ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 1, Issue 6, November 2015

Multi-user Data Sharing Authentication Protocol for Cloud Computing with Seclusion

Rudresh Bagade [1], Prof.C.R.Barde[2]

PG Student, Dept. Of Computer Engg., R.H.Sapat College of Engineering, Nashik, Maharashtra, India[1]

Assistant Professor, Dept. Of Computer Engg., R.H.Sapat College of Engineering, Nashik, Maharashtra, India[2]

ABSTRACT — Cloud computing will be a good emerging details interactive paradigm to be able to understand user's info remotely maintained inside a good on the internet cloud server. Cloud providers give the brilliant conveniences for the users to help appreciate your on-demand cloud applications devoid of considering the local infrastructure limitations. During your current information accessing, other users may be in an collaborative relationship, along with and so data sharing becomes significant for you to achieve productive benefits. The latest security products mainly focus towards authentication to realize the item the user's privative data are not able to be illegally accessed, but neglect an highly discreet privacy issue throughout a end user challenging the cloud server to get various other users with regard to data sharing. your challenged access get itself will probably reveal the user's privacy simply no matter whether or perhaps not This will probably get the facts accessibility permissions. throughout the actual paper, I propose the multi user based privacy-preserving authentication protocol in order to address above privacy issue with regard to cloud storage. On the SAPA, 1) shared gain access to authority is achieved by anonymous gain access to request for matching mechanism within safety as well as privacy considerations (e.g., authentication, data anonymity, person privacy, as well as forward security); 2) attribute based entry control is usually adopted in order to realize It an individual can single access its own data fields; 3) proxy re-encryption can be applied to help give the data sharing among your multiple users. Meanwhile, universal composability (UC) model is actually standard in order to prove that this SAPA theoretically offers your own design correctness. It indicates that the proposed protocol is usually attractive regarding multi-user collaborative cloud applications.

KEYWORDS- Cloud computing, authentication protocol, privacy preservation, multi user, universal composability.

I. INTRODUCTION

Cloud computing is usually a promising points technology architecture pertaining to both enterprises and also individuals. It launches a good attractive info storage as well as interactive paradigm with obvious advantages, like on-demand self services, ubiquitous network access, and also location independent resource pooling [1]. Towards the cloud computing, a typical ASSISTANCE architecture is usually anything to be a SERVICE (XaaS), in which infrastructures, platform, software, and others are applied with regard to ubiquitous interconnections. Recent studies have been worked to promote the cloud computing evolve towards The internet regarding solutions [2], [3]. Subsequently, security and privacy concerns are usually becoming press button inquiries in the increasing popularity

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 1, Issue 6, November 2015

regarding cloud services. Conventional security approaches mainly focus for the strong authentication to realize The idea a good person may remotely accessibility their own data throughout on demand mode. plus the diversity of an application requirements, users will probably want to be able to entry along with share each other's authorized details fields to be able to achieve productive benefits, which delivers new security and privacy challenges with regard to the cloud storage. An example can be introduced to recognize your own main motivation. In the cloud storage based supply chain management, there tend to be several interest groups (e.g., supplier, carrier, and retailer) for the system. Each group owns its users in which are permitted to admittance your current helped facts fields, as well as different users own relatively independent accessibility authorities. It means That any kind of 3 users via diverse groups should access various other data fields of your same file. There into, a great supplier may want for you to access a carrier's data fields, but This really is not sure whether your own carrier makes it possible for it's access request. Regardless of whether the carrier refuses it's request, ones supplier's admittance desire will be revealed as well as nothing considered for the the desired details fields. Actually, the supplier may not send the access get or even withdraw your unaccepted get in advance whether or not It firmly knows the item they get is actually refused by the carrier. This can be unreasonable to thoroughly disclose the supplier's confidential specifics without having virtually any privacy considerations. The above section discusses the introduction of cloud computing and privacy issues. Section II describes the literature survey of multi user privacy preserving protocol. Sections III defines problem definition .Section IV defines proposed solution. Section V briefly explains expected results and Section VI formalizes conclusion. Fig. 1 illustrates three revised cases in order to address above imperceptible privacy issue.

