ISSN (Online): 2349-7084

GLOBAL IMPACT FACTOR 0.238

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS VOLUME 1, ISSUE 4, OCTOBER 2014, PP 195-198

Anonymous Authentication of data storage in cloud computing administration with Decentralized Access

G.Gayathri Nikhila[1], A.Bhuvana Pramida[2], P.Jyothsna[3], K.Lavanya[4]
Department of CSE, G.Pullaiah College of Engineering and Technology. Kurnool
JNTU Anatapur, Andhra Pradesh, India

Abstract:-Cloud computing is a climbing processing standard in which stakes of the registering schema are given as an organization over the Web. As ensuring as it might be, this standard furthermore conveys quite a few people new difficulties for information security and access control when customers outsource touchy information for offering on cloud servers, which are not inside the same trusted domain as information owners. Regardless, in finishing hence, these results unavoidably display a considerable preparing overhead on the information owner for key dissemination and information organization when fine grained information access control is popular, and in this manner don't scale well. The issue of in the meantime achieving fine-graininess', versatility, and information classifiedness of access control truly still stays questionable. This paper addresses this open issue by, on one hand, describing and actualizing access approaches focused around information qualities, and, of course, allowing the information manager to delegate most of the figuring endeavors included in fine-grained information access control to un-trusted cloud servers without disclosing the underlying information substance. We fulfill this objective by misusing and joining methods of decentralized key policy Attribute Based Encryption (KP-ABE). Far reaching examination demonstrates that the proposed methodology is exceptionally productive and secure.

Keywords: Access Control, Cloud Computing, Key Policy Attribute Based Encryption (KP-ABE)

1. INTRODUCTION

Now a day's cloud computing could be a rationally developed technology to store knowledge from quite one consumer. Cloud computing is Associate in Nursing atmosphere that permits users to remotely store their knowledge. Remote backup system is that the advanced idea that reduces the price for implementing additional memory in a company. It helps enterprises and government agencies scale back their money overhead of knowledge management. they will archive their knowledge backups remotely to 3rd party cloud storage suppliers instead of maintain knowledge centers on their own. a private or a company might not need getting the required storage devices. Instead they will store their knowledge backups to the cloud and archive their knowledge to avoid any data loss just in case of hardware / software system failures. Even cloud storage is additional versatile, however the safety and privacy square measure offered for the outsourced knowledge becomes a significant concern. There square measure 3 objectives to be main issue Confidentiality – protective licensed restrictions on data access and speech act. The most threat accomplished once storing the information with the cloud. Integrity – guarding against improper data modification or destruction. Convenience – making certain timely and reliable access to and use of knowledge

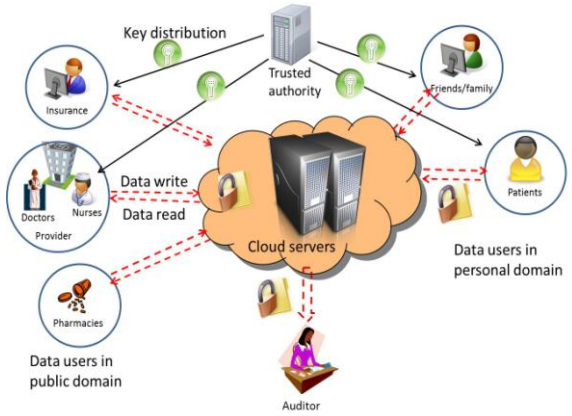

Fig1: Example diagram for data sharing with cloud storage.

ISSN (Online): 2349-7084

GLOBAL IMPACT FACTOR 0.238

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS VOLUME 1, ISSUE 4, OCTOBER 2014, PP 195-198

To achieve secure information group action in cloud, appropriate cryptography technique is employed. The information owner should inscribe the file then store the file to the cloud. If a 3rd person downloads the file, he/she could read the record if he/she had the key that is employed to decode the encrypted file. Typically this might be failure attributable to the technology development and therefore the hackers. to beat the matter there square measure ton of techniques introduced to form secure group action and secure storage. The encoding standards used for transmit the file firmly. The assured deletion technique aims to produce cloud shoppers associate degree choice of faithfully destroying their information backups upon requests. The encoding technique was enforced with set of key operations to keep up the secrecy Security and privacy protection in clouds square measure examined and Experimented by several researchers. Wang et al. [16] provides storage security mistreatment Reed-Solomon erasure correcting codes. Mistreatment Homomorphic encoding, [17] the cloud receives cipher text and returns the encoded price of the result. The user is ready to decrypt the result, however the cloud doesn't recognize what information it's operated on. Time-based file assured deletion that is 1st introduced in [5], implies that files is firmly deleted and stay for good inaccessible once a predefined period. The most plans is that a file is encrypted with a knowledge key by the owner of the file, and this information key's more encrypted with a sway key by a separate key manager (known as Ephemerizer [5]). The key manager could be a server that's answerable for cryptological key management. In [5], the key is time-based, that means that it'll be utterly removed by the key manager once associate degree expiration time is reached, wherever the expiration time is such once the file is 1st declared. While not the key, the information key and thus the information file stay encrypted and square measure deemed to be inaccessible. Thus, the most security property of file assured deletion is that even though a cloud supplier doesn't take away expired file copies from its storage, those files stay encrypted and forgotten. Associate degree open issue within the work [5] is that it's unsure that whether or not time-based file assured deletion is possible in observe, as there's no empirical analysis. we have a tendency to propose policy based mostly} file access [2] and policy based file assured deletion [2], [5], [7] for higher access to the files and delete the files that square measure set no a lot of. We have a tendency to propose effective renewal policy for creating higher approach to renew the policy while not downloading the information key and management keys that is accessible currently each day. Instead we are able to add a renew key with every file and transfer that keys whenever the file must be revived.

