International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Multi-Authority Access Control System using Verifiable Threshold in Public Cloud Storage

Y. Swapna , B.Shyam Prakash Reddy, M. Vidhya Reddy, MG. Radhika

(Assistant Professor), yenugulaswapna@gmail.com , shyamprakashreddybolla@gmail.com

vidhyareddy1113@gmail.com , radhika503vits@gmail.com

Dept.of Computer Science and Engineering, Vignan Institute of Technology and Science, Deshmukhi, Hyderabad.

***Abstract**:*

Attribute-based Encryption (ABE) is regarded as a promising cryptographic conducting tool to guarantee data owners' direct control over their data in public cloud storage. The earlier ABE 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, the single-point bottleneck problem remains unsolved. 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. In TMACS, taking advantage of (t; n) threshold secret sharing, the master key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any t authorities. Security and performance analysis results show that TMACS is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system. Furthermore, by efficiently combining the traditional multi-authority scheme with TMACS, we construct a hybrid one, which satisfies the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

Keywords

Attribute-based Encryption, multi-authority scheme, TMACS, attributes, master key..

1. Introduction

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet).

The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

- Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

- Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

- Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

2. Literature Review

1) DAC-MACS: Effective data access control for multi-authority cloud storage systems

AUTHORS: K. Yang, X. Jia, and K. Ren

Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is a promising technique for access control of encrypted data. It requires a trusted authority manages all the attributes and distributes keys in the system. In cloud storage systems, there are multiple authorities co-exist and each authority is able to issue attributes independently. However, existing CP-ABE schemes cannot be directly applied to the access control for multi-authority cloud storage systems, due to the inefficiency of decryption and revocation. In this paper, we propose DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, we construct a new multi-authority CP-ABE scheme with efficient decryption and also design an efficient attribute revocation method that can achieve both forward security and backward security. The analysis and the simulation results show that our DAC-MACS is highly efficient and provably secure under the security model.

2) Dacc: Distributed access control in clouds

AUTHORS: S. Ruj, A. Nayak, and I. Stojmenovic We propose a new model for data storage and access in clouds. Our scheme avoids storing multiple encrypted copies of same data. In our framework for secure data storage, cloud stores encrypted data (without being able to decrypt them). The main novelty of our model is addition of key distribution centers (KDCs). We propose DACC (Distributed Access Control in Clouds) algorithm, where one or more KDCs distribute keys to data owners and users. KDC may provide access to particular fields in all records. Thus, a single key replaces separate keys from owners. Owners and users are assigned certain set of attributes. Owner encrypts the data with the attributes it has and stores them in the cloud. The users with matching set of attributes can retrieve the data from the cloud. We apply attribute-based encryption based on bilinear pairings on elliptic curves. The scheme is collusion secure; two users cannot together decode any data that none of them has individual right to access. DACC also supports revocation of users, without redistributing keys to all the users of cloud services.

We show that our approach results in lower communication, computation and storage overheads, compared to existing models and schemes.

3) Expressive, efficient and revocable data access control for multi-authority cloud storage

AUTHORS: K. Yang and X. Jia Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

4) Privacy preserving cloud data access with multi-authorities

AUTHORS: T. Jung, X. Li, Z. Wan, and M. Wan Cloud computing is a revolutionary computing paradigm which enables flexible, on-demand and low-cost usage of computing resources. Those advantages, ironically, are the causes of security and privacy problems, which emerge because the data owned by different users are stored in some cloud servers instead of under their own control. To deal with security problems, various schemes based on the Attribute-Based Encryption have been proposed recently. However, the privacy problem of cloud computing is yet to be solved. This paper presents an anonymous privilege control scheme AnonyControl to address not only the data privacy problem in a cloud storage, but also the user identity privacy issues in existing access control schemes. By using multiple authorities in cloud computing system, our proposed scheme achieves anonymous cloud data access and fine-grained privilege control. Our security proof and performance analysis shows that AnonyControl is both secure and efficient for cloud computing environment.

5) Achieving secure, scalable, and fine-grained data access control in cloud computing

AUTHORS: S. Yu, C. Wang, K. Ren, and W. Lou Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secure under existing security models.