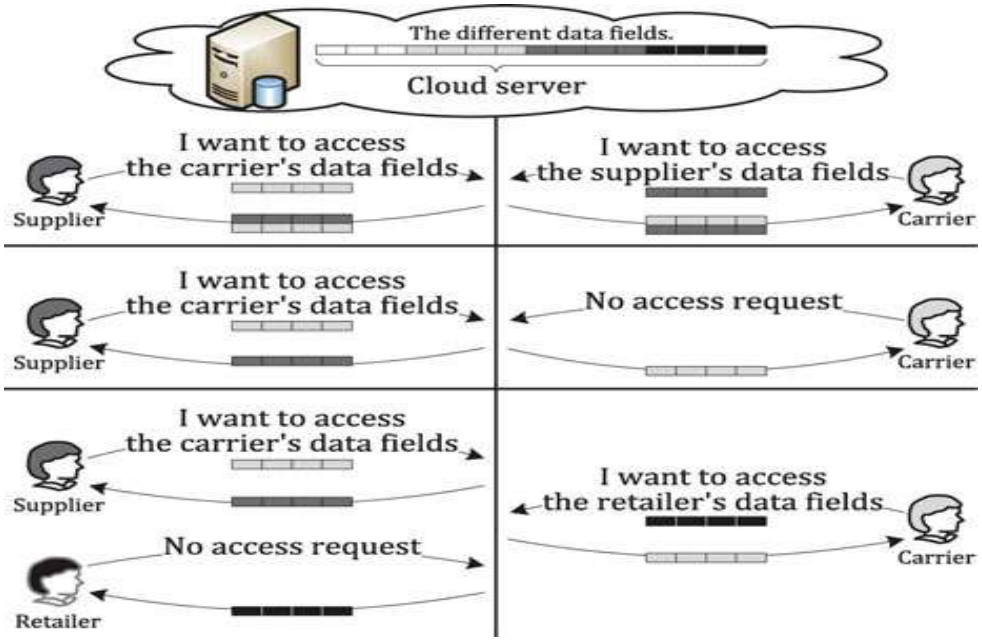

Fig. 1. Three possible cases during data accessing and data sharing in cloud applications

Case 1: Ones carrier furthermore wants to accessibility your supplier's data fields, and also the cloud server In the event inform each other along with transmit your shared access authority for you to the both users;

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 1, Issue 6, November 2015

Case 2: Your current carrier has simply no interest at some other users' data fields, thus it is granted info fields should be properly protected, meanwhile ones supplier's access request for will also be concealed;

Case 3: The carrier will want in order to admittance your current retailer's data fields, but This can be not certain whether or not your current retailer will accept it is request or maybe not. the retailer's authorized data fields In case not possibly be recognized no matter whether your own retailer has no interests in the carrier's data fields, and the carrier's request is also privately hidden.

II. LITERATURE SURVEY

Dunning and also Kresman [11] proposed a great anonymous ID assignment based facts sharing algorithm (AIDA) pertaining to multiparty oriented cloud and distributed computing systems. In the AIDA, a integer info sharing algorithm is designed on top connected with safe volume info mining operation, as well as adopts the variable and unbounded range involving iterations pertaining to anonymous assignment. Specifically, Newton's identities in addition to Sturm's theorem are generally obtained to its details mining, a distributed solution of certain polynomials in excess of finite fields enhances your current algorithm scalability, and Markov chain representations tend to be used to discover statistics towards expected number of iterations. Liu et al. [12] proposed a good multi-owner info sharing secure scheme (Mona) intended for dynamic groups at the cloud applications. The Mona aims to help recognize That an individual can securely share it is data with different users via your untrusted cloud server, as well as will successfully assist dynamic group interactions. On the scheme, a fresh given person may directly decrypt details files without having pre-contacting in data owners, and consumer revocation can be done by the revocation checklist without updating the discreet keys of the remaining users. Gain access to control is applied in order that virtually any consumer throughout a good group will anonymously utilize your current cloud resources, plus the details owners' real identities will probably single become revealed through the group manager for dispute arbitration. The idea indicates your current storage overhead and encryption computation cost tend to be independent with the amount of the users.

III. PROBLEM DEFINITION

Towards above three cases, safety security and also privacy preservation are generally both taken without revealing sensitive access desire related information. In ones cloud environments, an reasonable safety measures protocol should achieve your own right after requirements. 1) Authentication: a legal end user will probably access their own information fields, lone the authorized partial or even whole information fields will be identified by the legal user, in addition to any forged as well as tampered information fields cannot deceive the legal user. 2) Facts anonymity: virtually any irrelevant entity cannot know the exchanged data in addition to communication state even This intercepts your exchanged messages via an open channel. 3) Consumer privacy: almost any irrelevant entity cannot know or perhaps guess a good user's access desire, which represents a user's interest with another user's allowed information fields. If and sole whether the both users have mutual interests inside each other's authorized info fields, your current cloud server can inform the two users to be able to realize ones entry permission

