Anonymous authentication with Decentralized access control technique in clouds

[1] CHEVULA REKHA, [2] Mr. SHABBIR HUSSAIN

[1]M. Tech Student, Department of CSE ,Nalanda Institute Of Engineering and Technology, Kantepudi Village, SattenapalliMandal. Guntur Dist, Andhra Pradesh, India.

[2] Assistant Professor, Department of CSE ,Nalanda Institute Of Engineering and Technology, Kantepudi Village, Sattenapalli Mandal. Guntur Dist, Andhra Pradesh, India.

ABSTRACT— Cloud computing's multi-tenancy feature, which provides privacy, security and access control challenges, because of sharing of physical resources among untrusted tenants. In order to achieve safe storage, policy based file access control, policy based file assured deletion and policy based renewal of a file stored in a cloud environment, a suitable encryption technique with key management should be applied before outsourcing the data. In this paper a decentralized access control scheme is proposed for secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme. The proposed scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Moreover, the authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized.

1.INTRODUCTION

Cloud computing is a promising computing model which currently has drawn for reaching consideration from both the educational community and industry. By joining a set of existing and new procedures from research areas, for example, Service-Oriented Architectures (SOA) and virtualization, cloud computing is viewed all things considered a computing model in which assets in the computing infrastructure are given as services over the Internet. It is a new business solution for remote reinforcement outsourcing, as it offers a reflection of interminable storage space for customers to have data reinforcements in a pay-as- you- go way. It helps associations and government offices fundamentally decrease their financial overhead of data administration, since they can now store their data reinforcements remotely to third- party cloud storage suppliers as opposed to keep up data centres on their own. Numerous services like email, Net banking and so forth… are given on the Internet such that customers can utilize them from anyplace at any time. Indeed cloud storage is more adaptable, how the security and protection are accessible for the outsourced data turns into a genuine concern. The three points of this issue are availability, confidentiality and integrity. To accomplish secure data transaction in cloud, suitable cryptography method is utilized. The data possessor must encrypt the record and then store the record to the cloud. Assuming that a third person downloads the record, they may see the record if they had the key which is utilized to decrypt the encrypted record. Once in a while this may be failure because of the technology improvement and the programmers. To overcome the issue there is lot of procedures and techniques to make secure transaction and storage.

User Privacy in Cloud Computing :User privacy is also required in cloud. By using privacy the cloud or other users do not know the identity of the other user. The cloud can hold the user accounts for the data in cloud, and likewise, to provide services the cloud itself is accountable. The validity of the user who stores the data is also verified. There is also a need for law enforcement apart from the technical solutions

to ensure security and privacy.The cloud is also prone to data modification and server colluding attacks. The adversary can compromise storage servers in server colluding attack, so that server can modify data files even though the servers are internally consistent. The data needs to be encrypted to provide secure data storage. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques.

Search on Encrypted Cloud Data:Efficient search on encrypted data is also an important fear in clouds. The clouds should not know the query but it can able to return the records that satisfy the query. Searchable encryption used to achieve this scheme.

Security and privacy protection on cloud data:Users Authentication scheme using public key cryptographic techniques in cloud computing. Many homomorphic encryption techniques have been optional to ensure that the cloud is not able to read the data while performing computations on the data. By using this encryption scheme, the cloud receives cipher text of the data and performs computations on the cipher text and returns the encoded value of the result to user then the user is able to decode the result, even though the cloud does not know what data it has operated on. In such circumstances, it must be probable for the

2.RELATEDWORK:

Privacy Preserving Access Control with Authentication for Securing Data in Clouds,

AUTHORS: S. Ruj, M. Stojmenovic, and A. Nayak In this paper, we propose a new privacy preserving authenticated access control scheme for securing data in clouds. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing information. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

Toward Secure and Dependable Storage Services in Cloud Computing

AUTHORS: C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks toward the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanis m, utilizing the homomorphic token and distributed erasurecoded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

Cryptographic Cloud Storage

AUTHORS: S. Kamara and K. Lauter, We consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. We describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve our goal. We survey the benefits such an architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.

