iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4078

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Review Paper on Data Access Control using CP-ABE for Multi-Authority Cloud Storage System

Chetan Mane[1], Snehal Garud[2], Aishwarya Phalke[3], Suwarna Kapase[4], Deepak Waghmare[5]
[1,2,3,4,5] *Department of Computer Science and Engineering, YSPM's Yashoda technical Campus, Shivaji University, Satara, India.*

Abstract: ***Cloud computing is the system on which we can store data over a network and easily access it from anywhere. But in the case of public cloud storage systems, access control is a most concerning issue[4]. Cipher-text-Policy Attribute-Based Encryption (CP-ABE) is the most excellent technique to provide efficient and secure data access control for public cloud storage. Existing CP-ABE schemes offers single attribute authority to perform user legitimacy verification and also distributing secret keys, and as a result, performance degrades in the case of the large-scale cloud storage system. Users may be a long time waiting to obtain their secret keys, hence efficiency decreases[10]. In this paper, the system employs multiple attribute authorities to share the load of user legitimacy verification. CA (Central Authority) is there to generate secret keys for legitimacy verified users. Each of the authorities in scheme manages the whole attribute set individually. When any user accesses any type of data, AA informs the owner of respective data by a message containing username and details of data that user has been accessed. Auditing mechanism is there to detect which AA (Attribute Authority) is improperly performed the user legitimacy verification procedure.***

Keywords: AA (Attribute Authority), Access control, Auditing, CA (Central Authority), Cipher-text-Policy Attribute-Based Encryption (CP-ABE), Cloud storage.

I. INTRODUCTION

The term Cloud refers to a Network or the Internet. In other words, we can say that Cloud is something, which is present at a remote location. Cloud can provide services over the network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in a cloud. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., servers , networks, services, applications , storage) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1].

Cipher-text-Policy Attribute-Based Encryption (CP-ABE) is known as best promising technique as CP-ABE give data owners direct control based on access policies. In CP-ABE schemes, the access control is achieved by using cryptography, where an owner's data is encrypted with an access structure over attributes, and a secret key is labeled with user's own attributes[2][5][6]. Only with the attributes associated with the user's secret key which satisfy the access structure, can the user decrypt the respective ciphertext to obtain the plaintext.

CP-ABE schemes are not efficient since there is only single authority for all attributes, unavailability of this authority causes unavailability of a secret key to users[3]. In single authority schemes, only authority is responsible for checking the legitimacy of users before sharing secret keys with them and hence when it is not available, a user may have to wait for a long time to obtain secret key.

The solution to problems created due to single authority schemes is using multi-authority schemes which jointly manage universal authority sets such that each attribute is able to share secret keys to users independently[9]. By using multiple authorities, a load of user legitimacy verification on single authority is reduced[11].

In this paper, we use the system containing AA (Attribute Authority), which is responsible for performing user legitimacy verification and send an intermediate request to CA for obtaining secret key. CA (Central Authority), which is responsible for generating secret keys on the basis of intermediate request getting from AA, CA sends a secret key to AA without performing any verification. CA also generate a public key and distribute both keys. In this ways, multiple authorities work simultaneously and reduce time consumed process for user legitimacy verification procedure by a single authority. With the help of intermediate keys, CA is able to trace AA's mistakes related to verification procedure.

II. RELATED WORK

A. Attribute Based Data Sharing with Attribute Revocation[8]

This system uses semi-trusted on-line proxy servers and it enables the authority to revoke any user attributes without greater effort. This system uniquely integrated the technique of proxy re-encryption with CP-ABE, and also enables the authority to assign most of the lengthy tasks to proxy servers. The advantage of this system is More Secure against chosen ciphertext attacks. It provides importance to attribute revocation which is difficult for CP-ABE schemes.

1) Drawback: The storage overhead could be high if proxy servers keep all the proxy re-key.

B. Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems[15]

In this paper, an access control mechanism using CP-ABE to implement access control policies with efficient attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which takes advantage of the ABE and selective group key distribution in each attribute group.

1) Drawback: Huge issue in the implementation of authorization policies and the support of policy updates.

C. DACC: Distributed Access Control in Clouds[13]

In this paper, cloud stores the data without information about decryption. one or more Key Distribution Centers distribute keys to data owners and users. KDC may provide access to particular fields in several records. as a result, a single key replaces separate keys from owners. Owners and users are assigned a certain set of attributes. Owner encrypts the data with his attributes and stores them in the cloud. The users with an identical set of attributes can retrieve the data from the cloud. two users cannot together decode any data that none of them has individual right to access.

