Flexible and Fine Grained Secure Data Storage in Cloud Computing

Sana mokhashi[#1], Rashmi Rachh[*2]
[#]*Sana Mokhashi student VTU CSE Belagavi, India*
[#]*Rashmi Rachh associate Professor VTU CSE Belagavi, India*

Abstract:

Cloud computing is attaining esteem because of the services it offers, although security is yet an issue to be addressed. The data have to be stored securely on top of cloud to keep away as of the security breaches such as data leaks. To guarantee the security as well as achieve flexibly fine-grained file access control, attribute based encryption (ABE) was proposed as well as used in cloud storage system. This project aims to implement cipher text attribute based encryption scheme in which users with matching attributes with the access policy defined by the data owner are able to decrypt the data.

Keywords

cloud computing; attribute based encryption (ABE).

I. INTRODUCTION

Internet usage has been increased expansively in the past few years leading to the production of large data both in case of personal data plus business data. Storage of this data turns out to be a most important concern.

Cloud Computing refers to manipulating, configuring, as well as accessing the applications online. It presents online data storage, infrastructure as well as application. Cloud computing overcomes platform dependency issues. Therefore, the Cloud Computing is making our business application mobile as well as collaborative.

II. RELETED WORK

Rahila Fatima et al. [6] exhibited authorization of access arrangement and approach refreshes are the testing issues in information sharing framework. This issue can be fathomed by utilizing cryptographic systems. Figure content arrangement characteristic based encryption (CP-ABE) is one of the promising arrangements. It empowers information proprietors to characterize their own entrance strategies over client properties and implement the arrangements on the information to be circulated.

V. Monisha et al. [8] clarified that despite the fact that outsourcing information to the cloud is financially appealing for long haul substantial scale stockpiling, it doesn't instantly offer any assurance on information uprightness and classification.

Consequently, it is important to guarantee the clients that the secrecy of their information put away in cloud is safeguarded consistently.

Junbeom Hur etal. [9] Prescribed the absolute most difficult issues in information outsourcing situation are the requirement of approval approaches and the help of arrangement refreshes. Figure content arrangement trait based encryption is a promising cryptographic answer for these issues for upholding access control strategies characterized by an information proprietor on outsourced information. In any case, the issue of applying the property based encryption in an outsourced engineering acquaints a few difficulties with respect with the characteristic and client disavowal.

Dr. M. Newlin et al. [14] recommended that Attribute based encryption (ABE) is an effective encryption strategy utilized as a part of cloud computing, IoT, informal organizations and other innovative fields where security and protection are fundamental prerequisites of the framework. There are distinctive sorts of ABE plans and this article features the highlights of multi-authority quality based encryption (MA-ABE) plans.

Girija Patil et al [15] exhibited in Attribute- based Encryption (ABE) plot, attributes assume a significant part. Credits have been used to create an open key for encoding information and have been utilized as an entrance strategy to control clients' entrance. The entrance arrangement can be separated as either key-approach or figure content strategy.

Hiroaki Anada et al. [17] proposed a method of exclusively adjusting a attribute based encryption(ABE) secure against chosen plaintext assaults (CPA) into an ABE plot secure against chosen cipher text assaults (CCA) in the standard model. This shows the system on account of the Waters cipher-text strategy ABE (CP-ABE). Our system is useful when a Diffie-

Hellman tuple to be checked is in the terminal gathering of a bilinear guide.

III SYSTEM DESIGN

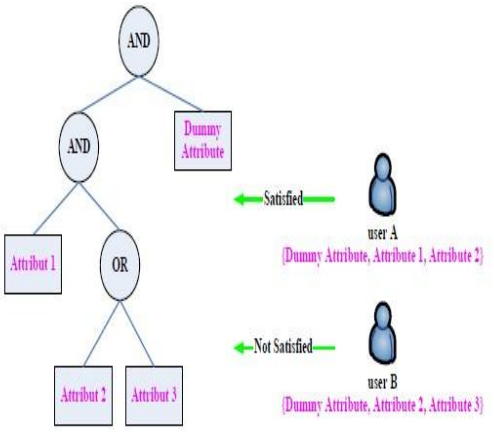


Fig 1.1: Access tree used in encryption [10]

V. RESULTS

TA is a trusted authority who validates user's attribute sets as well as creates corresponding private keys designed for them.

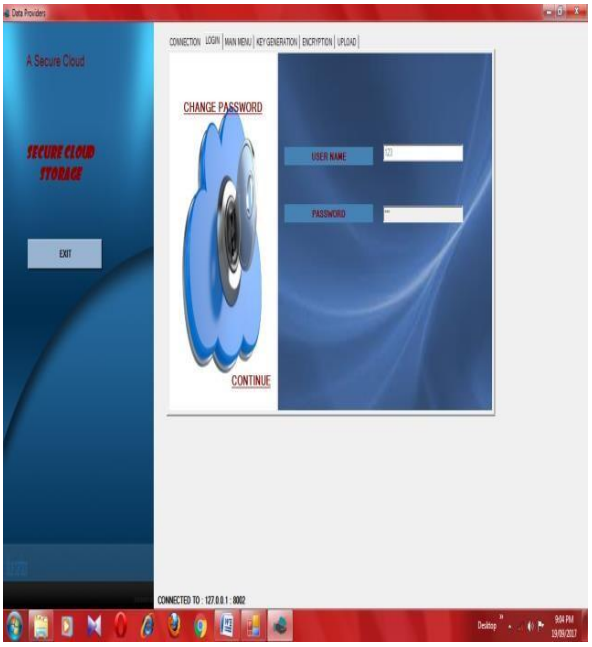
GM is a trustworthy group executive who produces certificates meant for users, renews the private keys of clients, as well as applies CSS used for re-encryption functions.

