Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2, Issue 11, November -2015

Access Control with Authentication for Securing Data in Clouds

Amey Shapad Agnihotri[1], Vaibhav Hindole[2], Kuber Sadanand Vishwas[3], Dhruv Mishra[4], ,Ashish Neeraj Dharkar[5], Prof. Dipalee Chaudharai[6]

[1-6]Department Of Computer Engineering,Dr.D.Y.PatilCollege Of Engineering Akurdi,Pune

Abstract — *We propose another decentralized access control plan for secure information stockpiling in mists that backings unknown verification. In the proposed plan, the cloud confirms the arrangement's credibility without knowing the client's character before putting away information. Our plan additionally has the included element of access control in which just substantial clients have the capacity to decode the put away data. The plan averts replay assaults and backings creation, adjustment, and perusing information put away in the cloud. We additionally address client denial. In addition, our confirmation and access control plan is decentralized and vigorous, not at all like different access control plans intended for mists which are brought together. The correspondence, calculation, and capacity overheads are tantamount to incorporated approaches.*

Keywords- Access control, authentication, attribute-based signatures, attribute-based encryption, cloud storage

I. INTRODUCTION

RESEARCH in Cloud computing is getting a considerable measure of consideration from both scholarly and mechanical world. In cloud computing, clients can outsource their calculation and capacity to servers (also called clouds) using Internet. This liberates clients from the bothers of keeping up assets on location. Mists can give a few sorts of administrations like applications (e.g., Google Apps, Microsoft online), infra structures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and stages to offer engineers some assistance with writing applications (e.g., Amazon's S3, Windows Azure). Security and protection insurance in mists are being investigated by numerous scientists. Wang et al. [1] tended to capacity security utilizing Reed-Solomon deletion revising codes. Validation of clients utilizing open key cryptographic strategies has been considered in [2].

Numerous homomorphic encryption strategies have been recommended [3], [4] to guarantee that the cloud is not ready to peruse the information while performing calculations on them. Utilizing homomorphic encryption, the cloud gets figure content of the information and performs calculations on the figure content and returns the encoded estimation of the outcome. The client can disentangle the outcome, however the cloud does not realize what information it has worked on. In such circumstances, it must be workable for the client to confirm that the cloud returns right results.

Existing task [5], [6], [7], [8], [9], [10], [11] on access control in cloud are concentrated in nature. But [11] and [11], every single other plan use ABE. The plan in [38] utilizes a symmetric key approach and does not bolster validation. The plans [7], [8], [9] don't bolster verification too. Prior work by Zhao et al. [8] gives protection safeguarding verified access control in cloud. On the other hand, the creators take a concentrated methodology where a solitary key circulation focus (KDC) conveys mystery keys and credits to all clients. Sadly, a solitary KDC is a solitary purpose of is appointment as well as hard to keep up due to the vast number of clients that are upheld 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. Although Yang et al. [12] 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. [9] proposed a distributed access control mechanism in clouds.

II. LITERATURE REVIEW

1) Privacy Preserving Access Control with Authentication for Securing Data in Clouds

AUTHORS: Sushmita Ruj

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.

2) Toward Secure and Dependable Storage Services in Cloud Computing

AUTHORS: Cong Wang

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 flexible distributed storage integrity auditing mechanism, utilizing the homomorphism 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.

3. Fuzzy Keyword Search over Encrypted Data in Cloud Computing

AUTHORS: Jin Li

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. Although traditional search able 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 we formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system us ability 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 our solution, we 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, we show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of fuzzy keyword search.

4. Cryptographic Cloud Storage

AUTHORS: SenyKamara

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 architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage

5. Identity-Based Authentication for Cloud Computing

AUTHORS: Hongwei Li

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.

III. SURVEY OF PROPOSED SYSTEM

We have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. 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.

IV. MATHEMATICAL MODEL

Let S is the Whole System Consist of

S= {I, P, O}.

Where,

I = Input.

I = {U, F}

U = User

F= File

The following information is then sent in the cloud

c = (C, T, σ, ϒ)

C = cipher text

σ = signature

ϒ = Claim policy

T = stamp

O= File Downloaded after decryption.

