IJDCST @ Nov-Dec-2018, Issue- V-6, I-5, SW-06
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Ensemble Attribute Based Encryption Control Cloud Data Access

Ramisetti Anitha[1], Korukonda Venkata Rathnam[2]

[1] M.Tech (C.S.E), Nova College of Engineering & Technology, A.P., India.

[1] Associate Professor, Department of CSE, Nova College of Engineering & Technology, A.P., India.

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 aensemble 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.

Keywords-Cloud computing, Anonycontrol, Access Control,security.

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.

Fig: 1. Structure of cloud computing

The goal of cloud computing is to applytraditional supercomputing, or high performance computing power, normally used by military andresearch 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.

LITERATURE SURVEY

1. Cipher text-Policy Attribute-Based Encryption
AUTHORS: Taeho Jung, Xiang-Yang Li, Zhiguo Wan, Meng WanIn several distributed systems a user can able to access data if a user posses a certain set of credentials or attributes. Presently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server stores the data, which is compromised, then the confidentiality of the data will be compromised. In this paper, we present a process for realizing complex access control on encrypted data that we say Cipher text-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even

if the storage server is untrusted; moreover, our systems are
secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to explain the encrypted data and built policies into user's keys; while in our system attributes are used to explain a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our systems are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we ensure an implementation of our system and give performance measurements.

2. Multi-authority attribute based encryption with honest-but-curious central authority
AUTHORS: Vladimir Bozovic , Daniel Socek , Rainer Steinwandt , and Viktoria I. Villanyi
An attribute based encryption scheme capable of handling multiple authorities were recently proposed by Chase. The scheme is built upon a single-authority attribute based encryption technique presented earlier by Sahai and Waters. Chase's construction uses a trusted central authority that is inherently able to do decrypting arbitrary cipher texts created within the system. We present a multi-authority attribute based encryption technique in which only the set of recipients defined by the encrypting party can decrypt a corresponding cipher text. The central authority is shown as "honest-but-curious": on the one hand it honestly follows the protocol, and on the other it is curious to decrypt arbitrary cipher texts thus violating the intent of the encrypting party. The advance scheme, which like its predecessors relies on the Bilinear DiffieHellman assumption, has a complexitycomparable to that of Chase's technique. We prove that our scheme is secure in the selective ID model and can tolerate an honest-but-curious central authority. Building on the proposal for multi-authority based attribute based encryption from; we constructed a scheme where the central authority is no longer capable of decrypting arbitrary cipher texts created within thesystem. In addition to viewing security in the selective ID model, we showed that the proposed system can able to tolerate an honest-but-curious central authority. Since both Chase's scheme and the proposed scheme rely on the same hardness assumption, and have a comparable complexity, the new scheme seems a viable alternative to Chase's construction. However, since the proposed method is capable of handling a curious yet honest central authority, the proposed scheme is suggested in applications where security against such a central authority is required.

3. Decentralizing Attribute-Based Encryption
AUTHORS: Allison Lewko, University of Texas at Austin alewko@cs.utexas.edu
We propose a Multi-Authority Attribute-Based Encryption (ABE) system. In this process, any party can become an authority and there is no requirement for any world
coordinationother than the innovation of an initial set of common reference parameters. A party can simply plays as an
ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in forms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, our
process does not require any central authority. In constructing our system, our largest technical hurdle is to create it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE technique authority "tied" together different components (representing different attributes) of a user's private key by randomizing the key. But in our system each component will come from a potentially different authority, where we think no coordination between such authorities. We create new techniques to tie keycomponents together and prevent collusion issues between users with different global identifiers. We prove our system secure using the new dual system encryption methodology where the security proof works by first converting the challenge cipher text and private keys to a half-functionalvform and then arguing security. We follow a recent variant of the dual system proof scheme due to Lewko and Waters and build our system using bilinear groups of Composite order. We prove security under same static assumptions to the LWvpaper in the random oracle model.