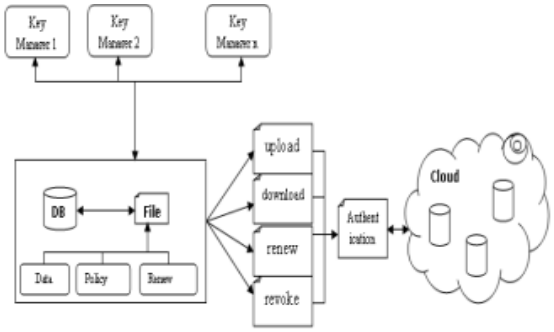

Fig2: System Architecture

First the shopper was genuine with the username and Password that is provided by the user. Then the user was asked to answer 2 security levels with his/her selection. Every security levels include five user selectable queries. The user might opt for anybody question from 2 security levels. The non-public key for cipher the file was generated with the mix of username, Password and also the answers for the safety level queries. Once generating the non-public key the shopper can request to the key manager for the general public key. The key manager can verify the policy related to the file. If the policy matches with the file name then same public key are going to be generated. Otherwise new public key are going to be generated. With the general public key and personal key the file are going to be encrypted and uploaded into the cloud. If a user needs to transfer the file he/she would be genuine. If the authentication succeeded, the file is going to be downloaded to the user. Still the user can't ready to browse the file contents. He / she ought to request the general public key to the key manager. in keeping with the authentication, the key manager can turn out the general public key to the user. Then the user might decipher the file mistreatment the login credentials given by the user and also the public key provided by

ISSN (Online): 2349-7084

GLOBAL IMPACT FACTOR 0.238

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS VOLUME 1, ISSUE 4, OCTOBER 2014, PP 195-198

the key manager. The shopper will revoke the policy and renew the policy attributable to the need.

II. KEY MANAGEMENT

In this paper, following are the Encrypted keys to safeguard knowledge files keep on the cloud Public Key: the general public secret's a random generated binary key, generated and maintained by the Key manager itself. Significantly used for encryption/ decoding. Private Key: it's the mix of the username, Password and 2 security question of user's selection. The non-public secret's maintained by shopper itself. Used for cipher / decipher the file. Access key: it's related to a policy. Non-public access secret's maintained by the shopper. The access secret's engineered on attribute based mostly encoding. File access is of browse or write. Renew key: Maintained by the shopper itself. Every has its own renew key. The renew secret's accustomed renew the policy of every necessary file at simple methodology.

III. PROJECTED WORK

A. Uploading / decoding: We used RSA algorithmic rule for encryption/Decryption. This algorithmic rule is that the verified mechanism for secure group action. Here we have a tendency to are mistreatment the RSA algorithmic rule with key size of 2048 bits. The keys are completely different ways and keep in four different places. If a user needs to access the file he/she might have to supply the four set of information to supply the only non-public key to manage encryption/decryption

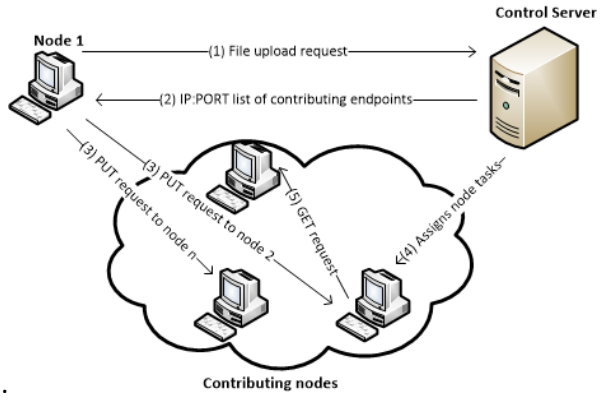

Fig 3. Contributing nodes association with Control severs.

