International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 9 – JUNE 2017.

A Secured and Efficient way for Data Access using Hierarchy-Attribute based Architecture on Cloud

Mohammed Sayeed Ahmed [#1], Harshavardhana Doddamani[*2] and Bharathi M [*2]

[#] *Department of CSE,SJCIT, Chickballapur,Karnataka, India*

***Abstract*— To solve the challenging problem of data sharing in cloud computing, Cipher text-policy attribute-based encryption (CP-ABE) has been a preferred encryption technology. The shared data files generally have the characteristic of multilevel hierarchy, particularly in applications like healthcare and the military. The hierarchy structure of shared files has not been explored in CP-ABE. In this project, we have proposed and implemented an efficient file hierarchy attribute-based encryption scheme in cloud computing.**

By using CP-ABE techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks which makes it more useful for the applications deployed on cloud. Earlier Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. So, our project is conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC).

***Index Terms*— Cipher text-policy attribute-based encryption (CP-ABE),Role-Based Access Control (RBAC),Attribute based Encryption,Cloud computing.**

I. INTRODUCTION

The advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data have to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. With widespread network technology and mobile terminal, online data sharing has become a new "pet", such as Facebook. Cloud computing is one of the most promising application platforms to solve the explosive expanding of data sharing. In cloud computing, for protecting the data from leaking, users need to encrypt their data before being shared. Access control is first line of defense that prevents unauthorized access to the shared data.

In cloud computing owner/authority accepts the user enrollment and creates some parameters. CSP (Cloud service provider) is the manager of cloud servers and provides multiple services for client. Data owner encrypts and uploads the generated cipher text to CSP. User downloads and decrypts the interested cipher text from CSP. The shared files usually have hierarchical structure. That is, a group of files are divided into a number of hierarchy subgroups located at different access levels. If the files in the same hierarchical structure could be encrypted by an integrated access structure, the storage cost of cipher text and time cost of encryption could be saved.

This project is including the modules that are uploading the files from the users also as well as they can download by using the secrete key. In existing system, there is no any restriction to users but this project. Retrieval result based on hierarchy by the cloud server according to some privileges criteria.

A. Problem Definition

To demonstrate the secured and efficient access to data from cloud by developing a web application. This application should allow the users to get registered with the cloud/service provider hosting the application. Usually Administrators and Data owners would have the privilege of storing/uploading data to the cloud. This application should provide privilege for a registered user to upload an encrypted file to the cloud. Users should also be able to download the files by using the secret key which is generated during the process of uploading the file.

B. Scope and Objectives

1) Scope

The scope of the project is to develop the software for user who use cloud for storing data and retrieving the data. User should be able to store and retrieve the files (functionality for Uploading and Downloading). Establishing security of the shared files by using CP-ABE scheme with hierarchical access and providing an efficient file sharing solution to the customers over the cloud.

2) Objectives

1. To provide secured way of storing data based on Ciphertext-Policy attribute-based encryption (CP-ABE) on the cloud server according to some privileges criteria having hierarchical access.

2. To give the result accurately and confidentially by using secret key while downloading the data from server.

II. LITERATURE SURVEY

To gain conceptual understanding some papers were studied which are related to security for accessing data over cloud.

A. Two Factor Authentication and Access Control for Cloud Computing Services

The system setup process consists of two parts. The first part TSetup is run by a trustee to generate public parameters. The second part A Setup is run by the attribute issuing authority to generate its master secret key and public key. The process of authenticating the user and access control mechanism consist of mainly two steps.

1) User Key Generation Phase

The user key generation process consists of three parts. First, the user generates his secret and public key in USetup. Then the security device is initialized by the trustee in Device Initialization. All the public parameters generated are used during the authentication process. Finally, the attribute issuing authority generates the user attribute secret key according to the user's attribute in AttrGen. The secret generated by the attribute issuing authority determines which all data the user can access and this key is stored in the user computer. The user has to use his own computer and the USB key storage each time for accessing the cloud. Additional recovery options are also provided.

