ISSN: 2321-7782 (Online)
Volume 4, Issue 3, March 2016
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Attribute based encryption of data stored in Clouds with Anonymous Authentication

Sachin R. Hakke[1]
Department of Computer Engineering
Sinhgad Institute of Technology
Lonavala, India

Prof. Manohar S. Chaudhari[2]
Department of Computer Engineering
Sinhgad Institute of Technology
Lonavala, India

Abstract: ***Plenty of the information keep in clouds is extremely sensitive, for instance, medical records and social networks. Security, safety and privacy are the important issues in cloud computing. In one hand, the user ought to demonstrate itself before initiating any dealing, and on the opposite hand, it should be ensured that the cloud does not tamper with the information that's outsourced. User privacy is additionally needed so the cloud or different users don't apprehend the identity of the user. We propose a brand new localised access control theme for secure information storage in clouds that supports anonymous authentication. Within the planned theme, the cloud verifies the believability of the series without knowing the user's identity before storing information. The scheme prevents replay attacks and supports conception, change, and reading data stored in the cloud. We also address user abrogate. Moreover, our authentication and access to used full control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The Intercourse, computation and storage overheads are comparable to centralized approaches.***

Keywords: ***Distributed Access full control, authentication by anonymous users, attribute-based signatures, encryption of attribute-based, cloud storage overview.***

I. INTRODUCTION

RESEARCH in cloud computing is extracting plenty of attention from each educational and industrial worlds. In cloud computing, users will store their computational work and storage to servers (referred as clouds) mistreatment net. This frees users from the nuisance of maintaining resources on-site. Clouds offers much varieties of services like applications as services (e.g., Google Apps, Microsoft online), infrastructure as services (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to contribute developers to write applications (e.g., Amazon's S3, Windows Azure).

Most of the information keep in clouds is very sensitive including medical records and gregarious networks. Therefore Security and privacy becoming vital problems in cloud computing. At one side the user might to evidence itself before initiating any dealings and on the other conflicting side it must be ensured that the cloud doesn't tampers with the information that is outsourced. In this situation User privacy is additionally needed so that the cloud or different users don't understand the identity of the user. The cloud servers could hold the users accountable for the data it outsources and likewise. The cloud is itself responsible for the services it provides. The validity of the user WHO stores the information is additionally verified. Except to the technical solutions to ensure security and privacy, there is conjointly a necessity for enforcement Recently, Wang et al. [2] self-addressed secure and dependable cloud storage.

II. LITERATURE SURVEY

A.-R. Sadeghi, T. Schneider, and M. Winandy, This paper details about various methods prevailing in literature of anonymous authentication mechanisms for data stored in clouds. It is a Decentralized access of desired system in which every system have the access control of data. The Cloud which is a Secured storage area where the anonymous authentication is must

used, so that only the permitted users can be accessed. Decrypting of data can be viewed by a valid users and can also stored information only by valid users. This Scheme prevents Replay attack which mean Eaves Dropping can be avoided, Support Creation of data inside storage, Reading data stored, and Modifying the data by unknown users in Cloud. User can cancel the data only by addressing through the cloud. The authentication, verification- and accessing the Cloud is Robust, Hence Overall Communication Storage are been developed by comparing to the Centralized approaches. This paper would motivate a lot of research in the area of Anonymous Authentication

Goyal, O. Pandey, A. Sahai, and B. Waters,With the recent adoption and diffusion of the data sharing paradigm in distributed systems such as cloud computing or online social networks there have been increasing demands and concerns for distributed data security. One of the most challenging problem in data sharing systems is the enforcement of access policies and the support of policies updates. Cipher text policy attribute-based encryption (CP-ABE) is becoming a promising cryptographic result to this issue. It enables data owners to define their own access definition over user attributes and enforce the policies on the data to be distributed. However, the profit comes with a major drawback which is known as a key escrow problem. The key generation center could decrypt any messages addressed to individual users by generating their private keys. This is not suitable for data sharing scenarios where the data owner would like to make their private data only accessible to designated users. In addition, applying CP-ABE in the data sharing system introduces next challenge with regard to the user revocation since the access policies are defined only over the attribute universe. Therefore in this study we propose a novel CP-ABEs schemes for a data sharing system by exploiting the characteristic of the system architecture. The proposed scheme features the following achievements: 1) the key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation center and the data-storing center, and 2) fine-grained user revocation per each attribute could be final by proxy encryption which takes the advantage of the selective attribute group key distribution on top of the ABE. The performance and security analyses indicate that the proposed system is efficient to securely manage the data distributed in the data sharing system.

