ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 2; Issue 6; Page No. 148-153

Secure Access Control on Shared Data In Cloud

Priyanka R. Chaudhari[1], Prof. Archana C. Lomte[2]

[1,2*]Computer Engineering Department,

Bhivarabai Sawant Institute of Technology & Research (BSIOTR),

Savitribai Phule Pune University, India Department & University

[1]priyanka10jun@gmail.com; [2]archanalomte@gmail.com

ABSTRACT

This paper surveys emerging access policies for shared data in cloud. We describe the quandaries and explore solutions for providing future storage and access to analysis outputs, concentrating totally on data. Access control in clouds is gaining attention because it is important that only authorized users have access to valid examine. The cloud verifies the authenticity of the series while not knowing the user's identity before storing data. Secure cloud system that attains policy based access control.

Keywords: *Cloud computing, authentication, Attribute-based encryption, Access control, Attribute-based signatures.*

INTRODUCTION:

T Different Computer users wants enough storage area to have all the details they've acquired may be a real challenge. A lot of people spend money on larger hard drives, external storage devices like thumb drives or compact discs [12]. Too many users might delete entire folders importance of old files in order to make space achievable information. Alternative option is: cloud storage. Cloud storage is part of cloud computing shown in fig1.

Many organizations in the market are currently adopting technology cloud computing. In cloud computing systems provide users access never to only storage, but probably processing power and computer applications installed on web network. Whereas cloud storage cloud seems to be it's one thing to try and do with weather fronts and storm systems, it genuinely is the word for preserving data from an off-site storage system maintained by yet another party [12]. Rather than storing information in your computer's disk drive or other local storage contrivance, it can preserve it to an online database. The Cyber World provides the link between computer and additionally database. If you want store your data on a cloud storage system, you'll get work it information from any location which has net access[12]. Does one use have to have a genuine storage contrivance or operate the same computer to preserve and retrieve your information? With the congruous storage system, you could potentially even sanction other people to locate the details, turning an individual project into a collaborative manner. Cloud computing is receiving a lot of attention from both academic and industrial worlds. In cloud computing, user will source their computation and storage to servers (also known as clouds) using Internet [1]. Clouds will offer many varieties of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Nimbus), and platforms to assist developers write applications (e.g., Amazon's S3, Windows Azure). A lots of data stored in clouds is extremely sensitive, as an example, medical records and social networks.

Security issue is a major issue for any computer systems. Many security issues managed by good access control. Malwares, virus, worms use system resources, take necessary information and damage necessary configurations and spreads all over the network. Antivirus software's are used to secure systems from virus attacks. However, a lot of resource had been used on preventing malicious software and fixing system susceptibilities.

Currently, computers and different servers become powerful. Cloud computing structure will full up use of powerful servers by making virtual machines on them and arrange the computation for various applications [13]. Infrastructure, platform and software are considered as services in cloud systems. All resource may be distributed for various applications. IaaS related to hardware of system. PaaS related to the operation system of computer system. SaaS related to soft wares and applications of computer system. In cloud computing

systems, malwares may be even fatal [14]. Viruses are spread simply & easily in virtual system than in real system. What is more, manager of virtual system may be the super user over several servers. If administrator access added by hackers then then whole system are in danger [15]. On the opposite side, antivirus software is expensive more computing resource than in older systems.

Security and privacy are thus very consequential issues in cloud computing. In one hand, the utilizer should authenticate it afore initiating any transaction, and on the other hand, it must be ascertained that the cloud does not tamper with the data that is outsourced

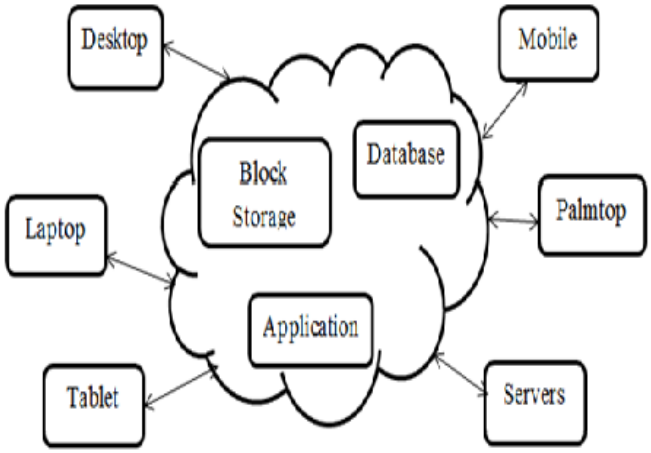

Figure 1: Cloud storage

Incipiently, Wang et al. [2] addressed secure and dependable cloud storage. The clouds should not know the query but should be able to return the records that satisfy the query with security and privacy protection in clouds by using a encryption [3][4]. The primary contributions for this paper would be the following [1].

