International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 4 Issue: 3 22-May-2015,ISSN_NO: 2321-3337

ANONYMOUS SUBSTANTIATION OF INFORMATION STORED IN CLOUDS USING TOKEN VERIFICATION ALGORITHM

N.Priyadharshini,N.kavitha,

Guide Name:Dr.M.Rajendiran,M.Krishnamoorthy

Assistant Professor Department of MCA,

Panimalar Enginnering College.

***Abstract* — *We propose a new anonymous substantiation scheme for secure data storage in clouds. In the proposed scheme, the cloud verifies the authenticity of the series 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*.**

Keywords—component; formatting; style; styling; insert (key words)

I. INTRODUCTION

Clouds can provide several types of services like Applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure).Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and

Privacy are, thus, very important issues in cloud computing. 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. User privacy is also required so that the cloud Or other users do not know the identity of the user.

II. PROPOSED SYSTEM

We propose our privacy preserving authenticated access control scheme. According to our scheme a user can create a file and store it securely in the cloud. This scheme consists of use of the two protocols ABE (Attribute Based Encryption) and ABS (Attribute Based Schema). There are three users, a creator, a reader, and writer. Creator Alice receives a token from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee gives her a token. There are multiple KDCs (here 2), which can be scattered.

ADVANTAGES:

Authentication of users who store and modify their data on the cloud.

The identity of the user is protected from the cloud during authentication

III. EXSISTING SYSTEM

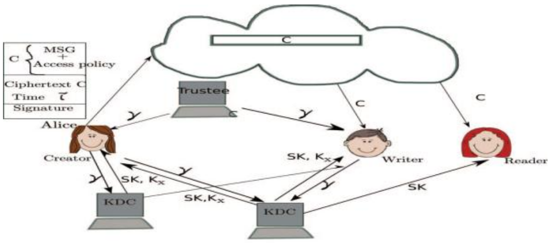
Existing DOSNs use cryptographic primitives that hide the data but reveal the access policies. At the same time there are privacy preserving variants of these cryptographic primitives that do not reveal access policies. They are however not suitable for usage in the DOSN context because of performance or storage constraints.

DISADVANTAGES:

Implemented in Centralized architecture

User Identity is not hidden

IV.SYSTEM ARCHITECTURE



V.MODULE DESCRIPTION

- **Login**

This module authorize user into the system. This adds security to the user data. The login credentials are secured by encryption and they are decrypted back by the server to avoid eavesdropping.

Granting Access

The user who want the data to be shared need to be authorized by the data owner. This is done by requesting for access token and access token is automatically sent to the user. The authorization token is mandatory to access the file. A user with not access token cannot view the file too.

Multiple Access

The module-2 is repeated for many times to grant access to many users. Here the data is not replicated but it is shared and also the data is read only for the users, so every user can read single data at a time. This enables the access anonymously to all the user who have access code.

Access Token Generation

In this module user must log in to the system as data owner and upload the data to the server. This module also has the secure upload facility and request of the user is not recorded (anonymously) to ensure the privacy of the user. The data is transferred from the data owner system to the cloud using http protocol. The access token is generated by the data owner.

VI.CONCLUSION

We have presented a decentralized access control techniquewith 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 in a decentralized way. 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.

VII. 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 Educations.

VIII.REFERENCES

[1]S. Ruj, M. Stojmenovic, and A. Nayak, “Privacy Preserving Access Control with Authentication for Securing Data in Clouds,” Proc.IEEE/ACM Int’l Symp. 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 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.

14th Int’l Conf. Financial Cryptography and Data Security, pp. 136- 149, 2010.

[5] 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.

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

[7] 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.

[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, http://www.hpl.hp.com/techreports/ 2011/HPL-2011-38.html, 2013.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,” Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[10] D.F. Ferraiolo and D.R. Kuhn, “Role-Based Access Controls,” Proc. 15th Nat’l Computer Security Conf., 1992.

[11] 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, June 2010.

[12] 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).