A.B. Lewko and B. Waters, with the recent adoption and diffusion of the data sharing paradigm in distributed systems such as cloud computing or online social networks there have been increasing demands and concerns for distributed data security. One of the most challenging problem in data sharing systems is the enforcement of access policies and the support of policies updates. Cipher text policy attribute-based encryption (CP-ABE) is becoming a promising cryptographic result to this issue. It enables data owners to define their own access policies over user selected attributes and enforce the policies on the data to be distributed.

S. Ruj, A. Nayak, and I. Stojmenovic, 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 into the 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 control 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.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

Propose Work: One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.

Mathematical Model:

1. Recommendation Generation by using following formula for a user with identity U U_u the KDC draws at random

K_{base} £ G. Let K

1=a0 $k_o = k_{base}^1$ □

. The following token is □ output

□= (u, K_{base} , K0, ṗ)

Where ṗ is signature on u K_{base} using the signing key $T_{Sig.}$

KDC Setup

Choose a, b £ Z randomly and compute $A_{ij} = h_j^a$, $B_{ij} = h_j^a$

For A_i £ A, j£ $[T_{max}]$ .The Private Key of ith KDC is

ASK[i] = (a, b) and public key APK[i] = ($(A_{ij}, B_{ij} / jE[t_{max}])$

Attribute Generation:

The token verification algorithm verifies the signature

Contained in □ using the signature verification key T in

TPK. This algorithm extracts K base from □ using (a, b)

From ASK[i] and computes

$K_z = K^{1}_{base}$ x £J [I, j].

the key K_z be checked for consistency using algorithm

ABS Key Check(TPK; APK[i], □ K_x which checks

e($k_r, A_{ij} B_{ij}^x$)=e(K_{base}, h_j),

for all x £ j[i,u] and j £[t_{max}]

Sign the algorithm ABS:

Sign (TPK) {APK[i]:i £AT[u]},

□{ K_z :x £ J_u },MSG,Y),

Has input the public key of the trustee, the secret key of the

Signer, the message to be signed and the policy claimY.The policy claim is first converted into the span program

M £ Z_q^t

With rows labeled with attributes. M_x Denotes

Row x of M. Let $\hat{\Pi}'$

0

Denote the mapping from rows to the

Attributes. So, $\hat{I}\prod^{'}$ (x)

Is the mapping from M_x to attribute x.A

vector v is computed that satisfies the assignment

{x:x£ j[i,u]}. Compute. u = H(MSG||y)Choose r_0 £ Z and r_i

i £ J_u , and compute

Y= $K_{base}^{¿}, S_i = (K_i^u)^f . g_2 g_1^u \ \square_i £ J_u$

W= $K_0^{¿}, P_j = \hat{I}\prod_{iEAt}[u](A_{ij} B_{ij}^i)_{¿}^m ij \quad (\square_j £[t])$

The signature is calculated as

Ó=(Y, W, S1, and S2.....St.P1.P2.....P1).

IV. Conclusion

We propose a fresh localised access control theme for secure info storage in clouds that supports anonymous authentication. At intervals the planned theme, the cloud verifies the credibility of the series while not knowing the user's identity before storing info. The theme prevents replay attacks and supports conception, change, and reading information keep within the cloud. The cloud will not apprehend the identity of the user United Nations agency stores info, but solely verifies the user's credentials. Key distribution is done in a redistributed manner. One limitation is that the cloud is aware of the access policy for every record keep within the cloud. In future, we might prefer to hide the attributes and access policy of a user. We have given a redistributed access management technique with anonymous authentication that provides user revocation and prevents replay attack.

Acknowledgement

This work is partially supported by NSERC Grant CRDPJ386874-09 and the grant: "Digital signal processing, and the synthesis of an information security system," TR32054, Serbian Ministry of Science and Education.

References

1. S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-M. Yiu, SPICE Simple Privacy-Preserving Identity-Management for Cloud Environment, Proc. 10th Intl Conf. Applied to Cryptography and Network Security, 2012.
2. S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng, Dynamic Secure Cloud Storage with Provenance, Cryptography and Security, 2012.
3. C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W.Lou, Privacy Preserving Public Auditing for Secure Cloud Storage, IEEE Trans. Computers, Feb.2013.
4. G. Ateniese, A.D. Santis, A.L. Ferrara, and B. Masucci, Provably Secure Time-Bound Hierarchical Key Assignment Schemes,J. Cryptology, 2012.
5. A. Sahai and B. Waters, Fuzzy Identity-Based Encryption, Proc. 22nd Intl Conf. Theory and Applications of Cryptographic Techniques, 2005.

AUTHOR(S) PROFILE

Sachin Hakke, received the B.E (Bachelor of Engineering) degree in Information Technology from Hi-tech Institute of Technology in 2009. During 2012, 2016 He now research with sinhgad institute of technology department of computer Engineering, Lonavala, India to study cloud computing and network security.