ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Providing Access Permissions to Legitimate Users by Using Attribute Based Encryption Techniques In Cloud

R.Udhayakumar[1], M. Jawahar[2], I.Ramasamy[3]

PG Student, Dept. Of CSE,KSR Institute For Engineering And Technology, Tiruchengode, India [1]

Asst. Prof., KSR Institute For Engineering And Technology, Tiruchengode, India [2]

PG Student, Dept. Of CSE, Fatima Michael College of Engineering and Technology, India [3]

Abstract—***Clouds are being used to store sensitive information about patients to enable access to medical professionals, hospital staff, researchers, and policy makers. It is important to control the access of data so that only authorized users can access the data. This scheme proposed validity of the message without revealing the identity of the user who has stored information in the cloud and also added feature of access control in which only valid users are able to decrypt the stored information. In Attribute Based Signature scheme to achieve versatile primitive users can allows a party to sign a message with fine-grained control over identifying information. In ABS, a signer, who possesses a set of attributes from the authority, can sign a message with a predicate that is satisfied by his attributes. The signature reveals no more than the fact that a single user with some set of attributes satisfying the predicate has attested to the message.***

Keywords— **Access control, Authentication, Attribute-based signatures, Attribute-based encryption, Cloud security.**

I. INTRODUCTION

In today's competitive environment, the service dynamism, elasticity, and choices offered by this highly scalable technology i.e. Cloud Computing are too attractive for enterprises to ignore. These opportunities, however, don't come without challenges, in the world of Information Technology cloud computing is the most exciting topic. Many organizations in the market are now adopting this technology. However, security and privacy are perceived as primary obstacles to its wide adoption. There are several critical security challenges and which motivate further investigation of security solutions for a trustworthy public cloud environment.Cloud computing is the newest term for the long-dreamed vision of computing as a utility. The cloud provides convenient, on-demand network access to a centralized pool of configurable computing resources.

A. Contributions

The main contributions of this paper are the following:

1) Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them.
2) Authentication of users who store and modify their data on the cloud.
3) The identity of the user is protected from the cloud during authentication.
4) The architecture is decentralized, meaning that there can be several KDCs for key management.
5) The access control and authentication are both collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized.
6) Revoked users cannot access data after they have been revoked.
7) The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information.
8) The protocol supports multiple read and write on the data stored in the cloud.
9) The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud.

II. RELATED WORK

Clouds are being used to store sensitive information about patients to enable access to medical professionals, hospital staff, researchers, and policy

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

makers. It is important to control the access of data so that only authorized users can access the data. Using ABE, the records are encrypted under some access policy and stored in the cloud. Users are given sets of attributes and corresponding keys. Only when the users have matching set of attributes, can they decrypt the information stored in the cloud.

III. EXISTING SYSTEM

Large number of data can be 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. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of he user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement.

A. Disadvantage

a) Lack in security.
b) More energy consumption.
c) More computational time.
d) Not efficient.

IV. PROPOSED SYSTEM

An access control model to enforce controlled information sharing in emergency situations is proposed. Model is able to enforce flexible information sharing within a single organization through the specification and enforcement of emergency policies.

Emergency policies allow the instantiation of temporary access control policies that override regular policies during emergency situations., each emergency is associated with one or more tacp templates, describing the new access rights to be enforced during specific emergency situations.

In emergency management scenarios the response plans are defined by experts on the field based on regulations and laws and based on reports resulting by the emergency preparedness phase, during which emergency managers conduct a risk assessment. That all these documents represent a solid base from which emergencies, emergency policies, and emergency obligations can be specified as shown in Fig 1.1.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