3. System Analysis

Existing System:

Attribute-based Encryption (ABE) is regarded as one of the most suitable schemes to conduct data access control in public clouds for it can guarantee data owners' direct control over their data and provide a fine-grained access control service. Till now, there are many ABE schemes proposed, which can be divided into two categories: Key-Policy Attribute-based Encryption (KP-ABE) and Ciphertext-Policy Attribute-based Encryption (CP-ABE).

In KP-ABE schemes, decrypt keys are associated with access structures while ciphertexts are only labeled with special attribute sets. On the contrary, in CP-ABE schemes, data owners can define an access policy for each file based on users' attributes, which can guarantee owners' more direct control over their data. Therefore, compared with KP-ABE, CP-ABE is a preferred choice for designing access control for public cloud storage.

Disadvantages Of Existing System:

In most existing CP-ABE schemes there is only one authority responsible for attribute management and key distribution. This only-one-authority scenario can bring a single-point bottleneck on both security and performance.

Once the authority is compromised, an adversary can easily obtain the only-one-authority's master key, then he/she can generate private keys of any attribute subset to decrypt the specific encrypted data.

Moreover, once the only-one-authority is crashed, the system completely cannot work well.

Although some multi-authority CP-ABE schemes have been proposed, they still cannot deal with the problem of single-point bottleneck on both security and performance mentioned above.

The adversary can obtain private keys of specific attributes by compromising specific one or more authorities.

Crash or offline of a specific authority will make that private keys of all attributes in attribute subset maintained by this authority cannot be generated and distributed, which will still influence the whole system's effective operation.

PROPOSED SYSTEM:

In this paper, we propose a robust and verifiable threshold multi-authority CP-ABE access control scheme, named TMACS, to deal with the single-point bottleneck on both security and performance in most existing schemes.

In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. Since in CP-ABE schemes, there is always a secret key (SK) used to generate attribute private keys, we introduce (t; n) threshold secret sharing into our scheme to share the secret key among authorities.

In TMACS, we redefine the secret key in the traditional CP-ABE schemes as master key. The introduction of (t; n) threshold secret sharing guarantees that the master key cannot be obtained by any authority alone.

Advantages Of Proposed System:

TMACS is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system.

To the best of our knowledge, this paper is the first try to address the single point bottleneck on both security and performance in CPABE access control schemes in public cloud storage.

In existing access control systems for public cloud storage, there brings a single-point bottleneck on both security and performance against the single authority for any specific attribute.

To the best of our knowledge, we are the first to design a multi-authority access control architecture to deal with the problem.

By introducing the combining of (t; n) threshold secret sharing and multi-authority CP-ABE scheme, we propose and realize a robust and verifiable multi-authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set.

Furthermore, by efficiently combining the traditional multi-authority scheme with ours, we construct a hybrid one, which can satisfy the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

