www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

CLOUD INFORMATION ENTRY RIGHTS AND CONFIDENTIALITY THOROUGH INCOGNITO ATTRIBUTE ORIENTED CRYPTOGRAPHY

[1] Mr. Snvasrk Prasad,[2] Y. Nikhitha,[3] V. Rakshitha,[4] S. Bhanu Prakash,[5] V. Vn Rajeev Chandra
[1]Assistant Professor,[2345]B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

Cloud computing is a revolutionary computing paradigm, which enables flexible, on- demand, and low-cost usage of computing resources, but the data is outsourcedto some cloud servers, and various privacy concerns emerge from it. Various schemes based on the attribute-based encryption have been proposed to secure thecloud 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 Anony Control to address not only the data privacy, but also the user identity privacy in existing access control schemes. Anony Control 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 privilegesof all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the Anony Control-F, which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both Anony Control and Anony Control-F are secure under the decisional bilinear Diffie– Hellman assumption, and our performance evaluation exhibits the feasibility of ourschemes.

I. 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.

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 ofsystems 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 computingcapabilities, 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 toconsumer 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 levelof 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.

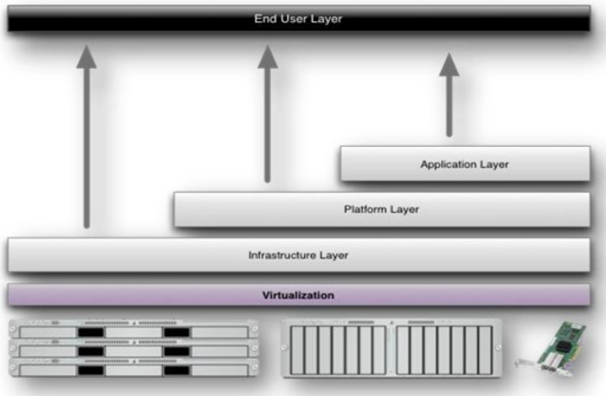
Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstractionappropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported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

On-demand self-service
Ubiquitous network access
Location transparent resource pooling
Rapid elasticity
Measured service with pay per use
jpinfotech.org

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 ofthese 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 yourlife so much easier!

7. Monitor projects more effectively. Stay within budget and ahead ofcompletion cycle times.

8. Less personnel training is needed. It takes fewer people to do more workon a cloud, with a minimal learning curve on hardware and software issues.

9. Minimize licensing new software. Stretch and grow without the need to buyexpensive software licenses or programs.

Improve flexibility. You can change direction without serious “people” or“financial” issues at stake.

II. LITERATURE SURVEY

TITLE: Attribute-based encryption for fine-grained access control of encrypted data

AUTHORS: V. Goyal, O. Pandey, A. Sahai, and B. Waters

ABSTRACT: As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving anotherparty your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP- ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keysare associated with access structures that control which ciphertexts a user is able to decrypt.

TITLE: Improving privacy and security in multi-authority attribute-basedencryption

AUTHORS: M. Chase and S. S. M. Chow

ABSTRACT: Attribute based encryption (ABE) [13] determines decryption ability based on a user’s attributes. In a multi-authority ABE scheme, multiple attribute- authorities monitor differ-ent sets of attributes and issue corresponding decryption keys to users, and encryptors can require that a user ob-tain keys for appropriate attributes from each authority be-fore decrypting a message. Chase [5] gave a multi-authorityABE scheme using the concepts of a trusted central author-ity (CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every ciphertext, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted author-ities. Moreover, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user’s attributes, which unnecessarilycompromises the privacy of the user. In this paper, we propose a solution which removes the trusted central authority, and protects the users privacy by preventingthe authorities from pooling their information on particular users, thus making ABEmore usable in practice.

