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.2017.4177

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)

TMACS: a robust and verifiable threshold multi-authority access control system in public cloud Storage

Ardra K[1], T Sivakumar [2]
Computer Science and Engineering, Anna University, Chennai

Abstract: ***It greatly attracts attention and interest from both academia and industry due to the profitability, but it also have challenges that must be handled before coming to our real life to the best of our knowledge. Data confidentiality should be guaranteed. The data privacy is not only about the data contents. Since the most attractive part of the cloud computing is the computation outsourcing, it is far beyond enough to just conduct an access control. Secondly, personal information (defined by each user's attributes set) is at risk because one's identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client's personal information. Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers.***
Keywords—Multi-Authority Access Control System, TMAACS

I. INTRODUCTION

This Project is to prevent the single-point bottleneck problem on both security and performance in existing schemes. In which multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. In this paper, from another perspective, we conduct a threshold multi-authority CP-ABE access control scheme for public cloud storage, named TMACS, in which multiple authorities jointly manage a uniform attribute set. Since in CP-ABE schemes, there is always a secret key used to generate attribute private keys, we introduce (*t*, *n*) threshold secret sharing into our scheme to share the secret key among authorities.

A. System Details

1) *Exiting System:* In Existing schemes involve only one authority to maintain the whole attribute set, which can bring a single-point bottleneck on both security and performance. Subsequently some multi-authority schemes are proposed in which multiple authorities separately maintain disjoint attribute subsets however single-point bottleneck problem remains unsolved.
2) *Proposed System:* In this proposed system, we implemented a technique called TMAC (Threshold Multi Access Cloud Storage.). This system will overcome the drawback of single bottle neck problem. This System consist of Multiple Attribute Authorities (Admin) but they are not inter linked between each other's. So the Unauthorized users cannot be compromise the Admin for Legal user's private key. So, the Legal Users can get the Provide Keys by requesting any t authorizes. So the Private Key transmission is more secured.

II. ARCHITECTURE

Architecture diagram (Figure 1) shows the relationship between different components of system.

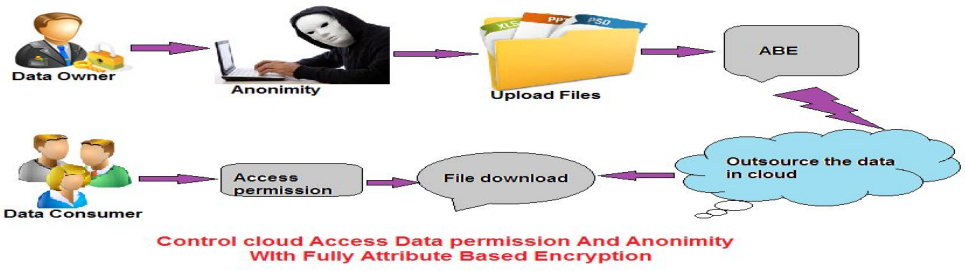


Figure 1: System Architecture

©IJRASET: All Rights are Reserved

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

There are three modules present in this architecture. Data Owner, Data User and Attribute Authorities.

A. Data Creator Module

1) Owner Authentication
2) Accepting key from CA (Public key)
3) Data Encryption

B. Data User Module

1) User Authentication
2) Request Private Key to AAs
3) Collect Private Key from AAs
4) Decrypting Data

C. Attribute Authority

1) Authentication
2) Verify and Forward Private key to Data user.

III. RESULTS

The results of Threshold Multi Access Control System in Cloud Storage are as follows.

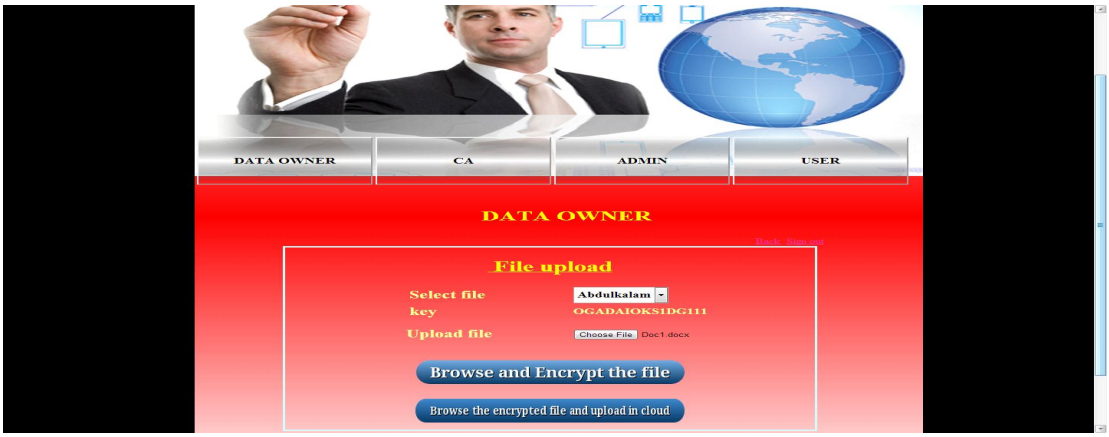


Figure 1: Owner Receiving Public key Key and Uploading Encrypted file

Figure 2: Public Key Generation By CA

©IJRASET: All Rights are Reserved

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

Figure 3: Account Activation by CA

Figure 4: User's Key Request to Admin

Figure 5: File decryption by User

©IJRASET: All Rights are Reserved

IV. FUTURE WORK

In this paper we Propose Threshold Multi-Authority Access Control System. In regards to future work we can Plan to Make Certified Authority to involve Generation of Both Public key and Private key instead to Attribute Authorities. This will make Security for Private key sharing to Legal User.