4. System Design and Implementation

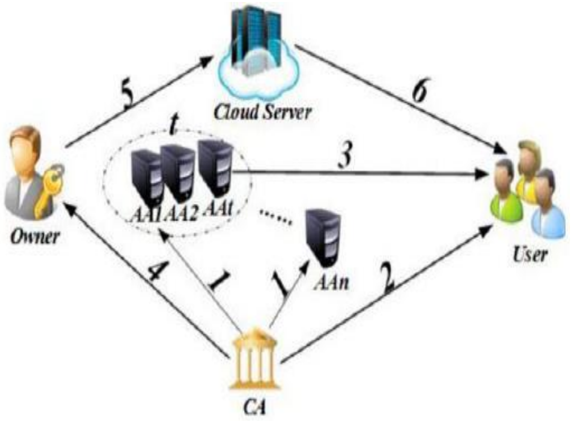


Fig 1: System Architecture

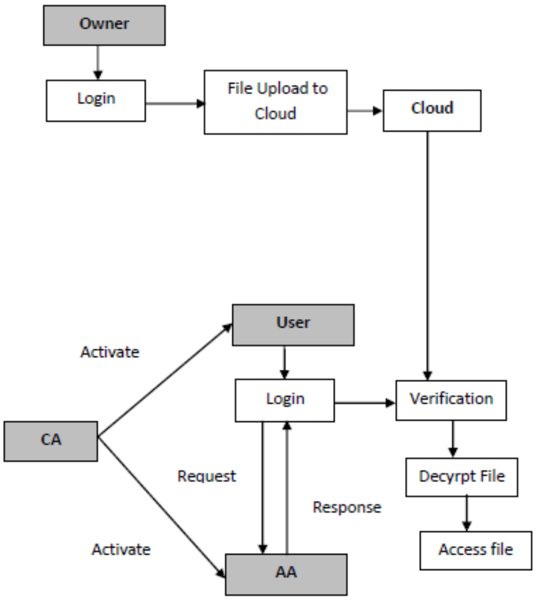


Fig 2: Data-Flow Diagram

Modules

- TMACS
- Data Access Control Scheme
- Certificate authority
- Attribute authorities

Modules Description

a) TMACS

The TMACS multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. In TMACS, a global certificate authority is responsible for the construction of the system, which avoids the extra overhead caused by AAs' negotiation of system parameters. CA is also responsible for the registration of users, which avoids AAs synchronized maintaining a list of users. However, CA is not involved in AAs' master key sharing and users' secret key generation, which avoids CA becoming the security vulnerability and performance bottleneck.design of TMACS is reusing of the master key shared among multiple attribute authorities. In traditional (t;n) threshold secret sharing, once the secret is reconstructed among multiple participants, someone can actually gain its value. Similarly, in CP-ABE schemes, the only-one-authority knows the master key and uses it to generate each user’s secret key according to a specific attribute set. In this case, if the AA is compromised by an adversary, it will become the security vulnerability. To avoid this, by means of (t;n) threshold secret sharing, the master key cannot be individually reconstructed and gained by any entity in TMACS.hat the master key a is actually secure. By this means, we solve the problem of reusing of the master key.

b) Data Access Control Scheme:

we propose a robust and verifiable threshold multi-authority CP-ABE access control scheme, named TMACS, to deal with the single-point bottleneck on both security and performance in most existing schemes. In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. Since in CP-ABE schemes, there is always a secret key (SK) used to generate attribute private keys, we introduce (t;n) threshold secret sharing into our scheme to share the secret key among authorities. In TMACS, we redefine the secret key in the traditional CP-ABE schemes as master key. The introduction of (t;n) threshold secret sharing guarantees that the master key cannot be obtained by any authorityalone. TMACS is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system. To the best of our knowledge, this paper is the first try to address the singlepoint bottleneck on both security and performance in CPABE access control schemes in public cloud storage.

c) Certificate authority :

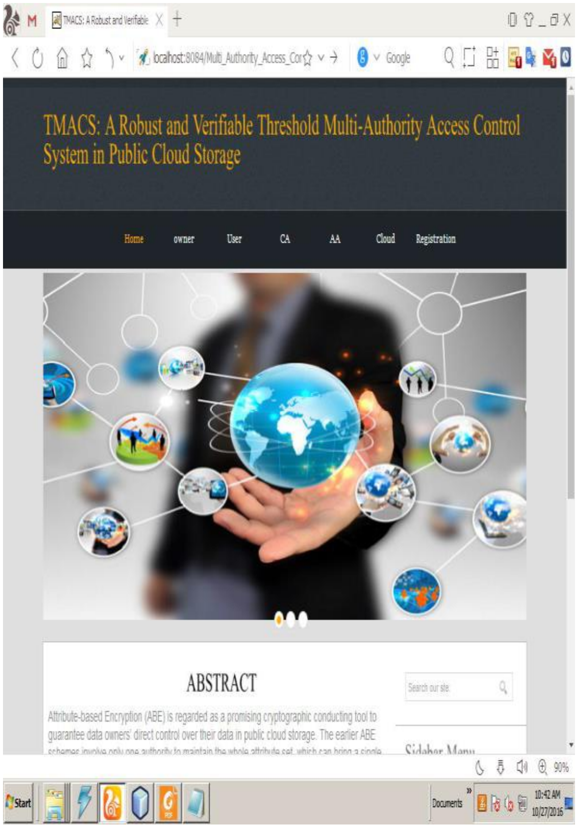
The certificate authority is a global trusted entity in the system that is responsible for the construction of the system by setting up system parameters and attribute public key (PK) of each attribute in the whole attribute set. CA accepts users and AAs’ registration requests by assigning a unique uid for each legal user and a unique aid for each AA. CA also decides the parameter t about the threshold of AAs that are involved in users’ secret key generation for each time. However, CA is not involved in AAs’ master key sharing and users’ secret key generation. Therefore, for example, CA can be government organizations or enterprise departments which are responsible for the registration. certificate authority is responsible for the construction of the system, which avoids the extra overhead caused by AAs’ negotiation of system parameters. CA is also responsible for the registration of users, which avoids AAs synchronized maintaining a list of users.

