

A Study on Provable Multi Copy Dynamic Data Possession in Cloud Computing Systems



R Bala Vigneshwar
M.Tech Student
VBIT College.



Mr. M Venkateswara Rao, M.Tech
Associate Professor
VBIT College.

ABSTRACT

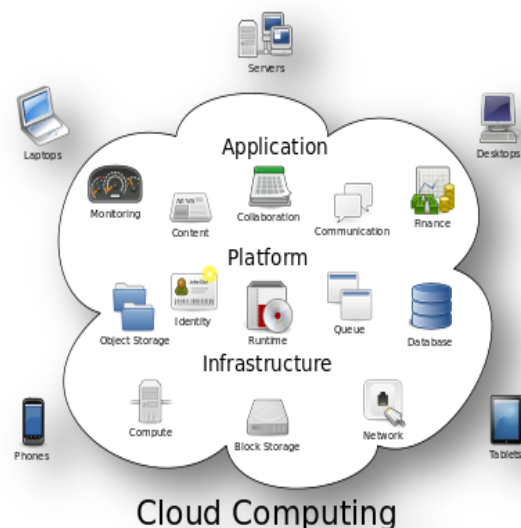
Cloud computing is a revolutionary computing paradigm, which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper, we present a semianonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semianonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the AnonyControl-F, which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie-Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes.

INTRODUCTION

What is cloud computing?

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.



Structure of cloud computing

How Cloud Computing Works?

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.

Characteristics and Services Models:

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.

EXISTING SYSTEM:

The user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semianonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. extend existing schemes by generalizing the access tree to a privilege tree. The privilege in our scheme is defined as similar to the privileges managed in ordinary operating systems.

DISADVANTAGE FOR EXISTING SYSTEM:

- 1) Anony Control decentralizes the central authority to limit the identity leakage and thus achieves semianonymity
- 2) The privilege is not possible scheme is defined as similar to the privileges managed in ordinary operating systems

PROPOSED SYSTEM:

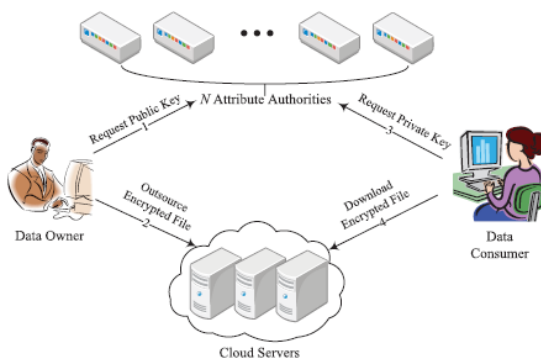
Our security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie-Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes. In the proposed scheme, an authority generates a set of random secret parameters and shares $gskj$ it with other authorities via secure channel, and is computed based on this parameters. It is believed that

DDH problem is intractable in the group of prime order p , therefore does not leak any statistical information about

ADVANTAGE OF PROPOSED SYSTEM:

- 1) The privilege is possible scheme is defined as similar to the privileges managed in ordinary operating systems
- 2) Security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie–Hellman assumption

SYSTEM ARCHITECTURE:



IMPLEMENTATION MODULES:

- Achieving full anonymity
- Fully Anonymous Multi-Authority CP-ABE
- Security Model
- Security Analysis

MODULES DESCRIPTION

Achieving full anonymity

We have assumed semi-honest authorities in AnonyControl and we assumed that they will not collude with each other. This is a necessary assumption in AnonyControl because each authority is in charge of a subset of the whole attributes set, and for the attributes that it is in charge of, it knows the exact information of the key requester. If the information from all authorities is gathered altogether, the complete attribute set of the key requester is recovered and thus his identity is disclosed to the authorities. In this sense, AnonyControl is semianonymous since partial identity information

(represented as some attributes) is disclosed to each authority, but we can achieve a full-anonymity and also allow the collusion of the authorities.

Fully Anonymous Multi-Authority CP-ABE:

The KeyGenerate algorithm is the only part which leaks identity information to each attribute authority. Upon receiving the attribute key request with the attribute value, the attribute authority will generate $H(\text{att}(i)r_i)$ and sends it to the requester where $\text{att}(i)$ is the attribute value and r_i is a random number for that attribute. The attribute value is disclosed to the authority in this step. We can introduce the above 1-out-of- n OT to prevent this leakage. We let each authority be in charge of all attributes belonging to the same category. For each attribute category c (e.g., University), suppose there are k possible attribute values (e.g., IIT, NYU, CMU ...), then one requester has at most one attribute value in one category.

Security Model

Setup \rightarrow $\mathbf{PK}, \mathbf{MK}_k$: This algorithm takes nothing as input except implicit inputs such as security parameters. Attributes authorities execute this algorithm to jointly compute a system-wide public parameter \mathbf{PK} as well as an authority-wide public parameter y_k , and to individually compute a master key \mathbf{MK}_k .