1) Distributed access control of information held in cloud to make sure only authorized users with valid attributes can access them.

2) Authentication of users who store and modify their data in the cloud.

3) The identity of a person is protected in the cloud during authentication.

4) The architecture is decentralized manner, as an example there could also be many key distribution center (KDCs) for key management.

5) The access control and authentication are each collusion resistant, as an example no 2 users will conspire and access information or manifest themselves, cons one by one not authorized.

6) Revoked users cannot access data after they've been revoked.

7) The protocol supports multiple read and writes on your data held in the cloud.

8) The expense is cherish this centralized approaches, and so the high ticket operations created for professionals done by the cloud.

TECHNIQUE PRELIMINARIES

A. Access Control:

Authorization for individual users is provided for authenticated users and anonymous users. Authorizations are given to users on the basis on key generation. The user easily uploads the encrypted data's to cloud the ring key for each file uploaded by the user is generated automatically. After that the user notes their member ring key for that data access to others. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. The benefits of their own, there do exist various motivations for cloud service providers to behave unfaithfully towards the cloud users regarding the status of their outsourced data

Types of access control:

a) User Based Access Control (UBAC),

b) Role Based Access Control (RBAC), and

c) Attribute Based Access Control (ABAC).

In UBAC, the access control list (ACL) contains the list of users who are authorized to access data. It is not practicable in clouds where there are many users[1]. In RBAC users are classified based on their individual roles. Data can be accessed by users who have homogeneous roles. The roles are defined by the system [11]. For instance, only faculty member and superior secretaries might have access to data but not the junior secretaries. ABAC is more elongated in scope, in which users are given attributes, and the information has affixed access policy. Only valid users with set of attributes, satiating the access policy, can access the data. For illustration, as mentioned in above example some records can be accessible by faculty members with more than 8 years' experience of senior administrators with more than or research experience of10 years. In [25] advantages & disadvantages of role based access control and Attribute Based Access Control. Some work about ABAC in clouds is mentioned in previous work. These work use a cryptographic called as Attribute Based Encryption (ABE). In health care system, Sensitive information concerning patients to allow access to medical professionals, policy producers, hospital worker, researchers, are stored in cloud. If we want to control data accessing then only valid users must access the data. Re cords or data is encrypted using different access policy like ABE to store

in cloud. Users are having certain sets of keys and attributes. Only those users having matched set of attributes, only they can decrypt the data stored in the cloud. Health care systems are also using access control discussed in [17], [18]. Access control is additionally raising position in on-line social networking where users are store their private information, data, videos and pictures and also share them with particular groups of communities which are belong to [15]. Such knowledge area units being keep in clouds. it's important that solely the approved users area unit given access to those information. The same state of affairs arises once knowledge is keep in clouds, for instance in Dropbox, and shared with bound teams of individuals. It is simply not enough to store the contents firmly within the cloud however it'd even be necessary to make sure obscurity of the user. For example, a user wants to store some private information but he want to hide data. However, the user would be able to show to the other users that they are authorized user who kept the data without skimpy the identity. There are different protocols such as mesh signatures [23], ring signatures [22], group signatures [24], which may utilize in these circumstances. Mesh signatures don't guarantee if the message is from one user or several users colluding along. Ring signature isn't a possible possibility for clouds wherever there area unit an outsized variety of users. Group signatures assume the existence of a gaggle which could not be potential in clouds. Due to such reasons, a new protocol is used known as Attribute Based Signature.

Different users have a claim predicate related to message in Attribute based signature. The predicated claim which helps to identify the user that he/she is as authorized, while not skimpy its identity. Another users or the cloud will verify the user and therefore the validity of the message keep. Attribute based signature (ABS) is combined with (ABE) to realize attested access management while not revealing the identity of the user to the cloud. Subsisting work on access control in the form of centralized manner is described in [16], [17], [18], [19], [20], [21].The different system in [17], [18], [21] do not support verification also. only [16], all other systems use attribute based encryption. The scheme in [16] uses a symmetric key scheme and doesn't maintenance authentication. In cloud, privacy preserving authenticated access control is given in [20]. A Centralized approach is considered by authors wherever only one key distribution center allocates attributes, secret keys to multiple users. Unluckily, due to only a single KDC which is difficult to manage the large number of users in a cloud environment. We give emphasis to that clouds ought to use a decentralized manner for distribution of secret keys and attributes to users in cloud.