P = Procedure:

Attribute-Based Encryption:

- **System Initialization:**

Select a prime q, generator g of G0, groups G0 and GT of order q, a map e :

G0 x G0 → GT, and a hash function H : {0,1}* → G0 that maps the identities of users to G0. Thehash function used here is SHA-1. Each KDC Aj ϵ A has a set of attributes Lj. The attributes disjoint.

$$SK[j] = \{\alpha_i, y_i, i \in L_j\}.$$

The public key of KDC Aj is published

$$PK[j] = \{e(g,g)^{\alpha_i}, g^{y_i}, i \in L_j\}.$$

Key Generation and Distribution by KDCs

User Uu receives a set of attributes I[j,u] from KDC Aj, and corresponding secret key ski;u for eachi ϵI[j,u]

$$sk_{i,u} = g^{\alpha_i} H(u)^{y_i},$$

Encryption by Sender:

The encryption function is ABE: Encrypt (MSG, X). Sender decides about the access tree X. LSSS matrix R can be derived as described in Section 3.2. Sender encrypts message MSG as follows:

1. Choose a random seed and a random vector vϵ, with s as its first entry; h is the number ofleaves in the access tree (equal to the number of rows in the corresponding matrix R).

2. Calculate $\lambda_x = R_x \cdot v$, where R_x is a row of R.
3. Choose a random vector $w \in \mathbb{Z}_q^h$ with 0 as the first entry.

5. For each row Rx of R, choose a random px ϵ Zq

6. The following parameters are calculated:

$$C_0 = MSGe(g,g)^s,$$
$$C_{1,x} = e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\pi(x)}\rho_x}, \forall x,$$
$$C_{2,x} = g^{\rho_x} \forall x,$$
$$C_{3,x} = g^{y_{\pi(x)}\rho_x} g^{\omega_x} \forall x,$$

Where,

Л(x) is mapping from Rx to the attribute i that is located at the corresponding leaf of the access tree.Theciphertext C is sent by the sender (it also includes the access tree via R matrix):

$$C = \langle R, \pi, C_0, \{C_{1,x}, C_{2,x}, C_{3,x}, \forall x\}\rangle.$$

Decryption by Receiver

The decryption function is ABE:

1. u calculates the set of attributes $\{\pi(x) : x \in X\} \bigcap I_u$ that are common to itself and the access matrix. X is the set of rows of R.

2. For each of these attributes, it checks if there is a subset X0 of rows of R, such that the vector (1, 0, . . . ,0) is their linear combination. If not, decryption is impossible. If yes, it calculates constants $c_x \in \mathbb{Z}_q$, such that $\sum_{x \in X'} c_x R_x = (1,0,\ldots,0)$.

1. Decryption proceeds as follows:

a. For each $x \in X'$, $dec(x) = \frac{C_{1,x} e(H(u), C_{3,x})}{e(sk_{\pi(x),u}, C_{2,x})}$.

b. U_u computes $MSG = C_0 / \Pi_{x \in X'} dec(x)$.

Attribute-Based Signature Scheme:

- **System Initialization**

Select a prime q, and groups of order q mapping e : G1 x G1→ G2.
generators of G1 and G2.
H hash function.
Where q is chosen at random.
The secret key for the trustee is TSK =(a0,TSig) and public key is
TPK =(G1;G2;H; g1;A0; h0; h1; . . . ; ht max; g2; TV er).

- **User Registration**

For a user with identity U u the KDC draws at random K base . The following token ¥ is output
¥= (u,Kbase,K0,p)

Where p is signature on u || K base using the signing key T Sig

- **KDC Setup**

Choose a, b randomly and compute for The private key of I th KDC is
ASK[i]=(a,b) and public key APK[i]=(Aij,Bij| € t max).

- **Attribute Generation**

Y using the signature verification key TV e r in
TPK. This algorithm extracts Kbase from Y using (a,b)
from ASK[i] and computes Kx=Kbase. The
key Kx can be checked for consistency using algorithm
ABS. Key Check(TPK;APK[i],Y, Kx), which checks

- **Sign**

$$ABS.Sign(TPK, \{APK[i] : i \in AT[u]\},$$
$$\gamma, \{K_x : x \in J_u\}, MSG, \mathcal{Y}),$$

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

signer, the message to be signed and the policy claim Y.

