that just the client will have the capacity to do it. At that point Registration technique is then taken after. These Details are stored in a database.

- Data Owner Login:

This indicates among the registered individual need to login, they ought to have the capacity to login by specifying their email id, secret key.

- Client/User Registration:

In the event that a client needs to get to the information from cloud, the registration is an obligatory stride to be taken after and information is overhauled in Database.

- User Login:

An approved client can download the record by utilizing document id which the Data Owner has indicated already.

- Access Control:

Data Owner can permit the entrance or deny access for getting to the information.

- Encryption and Decryption:

AES encryption and AES decoding is utilized for encryption and unscrambling. The record we have transferred which must be in scrambled frame and unscramble it. Data Owner can permit the entrance or deny access for getting to the information.

- Trusted Third Party Login:

In this module Trusted Third Party has screens the information Data Owners record by confirming the information Data Owner's document and stored the document in a database

CONCLUSIONS

With this work, we have decided another privacy challenge information accesses to in the cloud computing to accomplish protection preserving access power sharing. Authentication is Set up to ensure information privacy and information trustworthiness. Information namelessness is certainly accomplished following the wrapped qualities are traded amid transmission. Client protection is enhanced by mysterious access requests to secretly advise the cloud server about the users' entrance needs. Forward security is realized by the session checks to stop the session association. This means the recommended plan is conceivably used for upgraded security support in cloud applications.

REFERENCES

[1] Hong Liu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Qingxu Xiong Member, IEEE,and Laurence T. Yang, Member,IEEE,"Shared Authority Based Privacy-preserving Authentication Protocolin Cloud Computing"IEEE TRANSACTIONS ON PARALLELAND CLOUD SYSTEMS VOL:PP NO:99 YEAR 2014

[2] B.Sameena Begum, P.Ragha Vardhini,"Augmented Privacy-Preserving Authentication Protocol by Trusted Third Party in Cloud", NTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS VOLUME 2, ISSUE 5, MAY 2015, PP 378-382

[3] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang,

Student Member, IEEE,Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE,"Privacy-Preserving Public Auditing for Secure Cloud Storage",Proc. 34th IntlACM SIGIR Conf. Research and Development in Information, pp. 615-624,2015

[4] Larry A. Dunning, Member, IEEE, and Ray Kresman "Privacy Preserving

Data Sharing With Anonymous ID Assignment"IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8,NO. ,FEBRUARY 2013

[5] A. Mishra, R. Jain, and A. Durresi, Cloud Computing: Networking and Communication Challenges,IEEE Communications Magazine, vol. 50,

no. 9, pp, 24-25, 2012.

[6] R. Moreno-Vozmediano, R. S. Montero, and I. M.Llorente,Key challenges in Cloud Computing to Enable the Future Internet of ervicesIEEE Internet omputing, [online] eeexplore.ieee.org/stamp/stamp.jsp?tparnumber 6203493, 2012.

[7] K. Hwang and D. Li, Trusted Cloud Computing with Secure Resources and Data Coloring, IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, 2010.

[8] K. Yang and X. Jia, An Efficient and Secure Dynamic AuditingProtocol for Data Storage in Cloud Computing, IEEE Transactions on Parallel and Cloud Systems, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tparnumber=6311398, 2012.

[9] Y. Zhu, H. Hu, G. Ahn, and M. Yu, Collaborative Provable Data Possession for Integrity Verification in Multi-cloud Storage, IEEE ransactions

on Parallel and Cloud Systems, vol. 23, no, 12, pp. 2231-2244,2012.

[10] H. Wang, Proxy Provable Data Possession in Public Clouds,IEEE Transactions on Services Computing, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tparnumber=6357181, 2012.

[11] 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.

[12] 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 Cloud Systems, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=6374615, 2012.

[13] 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.

[14] 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.

[15] 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.

[16] S. Sundareswaran, A. C. Squicciarini, and D. Lin, Ensuring Cloud Accountability for Data Sharing in the Cloud, IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 4, pp. 556-568, 2012.

[17] Y. Tang, P. C. Lee, J. C. S. Lui, and R. Perlman, Secure Overlay Cloud Storage with Access Control and Assured Deletion, IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 903-916, 2012.

[18] Y. Zhu, H. Hu, G. Ahn, D. Huang, and S. Wang, Towards Temporal Access Control in Cloud Computing, in Proceedings of the 31st Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2012), pp. 2576-2580, March 25-30, 2012.

[19] S. Ruj, M. Stojmenovic, and A. Nayak, Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds,IEEE Transactions on Parallel and Cloud Systems, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=arnumber=6463404,2013.

[20] R. Sanchez, F. Almenares, P. Arias, D. Daz-Sanchez, and A.Marn, Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing, IEEE Transactions on Consumer Electronics, vol. 58, no. 1, pp. 95-103, 2012.