KeyGenerate($\mathbf{PK}, \mathbf{MK}_k, A_u$) \rightarrow \mathbf{SK}_u : This algorithm enables a user to interact with every attribute authority, and obtains a private key \mathbf{SK}_u corresponding to the input attribute set A_u . Encrypt($\mathbf{PK}, M, \{T_p\}_{p \in \{0, \dots, r-1\}}$) \rightarrow (\mathbf{CT}, \mathbf{VR}): This algorithm takes as input the public key \mathbf{PK} , a message M , and a set of privilege trees $\{T_p\}_{p \in \{0, \dots, r-1\}}$, where r is determined by the encrypter. It will encrypt the message M and returns a ciphertext \mathbf{CT} and a verification set \mathbf{VR} so that a user can execute specific operation on the ciphertext if and only if his attributes satisfy the corresponding privilege tree T_p . As we defined, T_0 stands for the privilege to read the file. Decrypt($\mathbf{PK}, \mathbf{SK}_u, \mathbf{CT}$) \rightarrow M or verification parameter: This algorithm will be used at file controlling (e.g. reading, modification, deletion). It takes as input the public key \mathbf{PK} , a ciphertext \mathbf{CT} , and

a private key **SK_u**, which has a set of attributes **A_u** and corresponds to its holder's **GD_u**.

Security Analysis

In the proposed scheme, an authority generates a set of random secret parameters and shares it with other authorities via secure channel, and is computed based on this parameters. It is believed that DDH problem is intractable in the group G_0 of prime order p , therefore does not leak any statistical information about \cdot . This implies even if an adversary is able to compromise up to $(N - 2)$ authorities, there are still two parameters kept unknown to the adversary.

SCREEN SHOTS

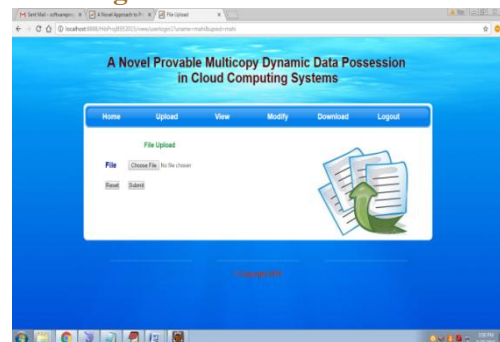
Home Page:



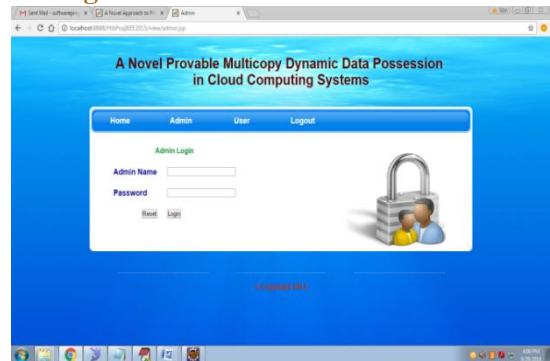
User Registration:



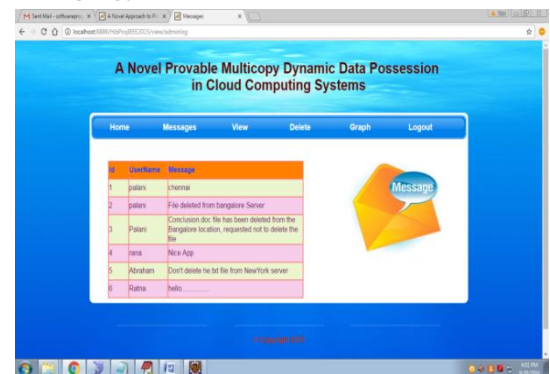
User Home Page:



Admin Login:



Admin Home:



CONCLUSION

This paper proposes a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities 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. More importantly, our system can tolerate up to $N - 2$ authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also conducted detailed security and performance analysis which shows that AnonyControl both secure and efficient for cloud storage system. The AnonyControl-F directly inherits the security of the AnonyControl and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of- n oblivious transfer. One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an

important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes who support efficient user revocation is one of our future works.

REFERENCES

- [1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.
- [2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.
- [3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th CCS*, 2006, pp. 89–98.
- [4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE SP*, May 2007, pp. 321–334.
- [5] M. Chase, "Multi-authority attribute based encryption," in *Theory of Cryptography*. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.
- [6] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proc. 16th CCS*, 2009, pp. 121–130.
- [7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," *Inf. Sci.*, vol. 180, no. 13, pp. 2618–2632, 2010.
- [8] V. Božović, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," *Int. J. Comput. Math.*, vol. 89, no. 3, pp. 268–283, 2012.
- [9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing," in *Proc. IEEE 7th SOSE*, Mar. 2013, pp. 573–577.
- [10] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2895–2903.
- [11] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.
- [12] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," *Bull. Korean Math. Soc.*, vol. 46, no. 4, pp. 803–819, 2009.
- [13] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, "Multiauthority ciphertext-policy attribute-based encryption with accountability," in *Proc. 6th ASIACCS*, 2011, pp. 386–390.
- [14] H. Ma, G. Zeng, Z. Wang, and J. Xu, "Fully secure multi-authority attribute-based traitor tracing," *J. Comput. Inf. Syst.*, vol. 9, no. 7, pp. 2793–2800, 2013.
- [15] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Public-Key Cryptography*. Berlin, Germany: Springer-Verlag, 2013, pp. 162–179.