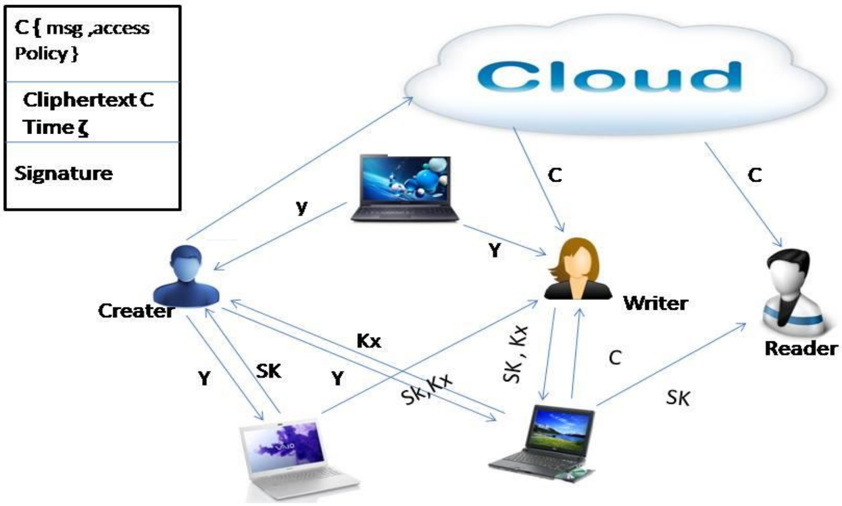
- **Verify**

Algorithm

$$ABS.Verify(TPK, \sigma = (Y, W, S_1, S_2, \dots, S_t,$$
$$P_1, P_2, \dots, P_t), MSG, \mathcal{Y}),$$

OUTPUT: Getting the appropriate file after above privacy preserving & Access Control.

V. SYSTEM ARCHITECTURE



1. Our Secure Cloud Storage Model

.

VI. CONCLUSION AND FUTURE WORK

We have exhibited a decentralized access control procedure with unknown verification, which gives client repudiation and anticipates replay assaults. The cloud does not know the client's character that stores data, yet just checks the client's certifications. Key conveyance is done in a decentralized manner. One impediment is that the cloud knows the entrance arrangement for every record put away in the cloud. In future, we might want to shroud the properties and access approach of a client.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

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] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-Based Authentication for Cloud Computing,” Proc. First Int’l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.

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

[4] A.-R. Sadeghi, T. Schneider, and M. Winandy, “Token-Based Cloud Computing,” Proc. Third Int’l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.

[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. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute Revocation,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.

[7] G. Wang, Q. Liu, and J. Wu, “Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services,” Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.

[8] 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.

[9] 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 (Trust Com), 2011.

[10] http://securesoftwaredev.com/2012/08/20/xacml-in-the-cloud,2013.

[11] W. Wang, Z. Li, R. Owens, and B. Bhargava, “Secure and Efficient Access to Outsourced Data,” Proc. ACM Cloud Computing Security Workshop (CCSW), 2009.

AUTHORS

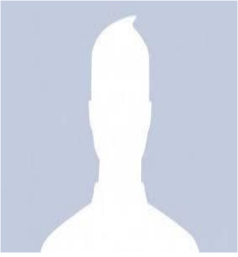
AMEY SHAPAD AGNIHOTRI, pursuing the B.E degree in Computer Engineering at D. Y. Patil College Of Engineering Akurdi, Pune,

VAIBHAV HINDOLE, pursuing the B.E degree in Computer Engineering at D.Y. Patil College Of Engineering Akurdi, Pune,

KUBER SADANAND VISHWAS, pursuing the B.E degree in Computer Engineering at D.Y. Patil College Of Engineering Akurdi, Pune,

DHRUV MISHRA, pursuing the B.E degree in Computer Engineering at D.Y. Patil College Of Engineering Akurdi, Pune,

ASHISH NEERAJ DHARKAR, pursuing the B.E degree in Computer Engineering at D.Y. Patil College Of Engineering Akurdi, Pune,



Prof. Dipalee Chaudharai, Assistant Professor of B.E degree in Computer Engineering at D.Y. Patil College Of Engineering Akurdi, Pune,