2) Access Authentication Phase

The access authentication process is an interactive protocol between the user and the cloud service provider. It requires the user to have his partial secret key, attribute secret key and the security device each time the user is accessing the cloud.

B. An Efficient Cloud-based Revocable Identity-based Proxy Re-encryption Scheme for Public Clouds Data Sharing

i) Identity-based encryption (IBE) eliminates the necessity of having a costly certificate verification process. However, revocation re-mains as a daunting task in terms of cipher text update and key update phases. In this paper, we provide an affirmative solution to solve the efficiency problem incurred by revocation. We propose the first cloud-based revocable identity-based proxy re-encryption (CR-IB-PRE) scheme that supports user revocation but also delegation of decryption rights. No matter a user is revoked or not, at the end of a given time period the cloud acting as a proxy will re-encrypt all cipher texts of the user under the current time period to the next time period. If the user is revoked in the forthcoming time period, he cannot decrypt the cipher texts by using the expired private key anymore. Comparing to some naive solutions which require a private key generator (PKG) to interact with non-revoked users in each time period, the new scheme provides definite advantages in terms of communication and computation efficiency.

C. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

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 another party 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, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

D. A Survey on File Hierarchy Based Encryption and Geo Encryption Scheme for Efficient Data Sharing in Cloud

Data sharing in cloud is very popular. In the cloud consists of different types of files. Normally in cloud for encryption cipher-text policy attribute based encryption(CP-ABE) method can be used. But it can only suitable for normal files. But the shared file is having the property of multi-level hierarchy. so for this type of file cipher – text policy attribute encryption(CP-ABE) is not possible particularly in health and military organization. More and more security is needed for this kind of organization. In this paper policy based file hierarchy encryption scheme and geo encryption scheme is used for shared file in cloud. In this the layer access structure are combine into one access structure and then the hierarchy are encrypted with combined structure. Here the ciphertext element related to attribute shared by files. Therefore, both the ciphertext data and cost of encryption saved. More over the proposed scheme is proved to be secure under the standard assumption of geo Encryption and the proposed scheme is more powerful in both encryption and decryption.

In the recent technology cloud computing is most powerful application in data sharing. In cloud computing the data is protected from leaking. The user encrypts the data before sharing into the cloud. Normally cipher-text policy attribute based encryption is a technique it more and more security and it is useful for general application. In cipher text policy user private key is associated with the set of attributes within the system. A user will be able to decrypt a ciphertext if and only if attributes satisfy the policy of respective cyphertext policies defined over attributes using conjunction and disjunction.

III. SYSTEM REQUIREMENT SPECIFICATIONS

System Requirement Specification (SRS) is the major part of process in the development of software. It consists the complete description, important functional requirements, ability to support, requirements for performance increase, design conditions etc. for any application. This technique is

very much useful in completing the goals while developing or implementing any of the software projects.

A. *Purpose of SRS*

Identify the product whose software requirements are specified in this document, including the revision or release number. If this SRS pertains to only part of the entire system, identify the portion or subsystem that it addresses. The purpose of the project "A Secured and Efficient way for Data Access using Hierarchy-Attribute based Architecture on Cloud" is to enable the user for uploading/downloading the files into the cloud in an encrypted form by using efficient CP-AB Encryption scheme with hierarchical access.

IV. USE CASE DIAGRAM:

The use cases are shown with respect requirement.

A. *Use case Diagram for owner:*

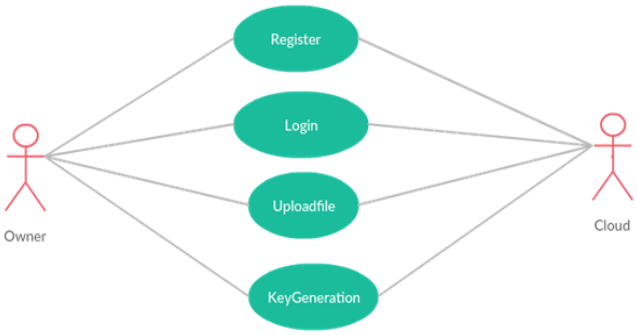


Fig:Use case diagram for admin

1.Register: Data owner going to register on cloud by entering email id, username, password, mobile number.

