IJRRECS/July 2014/Volume-2/Issue-7/2814-2819 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EXPOSURE TOWARDS SECURE DATA MANAGEMENT IN CLOUD SYSTEM

Karpe Shraddha Pravin[1], K.Nagi Reddy[2]

[1]M.Tech Student, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

[2]Professor, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

ABSTRACT:

The Significant usage of cloud computing necessitates the resources of the computing for data hosting and application running. To practise fine-grained access control that facilitates flexibility in specifying discrepancy right to use of individual users, collection of techniques have been developed. Data privacy is moreover attained in view of the fact that cloud Servers is not capable to gain knowledge of plaintext of data file. Proxy re-encryption with policy attribute-based encryption was merged to facilitate the data owner to hand over for the most part of the computation rigorous operations to cloud servers devoid of revealing the fundamental file contents.

Keywords: Cloud computing, Proxy re-encryption, Data privacy, Fine-grained access control.

1. INTRODUCTION:

The cloud provider handling the upholding of the servers, and storage and application containers was appreciated by the managers in particular the programmers. In the system of cloud data storage users stock up their information within the cloud and no longer hold the data locally as a result ease and accuracy of usage of the data files being accumulated on the distributed cloud servers have to be assured [4]. Cloud users may possibly way out to third party auditor, by periodic storage accuracy verification, while hoping to maintain their data private from third party auditor to accumulate the working out resource for ensuring the storage reliability of data of outsourcing. Third party auditor has competencies that

user, could not contain. It was assumed that the third party auditor, who is in auditing business, is consistent and self-governing and conversely, may damage the user if the third party auditor could become skilled at outsourced data [8]. Presuming the data owner and the servers storing data in similar trusted province by the conventional building where the servers are completely entrusted as an omniscient indication monitor that is accountable for enforcing and defining policies of access control. Key policy attribute-based encryption is a cryptography primitive public key in which data are connected with attributes used for each of which a key component of public is defined [1]. To make sure security, numerous organizations have a preference to keep responsive data under their personal control and make available data in a protected way. As an ideal applicant for data access managing in the promising environment of cloud computing, our system can able to become conscious about the needed security objectives, such as fine-grained access control, user access privilege discretion, user secret key responsibility and data privacy and can be provided [11]. To efficiently put into practice fine-grained access control that facilitates flexibility in specifying discrepancy right to use of individual users, collection of techniques have been developed. Proxy re-encryption with policy attribute-based encryption was merged to facilitate the data owner to hand over for the most part of the computation rigorous operations to cloud servers devoid of revealing the fundamental file contents [3]. Encrypting of data all the way through convinced cryptographic primitive and revealing keys of decryption only to authorized users used for helping the data owner benefit from the access control of fine-grained of data stored on unreliable cloud servers.

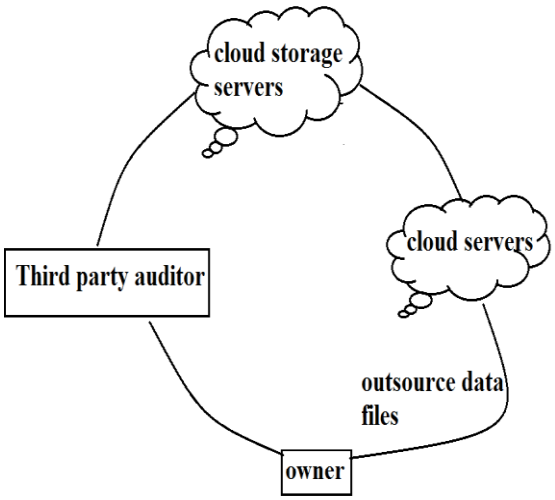

Fig1: An overview of encrypted cloud data

2. METHODOLOGY:

The on-demand temperament of infrastructure as a Service is severe towards making such leases striking, from the time when it permits users to expand or shrink their possessions permitting to their computational requirements, through exterior possessions to supplement their local resource base [14]. The significant usage of cloud computing necessitates the resources of the computing for data hosting and application running. In the recent times, because of unbearable insider within cloud system, customers do not wish for misplacing their secret information and additionally the malfunction of provision accessibility in support of numerous clients, has made quite a few struggle [9]. Infrastructure as a Service has urbanized in the modern times as a sustainable substitute to the acquirement and management of physical resources. Construction of cloud storage service exposed in fig1 consists of various objects such as customer who is one or other enterprise who includes data for deposition in the cloud and depends on the cloud [7]. An object that is accomplished by cloud service provider has vital storing space and a calculation resource is cloud server to deliver data storage service. Upholding of reliability of data is the significant concern which pertains to securing of cloud system in which data undergo breakage throughout the tasks of alterations towards the contributor of cloud system [2]. To transfer a cipher text that is encrypted under user public key into an additional cipher text that can be opened by another user's private key devoid of seeing the essential plaintext proxy re-encryption is a primitive of cryptographic in which a semi-trusted proxy is competent. Proxy re-encryption all along with policy attribute-based encryption makes easy the data owner to hand over computation meticulous operations towards cloud servers devoid of revealing the elementary file contents and allows the data owner to access his data files by minimum overhead in terms of working out effort and as a result fits well into the environment of cloud [16]. By means of encrypting with equivalent public key components, set of attributes were associated by the encryptor towards the message. Under user public key, proxy re-encryption is a primitive of cryptographic in which a semi-trusted proxy is competent to transfer a cipher text that is encrypted into an additional cipher text that can be opened by another user's private key devoid of