d) Attribute authorities:

The attribute authorities focus on the task of attribute management and key generation. Besides, AAs take part of the responsibility to construct the system, and they can be the administrators or the managers of the application system. Different from other existing multi-authority CP-ABE systems, all AAs jointly manage the whole attribute set, however, any one of AAs cannot assign users’ secret keys alone for the master key is shared by all AAs. All AAs cooperate with each other to share the master key. By this means, each AA can gain a piece of master key shareas its private key, then each AA sends its corresponding public key to CA to generate one of the system public keys. When it comes to generate users’ secret key, each AA only should generate its corresponding secret key independently. the master key shared among multiple attribute authorities. In traditional (t;n) threshold secret sharing, once the secret is reconstructed among multiple participants, someone can actually gain its value.

5. Results

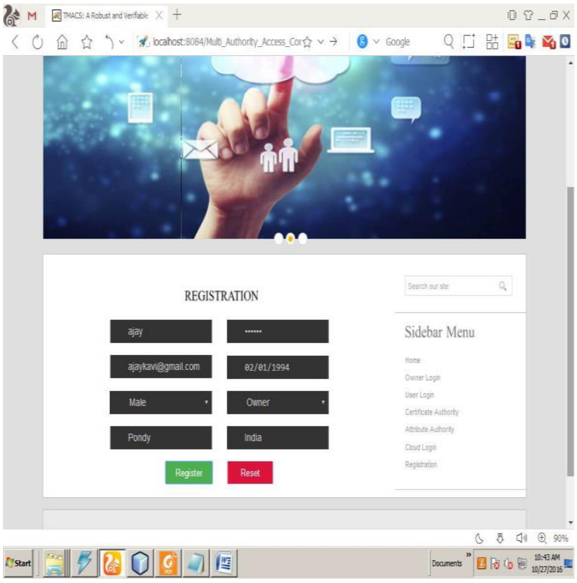
1) Home Page


TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage

ABSTRACT

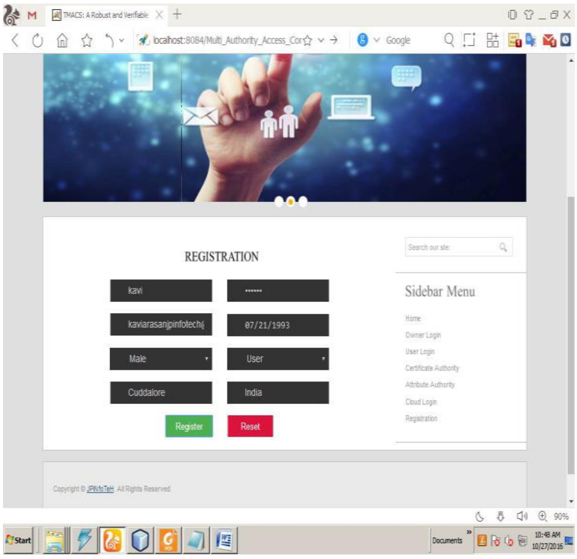
Attribute-based Encryption (ABE) is regarded as a promising cryptographic conducting tool to guarantee data owners' direct control over their data in public cloud storage. The earlier ABE schemes involve only one authority to maintain the whole attribute set, which can bring a single