2. Login: Here Data owner is going to login in to the cloud server using Username and password, if its incorrect it gives error

3.Upload File: Data owner upload the file with Encrypted form after entering into the cloud.

4.Key Generation: once data owner uploads the file secret key of the particular file will be generated.

B. *Use case Diagram for User:*

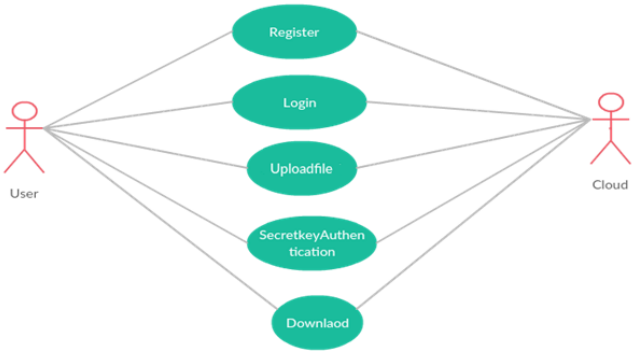


Fig:Use Case diagram for User

1. **Register:** User is going to register on cloud by entering email id, user name password, mobile number

2. User Login:

ii) Here user is going to login in to the cloud server using Username and password, if its incorrect it gives error.

iii)

3. Upload File:

iv) Once the user logs in he/she should have option to upload the file onto the cloud.

v)

vi)

4. Secure Key Authentication:

vii) As part of the upload process a secret key gets generated and it will be sent to the user for downloading the file.

viii)

5. File download:

ix) User is able to download respected file, only if he authenticates successfully otherwise file cannot be downloaded.

x)

V. SYSTEM ANALYSIS

The objective of the system analysis is to study the existing system and propose a suitable system based on the problem definition.

A. *Existing System*

In existing system, the user can download file by using secret key but every user can able to access every file there is restriction on file Structure. For each file has contain own secret key.

1) Advantages

xi) * Data can be downloading without verification.

xii) * Data recovery is easy.

xiii) * Low price as well as low space.

xiv) * There is no computation, and storage capacity is less.

2) Disadvantages

xv) * In existing system, there is no restriction on file access.

xvi) * Level of security is very less

B. *Proposed System*

In proposed system, we are providing the option to user for uploading the files into the cloud in the form of encrypted form by using efficient CPAB Encryption algorithm. As well as we provide the security and confidentiality for all uploaded files by enable the hierarchy based access to the particular files. This will be increasing the level of security.

1) Advantages of Proposed system

- User can upload the files in the form of encrypted.
- It uses encryption algorithms to secure the data or minimize the size of data
- The result of file request or download file is accurate.
- It will increase the level of security

- It is more secure and compatible.
- It enables the integrity and confidentiality.

xvii)

xviii)

2) Existing v/s proposed system

xix) Existing system does not have efficient algorithm for encryption whereas proposed system will have a facility to more secure algorithm.

xx) Existing system does not have uploading option to the users whereas proposed system provides the upload option to the users.

xxi) Existing system fails in confidentiality whereas proposed system enable the confidentiality.

3) Constraints

- The user can't access the data if the user is not connected to the internet.
- Storage capacity of the cloud is limited.
- The user always interacts with English GUI interface.

VI. SYSTEM DESIGN

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. Systems design implies a systematic approach to the design of a system. It may take a bottom-up or top-down approach, but either way the process is systematic wherein it takes into account all related variables of the system that needs to be created—from the architecture, to the required hardware and software, right down to the data and how it travels and transforms throughout its travel through the system.

A. Architectural Design

The architecture diagram describes the whole system is working in a systematic way.

