Survey on Cloud Computing With Decentralized Access Control

Mr. Rupesh Tandule[1], Prof. Pravin Malviya[2]
Department of Computer Science & Engineering
[1, 2] Shri Balaji Institute of Technology & Management, Betul, India

Abstract-*Cloud computing is a rising computing paradigm in which resources of the computing infrastructure are provided as services through the Internet. Cloud computing is the delivery of multiple computing services through the Internet. Cloud computing provide various services such as software, applications and information over the cloud on demand. Cloud has ability to provide dynamically scalable access for users, and the ability to share resources over the Internet. Cloud checks the authentication of the user without knowing the users identity. The main aim of system is secure data storage on clouds. A basic solution is to encrypt data files, and then upload the encrypted data into the cloud to preserve data privacy. This paper presents a survey of existing techniques with the novelties highlighting the need of intelligent sharing and validating technique for storing files on the cloud. This paper is motivated by arising need to provide high quality of security for the user with validation by using third party authority. In proposed system we add third party authority with decentralized access management theme to validate integrity of the files stores on cloud.*

Keywords-Cloud storage, access control, authentication, attribute-based encryption.

I. INTRODUCTION

Cloud computing is the conveyance of registering services on the Internet. Cloud services permit every person and organizations to utilize both software and hardware handled through third parties at remote locations. In Today's era because of the advances in network technology and emerged requirements ofcomputing resources causes organizations to out source their storage. Cloud provides, infrastructure as a service (IaaS), where a user make sutilization of an service providers computing, storage infrastructure; platform as a service(PaaS), where a client influences the providers. resources to execute custom applications; lastly software as a service (SaaS), where clients use software which is execute on the suppliers infrastructure.

Cloud guarantees the authorized user attempting to access information and services. Authentication of user accomplished utilizing different public key cryptographic methods. User should guarantee the cloud is not altering with information as well as computational outcomes. User's identity is hidden for security reasons. For instance, putting away medical records, the cloud should not to have the capacity of getting the records of a specific patient.

A method called homomorphic encryption [10] hides the information from the cloud with computation on the information. User sends messages encrypted using homomorphic encryption technique and cloud executes computations on encrypted messages and gives back outcomes to the user.

Generally, members are owners of the online social networking. They stores personal details, music, recordings, and pictures, videos on the cloud and users access information on the basis of access rights. A message posted by member or transfers a photo whenever seeable only to the friends and limited belonging groups.

Giving access rights to some authorized users and preventing the other user from getting an access to that information, is called access control. An approach called as user based access control permit to store a list of all authorized users in cloud who can access the information. In cloud computing, such records can be much long and frequently dynamic, which will make taking care of such records to a great degree troublesome. Every time list is verified whether the authorized user. This outcomes in a tremendous computation and storage values. Another approach, public keys of valid users is utilized to encrypt information and only they are able to decrypt information by secret keys. This technique brings similar information encryption for multiple times for every user as well as huge storage costs. Along, cryptographic technique called Attribute Based Encryption (ABE) [4] is used to gain access control in clouds. Users encrypt information by ABE with attributes and possess as well as store information on cloud. Users provide attributes and secret keys by given from a key distribution center KDC and similar attributes are able to decrypt the data.

II. LITERATURE REVIEW

Here first think of some as existing plans. Fuzzy IBE [9] offers two interesting new applications. The first is an

Identity Based Encryption system that uses biometric identity. That is one can see a user's biometric, for instance an iris scan, as that user identity depicted by a few traits and after that encode to the client utilizing their biometric character. Subsequent to biometric estimations are boisterous, it is bad to utilize existing IBE system. Be that as it may, the mistake resistance property of Fuzzy IBE takes into consideration a private key which is gotten from an estimation of a biometric to unscramble a ciphertext encoded with a somewhat diverse estimation of the same biometric. Also, Fuzzy IBE can be utilized for an application that can be called "attribute based encryption". In this application a gathering will wish to scramble an archive to all clients that have a certain set of characteristics. For instance, in a computer science department, the chairperson might need to encode an archive to all system personnel on a contracting board of trustees. For this situation it would encode to the character "hiring committee", "faculty", "systems". Any user who has a identify that contains these qualities could decrypt the archive. The point of interest to utilizing Fuzzy IBE is that the report can be put away on a straightforward untrusted capacity server as opposed to depending on trusted server to perform authentication checks before conveying a report. ABE was proposed by Sahai and Waters [9]. In ABE, a user has an arrangement of ascribes notwithstanding its remarkable ID. There are two classes of ABEs. In key-strategy ABE or KP-ABE [4], the sender has an entrance strategy to encode information. An essayist whose properties and keys have been repudiated can't compose back stale data. The recipient gets traits and mystery keys from the characteristic power and can unscramble data in the event that it has coordinating traits. In Cipher content approach, CP-ABE, the recipient has the entrance arrangement as a tree, with attributes as leaves and monotonic access structure with AND, on the other hand and other threshold gates.