seeing the essential plaintext [12]. Data privacy is moreover attained in view of the fact that cloud Servers is not capable to gain knowledge of plaintext of data file. For dropping the working out transparency on Cloud Servers and save information of providing owner, we obtain benefit of lazy re-encryption system and permit Cloud Servers to combined calculation tasks of manifold system procedure [5]. By existing works which intends at securing storage of data on untrusted servers unauthorized users, together with cloud servers, are not able to decrypt in view of the fact that they do not have the keys of data decryption and has been extensively adopted. The accession arrangement of every user is put into practice by an access tree. Interior nodes concerning accession tree are threshold gates [15]. Leaf nodes concerning access tree are connected by means of data file elements. Most important concern with this instinctive system is that it would commence an intense computation transparency for data possessor to re-encrypt files of data and may necessitate data possessor to be constantly online to make available undisclosed key update service in support of users [10]. To decide this issue, methods of proxy re-encryption were combined and delegate responsibilities of data file re-encryption and consumer secret key renew to Cloud Servers. To every user that is typically defined as a tree of access over data attributes, an access structure is assigned that means nodes of interior of the access tree are leaf nodes and threshold gates connected with attributes [6]. The user secret key is definite so that the user is capable to decrypt a cipher text if and as long as the data attributes assure his structure of access in the direction of reflecting the access structure. A cryptography primitive public key that is intended for communications of one-to-many is key policy attribute-based encryption where data are connected with attributes intended for each of which a key component of public is defined [13]. After occurrence of a user revocation event, Cloud Servers very soon evidence information submitted by data possessor. When there is a file data accession demand from a user, cloud servers re-encrypt appealed files and modernize requesting secret key of user. When data possessor redefines a convinced set of aspect for function of user revocation, he moreover makes equivalent proxy re-encryption keys also send them towards Cloud Servers can update user secret key

components as well as re-encrypt data files consequently devoid of knowing fundamental plaintexts concerning data files which improvement releases data possessor from promising huge computation transparency on user revocation. The system of encrypted cloud service comprises user, cloud server and the data owner who has an assemblage of the data files that are to be outsourced on the cloud server in the form of encrypted on the other hand maintains the capacity to search by means of them for the reasons of effectual exploitation of the data. By means of a minimum overhead in terms of working out effort, it permits data owner to be in command of access of his data files and as a result fits well into the environment of cloud.

3. RESULTS:

It is as safe as the intuitive system that is provably protected and proves data secrecy between malicious users and cloud servers under collusion attacks. Adversary has the similar ability as meticulous cloud servers for many secret keys of unlawful users. If the intricacy for every operation of our scheme is no longer reliant to the number of users within the system achieves the scalability. Introduced system is able to become aware about the needed security objectives, for instance user secret key responsibility and data privacy, fine-grained access control and user access privilege discretion. In the promising environment of cloud computing the system is provided as an ideal applicant for data access managing.

4. CONCLUSION:

For dropping the working out transparency on Cloud Servers and save information of providing owner, we obtain benefit of lazy re-encryption system and permit Cloud Servers to combined calculation tasks of manifold system procedure. Key policy attribute-based encryption is a cryptography primitive public key in which data are connected with attributes used for each of which a key component of public is defined. Encrypting of data all the way through convinced cryptographic primitive and revealing keys of decryption only to authorized users used for helping the data owner benefit from the access control of fine-grained of data stored on unreliable cloud servers. As an ideal applicant for data access managing in the promising environment of cloud computing, our system can able to become conscious about the needed security objectives, such as fine-

grained access control, user access privilege discretion, user secret key responsibility and data privacy and can be provided.

REFERENCES:

[1] M. Atallah, K. Frikken, and M. Blanton, "Dynamic and efficient key management for access hierarchies," in *Proc. of CCS'05*, 2005.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in *Proc. of NDSS'05*, 2005.

[3] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in *Proc. of SP'02*, 2002.

[4] 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/ admnsimp/pl104191.htm, 1996.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. Of CCS'06*, 2006.

[6] "Achieving Secure, Scalable, and Fine-grained DataAccess Control in Cloud Computing", Shucheng Yu_, Cong Wang†, Kui Ren†, and Wenjing Lou, 2010

[7] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in *Proc. of NDSS'05*, 2005.

[8] J. Anderson, "Computer Security Technology Planning Study," Air Force Electronic Systems Division, Report ESD-TR-73-51, 1972, http: //seclab.cs.ucdavis.edu/projects/history/.

[9] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *Proc. of ESORICS '09*, 2009.

[10] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in *Proc. of VLDB'07*, 2007.

[11] 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, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.

[12] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable secure file sharing on untrusted storage," in *Proc. of FAST'03*, 2003.

[13] S. Yu, K. Ren, W. Lou, and J. Li, "Defending against key abuse attacks in kp-abe enabled broadcast systems," in *Proc. of SECURECOMM'09*,2009.

[14] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in *Proc. of NDSS'03*, 2003.

[15] M. Atallah, K. Frikken, and M. Blanton, "Dynamic and efficient keymanagement for access hierarchies," in *Proc. of CCS'05*, 2005.

[16] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in *Proc. of NDSS'03*, 2003.