TITLE: Secure threshold multi authority attribute based encryption without acentral authority

AUTHORS: H. Lin, Z. Cao, X. Liang, and J. Shao

ABSTRACT: An attributebased encryption scheme (ABE) is a cryptographic primitive in which every user is identified by a set of attributes, and some function of these attributes is used to determine the ability to decrypt each ciphertext. Chase proposed the first multi authority ABE scheme in TCC 2007 as an answer to an open problem presented by Sahai and Waters in EUROCRYPT 2005. However, her scheme needsa fully trusted central authority which can decrypt every ciphertext in the system. This central authority would endanger the whole system if it’s corrupted.

TITLE: Multi-authority attribute-based encryption with honest-but-curious central authority

AUTHORS: V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi

ABSTRACT: An attribute-based encryption scheme capable of handling multiple authorities wasrecently proposed by Chase. The scheme is built upon a single-authority attribute- based encryption scheme presented earlier by Sahai and Waters. Chase's construction uses a trusted central authority that is inherently capable of decrypting arbitrary ciphertexts created within the system. We present a multi-authority attribute- based encryption scheme in which only the set of recipients defined by the encrypting party can decrypt a corresponding ciphertext. The central authority is viewed as ‘honest- but-curious’: on the one hand, it honestly follows the protocol, and on the other hand, it is curious to decrypt arbitrary ciphertexts thus violating the intent of the encrypting party. The proposed scheme, which like its predecessorsrelies on the Bilinear Diffie–Hellman assumption, has a complexity comparable tothat of Chase's scheme. We prove that our scheme is secure in the selective ID model and can tolerate an honest-but-curious central authority.

TITLE: Attribute-based secure data sharing with hidden policies in smart grid

AUTHORS: J. Hur

ASTRACT: Smart grid uses intelligent transmission and distribution networks to deliver electricity. It aims to improve the electric system's reliability, security, and efficiency through two-way communication of consumption data and dynamic optimization of electric-system operations, maintenance, and planning. The smart grid systems use fine-grained power grid measurements to provide increased grid stability and reliability. Key to achieving this is securely sharing the measurementsamong grid entities over wide area networks. Typically, such sharing follows

policies that depend on data generator and consumer preferences and on time- sensitive contexts. In smart grid, as well as the data, policies for sharing the data may be sensitive because they directly contain sensitive information, and reveal information about underlying data protected by the policy, or about the data owner or recipients. In this study, we propose an attribute-based data sharing scheme in smart grid. Not only the data but also the access policies are obfuscated in grid operators' point of view during the data sharing process. Thus, the data privacy and policy privacy are preserved in the proposed scheme. The access policy can be expressed with any arbitrary access formula. Thus, the expressiveness of the policyis enhanced. The security is also improved such that the unauthorized key generation center or the grid manage systems that store the data cannot decrypt the data to be shared. The computation overhead of recipients are also reduced by delegating most of the laborious decryption operations to the more powerful grid manage systems.

III. SYSTEM ANALYSIS & DESIGN

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

- 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

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 Nis joint sets and controlled by each authority, therefore each authority is aware of only part of attributes.

ADVANTAGES

- 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.

SYSTEM ARCHITECTURE

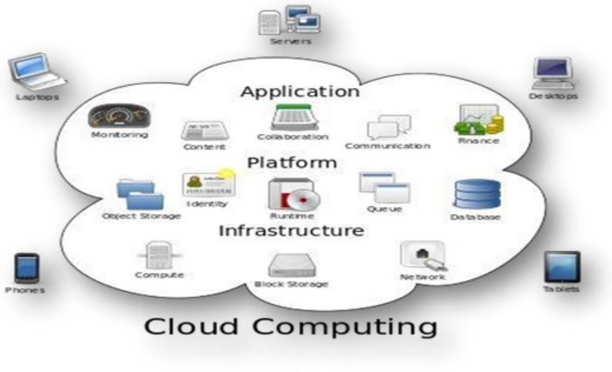


Fig. SYSTEM ARCHITECTURE

IV. IMPLEMENTATION

MODULES

- Attribute Authorities
- Data Owners
- Cloud Server
- Data Consumers

MODULE 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 attributekey 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