1) Drawback: Technique is only efficient in truthful networks; we have to care in case of un-trusted networks.

D. Scalable and Secure Sharing of Personal Health Records in Cloud Computing using ABE[14]

In this paper, information is stored on semi-trusted servers, the encryption techniques from Multi-authority ABE and Key-Policy ABE are combined into a single module. Use of MA-ABE technique proves useful for key management and KP-ABE handles security threat of colluding users.

1) Drawbacks: 1. Existing attribute revocation methods depends on a trusted server.
2) They are not suitable for dealing with the attribute revocation problem in data access control in multi-authority cloud storage systems.
3) Lack of efficiency in system mechanism.

E. Improving Privacy and Security in Multi-Authority Attribute-Based Encryption[12]

CA has the power to decrypt every ciphertext which may be conflicting user's privacy. In this paper, a system does not contain central authority and protects the users' privacy by preventing the authorities from pooling their information on particular users, as a result making ABE more usable in practice.

1) Drawback: The system provides less secrecy about encryption because control is handled by many authorities.

F. Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation[7]

Easier architecture supports fine-grained access control policies and dynamic group membership by using ABE. It is possible to remove access from a user without issuing new keys to other users or re-encrypting existing ciphertexts. Easier contains a proxy that participates in the decryption process and enforces revocation constraints. The proxy is minimally trusted and cannot decrypt ciphertexts or provide access to previously revoked users.

1) Drawback: Provides fewer security factors than using CP-ABE scheme.

G. Cipher Text Policy Attribute Based Encryption with Anonymous Access Policy[16]

In this paper, access policy does not sent with the ciphertext, by which we are able to preserve the privacy of the encryptor. The system is constructed under Decision Bilinear Diffe-Hellman assumption which is secure.

1) Drawback: There is key escrow problem.

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

III. PROBLEM STATEMENT

To implement multi-authority data access control for cloud storage system with attribute-based encryption.