It's natural for clouds that having various Key Distribution Centers in different locations in the world. Distributed access scheme is proposed in [21]. However, that mechanism is not giving the facility of user authentication. The other disadvantage was that an user is able to create and store a data in file and other various users can only get access of read the file. Only creator having the facility of write access but all the another users was not having permission of write access. In [11] the scheme is able to validate the validity of the message while not revealing the uniqueness of the user who has kept information in the cloud. In [20] they use attribute based signature scheme to attain validity, authenticity and confidentiality.

Unlike [20], scheme in [11] is sturdy on replay attacks, during which an user will replace original data with decayed data from a preceding write, even through it was not legal claim policy. This is very significant thing as a result of an user, revoked all of its attributes, would possibly now not be able to write to the cloud. We have a tendency to thus add this further feature in their system and modify [20] suitably. Their system additionally permits multiple writes that wasn't allowable by [21]

Access Policies:

Access policies can take these things formats: 1) Boolean functions of attributes, 2) Linear secret sharing scheme (LSSS) matrix, or 3) Monotone span programs. Any type of access structure is usually converted to a Boolean function [6].

Attribute-Based Signature Scheme (ABS) [5]:

1. System Initialization
2. User Registration
3. KDC Setup
4. Attribute Generation
5. Sign
6. Verify

Attribute-Based Encryption (ABE) [6]:

Attribute-Predicated Encryption (ABE) provides an incipient way for access control of encrypted data. First introduced the public-key cryptography attribute predicated encryption (ABE) for cryptographically enforced access control. The main goal for these models is to provide security and access control. The main characteristics are to offer flexibility, scalability and secured access control. In classical model, this can be achieved only when utilizer and server are in a trusted domain. In ABE both the utilizer secret key and the cipher text are associated with a set of attributes. A utilizer is

able to decrypt the cipher text if and only if at least a threshold number of attributes overlap between the cipher text and utilizer secret key

1. System Initialization
2. Key Generation and Distribution by KDCs
3. Encryption by Sender
4. Decryption by Receiver

Key-Policy ABE

To enable more general access control proposed a key-policy attribute-based encryption (KP-ABE) scheme. It is the modified form of classical model of ABE. Discovering KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes.

1. KP-ABE the sender has an access policy to encrypt data.
2. The receiver receives attributes and secret keys from the attribute Authority
3. Decrypt data if matching occur

Privacy Preserving Authenticated Access Control Scheme [1]: An individual can make a file and store it securely with the cloud. This scheme comprises of utilization of the two protocols ABE and ABS.