Identity-Based Authentication for Cloud Computing

AUTHORS: H. Li, Y. Dai, L. Tian, and H. Yang Cloud

computing is a recently developed new technology for complex systems with massive-scale services sharing among numerous users. Therefore, authentication of both users and services is a significant issue for the trust and security of the cloud computing. SSL Authentication Protocol (SAP), once applied in cloud computing, will become so complicated that users will undergo a heavily loaded point both in computation and communication. This paper, based on the identity-based hierarchical model for cloud computing (IBHMCC) and its corresponding encryption and signature schemes, presented a new identity-based authentication protocol for cloud computing and services. Through simulation testing, it is shown that the authentication protocol is more lightweight and efficient than SAP, specially the more lightweight user side. Such merit of our model with great scalability is very suited to the massive-scale cloud.

Improving Privacy and Security in Multi-Authority Attribute-Based Encryption

AUTHORS: M. Chase and S.S.M. Chow Attribute based encryption (ABE) [13] determines decryption ability based on a user's attributes. In a multiauthority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users, and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase gave a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every ciphertext, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted authorities. Moreover, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user's attributes, which unnecessarily compromises the privacy of the user. In this paper, we propose a solution which removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice.

3. EXSISTING SYSTEM

Existing work on access control in clouds are centralized in nature. All schemes use ABE or symmetric key approach and does not support authentication. Earlier work provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where a single Key Distribution Center (KDC) distributes secret keys and attributes to all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. Therefore, emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. Although a decentralized approach is proposed in some of the existing papers, their technique does not authenticate users, who want to remain anonymous while accessing the cloud. In an earlier work, a distributed access control mechanis m in clouds was proposed. However, the scheme did not provide user authentication. The other draw back was that a user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator. Cloud servers are prone to Byzantine failure, where a storage server can fail in arbitrary ways. The cloud is also prone to data modification and server colluding attacks. In server colluding attack, the adversary can compromise storage servers, so that it can modify data files as long as they are internally consistent. To provide secure data storage, the data needs to be encrypted. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques. Efficient search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to return the records that satisfy the query. This is achieved by means of searchable encryption. The keywords are sent to the cloud encrypted, and the cloud returns the result without knowing the actual keyword for the search. The problem here is that the data records should have keywords associated with them to enable the search. The correct records are returned only when searched with the exact keywords. Security and privacy protection in clouds are

being explored by many researchers. Many homomorphic encryption techniques have been suggested to ensure that the cloud is not able to read the data while performing computations on them. Using homomorphic encryption, the cloud receives cipher text of the data and performs computations on the cipher text and returns the encoded value of the result. The user is able to decode the result, but the cloud does not know what data is has operated on. In such circumstances, it must be possible for the user to verify that the cloud returns correct results.

Disadvantages of Existing system

- The identity of the user is not protected from the cloud during authentication.
- There can be only one KDC for key management.
- Access control of data stored in cloud is centralized.
- Two users can collude and access data or authenticate themselves, if they are individually not authorized.

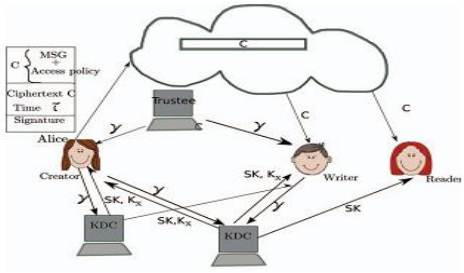
4.PROPOSED SYSTEM

Here we have implemented various methodlogy releted to the security of data or files in clouds system. Basically the data store in clouds my be vulnerable to many kinds of attacks over the clouds system ,securing the data in clouds system must be import tasks for developer to develop a system were all the possible type of attacks can be nullified. Various security level has be implemented over the clouds system which make the clouds system more secured over various types of attacks. - Validate user only access data to read & write.

- Validate owner can upload data to the clouds system.
- The uniqueness of the user and owner is protected from the cloud during validation process with their identification.
- Validate owner can delete data over the clouds by using secret keys.
- The system also has the feature of access control in which only legal users are able to decrypt and encrypt the stored information in clouds system.
- The system prevents replay attacks and supports development, variation, and evaluation data stored in the cloud for both user and owner.
- Secret keys the important part or roles in clouds system.