IV. SYSTEM MODEL

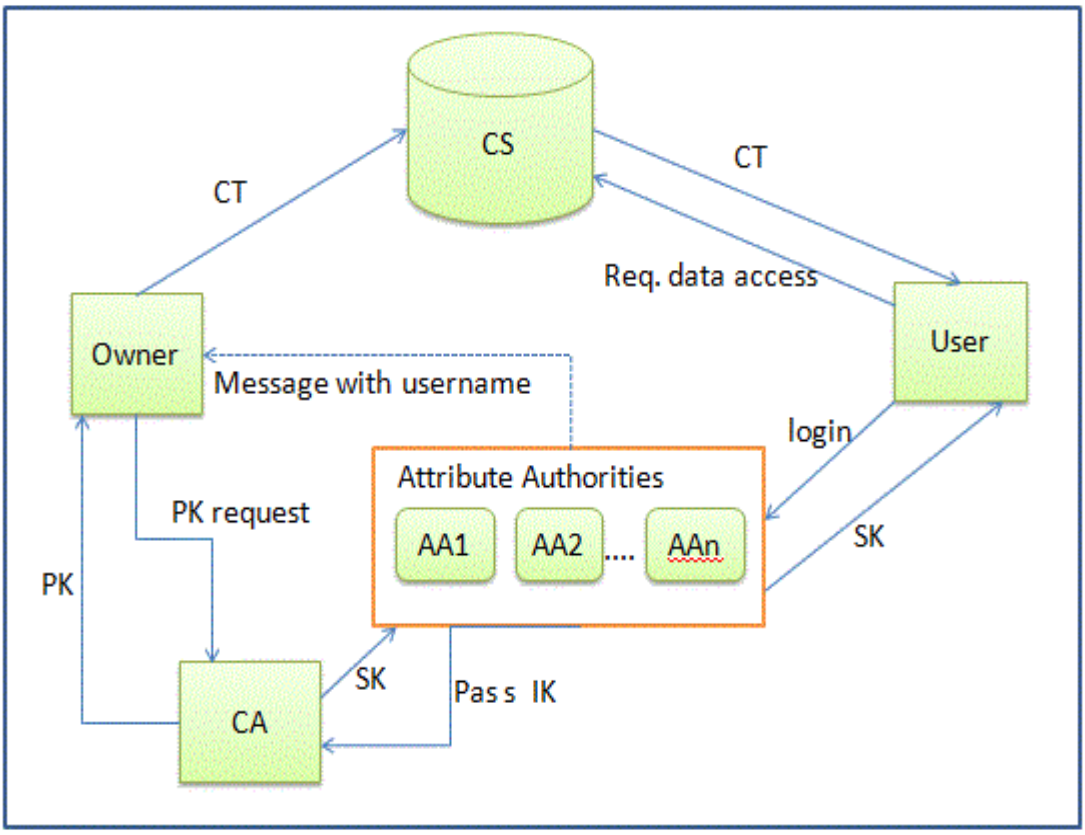


Fig. 1 System Architecture

As shown in fig.1, system model shows five entities: central authority (CA), multiple attribute authorities (AAs), data owner (Owners), data consumer (Users), and a cloud service provider.

A. AA (Attribute Authority)

It is responsible for user legitimacy verification procedure, and then sending an intermediate key to CA for legitimacy verified users. AAs can work simultaneously to perform user legitimacy verification. When any user accesses any type of data, AA informs the owner of respective data by a message containing the username.

B. CA (Central Authority)

It is responsible for generating secret keys and public keys. It generates a secret key on the basis of received intermediate key from AAs. As a main part of the system, CA has the capacity to trace misbehavior of AA during user legitimacy verification procedure.

C. Data Owner (Owner)

A person who encrypts the data under symmetric encryption algorithm. The owner also encrypts the symmetric key under the policy according to a public key received from CA. After that, Owner stores this encrypted symmetric key and data onto the cloud.

D. User

A user has the set of attributes and the secret key associated with it. The user can easily get encrypted data from a cloud but he is able to decrypt it if and only if his/her attribute set satisfies access policy relating encrypted data.

E. Cloud Server

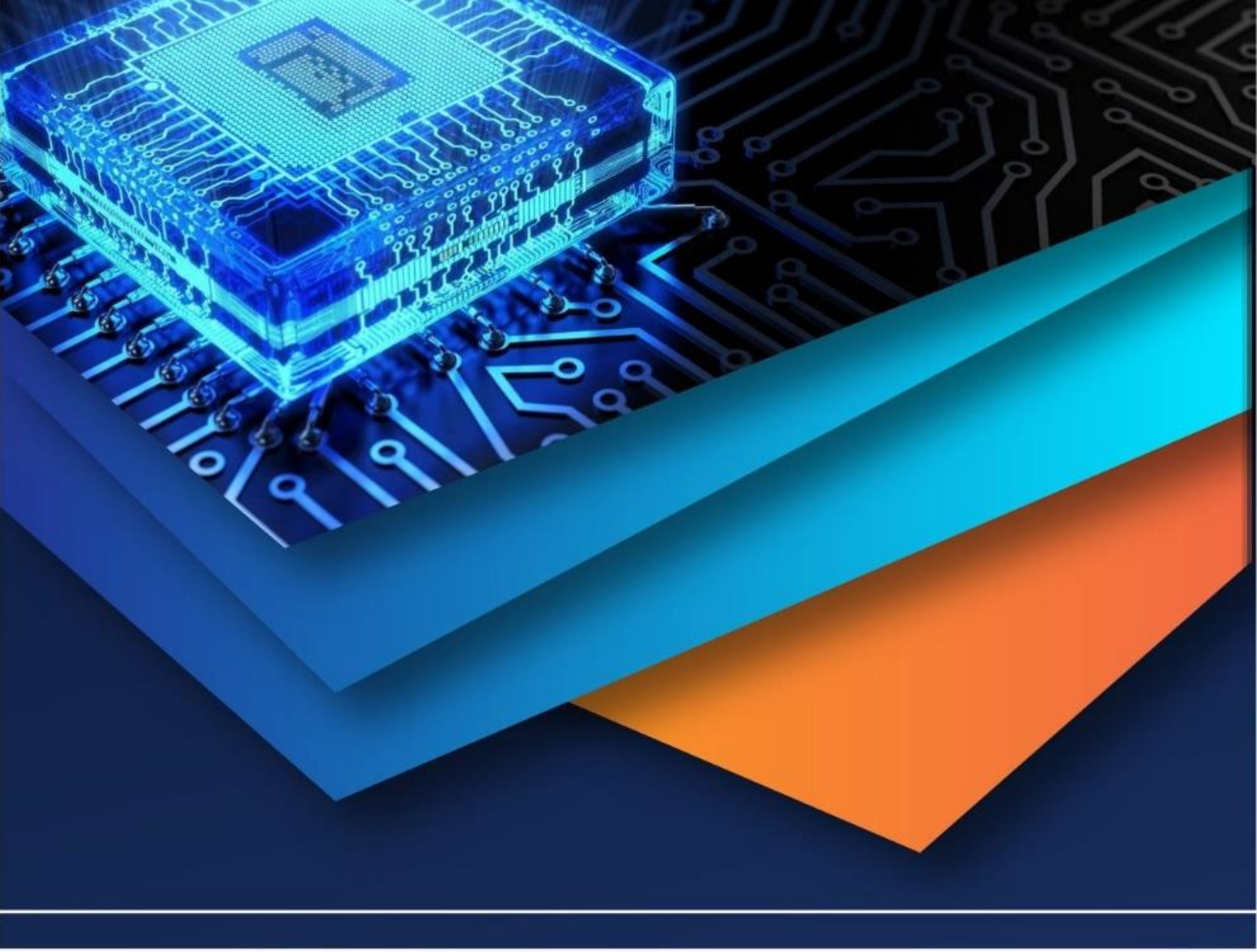
It introduces global and public platform for owners to store their encrypted data onto a cloud. Any user is able to download the encrypted data.