2) Owner Registration



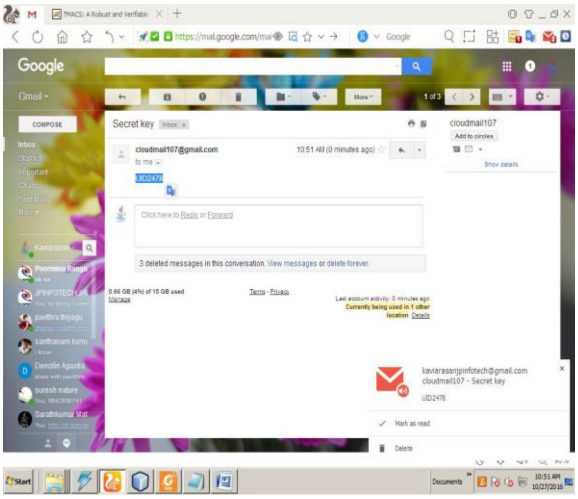
ajay
******
ajaykavi@gmail.com
02/01/1994
Male
Owner
Pondy
India

3) User Registration



kavi
******
kaviarasanjpinfotech|
07/21/1993
Male
User
Cuddalore
India

4) Activate user details



Secret key

cloudmail107@gmail.com

to me

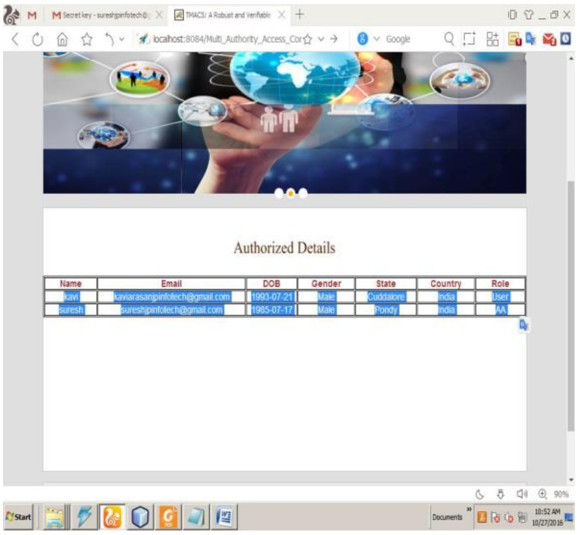
UID2478

Click here to Reply or Forward

3 deleted messages in this conversation. View messages or delete forever.

kaviarasanjpinfotech@gmail.com
cloudmail107 - Secret key
UID2478

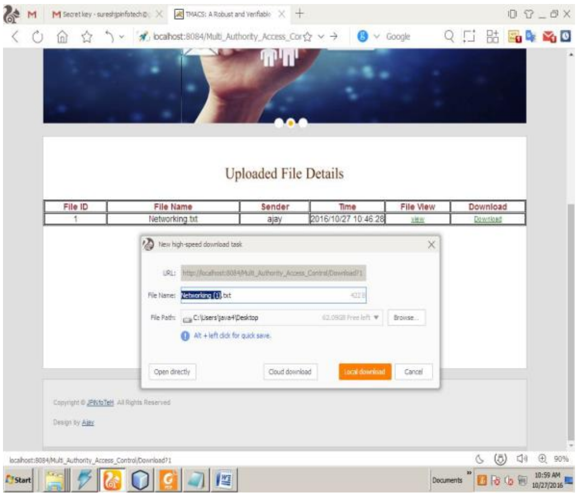
5) Authorized Details



Authorized Details

Name	Email	DOB	Gender	State	Country	Role
kavi	kaviarasanjpinfotech@gmail.com	1993-07-21	Male	Cuddalore	India	User
suresh	sureshjpinfotech@gmail.com	1965-07-17	Male	Pondy	India	AA

6) Download File



Uploaded File Details

File ID	File Name	Sender	Time	File View	Download
1	Networking.txt	ajay	2016/10/27 10:46:28	view	Download