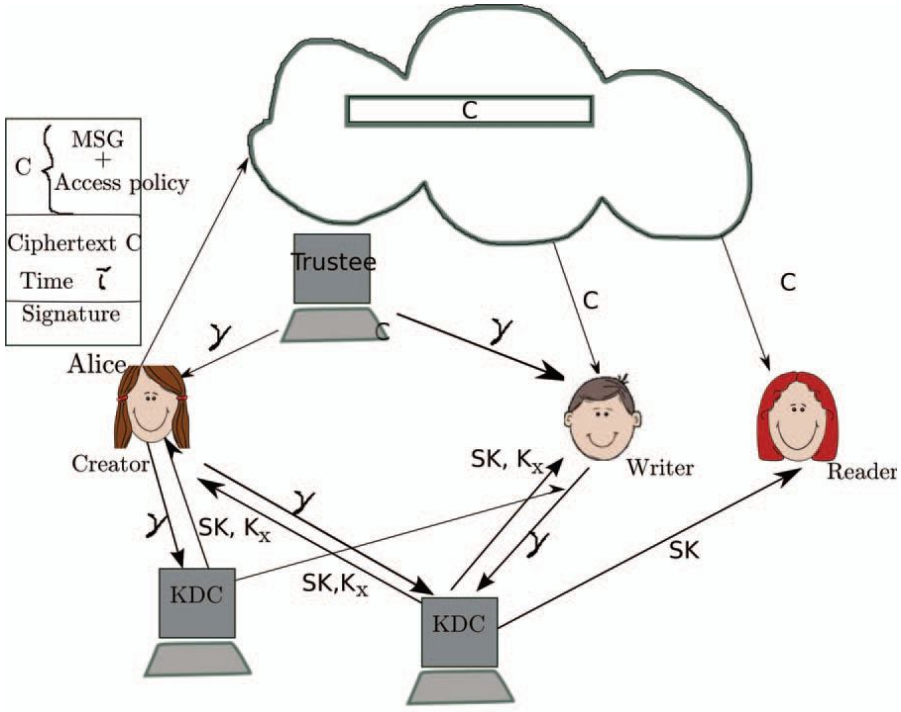


Fig 1.1: Secure Cloud Storage Model

A. Advantage

a) **Functionality** is the required functions available, including interoperability and security.

b) **Reliability** maturity, fault tolerance and recoverability

c) **Usability** how easy it is to understand, learns, and operate the software system

d) **Efficiency** performance and resource behavior.

e) **Maintainability** Maintaining the software.

f) **Portability** can the software easily be transferred to another environment, including install ability.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

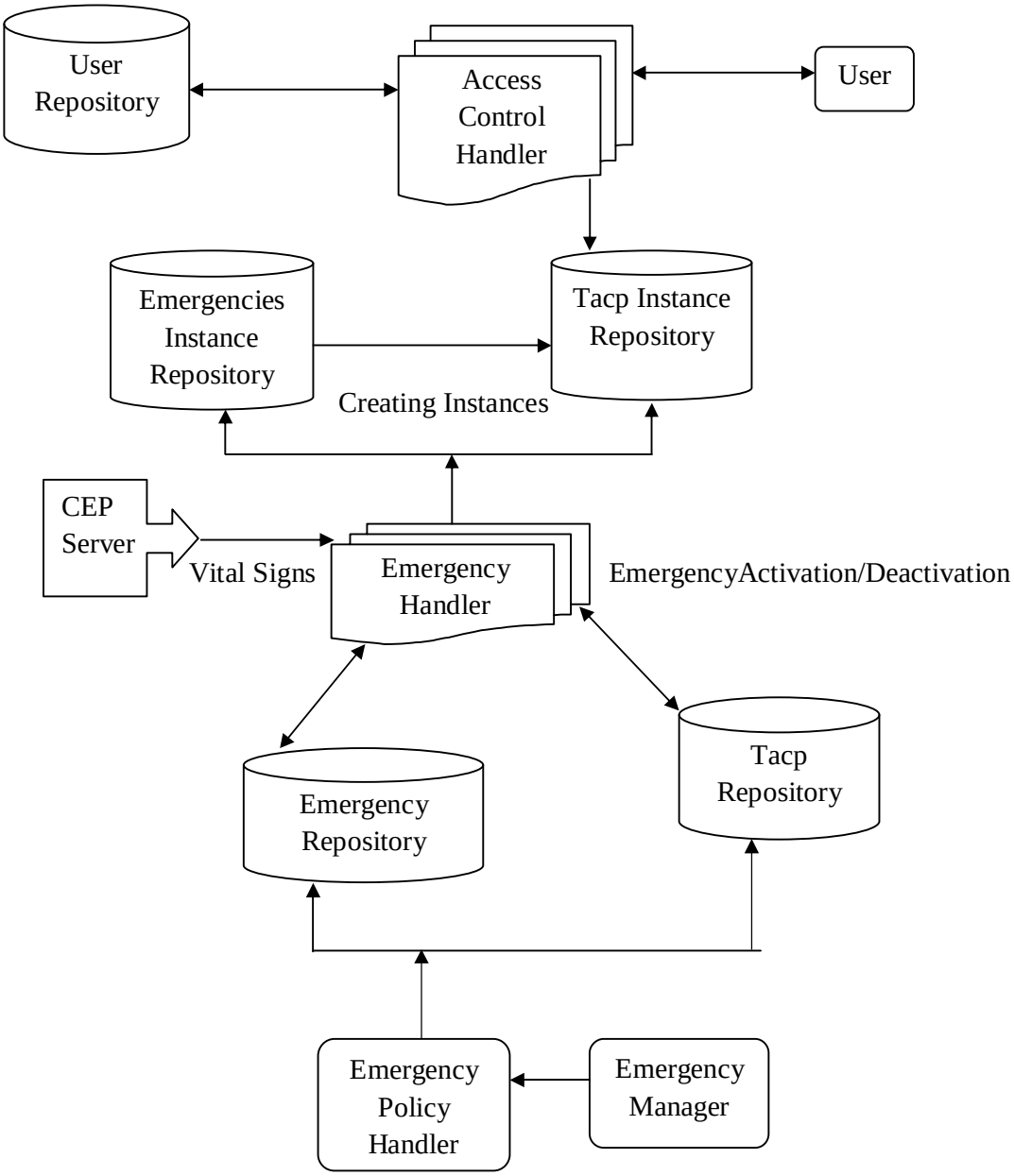
An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