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 1, Issue 6, November 2015

sharing. 4) Forward security: any adversary can't correlate a couple of communication sessions in order to derive your prior interrogations according to the now captured messages. Researches has become worked to help strengthen safety measures protection and privacy preservation inside cloud applications, and there are numerous cryptographic algorithms to be able to address potential stability and privacy problems, similar to security architectures [4], [5], information possession protocols [6], [7], data public auditing protocols [8], [9], [10], safe and sound information storage and info sharing protocols [11], [12], [13], [14], [15], [16], access control mechanisms [17], [18], [19], privacy preserving protocols [20], [21], [22], [23], and switch management [24], [25], [26], [27]. However, almost all before researches focus on the authentication to be able to recognize This lone a legal individual may access its granted data, in which ignores the idea some other users may want to help access along with share each other's allowed details fields to achieve productive benefits. Any time a good end user challenges the cloud server to be able to ask other users regarding info sharing, the access ask itself can reveal your user's privacy simply no matter whether or not This will receive your info gain access to permissions. In this work, we aim to address the user's sensitive gain access to desire related privacy through facts sharing at the cloud environments, and This really is significant in order to design a humanistic security scheme in order to simultaneously achieve data gain access to control, access authority sharing, and privacy preservation. In your paper, I address the aforementioned privacy issue in order to propose the multi user based privacy-preserving authentication protocol (SAPA) for its cloud info storage, which realizes authentication along with authorization without compromising a great user's secret information. your own main contributions are Equally follows.

1) Name the latest privacy challenge in cloud storage, and address an highly discreet privacy issue throughout the user challenging ones cloud server with regard to info sharing, in which ones challenged request for itself cannot reveal the user's privacy absolutely no matter regardless of whether That will probably obtain the accessibility authority.

2) Propose an authentication protocol to enhance a user's entry obtain related privacy, along with the shared access authority will be attained by anonymous access request matching mechanism.

3) Apply cipher text-policy attribute based accessibility control to understand That the end user will probably reliably accessibility it is own data fields, and adopt your own proxy re-encryption to provide temp allowed data sharing among multiple users.

IV. PROPOSED SOLUTION

In this paper, we address the aforestated privacy problem to propose a multi user based privacy preserving authentication protocol for the cloud data storage, which perceives authentication and authorization without compromising a user's private information. The main handouts are as follows. 1) Identify a new privacy challenge in cloud storage, and address a minute privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot disclose the user's privacy no matter whether or not it can obtain the access authority. 2) Propose an authentication protocol to strengthen a user's access request related privacy, and the shared access authority is achieved by incognito access request matching mechanism. 3) Apply cipher text-policy attribute

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 1, Issue 6, November 2015

based access control to realize that a user can faithfully access its own data fields, and adopt the proxy re-encryption to provide temp authorized data sharing among multiple users

V. EXPECTED RESULTS

1. To store data remotely in an online cloud.
2. To achieve multi user based privacy-preserving authentication protocol to address above privacy issue for cloud storage.
3. To achieve attribute based access control is adopted to realize that the user can only access its own data fields;
4. To achieve shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security);
5. To achieve proxy re-encryption is applied to provide data sharing among the multiple users.

VI. CONCLUSION

In the particular work, I have identified the latest privacy challenge during facts accessing for the cloud computing in order to achieve privacy-preserving gain access to authority sharing. Authentication is established to be able to guarantee details confidentiality and data integrity. Data anonymity can be completed because the wrapped values are exchanged through transmission. User privacy can be enhanced from anonymous admittance requests to help privately inform the cloud server In regards to the users' access desires. Forward safety will be realized with the session identifiers to prevent your session correlation. The idea indicates This the proposed scheme will be perhaps applied regarding privacy preservation in cloud applications.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," Nat'l Inst. of Standards and Technology, 2009.

[2] A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges," IEEE Comm. Magazine, vol. 50, no. 9, pp. 24-25, Sept. 2012.

[3] R. Moreno-Vozmediano, R.S. Montero, and I.M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services,"IEEEInternet Computing,vol.17,no. 4,pp. 18-25,http:// ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203493, July/Aug.2013.

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

[5] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer, vol. 45, no. 7, pp. 73-78, 2012.

[6] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable DataPossession for Integrity Verification in Multi-Cloud Storage," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.

[7] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Trans. Services Computing, vol. 6, no. 4, pp. 551-559, http:// ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, Oct.-Dec. 2012.

ISSN (Online) : 2454-4159
International Journal of Advanced Research in Science Management and Technology
IJARSMT
Volume 1, Issue 6, November 2015

[8] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717-1726, http:// ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398, Sept. 2013.

[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859-25, May 2011.

[10] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[11] L.A. Dunning and R. Kresman, "Privacy Preserving Data Sharing with Anonymous ID Assignment," IEEE Trans. Information Forensics and Security, vol. 8, no. 2, pp. 402-413, Feb. 2013.

[12] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, http:// ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, June 2013.

[13] S. Grzonkowski and P.M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," IEEE Trans. Consumer Electronics, vol. 57, no. 3, pp. 1424-1432, Aug. 2011.

[14] M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Trans. Knowledge and Data Eng., vol. 25, no. 11, pp. 2602-2614, http://ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, Nov. 2013.

[15] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.

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