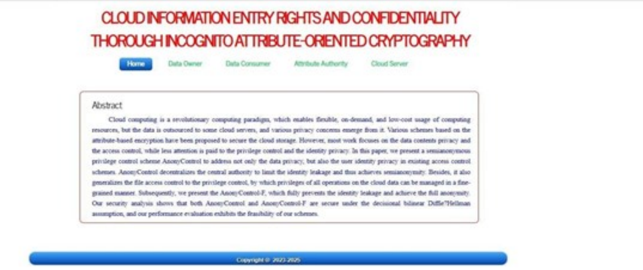
Data Owners:

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.

V. SCREENSHOTS

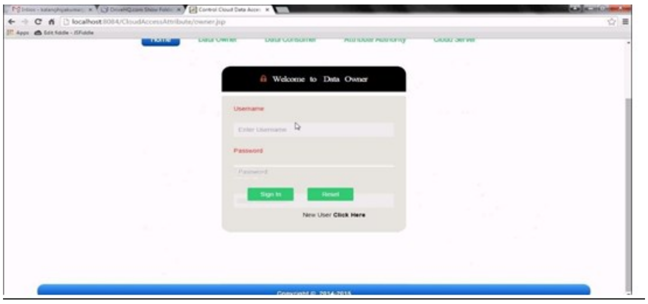

CLOUD INFORMATION ENTRY RIGHTS AND CONFIDENTIALITY THOROUGH INCOGNITO ATTRIBUTE-ORIENTED CRYPTOGRAPHY

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.