B. Proposed Architecture



V. COMPARATIVE STUDY

In compare my scheme with other access control schemes and show that my scheme supports many features that the other schemes did not support. 1-W-M-R means that only one user can write while many users can read. M-W-M-R means that many

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

users can write and read. In see that most schemes do not support many writes which is

supported by our scheme. In my scheme is robust and decentralized, most of the others are centralized. My scheme also supports privacy preserving authentication, which is not supported by others. Most of the schemes do not support user revocation as shown in Tab 1.1.

Schemes	Fine-grained Access Control	Centralized/ Decentralized	Write/ Read Access	Type of Access Control	Privacy preserving authentication	User Revocation?
Cryptography based Access Control	Yes	Centralized	1-W-M-R	Symmetric Key Cryptography	No authentication	No
Fine grained Access Control	Yes	Centralized	1-W-M-R	ABE	No authentication	No
Cryptography ABE	Yes	Centralized	1-W-M-R	ABE	No authentication	No
Distributed Access Control	Yes	Decentralized	1-W-M-R	ABE	No authentication	No
RBAC & ABAC ABS Scheme	Yes	Decentralized	M-W-M-R	ABE	Authentication	Yes

Tab 1.1: Comparative Scheme

VI.CONCLUSION

Extension of the emergency access control model presented in with the possibility of defining administration policies, which subjects are enabled to define emergency policies and over which scope. They have implemented an extended version of the prototype presented in and carried out an extensive set of test to check what is the impact of emergency policies into an access control system. A set of correctness checks have also been to useless activation/deactivation of emergencies. To avoid possible proliferation of policies due to template instantiation, there

are currently investigating to instantiate tacps during the access request evaluation. This would allow us to instantiate only those policies indeed needed to take the deny/grant decision. However, this requires storing contextual information as soon as an emergency occurs, so as to be able to instantiate and evaluate conditions on tacp only if the protected resource is requested.

REFERENCES

1. Amiya Nayak and Sushmita Ruj(2013)" Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds"in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS.
2. Bethencourt,J. and Sahai,A. and Waters,B.(2007) "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy.* , pp. 321–334.
3. Bhargava,B. and Owens,R. and Wang,W. (2009) "Secure and efficient access to outsourced data," in *ACM Cloud Computing Security Workshop (CCSW).*
4. Borisov,N. and Jahid,S. and Mittal,P. (2011) "EASiER: Encryption-based access control in social networks with efficient revocation," in *ACM ASIACCS.*
5. Boyen,X. (2007) "Mesh signatures," in *EUROCRYPT,* ser. Lecture Notes in Computer Science, vol. 4515. Springer, pp. 210–227.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

6. Cao,N. and Ren,K. and Wang,Q. (2010) "Fuzzy keyword search over encrypted data in cloud computing," in *IEEE INFOCOM.* , pp. 441–445,
7. Chase,M .(2007) "Multi-authority attribute based encryption," in *TCC*, ser. Lecture Notes in Computer Science, vol. 4392. Springer, pp. 515–534, 2007.
8. Chase,M. and Chow,S.S.M. (2009) "Improving privacy and security in multiauthority attribute-based encryption," in *ACM Conference on Computer and Communications Security*, pp. 121–130.
9. Dai,Y. and Tian,L. and Yang,H. (2009) "Identity-based authentication for cloud computing," in *CloudCom*, ser. Lecture Notes in Computer Science, vol. 5931. Springer, pp. 157–166.
10. Goyal,V. and Pandey,O. and Sahai,A. and Waters,B.(2006) "Attribute-based encryption for fine-grained access control of encrypted data," in *ACM Conference on Computer and Communications Security*, pp. 89–98.