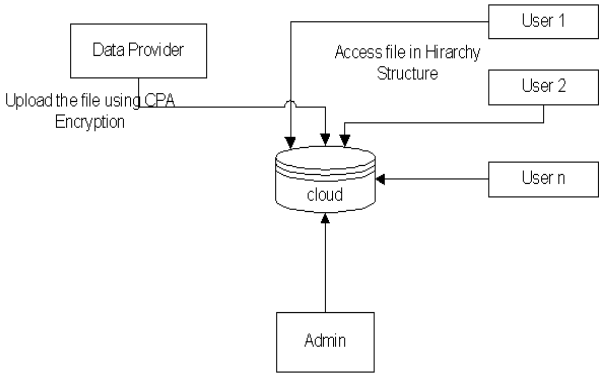


Fig.Architecture diagram

Data User Module: This module includes the user registration login details.

Data Owner Module: This module helps the owner to register them details and also include login details.

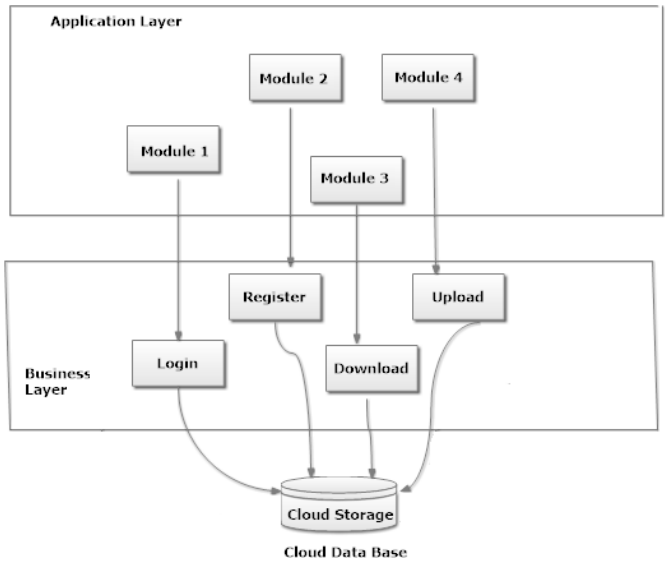
File Upload Module: This module helps his file the owner to upload with encryption using AES algorithm for key generation and CPABE for file encryption. This ensures the files to be protected from unauthorized user.

File Request Module: This module ensures the user to request the file.

File Download Module: This module allows the user to download the file using his secret key to decrypt the downloaded data.

Uploaded and Downloaded File: This module helps to users for uploading the file and also downloading the files by using Secure key.

B. Logic View



xxii) The architectural design includes three tiers: application tier, business tier and the database. Application layer includes the user interface for the admin and the user. This layer includes user registration, login, etc…

xxiii)

xxiv) Business tier includes business logic of all the modules where data undergoes various modules. The results of all the modules performed on the data are stored in the centralized cloud storage data base.

C. Detailed Design

Any design is incomplete without the UML. Detail design consists of:

1. Class Diagram
2. Sequence Diagram
3. Data flow diagrams
4. Flow Diagram

D. Class diagram

Class diagram is a structure diagram which explain the details of designed system in the form of classes and interfaces, and also it provide the futures of the classes, constraints and relationships - associations, etc.