4. Accountable Authority Cipher text-Policy Attribute-Based Encryption with White-Box Traceability and Public Auditing in the Cloud
AUTHORS: JiantingNin ,XiaoleiDong , Zhenfu Cao and Lifei Wei
As a sophisticated mechanism for secure well-grained access control, cipher text-policy attribute-based encryption (CPABE) is a highly promising solution for commercial applications like cloud computing. But there still exists one major issue awaiting to be solved, that is, the prevention of key abuse. The existing CP-

ABE systems missed this critical functionality, hindering the wide utilization and commercial application of CP-ABE systems to date. Here we address two practical problems about the key abuse of CP-ABE: The key escrow problem of the half-trusted authority; and, Themalicious key delegation problem of the users. For the semitrustedauthority, its misconduct (i.e., illegal key (re-)distribution) should be caught and prosecuted. And for a user, his/her malicious conduct (i.e., illegal key sharing) need be traced. We affirmatively solve these two key abuse issues by proposing the first accountable authority CP-ABE with white box traceability that supports policies expressed in any monotone access structures. And we provide an auditor to judge publicly whether a suspected user is guilty or is framed by the authority. In this process, we addressed two practical problems about the key abuse of CP-ABE in the cloud, and have presented an accountable authority CP-ABE technique
supporting white-box traceability and public auditing. Specifically, the proposed system could trace the spiteful users for illegal key sharing. And for the half trusted authority, it'sillegal key (re-)distributing misconduct could be caught and prosecuted. Furthermore, we have provided an auditor to judge whether a malicious user is naive or framed by the authority. As far as we know, this is the first CP-ABE technique that simultaneously encourages white-box traceability, accountable authority, public auditing. We have also proved that the new
system is total protection in the standard model. Note that there exists a stronger notion for traceability called black-box traceability. In black-box scenario, the malicious user can hide the decryption algorithm by tweaking it, as well as the decryption key. And in this case, the advanced system with white-box traceability in this paper will fail since both the decryption key and decryption algorithm are not good. In our future work, we will focus on constructing an accountable authority CP-ABE technique which is black-box traceability and public auditing.

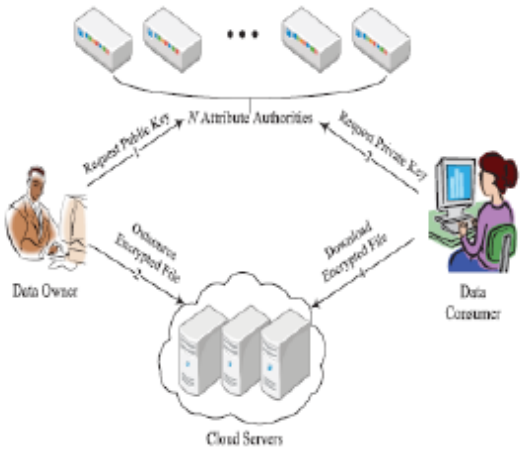

Fig.2. System Architecture.

EXISTING SYSTEM

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. Besides the fact that we can express arbitrarily general encryption policy, our system also tolerates the compromise attack towards attributes authorities, which is not covered in many existing works. We extend existing schemes by generalizing the access tree to a privilege tree. we extend existing schemes by generalizing the access tree to a privilege tree.

The key point of the identity information leakage we had in our previous scheme as well as every existing attribute based encryption schemes is that key generator issues attribute key based on the reported attribute, and the generator has to know the user's attribute to do so.

PROPOSE SYSTEM

Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage.

Various techniques have been proposed to protect the data contents privacy via access control. we propose AnonyControl and AnonyControl-F to allow cloud servers to control users' access privileges without knowing their identity information. They will follow our proposed protocol in general, but try to find out as much information as possible individually.

The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. We firstly implement the

real toolkit of a multiauthority based encryption scheme AnonyControl and AnonyControl-F.

BENEFITS OF CLOUD COMPUTING

1. **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
2. **Reduce spending on technology infrastructure** Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
3. **Globalize your workforce on the cheap.** People worldwide can access the cloud, provided they have an Internet connection.
4. **Streamline processes.** Get more work done in less time with less people.
5. **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.
6. **Improve accessibility.** You have access anytime, anywhere, making your life so much easier!
7. **Monitor projects more effectively.** Stay within budget and ahead of completion cycle times.
8. **Less personnel training is needed.** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
9. **Minimize licensing new software.** Stretch and grow without the need to buy expensive software licenses or programs.
10. **Improve flexibility.** You can change direction without serious "people" or "financial" issues at stake.