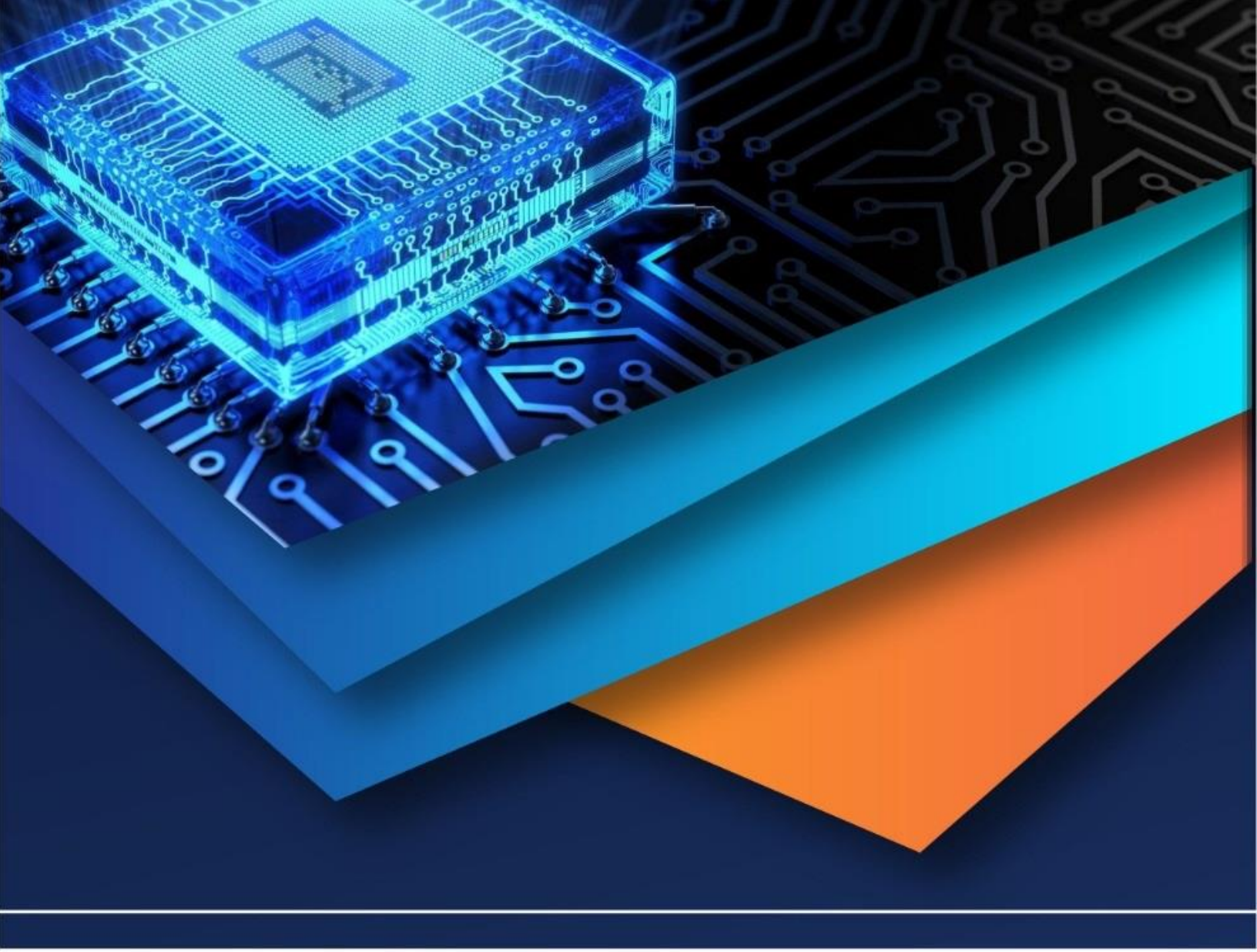
V. CONCLUSION

This paper proposes a semi-anonymous attribute-based privilege control scheme Anonymity Control and a fully-anonymous attribute-based privilege control scheme Anonymity Control to address the user privacy problem in a cloud storage server. Using Attribute authority in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information.

REFERENCES

[1] Bethencourt J, Sahai A and Waters B (2007), "Ciphertext-policy attribute- based encryption," in Proc. IEEE SP, pp. 321–334.
[2] Chase M (2007), "Multi-authority attribute based encryption," in Theory of Cryptography. Berlin, Germany: Springer-Verlag, pp. 515–534.
[3] Chase M and Chow S S M (2009), "Improving privacy and security in multi-authority attribute-based encryption," in Proc. 16th CCS, pp. 121–130.
[4] Goyal V, Pandey O, Sahai A and Waters B (2006), "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th CCS, pp. 89–98.
[5] Sahai A and Waters B (2005), "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, pp. 457–473.
[6] Shamir A (1985), "Identity-based cryptosystems and signature schemes," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, pp. 47–53.
[7] Lin H, Cao Z, Liang X, and Shao J (2010), "Secure threshold multi authority attribute based encryption without a central authority," Inf. Sci., vol. 180, no. 13, pp. 2618–2632.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)