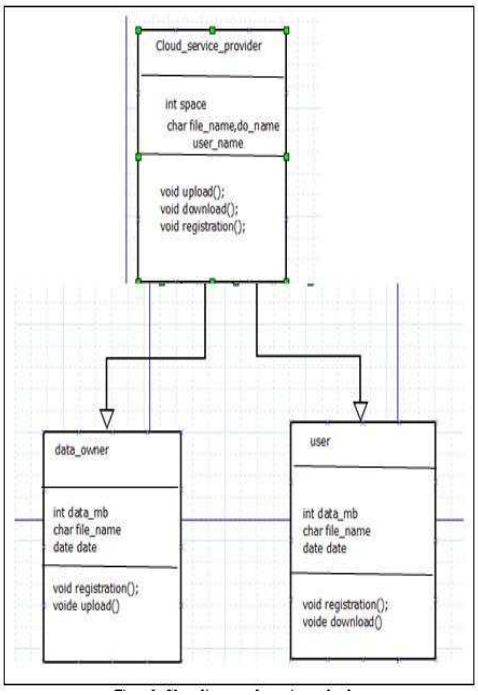


Fig:class diagram

E. Sequence Diagram:

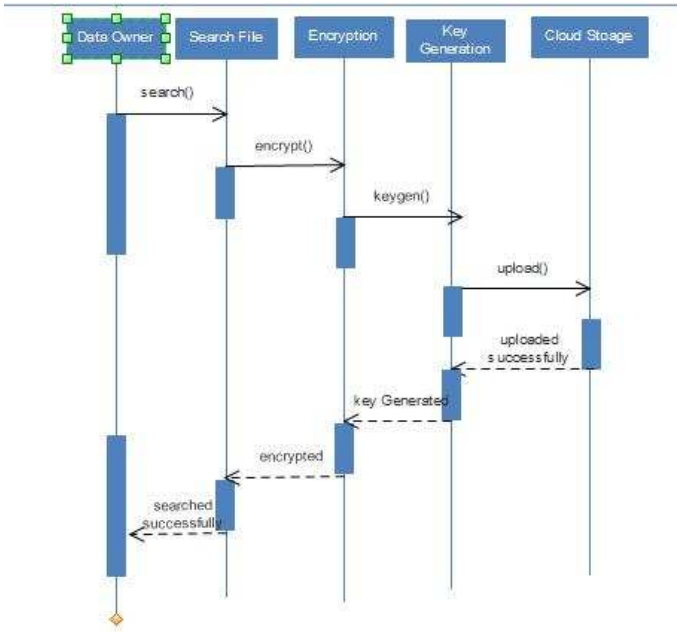


Fig:Sequence diagram of Data owner

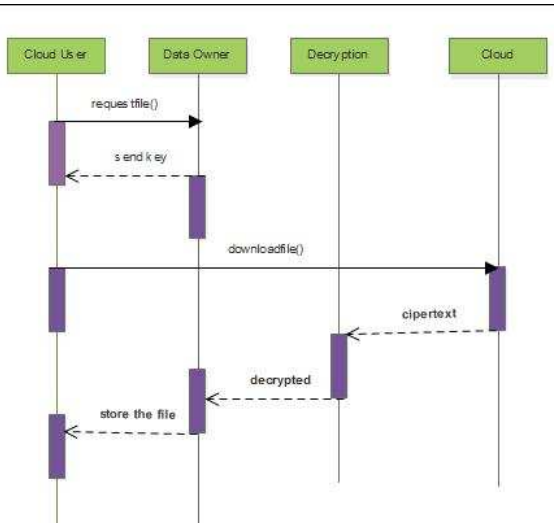


Fig:Sequence diagram of user

The figure shows a main window appears where the user enters user name and password and logs in to get the main menu. He can add the files into the cloud server and user wants to login into the cloud for access the file he should be valid user and once he login he can look for the file which is stored in the cloud and provide the secret key. Once the secret key is provided then he can download the file.

VII. SYSTEM IMPLEMENTATION

An implementation is a realization of a technical specification or algorithm as a program, software component, or other computer system through computer programming and deployment.

A. Tools and languages used:

Data base used is MYSQL, since it is an open source database system, occupies less space on disk and can be installed in all major operating system.

JavaScript is used for providing alert message and pop up message if any invalid entry. PHP is used for server side scripting since one can connect to database easily and it is relatively fast.

Jquery and CSS are used for creating Animation for Webpages and also border and shadow applied for data submission form.

B. Module Description

1) Registration Page

Purpose	The purpose of this test is to ensure that the user can registrar.
External Dependencies	Ensure that the Cloud Device has internet connectivity.
Test Description	1) Click the registration page. 2) Fill the given Entry Type. 3) Click the Submit button.
Expected Results	Its shows the Successful registration message.

2) User Login Page

Purpose	The purpose of this test is to ensure that the user can login.
External Dependencies	Ensure that the Cloud Device has internet connectivity.
Test Description	1) Click the login page. 2) User provides the username and password correctly. 3) Click the login button.
Expected Results	User can able to access the next page.