KP-ABE [4] is a crypto system for fine grained sharing of encoded information. In KP-ABE cipher text are mark with attribute and private key are connected with access structures that control which cipher text a user can decrypt. It is utilized for securing touchy information store away by outsiders on the web. In this system each ciphertext is named by the encryptor with an arrangement of unmistakable qualities. Each private key is connected with an entrance structure that indicates which kind of ciphertext the key can decode. Note this setting is reminiscent of mystery sharing plans. Utilizing known procedures one can manufacture a mystery sharing plan that indicates that an arrangement of gatherings must collaborate with a specific end goal to remake a mystery. For instance, one can indicate a tree access structure where the inside hubs comprise of AND as well as entryways and the leaves comprise of various gatherings. Any arrangement of gatherings that fulfill the tree can remake the mystery. In this development each user's key is connected with a tree-access structure where the leaves are connected with qualities. A user can unscramble a ciphertext if the traits connected with a ciphertext fulfill the key's entrance structure. The essential contrast between this setting and mystery sharing plans is that while mystery sharing plans take into consideration collaboration between various gatherings, in this setting, this is explicitly prohibited. Case in point, if Alice has the key connected with the entrance structure "X AND Y", what's more, Bob has the key connected with the entrance structure "Y What's more, Z", framework would not need them to have the capacity to unscramble a ciphertext whose just trait is Y by conniving. To do this, this framework adjusts and sums up the strategies to manage more intricate settings. This cryptosystem gives an effective apparatus for encryption with fine-grained access control for applications, for example, sharing review log data.

CP-ABE [3] is an approach to obtain complex control on encrypted data. This technique is utilized to keep encoded information secret. In this system, a user's private key is related with a arbitrary number of attributes communicated as strings. Then again, when a gathering encodes a message in this framework, they indicate a related access structure over properties. A user just can unscramble a ciphertext if that client's properties go through the cipher text's entrance structure. At a numerical level, access structures in this framework are portrayed by a monotonic "access tree", where hubs of the access structure are made out of limit entryways and the takes off portray characteristics. There AND entryways can be built as n of n limit entryways as well as doors as 1 of n edge entryways. Moreover, this plan can deal with more unpredictable access controls, for example, numeric extents by changing over them to little access trees.

Multi-Authority Attribute-Based Encryption [8] metho permits any polynomial number of free authorities to attributes and disperse secret keys. An encryptor can pick, for every power, a number dk and an set of attributes; he can then encode a message such that a user can just unscramble on the off chance that he has in any event dk of the given attributes from every power k. Pursues scheme [8] is skilled of handling of disjoint arrangements of qualities that are appropriated among different powers. In this plan, an encrypting party indicates an arrangement of attributes AC with the properties in AC being controlled by a few powers. Give Ak a chance to be the set of attributes controlled by power k. At that point the ciphertext C related with the trait set AC must be decoded by those clients with an arrangement of traits Au for which the cardinality of the crossing point Au Ak AC surpasses the individual edge dk, for every power k. one of the principle

challenges in executing such a multi-power trait based encryption plan is the anticipation of conspiracy assaults among user that acquire secrete key parts from various powers. Also, it is alluring that there be no correspondence between the singular powers. To defeat these troubles, Chase's plan depends on a trusted focal power. The subsequent plan is fit for enduring different tainted powers, in any case, the genuineness of the focal power stays of key significance since, by the narrowing from [4], and the trusted power has the capacity of decrypting each ciphertext.

Paper Name	Author	Proposed Work
Fuzzy Identity-BasedEncryption(IEEE)	A. Sahai and B. Waters	User has a set of attributes in addition to its unique ID. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities.
Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data(ACM)	V. Goyal, O. Pandey, A. Sahai, and B. Waters	In KP-ABE cipher text are label with attributes and private key are associated with access structures that control which cipher text a user is able to decrypt.
Ciphertext-Policy Attribute-Based Encryption (IEEE)	A. Sahai and B. Waters	Receiver has the access policy in the form of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates, RBAC based.
Attribute-Based Signatures(IEEE)	H.K. Maji, M. Prabhakaran, and M. Rosulek	This method allows any number of independent authorities called KDC to monitor attributes and distribute secret keys.
DACC (IEEE)	S. Ruj, M. Stojmenovic, A. Nayak	ABE is Used with ABS for authentication without disclosing the identity of the user.