V. CONCLUSIONS

Cipher-text-Policy Attribute-Based Encryption (CP-ABE) used as a promising technique to provide secure data access control and employs multiple attribute authorities to share the load of user legitimacy verification. A Central authority (CA) is generating secret keys. Auditing mechanism detects which Attribute Authority (AA) incorrectly or maliciously performed the legitimacy verification procedure.

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology Gaithersburg, 2011.
[2]] Kaiping Xue, Yingjie Xue, Jianan Hong, Wei Li, Hao Yue,“RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage”, IEEE Trans. on Information Forensics and Security 2016.
[3] K. Chandrasekaran and Manoj V. Thomas, "Distributed Access Control in Cloud Computing Systems," John Wiley & Sons, Ltd. 2016.
[4] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, “Enabling personalized search over encrypted outsourced data with efficiency improvement,” IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 9, pp. 2546–2559, 2016.
[5] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271–2282, 2013.
[6] M. Chase and S. S. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in Proceedings of the 16th ACM conference on Computer and Communications Security (CCS 2009). ACM, 2009, pp. 121–130.
[7] S.Jahid, P.Mittal, and N.Borisov, „„Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,‟‟‟‟ in Proc. 6th ACM Symp. Information, Computer, and Comm. Security (ASIACCS‟‟11), 2011, pp. 411-415.
[8] S.Yu, C.Wang, K.Ren, and W.Lou, Attribute Based Data Sharing with Attribute Revocation,‟‟‟‟ in Proc. 5th ACM Symp. Information, Computer, and Comm. Security (ASIACCS‟‟10), 2010, pp. 261-270.
[9] K. Xue and P. Hong, “A dynamic secure group sharing framework in public cloud computing,” IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.
[10] Peidong Sha ,Zhixiang Zhu,”The modification of RSA to adapt fully homomorphic encryption algorithm in cloud computing”, 4th international conference on cloud computing and intelligence systems(CCIS),2016
[11] W. Li, K. Xue, Y. Xue, and J. Hong, “TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage,” I EEE Transactions on Parallel & Distributed Systems, vol. 27, no. 5, pp. 1484–1496, 2016
[12] Melissa Chase, Sherman S.M. Chow∗ Improving Privacy and Security in Multi-Authority Attribute-Based Encryption, 2009 ACM
[13] S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed access control in clouds,” in Proceedings of the 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2011). IEEE, 2011, pp. 91–98.
[14] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou, “Scalable and secure sharing of personal health records In cloud computing using ABE ”, IEEE transactions on parallel and distributed systems, vol. 24, no. 1, January 2013.
[15] 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.
[16] A Balu, K.Kuppusamy, Ciphertext policy Attribute-based Encryption with anonymous access policy, International Journal of peer-to-peer networks (IJP2P), October 2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY