A survey on Anonymous User Authentication with Secured storage and sharing of data on cloud

Manisha D Karad, Milind Vaidya

Abstract— **In current era cloud computing is highly popular service as far as applications , infrastructure , other platforms for developer are concern. User now prefers to keep data on cloud by considering it is safe and untouched by other users. Sometimes data on cloud is so sensitive like medical records , financial information etc. So it is keen and prime requirement that in one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. Along with this hiding identity of user owns such sensitive information is also one of the important criteria.**

We propose a new decentralized access control scheme for secure data storage in clouds, that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the ser without knowing the user's identity before storing data. 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. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized

Index Terms - Access control , cloud , decentralized , decrypt

INTRODUCTION

Security and privacy are very important issues in cloud computing as far as sensitive data on cloud is concern. Hence sensible information exposure to cloud may sometimes risky. Hence data present on cloud should also be encrypted which helps to hide it from cloud. Though the data is encrypted it must be searchable. It is just not enough to store the contents securely in the cloud but it might also be necessary to ensure anonymity of the user i.e. user identity should hide. To get all these facilities and proper data access protocol , Sushmita Ruj, Milos Stojmenovic, Amiya Nayak [1] proposed a system following decentralized approach in which several modules performs separate tasks like user authentication , encryption key distribution , data storage etc. This decentralized approach manages to hide user identity and secure data from cloud. Before actual implementation of this decentralized control we have to go through some existing approach along with their flaws and benefits.

1)Toward Secure and Dependable Storage Services in Cloud Computing By 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, they propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded 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. But main drawback of system is data is stored as it is on cloud. To secure data it must be encrypted one.

2) Fuzzy keyword search over encrypted data in cloud computing By J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou : As Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud. For the protection of data privacy, sensitive data usually have to be encrypted before outsourcing, which makes effective data utilization a very challenging task.

Manuscript received Jan, 2016.

***Manisha karad**, Computer Department, Savitribai Phule University AVCOE Sangnmer., nashik, India, 9823089909*

***Prof. Milind Vaidya**, Computer Department, Savitribai Phule University AVCOE, Sangnmer., India.*

Although traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords and selectively retrieve files of interest, these techniques support only exact keyword search. That is, there is no tolerance of minor typos and format inconsistencies which, on the other hand, are typical user searching behavior and happen very frequently. This significant drawback makes existing techniques unsuitable in Cloud Computing as it greatly affects system usability, rendering user searching experiences very frustrating and system efficacy very low. In this paper, for the first time they formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. In their solution, they exploit edit distance to quantify keywords similarity and develop an advanced technique on constructing fuzzy keyword sets, which greatly reduces the storage and representation overheads. Through rigorous security analysis, they show that their proposed solution is secure and privacy-preserving, while correctly realizing the goal of fuzzy keyword search.

3)Cryptographic cloud storage By S. Kamara and K. Laute : They 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. They describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve our goal. They 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. The main problem with this is 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.

4)Identity-based authentication for cloud computing By 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. This paper helps us to understand the details regarding user identity verification protocol.

I. PROPOSED SYSTEM

Proposed a decentralized approach; their technique does not authenticate users, who want to remain anonymous while accessing the cloud. In an earlier work, Ruj et al. proposed a distributed access control mechanism in clouds. However, the scheme did not provide user authentication. The other drawback 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. In the preliminary version of this paper, we extend our previous work with added features which enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud. In this version we also address user revocation. We use attribute based signature scheme to achieve authenticity and privacy.

Advantages:

We extend our previous work with added features which enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud.

Proposed system is solution for the bottle neck areas like multi user management on cloud, encrypted data on cloud, searchable encrypted data, data access protocols , user authentication by hiding his identity. Using proposed system and with decentralized approach different key management devices can be arranged that helps to distribute the control concentration. Also this system effectively manages user revocation.

Existing System

Existing work on access control in cloud are centralized in nature. Except and , all other schemes use attribute based encryption (ABE). The scheme in uses a symmetric key approach and does not support authentication. The schemes do not support authentication as well. Earlier work by Zhao *et al.* provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where a single key distribution centre (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. We, 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.

Disadvantage:

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

Before actual looking into details of proposed approach following are some notations with their meaning

A] ϒ : Token Given By Trustee
B] SK : Secret Keys Given by KDC for decryption
C] Kx : These are keys for signing
D] Ci : Cipher text stored on cloud i.e. encrypted data

3.1 System Flow

As per figure 1 there are four application running on at different end connected via LAN, Internet.