1. Data Storage in Clouds
2. Reading from the Cloud
3. Chatting with the Cloud
4. User Revocation

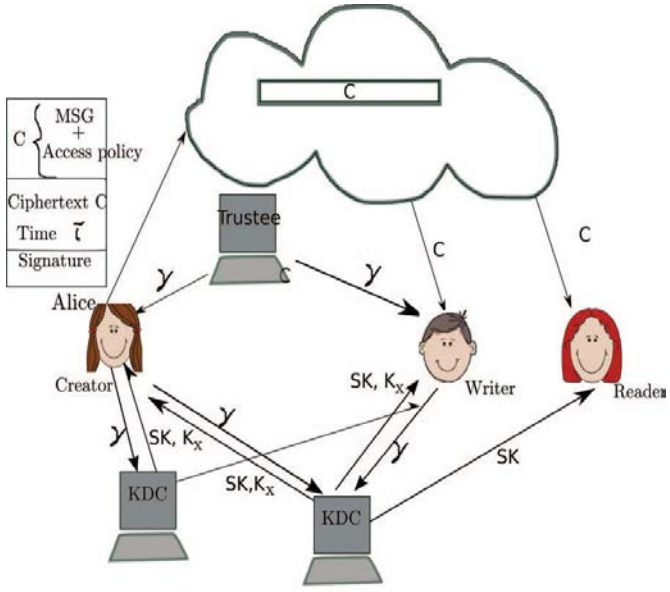

Figure 2: Model of secured Cloud storage

You'll find three users, a creator, a reader, and writer. Creator receives a token ¥ from the trustee, that is assumed that should be honest. A trustee is a person like the government who manages social insurance numbers. A creator on presenting the token to several KDCs receives keys for encryption/decryption and signing. The access policy decides no one can access the results held in the cloud. The creator elects for the claim policy ¥, to prove her authenticity and signs the message under this claim. The cipher text C with signature is c, and is also brought to the cloud. The cloud verifies the signature and also stores the cipher text C. Two readers wants to read simple things, the cloud sends C. If a computer owner has attributes matching with access policy, it can decrypt and retrieve original data. Write proceeds just like as file formation. By labeling the verification process to the cloud, it relieves the individual users from long-drawn-out verifications[1].

Two readers' wants to read simple things some data held in the cloud, it attempts to decrypt it using different features it offers keys it receives from the Key Distribution Centers. If it has enough attributes equivalent when using the access policy, then it decrypts the results held in the cloud as shown in fig 2[1].

Types of Privacy Preserve Policy

1. Pull Based Policy:

In the pull approach, since serving the data is tied to the claim of data, the effort of serving the data is fully utilized. However, since the change (or lack of it) on the attribute value and server capability to serve.

2. The PUSH Based Policy:

In the push approach, since the serving of the data can be done based on the change in the value of attribute, it is more efficient. Though the push approach may seem to be the answer for monitoring.

Identity-Based Group Signature Scheme [7]:

An identity-based group signature scheme is thought to be lots of people of an over-all group signature scheme and an identity-based one is an organization signature, though public key for verification is just the group's identity. It involves the following six algorithms: Setup, Extract, Join, Sign, Verify and Open. An identity-based group signature scheme is an electronic signature scheme was comprised of the following six procedures:

- Setup: On input a burglar alarm 1k, the probabilistic algo outputs the PKG's public key pk and secret key sk.
- Extract: On input PKG's sk secret key and ID identity, sID algorithm outputs.
- Iss/Join: A protocol from the group manager and an individual with identity IDi. The protocol's output is a subscription certificate Ai.
- Sign: A probabilistic algorithm that on input an organization public key ID, a subscription certificate Ai in adding to a message m, output the group signature σ of m.
- Verify: An algorithm takes as input PKG's public key pk plus the group's identity ID, the group signature σ,

what it's all about m, output 1 or 0 to denote accept or reject.

- Open: The deterministic algorithm takes as input what it's all about m, σ signature, sk group manager's secret key to go back the identity underlying the signature.

Access is a user oriented class, as well as authentication and uniqueness stealing issues. Account and service hijacking: Account and service hijacking involves phishing and software susceptibilities where attackers steal credentials and gain an unauthorized the ways to access server [9]. This unauthorized access is a menace to confidentiality, availability, integrity of service and data[9]. Malicious insider: Malicious insiders severely impact the organization. These attacks penetrate corporate and do brand damage, financial and productivity loses [9].

DATA SECURITY IN CLOUD

Different from several fields during which an enormous gap exists between tutorial analysis and business applications, cloud Computing has concerned attentions from each side since the terribly starting. for instance, secure knowledge storage and management is a vital element of the protection steerage. The association of which has the leading firms in cloud computing like eBay, Visa, sun, and McAfee. within the steerage, a secure knowledge outsourcing service ought to be evaluated from a minimum of the subsequent aspects like robust secret writing and climbable key management, user provisioning, de-provisioning, and knowledge lifecycle management and system availableness and performance.

First authenticates a user who desires to put in writing to the cloud. A user should only write provided the cloud is in position to validate it access to the claim. An invalid user cannot receive the attributes from a KDC, if it doesn't have the identifications from the trustee. If a user's identifications are revoked, then it cannot switch data with previous data, thus preventing replay attacks.

1. Access control scheme is secure, collusion resistant and permits access only to authorized users.
2. Authentication of data information is correct, collusion secure, immune to the replay of attacks, and protects privacy of the user.

We tend to make sure that only a legitimate valid user with valid access claim is just able to store the message within the cloud. A user who desire to create a file and tries to make a wrong access claim, cannot do so, thus it'll not have attribute keys Kx from the connected KDCs. Since the message is encrypted, a user without valid access policy cannot decrypt and change the information. A user who wants to create a file and tries to make a wrong access claim, cannot do so, since it will not have attribute keys Kx from the related KDCs. Since the message is encrypted, a user while not valid access policy cannot decrypt and alter the knowledge.

