CONTROL CLOUD DATA ACESS PRIVELAGE AND ANONYMITY WITH FULLY ANONYMOUS ATTRIBUTE BASED ENCRYPTION

[1]O.RAMYA TEJA, [2]K. SATHWIKA REDDY, [3]G. ARUNDATHI, [4]G. NIKHITHA REDDY

[1]Assistant Professor, Department of Information Technology, **MALLA REDDY ENGINEERING COLLEGE FOR WOMEN**, Maisammaguda, Dhulapally Kompally, Medchal Rd, M, Secunderabad, Telangana.

[2, 3,4] Student, Department of Information Technology, **MALLA REDDY ENGINEERING COLLEGE FOR WOMEN**, Maisammaguda, Dhulapally Kompally, Medchal Rd, M, Secunderabad, Telangana.

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 semi-anonymous 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.

I. 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.

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

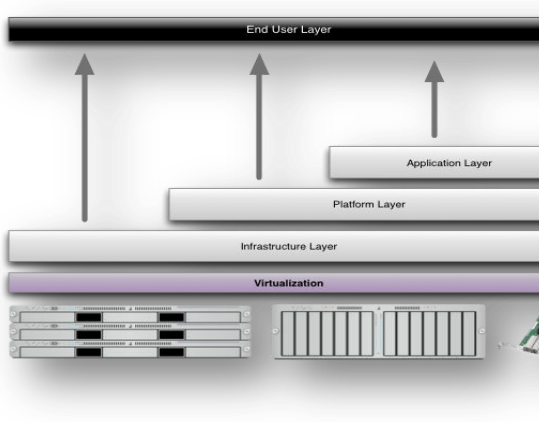
the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

- **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.

Characteristics of cloud computing

Services Models:

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.



Structure of service models

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.

II.LITERATURE SURVEY

- The field of attribute-based encryption (ABE) has evolved significantly to address the challenges of fine-grained data access control and security in various contexts, including cloud computing. The work by V. Goyal, O. Pandey, A. Sahai, and B. Waters (2006) introduces "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data". This study presents Key-Policy Attribute-Based Encryption (KP-ABE), a cryptographic system that enhances the granularity of data sharing by associating ciphertexts with attribute sets and linking private keys to specific access structures. This method allows for more precise control over who can decrypt the data, addressing limitations in traditional encryption schemes that only offer coarse-grained access. Building on this, M. Chase and S. S. M. Chow (2009) explore improvements in "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption". Their work focuses on multi-authority ABE schemes, where multiple authorities manage different attribute sets. The paper proposes enhancements to avoid the privacy pitfalls of previous models, such as those that relied on a central authority capable of decrypting all ciphertexts, thus exposing user information. The authors suggest removing the central authority and preventing the aggregation of user attributes across authorities to bolster privacy and usability.
- In a similar vein, H. Lin, Z. Cao, X. Liang, and J. Shao (2013) present "Secure Threshold Multi-Authority Attribute-Based Encryption Without a Central Authority". This paper

introduces a threshold multi-authority fuzzy identity-based encryption (MA-FIBE) scheme, which eliminates the need for a central authority. The scheme requires a user to obtain decryption rights from a subset of attribute authorities, thus mitigating the risk of a single point of failure and enhancing system security through distributed control.

- V. Božović, D. Socek, R. Steinwandt, and V. I. Villányi (2014) further extend this research with their paper "Multi-Authority Attribute-Based Encryption with Honest-But-Curious Central Authority". They propose an ABE scheme where a central authority, although honest, may be curious about the data. The scheme ensures that only authorized recipients can decrypt ciphertexts while allowing the central authority to follow the protocol honestly but remain curious, thus offering a balance between security and practicality.
- Finally, J. Hur (2015) addresses the application of ABE in smart grid environments in "Attribute-Based Secure Data Sharing with Hidden Policies in Smart Grid". This study focuses on the secure sharing of sensitive data and access policies within smart grids. It introduces a scheme where both the data and the access policies are obfuscated to prevent unauthorized access and protect privacy. The approach enhances policy expressiveness and reduces the computational burden on recipients by delegating decryption tasks to more capable grid management systems.

III.EXISTING SYSTEM

- Various techniques have been proposed to protect the data contents privacy via access control. Identity-based encryption (IBE) was first introduced by Shamir, in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it.
- Few years later, Fuzzy Identity-Based Encryption is proposed, which is also known as Attribute-Based Encryption (ABE).
- The work by Lewko *et al.* and Muller *et al.* are the most similar ones to ours in that they also tried to decentralize the central authority in the CP-ABE into multiple ones.

- ❖ Lewko *et al.* use a LSSS matrix as an access structure, but their scheme only converts the AND, OR gates to the LSSS matrix, which limits their encryption policy to boolean formula, while we inherit the flexibility of the access tree having threshold gates.
- ❖ Muller *et al.* also supports only Disjunctive Normal Form (DNF) in their encryption policy.

disadvantages of existing system

- The identity is authenticated based on his information for the purpose of access control (or privilege control in this paper).
- Preferably, any authority or server alone should not know any client's personal information.
- The users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes considerable problems in implementation.

IV.PROPOSED SYSTEM

- ❖ The data confidentiality, less effort is paid to protect users' identity privacy during those interactive protocols. Users' identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes.
- ❖ We propose AnonyControl and AnonyControl-Fallow cloud servers to control users' access privileges without knowing their identity information. In this setting, each authority knows only a part of any user's attributes, which are not enough to figure out the user's identity. The scheme proposed by Chase et al. considered the basic threshold-based KP-ABE. Many attribute based encryption schemes having multiple authorities have been proposed afterwards.
- ❖ In our system, there are four types of entities: *N Attribute Authorities* (denoted as *A*), *Cloud Server*, *Data Owners* and *Data Consumers*. A user can be a Data Owner and a Data Consumer simultaneously.
- ❖ Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute

set is divided into N is joint sets and controlled by each authority, therefore each authority is aware of only part of attributes.

advantages of proposed system

- 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*.
- The proposed schemes are tolerant against authority compromise, and compromising of up to $(N-2)$ authorities does not bring the whole system down.
- We provide detailed analysis on security and performance to show feasibility of the scheme *AnonyControl* and *AnonyControl-F*.
- We firstly implement the real toolkit of a multiauthority based encryption scheme *AnonyControl* and *AnonyControl-F*.

V.IMPLEMENTATION

1. Attribute Authorities
2. Data Owners
3. Cloud Server
4. Data Consumers

MODULES DESCRIPTION:

Attribute Authorities:

Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting his/her attributes.

Data Consumers:

Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities.

Data Owners:

Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. Then, the owner defines the access policies over attributes from multiple attribute authorities and

encrypts the content keys under the policies.

Cloud Server:

Then, the owner sends the encrypted data to the cloud server together with the cipher-texts. They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the cipher text; the user is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data.

VI.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 Anony- Control 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 [39]–[41] who support efficient user revocation is one of our future works.

VII.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. 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. 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.

[16] J. Hur, “Attribute-based secure data sharing with hidden policies in smart grid,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171–2180, Nov. 2013.