The four applications are:

1. User Application
2. Trustee
3. KDC: Key Distribution Server that provide keys for encryption and signature
4. Cloud: Cloud Service provider that store user information

The above 4 applications work collectively as one application. The interfacing between these application is done using API(Application program interface) calling and using HTTP protocol.

The following is the workflow of the system.

Upload Data On Cloud :

1. User Register on trustee by providing his/her personal information

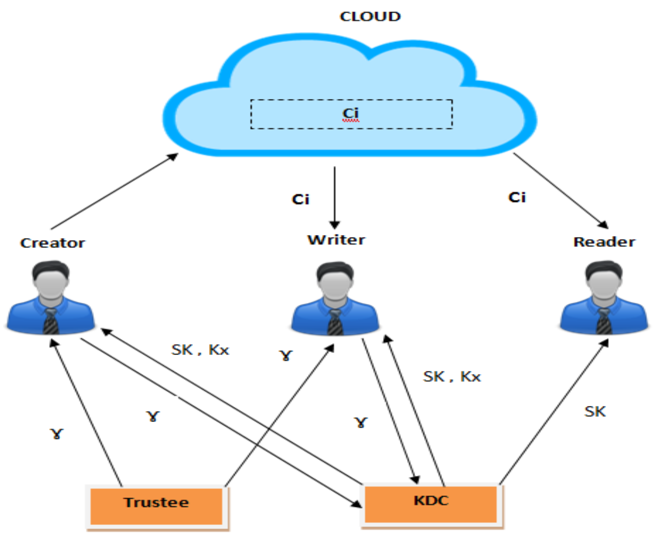

Figure 1 : System Diagram

2. While Login user will token L from the server if he/she is a valid user.
3. Using token L user ask KDC for Keys.
4. KDC provide 4 keys : PK, SK for encryption/decryption and ASK,APK for signing/verifying and KDC token KL
5. Using SK user encrypt the file using Attribute Based Encryption algorithm.
   C = ABE.Encrypt(MSG,SK)
6. User generates authentication policy for file P
7. User signs the encrypted message using SK
   σ = ABS.Sign(L, KL, C, P)
8. The information is send to cloud
9. Following is the information details which is sent to cloud
   c = (C, L, σ, P)
10. At Cloud end, after receiving the data from verifies the access claim using the algorithm ABS.Verify. The creator checks the value of V = ABS.Verify(L,σ, C, P). If V = 0, then authentication has failed and the message is discarded. Else, the message (C, P) is stored in the cloud.

To Download File from Cloud :

- Verification of user is done as per the above process.
- User requests data from the cloud
- The cloud sends the cyphertext C using SSH protocol after matching access permission P.
- Decryption proceeds using algorithm ABE. Decrypt(C, SK) and the message MSG is calculated

When user upload the data , he creates some sharing details having other user privileges. When user wants to revoke particular user then following are steps to be followed

To Revoke user :

Basic principle behind user revocation is owner of data update the privileges details and update data with new keys and send details to group members other than revoked user.

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 = $Me(g,g)^{Snew}$ 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.

We note here that the new value of C1,x is not stored in the cloud but transmitted to the non-revoked users who have attribute corresponding to x. This prevents a revoked user to decrypt the new value of C0 and get back the message.
Here Rx is access matrix of dimension m × h , s is secret key and Snew is new secret key , C1 is new cipher text generated , Co is cipher text generated and stored to cloud.

II. CONCLUSION

Proposed system is decentralized system in which distributed nodes work together for data security on cloud by implementing encryption facility , also these nodes manages multi user tasks like sharing , writing data , reading data etc. Due to this decentralized approach keys are managed at different node hence cloud is not having keys for decryption hence data security is assured. Also KDC is not having data hence only encryption keys are not useful to it. Three types of user like owner , writer and reader has respective access control to the data. Hence this system is also manages hierarchical scenarios as far as user’s role is concern.

III. REFERENCES

1) Sushmita Ruj, Milos Stojmenovic, Amiya Nayak "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" IEEE Transactions on Parallel and distributed system: Vol:25 No:2 Year 2014

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.

9) D. F. Ferraiolo and D. R. Kuhn, “Role-based access controls,” in 15th National Computer Security Conference, 1992.

10) 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 multiowner settings,” in SecureComm, pp. 89–106, 2010.

AUTHER PROFILE

Manisha D Karad received the BE degree in Computer Engineering form University of Pune in 2010. Currently she is pursuing master degree in computer Department Computer Engineering Amrutvahini C. o. E, Sangamner under University of Pune.

Prof. M B Vaidya received the Master degree in Computer ScienceEngineering form University of Pune .He is currently working Assistant Professor Department of Computer Engineering,Amrutvahini colleage of Engg ,Sangamner,Maharashtra,India