ADVANTAGES

1. **Price:** Pay for only the resources used.
2. **Security**: Cloud instances are isolated in the network from other instances for improved security.
3. **Performance:** Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
4. **Scalability:** Auto-deploy cloud instances when needed.
5. **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
6. **Control:** Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
7. **Traffic:** Deals with spike in traffic with quick deployment of additional instances to handle the load.

MODULE DESCRIPTION:

Number of Modules

After careful analysis the system has been identified to have the following modules:

1. **Registration based Social Authentication Module**
2. **Security Module**
3. **Attribute-based encryption module.**
4. **Multi-authority module.**

1. Registration -Based Social Authentication Module:

The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password),and then a few(e.g., 5) friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice's friend list and are appointed as Alice's Registration.

2. Security Module:

Authentication is essential for securing your account and preventing spoofed messages from damaging your online reputation. Imagine a phishing email being sent from your mail because someone had forged your information. Angry recipients and spam complaints resulting from it become your mess to clean up, in order to repair your reputation.trustee-based social authentication systems ask users to select their own trustees without any constraint. In our experiments (i.e., Section VII), we show that the service provider can constrain trustee selections via imposing that no users are selected as trustees by too many other users, which can achieve better security guarantees

3.Attribute-based encryption module.

Attribute-based encryption moduleis using foreach and every node encrypt data store. After encrypted data and again the re-encrypted the same data is using for fine-grain concept using user data uploaded. the attribute-based encryption have been proposed to secure the cloud storage.Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter's identity has some overlaps with the one specified in the ciphertext.

4.Multi-authority module.

A multi-authority system is presented in which each user has an id and they can interact with each key generator (authority) using different pseudonyms. Our goal is to achieve a multi-authority CP-ABE which achieves the security defined above; guarantees the confidentiality of Data Consumers' identity information; and tolerates compromise attacks on the authorities or the collusion attacks by the authorities. This is the first implementation of a multi-authority attribute based encryption scheme.

CONCLUSION

This paper introduces a semi-anonymous attribute-based privilege control scheme AnonyControl and a fullyanonymousattribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. By using the multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while controlling privilege control based on users' identity information. More importantly, our system can accept up to N −2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also direct detailed security and performance analysis which shows that AnonyControl both efficient and secure for cloud storage system. The AnonyControl-F directly inherits thesecurity of the AnonyControl and thus is equivalently secure
as it. One of the upcoming future works is to introduce the efficient user repudiation mechanism on top of our anonymous ABE. Supporting user repudiation is an important issue in the real application, and this is a great challenge in the application of ABE schemes.

REFERENCES

[1] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, Meng Wan," Cipher text- Policy Attribute-Based Encryption", T Jung - 2015.

[2] Vladimir Bozovic , Daniel Socek , Rainer Steinwandt , and Viktoria I. Villanyi. "Multi-authority attributes based encryption with honest-butcuriouscentral authority".

[3] White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes JiantingNing, Xiaolei Dong, ZhenfuCao, Senior Member, IEEE, Lifei Wei, and Xiaodong Lin, Senior Member, IEEE

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in EUROCRYPT. Springer, 2005, pp. 457–473

[5] 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. [6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE SP, May 2007, pp. 321–334. [6] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.

[7] h.lin,z.cao,x.liang,andj.shao, "secure threshold multi authority Attribute based encryption without a central authority," inf. Sci., vol. 180, No. 13, pp. 2618–2632, 2010.

[8] v. Božovi´c, 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. IeeeInfocom**,** APR. 2013, PP. 2895–2903.

[11] 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.

[12] 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. [13] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.

[14] j. Li, q. Huang, x. Chen, s. S. Chow, d. S. Wong, and d. Xie, "multiauthorityCiphertext-policy attribute-based encryption with accountability," In proc. 6th asiaccs, 2011, pp. 386–390.

[15] 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.