5.PROPOSED PRIVACY PRESERVING AUTHENTICATED ACCESS CONTROL SCHEME:

(8) In this section we tend to propose our privacy protective attested access management theme. in line with our theme a user will produce a file and store it firmly within the cloud. This theme consists of use of the 2 protocols ABE and ABS, as mentioned in Section III-D and III-E severally. we'll initial discuss our theme in details then offer a concrete example to demonstrate how it works. we tend to visit the Fig. 1. There area unit 3 users, a creator, a reader and author. Creator Alice receives a token γ from the trustee, UN agency is assumed to be honest. A trustee will be somebody just like the federal UN agency manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee offers her a token γ.



Our secure cloud storage model

There are multiple KDCs (here 2), which may be scattered. for instance, these may be servers in numerous elements of the globe. A creator on presenting the token to 1 or a lot of KDCs receives keys for encryption/decryption and language. In the Fig. 1, SKs area unit secret keys given for coding, Kx area unit keys for language. The message MSG is encrypted below the access policy X. The access policy decides UN agency will access the information hold on within the cloud. The creator decides on a claim policy Y, to prove her believability and signs the message below this claim. The ciphertext C with signature is c, and is shipped to the cloud. The cloud verifies the signature and stores the ciphertext C. once a scaner needs to read, the cloud sends C. If the user has attributes matching with access policy, it will rewrite and obtain back original message.

A . Data Storage in clouds:

The user on presenting this token obtains attributes and secret keys from one or additional KDCs. A key for AN

attribute x happiness to KDC Ai is calculated as K x = Kbase1/(a+bx) , where (a, b) ∈ ASK[i]. The user conjointly receives secret keys skx,u for encrypting messages. The user then creates AN access policy X that may be a monotone Boolean perform. The message is then encrypted beneath the access policy as

$$C = ABE.Encrypt(MSG, \mathcal{X})$$

The user conjointly constructs a claim policy Y to modify the cloud to evidence the user. The creator doesn't send the message M SG as is, however uses the time stamp τ and creates H(C)|| τ. This is done to stop replay attacks. If the time stamp isn't sent,then the user will write previous stale message back to the cloud with a sound signature, even once its claim policy and attributes have been revoked. the initial work by Maji et al. suffers from replay attacks. In their theme, a author will send its message and correct signature even once it now not has access rights. In our theme a author whose rights are revoked cannot create a brand new signature with new time stamp and therefore cannot write back stale data.

B. Reading from the cloud:

When a user requests information from the cloud, the cloud sends the ciphertext C mistreatment SSH protocol. Coding income mistreatment algorithm ABE.Decrypt(C,) and therefore the message MSG is calculated.

C. Writing to the cloud:

To write to AN already existing file, the user should send its message with the claim policy as done throughout file creation. The cloud verifies the claim policy and oncondition that the user is authentic and it is allowed to write down on the file.

D. User revocation:

It should be guaranteed that clients ought not to have the adaptability to get to data. Regardless of they have coordinating bargain of qualities. Thus, the proprietor has to change the droop on data and send redesigned information to different clients. The arrangement of individuality will be controlled by the disavowed client is noted and each one clients change their hang on data that have characteristics i ∈ Iu. In accusation afraid dynamically the overall population and mystery keys of the littlest arrangement of qualities that region unit expected to translate the information. We tend to don't believe this prejudice as an after effect of here very surprising data range unit encoded by a proportional arrangement of properties, so such a microscopic arrangement of individuality is entirely unexpected for different clients. For every such information record, the subsequent steps area unit then carried out:

1) A new value of s, snew ∈ Zq is selected.

2) The first entry of vector vnew is changed to new snew.

3) λx = Rxvnew is calculated, for each row x corresponding to leaf attributes in Iu.

4) C1,x is recalculated for x.

5) New value of C1,x is securely transmitted to the cloud.

6) New C0 = M e(g, g) snew is calculated and stored in the cloud.

7) New value of C1,x is not stored with the data, but is transmitted to users, who wish to decrypt the data.

6 EXPERIMENTS

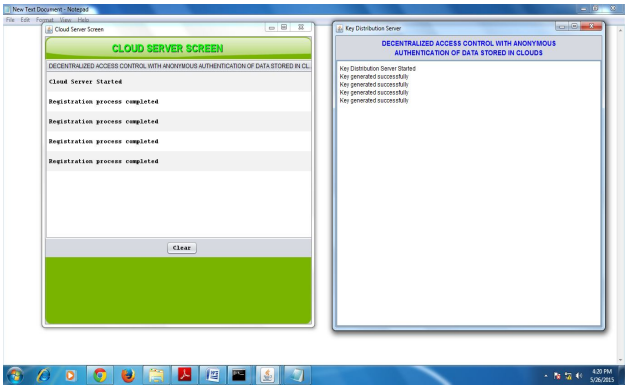
6.1 Experimental Results:

New user has to register

After successfully registering users, one master key will be generated for each user in kdc/keys folder.