There are certain guidelines that cloud security solution suppliers ought to kept in mind after they distributes their accommodation to cloud accommodation client during a public cloud solution.

Validate the access controls: Set up data access control with rights and then verify these access controls by the cloud service supplier whenever data is getting used by cloud service client. To implement access control strategies for client facet, the cloud service supplier should describe and ensure that the only approved users can access the user or client's data.

Control the client access devices: Make sure the client's access devices or points like gazettes, virtual terminals, Personal Computers, pamphlets and mobile phones are secure enough. His loss of an endpoint access device or access to the device by an unauthorized user can cancel even the best security protocols in the cloud. Be sure the user computing devices are managed properly and supportive advanced authentication structures and secured from malware functioning.

Monitoring Data Access: cloud service suppliers need to assure concerning whom, once and what information is being accessed for what purpose. for instance several web site or server had a security criticism relating to snooping activities by many of us like paying attention to voice calls, reading emails and private information etc..

Share demanded records and Verify the info, data deletion: If the user or client has to report its compliance, then the cloud service supplier can share diagrams or other than data or provide audit records to the patron or user. Conjointly verify the correct deletion of information from shared or reused devices. Several suppliers don't offer for the correct demagnetization of information from drives whenever the drive area is abandoned. Impose the secure deletion method and have that method written into the contract [8]. Security check events: Make sure that the cloud service supplier provides enough details concerning fulfillment of guarantees, break remedy and reportage contingency. These security events can describe responsibility, guarantees and actions of the cloud computing service supplier.

CONCLUSION

The Cloud computing provides facility of knowledge storage and access for cloud users, however once outsourcing {information|the info|the information} to a 3rd party causes safety issue of cloud knowledge thus

data are protected by limiting the information. Anonymous user conjointly access knowledge within the cloud. The cloud solely verifies the user's credentials. One restriction is that the cloud kens the access policy for every record keep within the cloud. In future, we'd relish covering the attributes and accessing policy of a user.

REFERENCES:

1. Sushmita Ruj, Milos Stojmenovic and Amiya Nayak "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, February 2014.
2. Wang, Q. ang, 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.
3. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, pp. 441- 445, 2010.
4. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136- 149, 2010.
5. H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.
6. A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT),pp. 568-588, 2011.
7. Zhusong Liu"A Secure Anonymous Identity-based Access Control over Cloud Data" Fourth International Conference on Emerging Intelligent Data and Web Technologies, IEEE DOI 10.1109/EIDWT.2013.
8. Tackle your client's security issues with cloud computing in 10steps ttp://searchsecuritychannel. techtarget.com/tip/Tackle-your-clients-security-issues- with-cloud-computing-in-10-step
9. Tripathi and A. Mishra, "Cloud computing security considerations," in 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), 2011, pp. 1–5.
10. D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in 15th National Computer Security Conference, 1992.
11. S. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 556–563, 2012.
12. Raju M*, Lanitha B" Review of Cloud Storage in Privacy Access Control" IJSRCSSE Volume 4, Issue 3, March 2014.
13. H. Gonz´alez-V´elez and M. Kontagora: Performance evaluation of MapReduce using full virtualisation on a departmental cloud. Int. J. Appl. Math. Comput. Sci. 21, 275—284 (2011).
14. Ren Kui, Wang Cong, Wang Qian: Security Challenges for the Public Cloud. IEEE INTERNET COMPUTING. 16, 69--73 (2012)
15. Garber Lee: Serious Security Flaws Identified in Cloud Systems. COMPUTER. 44,21—23 (2011)
16. W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in ACM Cloud Computing Security Workshop (CCSW), 2009.
17. 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," in SecureComm, 2010, pp. 89–106.
18. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ACM ASIACCS, 2010, pp. 261–270.
19. G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in ACM CCS, 2010, pp. 735–737.
20. F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in ISPEC, ser. Lecture Notes in Computer Science, vol. 6672. Springer, 2011, pp. 83–97.
21. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in IEEE TrustCom, 2011.
22. R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in ASIACRYPT, ser. Lecture Notes in Computer Science, vol. 2248. Springer, 2001, pp. 552–565.
23. X. Boyen, "Mesh signatures," in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 4515. Springer, 2007, pp. 210–227.
24. D. Chaum and E. van Heyst, "Group signatures," in EUROCRYPT, 1991, pp.257–265.
25. D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," IEEE Computer, vol. 43, no. 6, pp. 79–81, 2010.