3) Admin Login Page

Purpose	The purpose of this test is to ensure that the Admin can login.
External Dependencies	Ensure that the Cloud Device has internet connectivity.
Test Description	1) Click the login page. 2) Fill the given Entry Type. 3) Click the Submit button.
Expected Results	Its shows the admin page.

4) Upload Module

Purpose	The purpose of this test is to ensure that the Admin can upload the files.
External Dependencies	Ensure that the Cloud Device has internet connectivity.
Test Description	1) Click the upload button for upload the file into cloud. 2) Select the file to upload. 3) Click the upload button.
Expected Results	Its shows the Successful upload message.

5) Download Module

Purpose	The purpose of this test is to ensure that the user can download the files.
External Dependencies	Ensure that the Cloud Device has internet connectivity.
Test Description	1) Click the search button for download the file from cloud. 2) Select the file name for download. 3) Enter the OTP key for download. 4)Click the Submit button
Expected Results	Its shows the Successful download the file.

VIII. CONCLUSION AND FUTURE ENHANCEMENT

This Section is about to discussion of the conclusion of this project work and also the future enhancement .

A. Conclusion

File Hierarchy CP-ABE is a feasible scheme which has much more flexibility and is more suitable for general application. Multiple hierarchical files sharing is resolved using layered model of access structure. In proposed system both ciphertext storage and time cost of encryption are saved. It enables the integrity and confidentiality

B. Future Enhancement

To develop a full-fledged application by taking a realistic organization hierarchy of a company and incorporate the security features demonstrated out of this project which would cater to the needs of the organization. This must be incorporated in the context of a cloud based application where file sharing needs utmost security.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," *ACM SIGCOMM multComput. Commun. Rev.*, vol. 39, no. 1, pp. 50–55, 2009.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *RLCPS, January 2010, LNCS. Springer, Heidelberg*.

[3] A. Singhal, "Modern information retrieval: A brief overview," *IEEE Data Engineering Bulletin*, vol. 24, no. 4, pp. 35–43, 2001.

[4] I. H. Witten, A. Moffat, and T. C. Bell, "Managing gigabytes: Compressing and indexing documents and images," Morgan Kaufmann Publishing, San Francisco, May 1999.

[5] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," *IEEE Pervasive Comput.*, vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

[6] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, "TIMER: Secure and reliable cloud storage against data re-outsourcing," in *Proc. 10th Int. Conf. Inf. Secur. Pract. Exper.*, vol. 8434. May 2014, pp. 346–358.

[7] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in *Proc. 19th Eur. Symp. Res. Comput. Secur.*, vol. 8712. Sep. 2014, pp. 257–272.

[8] T. H. Yuen, Y. Zhang, S. M. Yiu, and J. K. Liu, "Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks," in *Proc. 19th Eur.Symp. Res. Comput. Secur.*,vol. 8712. Sep. 2014, pp. 130–147.

[9] K. Liang *et al.*, "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1667–1680, Oct. 2014.

[10] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, "*k*-times attribute-based anonymous access control for cloud computing," *IEEE Trans. Comput.*, vol. 64, no. 9, pp. 2595–2608, Sep. 2015.

[11] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained two factor access control for Web-based cloud computing services," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 484–497, Mar. 2016.

[12] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer, May 2005, pp. 457–473.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, Oct. 2006, pp. 89–98.

[14] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, "Efficient attribute-based encryption from R-LWE," *Chin. J. Electron.*, vol. 23, no. 4, pp. 778–782, Oct. 2014.

[15] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Secur. Privacy*, May 2007, pp. 321–334.

[16] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, Oct. 2007, pp. 456–465.

[17] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. 10th Int. Workshop Inf. Secur. Appl.*, Aug. 2009, pp. 309–323.

[18] X. Xie, H. Ma, J. Li, and X. Chen, "An efficient cipher text-policy attribute-based access control towards revocation in cloud computing," *J. Universal Comput. Sci.*, vol. 19, no. 16, pp. 2349–2367, Oct. 2013.

[19] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 763–771, May 2014.