Node 1 send the request to Control server ,control server send the response as IP Port List, from node 1 put request to node 2….node n.,Control server assigns node tasks to Contributing nodes so that node 1 can send the request inorder to upload the file and download the file.

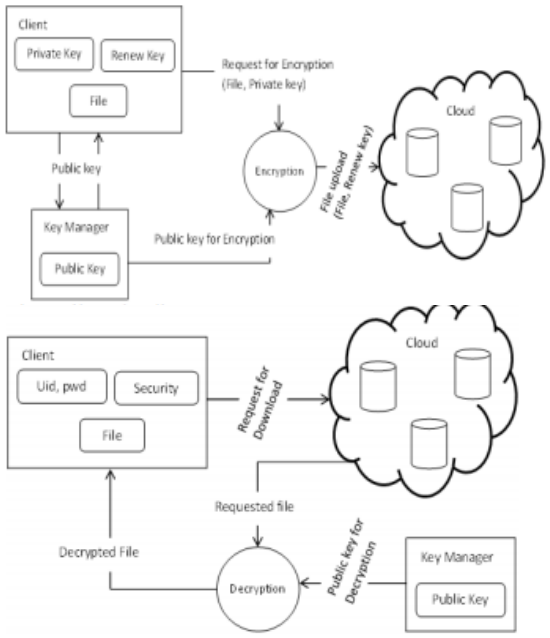

Fig4(a) File Uploading in Cloud
Fig4(b) File downloading in Cloud

B. Policy Revocation for File Assured Deletion

The policy of a file could also be revoked [8] beneath the request by the consumer, once expiring the fundamental quantity of the contract or fully move the files from one cloud to different cloud surroundings. Once any of the on top of criteria exists the policy are going to be revoked and therefore the key manager can fully removes the general public key of the associated file. Thus nobody recover the key of a revoked enter future. For this reason we will say the file is assuredly deleted. Automatic file revocation [12] theme is additionally introduced to revoke the file from the cloud once the file reaches the expiration and therefore the consumer didn't renew the files period.

D. File Access management

Ability to limit and management the access to host systems and applications via communication links. To

achieve, access should be known or genuine. Once achieved the authentication method the users should come with correct policies with the files. To recover the file, the consumer should request the key manager to come up with the general public key. For that the consumer should be genuine. The attribute based mostly cryptography normal is employed for file access that is genuine via associate attribute related to the file. With file access management the file downloaded from the cloud are going to be within the format of scan solely or write supported. Every user has related to policies for every file. The right user can access the correct file. For creating file access the attribute based mostly cryptography theme is used.

V. CONCLUSION

We propose secure cloud storage victimization redistributed access management with anonymous authentication. The files area unit related to file access policies that accustomed access the files placed on the cloud. Uploading and downloading of a file to a cloud with normal Encryption/Decryption is safer. Revocation is that the necessary theme that ought to take away the files of revoked policies. Thus nobody will access the revoked enter future. The policy renewal is formed as simple as potential. The renew secret's side to the file. Whenever the user needs to renew the files he/she might directly transfer all renew keys and created changes to it keys, then transfer the new renew keys to the files hold on within the cloud.

REFERENCES

[1] S Sushmita Ruj, Milos Stojmenovic and Amiya Nayak,"Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE TRANSACTIONS ON PARALLEL AND CLOUD SYSTEMS

[2] Yang Tang, Patrick P.C. Lee, John C.S. Lui and Radia Perlman,"Secure Overlay Cloud Storage with Access Control and Assured Deletion", IEEE Transcations on dependable and secure computing, VOL. 9, NO. 6, NOVEMBER/DECEMBER 2012

[3] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in ACM CCS, , pp. 735–737, 2010

[4] Y. Tang, P.P.C. Lee, J.C.S. Lui, and R. Perlman, "FADE: Secure Overlay Cloud Storage with File Assured Deletion," Proc. Sixth Int'l ICST Conf.Security and Privacy in Comm. Networks (SecureComm), 2010

[5] R. Perlman, "File System Design with Assured Delete," Proc. Network and Cloud System Security Symp. ISOC (NDSS), 2007

[6] Ruj, A. Nayak, and I. Stojmenovic, "DACC: Cloud access control in clouds," in IEEE TrustCom, 2011

[7] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), Apr. 2010

[8] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and Efficient Access to Outsourced Data," Proc. ACM Workshop Cloud Computing Security (CCSW), Nov. 2009

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, May 2006

[10] R. Geambasu, J.P. John, S.D. Gribble, T. Kohno, and H.M. Levy, "Keypad: Auditing File System for Mobile Devices," Proc. Sixth Conf. Computer Systems (EuroSys), Apr. 2011