CSS in our procedure related with the sub-tree is outsourced on the way to E-CSP. To firmly farm out decryption procedure with weighty bilinear calculation, client's private key is unsighted as in [11].

structure needs to be satisfied by the user as well as public key K0 returns cipher text CT. This algorithm is designed in such a way that the users holding satisfying attributes which satisfies the access structure T be able to decrypt the cipher text and retrieve the data.

• **Key-Generation.** This algorithm takes as input master key MK public key PK as well as attributes set of user returns the secret key SK.

• **Decryption.** The decryption algorithm Dec (CT, SK, PK) :Input to this algorithm is cipher text CT, secret key SK as well as public key PK then outputs a encrypted message M .If the equation T(A)=1 then only the algorithm outputs the message M otherwise it will shows an error .



IV SYSTEM IMPLEMENTATION

This chapter deals with implementation of CP-ABE scheme using four main algorithms which are very fundamental for the implementation CP-ABE scheme.

• ***Setup:*** This algorithm setup (k) takes a security parameter as an input and returns the public key PK and master key MK.

• ***Encryption.*** The algorithm Enc (M, T, PK) takes as input message M, access structure T this access

VI. CONCLUSIONS

The cipher text attribute based encryption scheme has been implemented in this project .This work can be extended for management of revoked users in system as a future work. . The issue of user revocation can be solved efficiently by introducing the concept of user group. When any user leaves, the group manager will update users' private keys except for those who have been revoked

REFERENCES

[1] A.Sahai and B. Waters, "Fuzzy Identity-Based Encryption,"EUROCRYPT'05, LNCS, vol. 3494, pp. 457-473, 2005.

[2] J.Bethencourt, A. Sahai and B. Waters, "Cipher text-Policy Attribute –Based Encryption, "Proc. IEEE Symposium on Security and Privacy, pp.321-334, May 2007, doi:10.1109/SP.2007.11.

[3] V.Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, "Proc.13th ACM Conference on Computer and Communications Security (CCS '06), pp. 89-98, 2006, doi:10.1145/1180405.1180418.

[4] D.Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal of Computing, vol. 32, no. 3,pp. 586-615,2003.

[5] A.Boldyreva, V. Goyal, and V. Kumar, "Identity- Based Encryption with Efficient Revocation,"Proc.15th ACM conference on Computer and communications security(CCS ' 08),pp. 417-426,2008.

[6] Rahila Fatima, Dr. S. S. Lomte, Saad Siddiqui "Attribute - Based Data Sharing" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 10, October 2015

[7] V.Monishaa, N.R. Rejin Paul" An Efficient Re-encryption Scheme for Secure and Scalable Data Storage in Cloud**"** International Journal of Computer Science and Engineering Communications Vol.3, Issue 3, 2015, Page.1069-1075

[8] P.K. Tysowski and M. A. Hasan, "Hybrid Attribute- Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds," *IEEE Transactions* on Cloud Computing, pp. 172-186, 2013.

[9] Junbeom Hur and Dong Kun Noh"Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 7, JULY 2011.

[10] Jiguo Li, Wei Yao, Yichen Zhang, Huiling Qian and Jinguang Han "Flexible and fine gained data storage in cloud computing " IEEE TRANSACTIONS ON JOURNAL NAME, MANUSCRIPT ID

[11] M.Green, S. Hohenbergerand B. Waters, "Outsourcing the decryption of ABE ciphertexts,"Proc.20th USENIX Conference on Security (SEC '11), pp. 34, 2011.

[12] J.Li, X.F. Chen, J.W. Li, C.F. Jia, J.F. Maand W.J. Lou, "Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryp-tion,"Proc.18th European Symposium on Research in Computer Security(ESORICS '13),LNCS8134,Berlin: Springer-Verlag, pp. 592-609, 2013.

[13] J.W. Li, C.F. Jia, J. Liand X.F. Chen, "Outsourcing Encryption of At-tribute-Based Encryption with Mapreduce,"Proc.14th International Conference on Information and Communications Security (ICICS '12), LNCS7618, Berlin: Springer-Verlag, pp. 191-201, 2012.doi:10.1007/978-3-642-34129-8_17

[14] Dr.M.Newlin Rajkumar, Ancy George, Brighty Batley"An Overview of Multi-Authority Attribute Based Encryption Techniques "International Journal of Advanced Research in Computer and Communication EngineeringVol. 3, Issue 9, September 2014

[15] Girija Patil" Privacy-Preserving Decentralized Key Policy Attribute-Based Encryption" Girija Patil / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6), 2014, 8225-8228

[16] J.G. Han, W. Susilo, Y. Mu and J. Yan, "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption, "IEEE Transactions on Parallel and Distributed Systems,vol.23, no.11, pp. 2150-2162, Nov 2012, doi: 10.1109/TPDS.2012.50.

[17] Hiroaki Anada, Seiko Arita" Short CCA-Secure Cipher text-Policy Attribute-Based Encryption" 978-1- 5090-6517-2/17/$31.00 ©2017 IEEE