Copyright © 2023-2025

FIG 1 : HOME PAGE

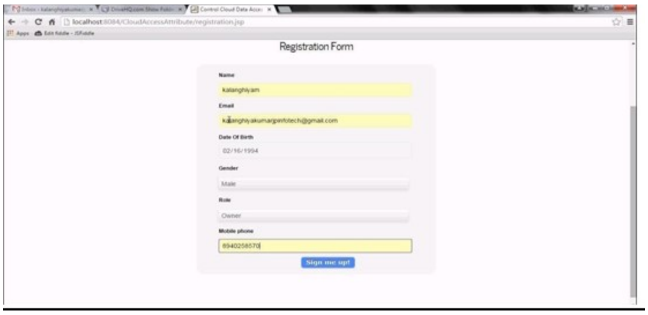

localhost:8084/CloudAccessAttribute/owner.jsp

Welcome to Data Owner

Username: Enter Username

Password: Password

FIG 2: DATA OWNER LOGIN


localhost:8084/CloudAccessAttribute/registration.jsp

Registration Form

Name: kalanghiyam

Email: kalanghiyakumarjpinfotech@gmail.com

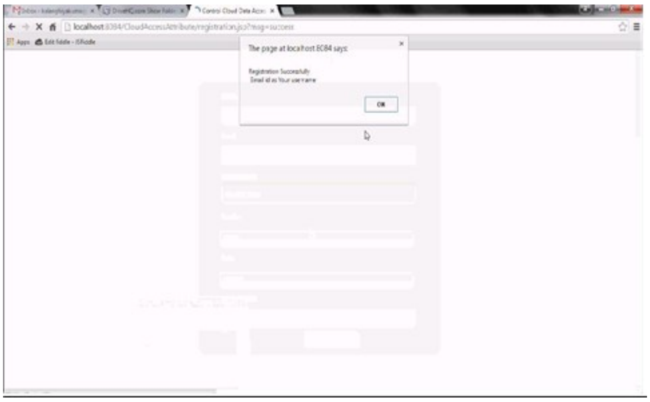
Date Of Birth: 02/16/1994

Gender: Male

Role: Owner

Mobile phone: 8940258570

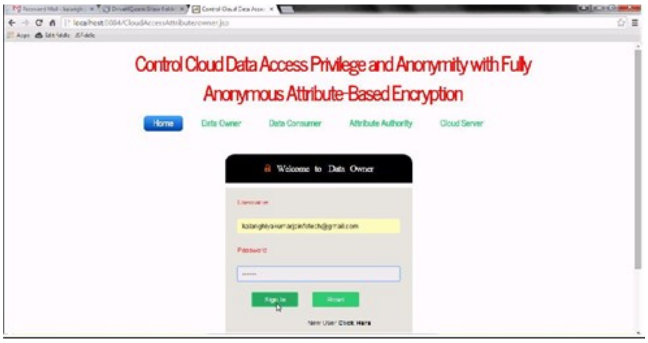
FIG 3 : USER REGISTRATION


localhost:8084/CloudAccessAttribute/registration.jsp?msg=success

The page at localhost:8084 says:

Registration Successfully
Email id as Your username

FIG 4 : REGISTRATION SUCCESS


localhost:8084/CloudAccessAttribute/owner.jsp

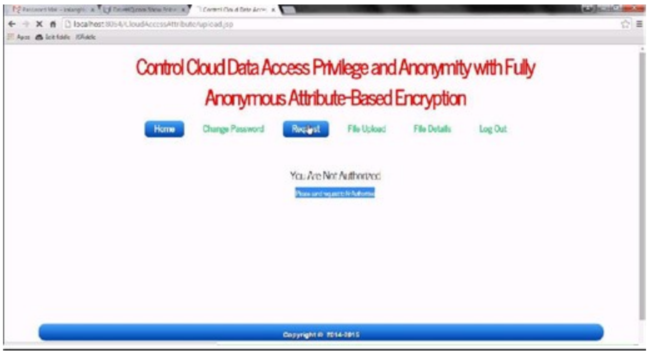
Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption

Welcome to Data Owner

Username: kalanghiyakumarjpinfotech@gmail.com

Password: ••••••

FIG 5: LOGIN PAGE


localhost:8084/CloudAccessAttribute/upload.jsp

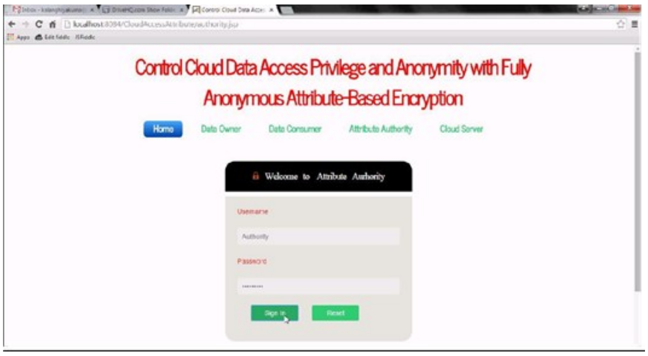
Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption

You Are Not Authorized

Please send request to Authority

Copyright © 2014-2015

FIG 6: ACCESSING REQUEST PAGE


localhost:8084/CloudAccessAttribute/authority.jsp

Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption

Welcome to Attribute Authority

Username: Authority

Password: ••••••••

FIG 7: ATTRIBUTE AUTHORITY LOGIN

VI. CONCLUSION

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.

FUTURE SCOPE

- This project aims to solve security challenges in the cloud by ensuring your information is entered and kept confidential safely. Using an innovative approach called "Cloud Information Entry Rights and Confidentiality through Incognito Attribute-Oriented Cryptography," it plans to create a smart system that adapts to user needs while keeping data private. The goal is to make cloud data management secure, user-friendly, and adaptable.
- In the complex world of cloud security, this project addresses the challenges of safely entering and keeping information private. Through "Cloud Information Entry Rights and Confidentiality through Incognito Attribute-Oriented Cryptography," it aims to create a smart system that adapts to user needs, providing a secure and private.

REFERENCES

1. A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advancesin 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.