IV.PROPOSED SYSTEM

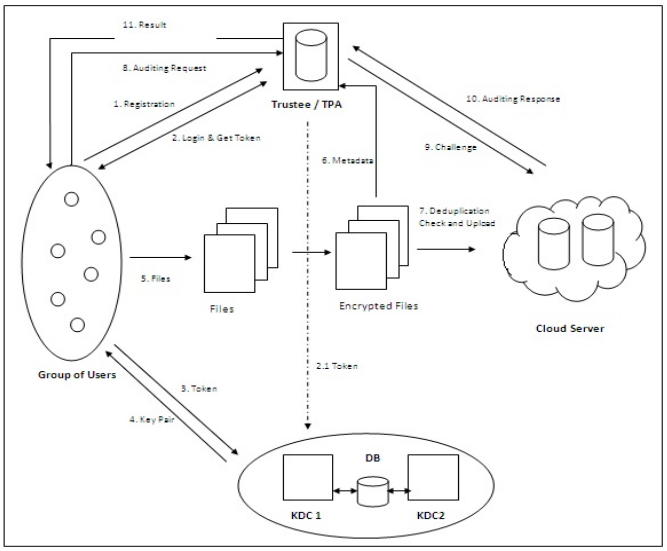

Figure 1: System Architecture

The proposed architecture is decentralized, meaning that there are several KDCs are used for key management. Creator, reader and writer be the different users in system. User receives a token from the trustee. A trustee can be someone like the federal government who manages user ID's etc. A user after validating the token from one or multiple KDC's, receives key pairs for encryption / decryption. The message is encrypted under the access policy. The access policy decides who can access the data stored in the cloud. After encrypting the file user generate the hash of file using SHA1 algorithm and Deduplication check is performed by matching the current hash with the previously uploaded files hash at cloud server. If current hash is matches with existing hash then user gets the link of file & there is no need to upload the file at cloud server as the same file is available at cloud server.

The creator decides on an access policy, to prove his/her authentication and signs the message using this claim. The cipher-text or Encrypted File is sent to cloud server while the hash of file is sent to TPA. TPA verifies the integrity of file on behalf of user request by proof generation and proof verify and result sent to the requested user. When a reader wants to read the file, then he/she request for file to cloud server, the cloud sends cipher-text or encrypted file. If the user

has attributes matching with access policy, he/she can decrypt the ciphertext and get original message. Writing process is similar to file creation. When a reader wants to read data in the cloud, it tries to decrypt data in by using the secret keys which he receives from the KDCs. If user has sufficient attributes matching with the access policy, then he/she can decrypt the information stored in the cloud.

V.CONCLUSION AND FUTURE SCOPE

This paper presented an all-inclusive survey on data storage techniques without knowing the users identity. The main features, the advantages and disadvantages of each system are described. Cloud computing provide various services such as software, applications and information over the cloud on demand. One of the most primary services presented by cloud providers is data storage. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. Preserving Identity privacy is one of the most significant problems for the wide deployment of cloud computing. As per survey, there is need of novel approach for decentralized access management theme to validate integrity of the files stores on cloud. In proposed system we add third party authority with decentralized access management theme to validate integrity of the files stores on cloud.

REFERENCES

[1] 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.

[2] S. Ruj, M. Stojmenovic, A. Nayaks “Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds,” IEEE transactions on parallel and distributed systems, pp□384□394, f 2014.

[3] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext Policy Attribute Based Encryption,” Proc. IEEE Symp. Security and Privacy, pp. 321334, 2007.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute Based Encryption for Fine Grained Access Control of Encrypted Data,” Proc. ACM Conf. Computer and Comm. Security, pp. 89□98, 2006.

[5] M. Li, S. Yu, K. Ren, and W. Lou, “Securing Personal Health Records in Cloud Computing: Patient Centric and Fine-Grained Data Access Control in Multi Owner Settings,” Proc. Sixth Int’l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89□106, 2010.

[6] S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed Access Control in Clouds,” Proc. IEEE 10th Int’l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[7] F. Zhao, T. Nishide, and K. Sakurai, “Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute Based Cryptosystems,” Proc. Seventh Int’l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.

[8] M. Chase, “Multi-Authority Attribute Based Encryption,” Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515□534, 2007.

A. Sahai and B. Waters, “Fuzzy Identity Based Encryption,” Proc. Ann. Intal Conf. Advances in Cryptology (EUROCRYPT), pp. 457473, 2005.

B. Gentry, “A Fully Homomorphic Encryption Scheme,” PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009.

[9] Nalini C.Iyer and Sagarika Mandal,”Implementation of Secure Hash Algorithm-1 using FPGA” ISSN 0974 - 2239 Volume 3, Number 8 (2013), pp. 757-764 http://www. irphouse.com/ijict.htm