

## Implementation of Attribute- Based Encryption in Maintaining User Privilege and Anonymity over Cloud Data

**M.Parimala**

Associate Professor

Department of CSE

Tirumala Engineering College.

**K.Pradeep Reddy**

Associate Professor

Department of CSE

Tirumala Engineering College.

**G.Chaithanya**

M.Tech Student

Department of CSE

Tirumala Engineering 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 semi anonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes.*

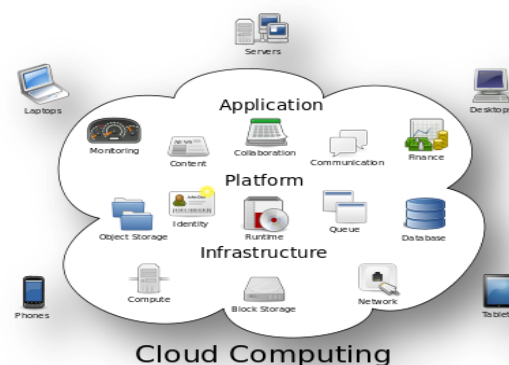
*AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, 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.

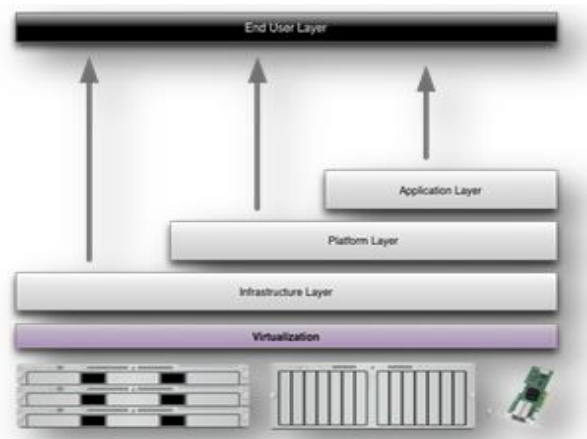
5 Essential Characteristics of Cloud Computing



### 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.

### 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  $\rightarrow \text{PK}, \text{MK}_k$  : 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  $\text{PK}$  as well as an authority-wide public parameter  $\text{y}_k$ , and to individually compute a master key  $\text{MK}_k$ .  $\text{KeyGenerate}(\text{PK}, \text{MK}_k, \text{Au}) \rightarrow \text{SK}_u$ : This algorithm enables a user to interact with every attribute authority, and obtains a private key  $\text{SK}_u$  corresponding to the input attribute set  $\text{Au}$ .  $\text{Encrypt}(\text{PK}, M, \{\text{Tp}\}_{p \in \{0, \dots, r-1\}}) \rightarrow (\text{CT}, \text{VR})$ : This algorithm takes as input the public key  $\text{PK}$ , a message  $M$ , and a set of privilege trees  $\{\text{Tp}\}_{p \in \{0, \dots, r-1\}}$ , where  $r$  is determined by the encrypter. It will encrypt the message  $M$  and returns a ciphertext  $\text{CT}$  and a verification set  $\text{VR}$  so that a user can execute specific operation on the ciphertext if and only if his attributes satisfy the corresponding privilege tree  $\text{Tp}$ . As we defined,  $\text{T}_0$  stands for the privilege to read the file.  $\text{Decrypt}(\text{PK}, \text{SK}_u, \text{CT}) \rightarrow M$  or verification parameter: This algorithm will be used at file controlling (e.g. reading, modification, deletion). It takes as input the public key  $\text{PK}$ , a ciphertext  $\text{CT}$ , and a private key  $\text{SK}_u$ , which has a set of attributes  $\text{Au}$  and corresponds to its holder's  $\text{GID}_u$ .

### 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.

### INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

### OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in a maze of instant. Thus the objective of input design is to create an input layout that is easy to follow

### **OUTPUT DESIGN**

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displayed for immediate need and also the hard copy output. It is the most important and direct source of information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analyzing design computer output, they should identify the specific output that is needed to meet the requirements.

2. Select methods for presenting information.

3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- ❖ Convey information about past activities, current status or projections of the future.
- ❖ Signal important events, opportunities, problems, or warnings.
- ❖ Trigger an action.
- ❖ Confirm an action.

### **SYSTEM TESTING**

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way

to check the functionality of components, sub-assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

### **TYPES OF TESTS**

#### **Unit testing**

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application. It is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results

#### **Integration testing**

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfactory, as shown by successful unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

#### **Functional test**

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals. Functional testing is centered on the following items:

**Valid Input** : identified classes of valid input must be accepted.

**Invalid Input** : identified classes of invalid input must be rejected.

**Functions** : identified functions must be exercised.

**Output** : identified classes of application outputs must be exercised.

**Systems/Procedures:** interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

### System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

### White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

### Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the

software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

### 6.1 Unit Testing:

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

### Test strategy and approach

Field testing will be performed manually and functional tests will be written in detail.

### Test objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

### Features to be tested

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

### 6.2 Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

### Test Results:

All the test cases mentioned above passed successfully. No defects encountered.

### 6.3 Acceptance Testing:

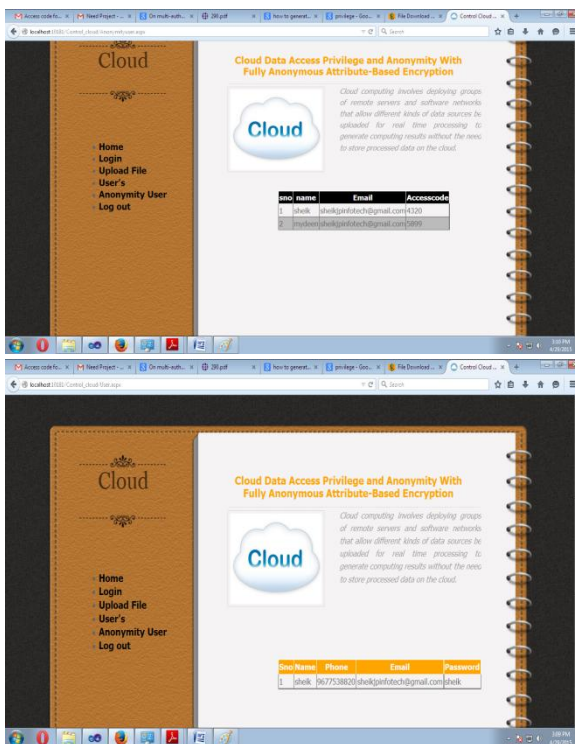
User Acceptance Testing is a critical phase of any project and requires significant participation by the end

user. It also ensures that the system meets the functional requirements.

**Test Results:**

All the test cases mentioned above passed successfully. No defects encountered.

**RESULTS:**



**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] 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.