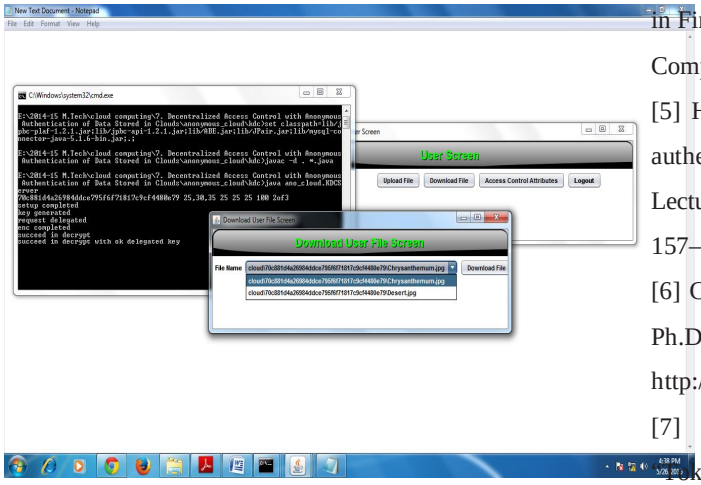
After successfully registering users , cloud space will be assigned for each user in cloud/cloud folder.

After successfully registering the users:



We have given the access permission for the age 25, 30 and 35.

Age 25 people accessing the data:



7.CONCLUSION

In this paper, a decentralized access control technique with anonymous authentication is proposed, which provides user revocation and prevents replay attacks. The files are associated with file access policies, that used to access the files placed on the cloud. More security is assured when uploading and downloading of a file to a cloud is performed with standard Encryption/Decryption techniques. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, the work can be done to hide the attributes and access policy of a user.

8.REFERENCES

[1] 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.

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

[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in IEEE INFOCOM. , pp.441–445, 2010.

[4] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol.6054. Springer, pp. 136–149, 2010.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in CloudCom, ser. Lecture Notes in Computer Science, vol.5931. Springer, pp. 157–166,2009.

[6] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation,Stanford University, 2009, http://www.crypto.stanford.edu/craig.

[7] A.-R. Sadeghi, T. Schneider, and M. Winandy, Token-based cloud computing," in TRUST, ser. Lecture Notes in Computer Science, vol. 6101. Springer, pp. 417–429,2010.

[8] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg,Q. Liang, and B. S. Lee, "Trustcloud: A framework for accountability and trust in cloud computing," HP Technical Report HPL-2011-38. Available at http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure rovenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," in ACM ASIACCS,pp. 282–292, 2010.

[10] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in 15th National Computer Security Conference, 1992.

[32] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in ACM Conference on Computer and Communications Security, pp. 121–130, 2009.

[26] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *EUROCRYPT*,
ser. Lecture Notes in Computer Science, vol. 3494. Springer, pp. 457–473,
2005.

[27] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption
for fine-grained access control of encrypted data," in *ACM Conference on*
Computer and Communications Security, pp. 89–98, 2006.

[29] X. Liang, Z. Cao, H. Lin and D. Xing, "Provably Secure and Efficient

Bounded Ciphertext Policy Attribute Based Encryption," in *ACM ASIACCS*, pp 343–352, 2009.

[35] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *EUROCRYPT*, ser. Lecture Notes in Computer Science, vol. 6632. Springer, pp. 568–588, 2011.

[30] M. Chase, "Multi-authority attribute based encryption," in *TCC*, ser. Lecture Notes in Computer Science, vol. 4392. Springer, pp. 515–534, 2007.

[31] H. Lin, Z. Cao, X. Liang and J. Shao, "Secure Threshold Multi-authority Attribute Based Encryption without a Central Authority," in *INDOCRYPT*, ser. Lecture Notes in Computer Science, vol. 5365, Springer, pp. 426–436, 2008.

[28] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*. , pp. 321–334, 2007.