New high-speed download task

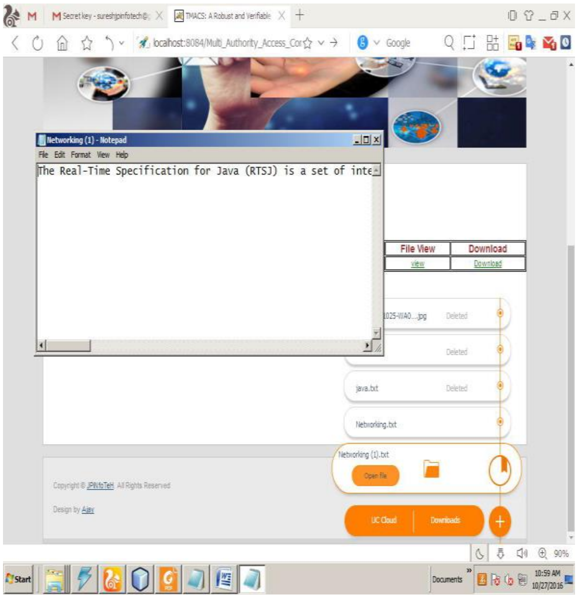
URL: http://localhost:8084/Multi_Authority_Access_Control/Download?1

File Name: Networking (1).txt

File Path: C:\Users\java4\Desktop

Alt + left click for quick save.

7) Logout User Session



Networking (1) - Notepad

```
The Real-Time Specification for Java (RTSJ) is a set of inte
```

6. Conclusion

In this paper, we propose a new threshold multi-authority CP-ABE access control scheme, named TMACS, in public cloud storage, in which all AAs jointly manage the whole attribute set and share the master key a. Taking advantage of (t; n) threshold secret sharing, by interacting with any t AAs, a legal user can generate his/her secret key. Thus, TMACS avoids any one AA being a single-point bottleneck on both security and performance. The analysis results show that our access control scheme is robust and secure. We can easily find appropriate values of (t; n) to make TMACS not only secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system. Furthermore, based on efficiently combining the traditional multi-authority scheme with TMACS, we also construct a hybrid scheme that is more suitable for the real scenario, in which attributes come from different authority-sets and multiple authorities in an authority-set jointly maintain a subset of the whole attribute set. This enhanced scheme addresses not only attributes coming from different authorities but also security and system-level robustness. How to reasonably select the values of (t; n) in theory and design optimized interaction protocols will be addressed in our future work.

7. References

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Instit. Standards Technol., vol. 53, no. 6, p. 50, 2009.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. 14th Financial Cryptography Data Security, 2010, pp. 136–149.

[3] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan.-Feb.2012.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. 24th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 457–473.

[5] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. 14th ACM Conf. Comput. Commun. Security, 2014, pp. 195–203.

[6] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Proc. 29th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2010, pp. 62–91.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[8] N. Attrapadung, B. Libert, and E. Panafieu, "Expressive keypolicy attribute-based encryption with constant-size ciphertexts," in Proc. 14th Int. Conf. Practice Theory Public Key Cryptography, 2011, pp. 90–108.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[10] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. 14th Int. Conf. Practice Theory Public Key Cryptography, 2011, pp. 53–70.

[11] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Proc. 35th Int. Colloquium Automata, Lang. Programm., 2008, pp. 579–591.

[12] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. 14th Eur. Symp. Res. Comput. Security, 2009, pp. 587–604.

[13] M. Chase, "Multi-authority attribute based encryption," in Proc. 4th Theory Cryptography Conf., 2007, pp. 515–534.

[14] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2011, pp. 568–588.

[15] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multiauthority attribute based encryption without a central authority," Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.

[16] T. Pedersen, "A threshold cryptosystem without a trusted party," in Proc. 10th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 1991, pp. 522–526.

[17] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

[18] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," Electron. Commun. Japan (Part III: Fundam. Electron. Sci.), vol. 72, no. 9, pp. 56–64, 1989.

[19] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in Proc. 28th Annu. Symp. Found. Comput. Sci., 1987, pp. 427–438.

[20] K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proc. 32nd IEEE Int. Conf. Comput. Commun., 2013, pp. 2895–2903.

[21] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in Proc. 10th IEEE Int. Conf. Trust, Security Privacy Comput. Commun., 2011, pp. 91–98.

[22] K. Yang and X. Jia, "Expressive, efficient and revocable data access control for multi-authority cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744, Jul. 2013.