ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Cloud Based Secure Document Sharing and Access Control for Corporate User

Kanchan S. Gajghate[1], Prof. R. V. Mante[2], Dr. K. P.Wagh[3]

M. Tech. Scholar, Department of Computer Science, Government college of Engineering, Amravati, Maharashtra, India[1]

Professor, Department of Computer Science, Government college of Engineering, Amravati, Maharashtra, India[2]

Assistant Professor, Department of Information Technology, Government college of Engineering, Amravati, Maharashtra, India[3]

ABSTRACT: Now a day Cloud Services is very popular mode for company to store their data online. Cloud services has maintain many services data storage, big data management, information system, data security and etc. and its also used for storage personal, private and secure data. This service provides better technical management for intended users to share their data securely. In this we combine time and attribute factor for time-sensitive data in public cloud storage. And also introduce the fine-grained access control for two factor authentication in web based cloud storage. We propose new advanced ABE(Attribute-Based Encryption) technique, also propose two factor authentication in which user have to go through two authentication verification typically password based and mobile based. For fine-grained access control we design systematic approach for time–sensitive data. In TAFC model, the access policy attribute store in secret key. To overcome this we design two files one is original file and another one is meta-data file. In meta-data file the access policy attribute stored in separately. Original file secret key and meta-data file secret key are dependent on each other. In our proposed system, if user want to change or update any document, he/she directly change or remove document without any encryption and decryption. By using our proposed system the size of cipher-text is remain constant. Implementation, analysis and demonstrate shows that our scheme is efficient, secure and effective.

KEYWORDS: Cloud Storage, Access control, Time-sensitive data, Fine granularity, Two-Factor.

I. INTRODUCTION

Cloud computing is the new term for vision of computing as a utility, enables convenient, on-demand network. It's a essential host of computer system that allow enterprises to sell, buy, lease, or software and other resources over the network. It is not depends on a server or any machine that physically exists, in a virtual system. There are manage application like data storage, data management, data sharing and medical information system etc. mobile app and thin client are stored user's data and business software on remote location, and through web browser end user access cloud applications. The advantages of Cloud Computing include: On-demand self-service, location independent resource pooling, rapid resource elasticity, and transference of risk. As we are storing data on cloud then we have to pay rent for the storage, more the data more the storage space we have to pay for. Sometimes it happens that we store the same data repeatedly. Actually when same data is stored again and again then we are wasting space and increasing rent. For Accessing time-sensitive data user have to login cloud services to store the data. Access control propose attribute-based access control and its better for users. It provides attribute based policy and also provides access control policy for different users. In this, they used CP-ABE and KP-ABE technique, so encryption and decryption are being done using this technique. In proposed system, we proposed advanced ABE(Attribute-Based Encryption) technique.

Cloud storage used as most of the application. These are some points that motivate to implement this system:

1. In CP-ABE technique, the access policy attribute will be stored in secret key. The document will be encrypted using this secret key. Therefore the size of the cipher text will increases according to the size of access policy

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

attributes. Also if user want to update/remove attributes, we have delete/decrypt existing document and again encrypt it.

2. To overcome this problem we will store the access policy attributes separately in meta-data file. document will be dependent on meta-data file. so the user can update/remove attribute any time without document decryption, by using our system cipher text size will remain constant.
3. In access policy file that maintain attribute of other users who will get access permission.ion of document decrypt.
4. We also proposed the two factor authentication for fine-gained access control, in two factor authentication typically password based and mobile based.

This paper is organized as follows. Section II presents related work. The details of methods used for system implementation in section III. The proposed algorithm, experimental evaluation and conclusion in describes in section IV and section V, VI.

II. RELATED WORK

K.YANG [1] propose A new CP-ABE scheme that achieve backward and forward security(DAC-MACS) with attribute revocation method and well organized decryption scheme. The associated components are need to be updated if the revoked attribute in cipher text and secret key that incur revocation method has less computation cost. I shows that DAC-MACS is secure oracle model and has less computation cost, less communication cost and storage overhead. In this, the issues of secret keys and attribute of system all manage by the expert. So the expert has authority to encrypt and decrypt all the data, its limitation of that system.

DABKS: Dynamic attribute based Keyword search in cloud computing", [3] proposes a proxy encryption that incorporates attribute-based keyword search that used for secret sharing scheme. DABKS scheme propose efficient approach to update of access policy and fine-grained access control for search engine. This scheme has full advantage of update operations to the CSP of cloud resources by delegating policy. The results shows that this system is feasible and effective. This system supports only the single key word search. Data owner update delegate policy operations that reduces it security its disadvantage of that system.

MING LI,SHUCHENG[2], This paper proposes centric frame work of data access control for a patient that stored personal health records in trusted authority. To allow fine-grained access control partially trusted cloud server give complete control to patient that encrypt their own PHR files. to reduce the complexity of key management framework addresses is the unique challenges brought by multiple users and PHR owner. The limitation of this paper is Data owner (patient) will need to generate it is a burden him/her.

Clock based proxy Re-encryption scheme in unreliable cloud,[4] focus on proxy re-encryption and cipher text policy attribute based encryption allows the cloud that can be delegated to re-encrypt data for the benefit of data owner that share secret key. Cloud allow data owner to re-encrypt the cipher text policy attribute based encryption to delegated users. When user's request reaches to CSP and data owner issues ticket to the data owner its big challenge to time lag. The time lag didn't know that user may send the delay request to update the cloud.

Ke Yuan,[7] propose concept of TRSE that can be used to solve retrieval problem of time-dependent cipher text. In PKTRSE model, to search keywords on the cloud server the sender chooses a release time. So that the receiver can not receive that keywords till the release time. Its provide more security of PKTRSE. For security model they formalize the notion of PKTRSE. They also proposed how to combine TR-PKhE with PEKS by using other cryptographic technique and used two graphics construction that prove security provide of shoulder suffering plain text attack.

III. SYSTEM IMPLEMENTATION

In proposed system we combine time and attribute factor to provide security for time-sensitive data. To remove drawback of CP-ABE and KP-ABE we maintain separate file on the server. We are used Two files in system model. The first file that contain all original document and second file that contain meta-data file. The meta-data file, maintain attributes and release time will be separate file on that system. Its more Benficial to user, because if he/she want to

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

changes or add some new access policy on the file, then he/she first decrypt or delete that document and make changesand again encrypt it. but using this proposed system user will changes or update document without original document decryption. User onlychangesin the meta-data file. so that its reduces the computation time.We also propose the two-factor authentication which increases the security and performance analysis of the system and avert from shoulder surfing and key logger attack. In attribute and time management, Attributes and release time will be stored in a meta-data file in encrypted format. If user wants to change/ remove attributes, he/she need to decrypt only Access policy file instead of whole document.

Fig.1 shows the two factor authentication, any company user login with its user id and passwords, after password authentication, user will get QR code on screen, User have to install one android app on his mobile using that android app user have to able read QR code. The app will fetch mobile's IMEI no. after fetching IMEI no is verified with registered IMEI no, after verification user will get OTP on screen. Then User have to enter that OTP in server. User can access his account and upload /download any document.

A. *Flowchart Of Two Factor Authentication :*

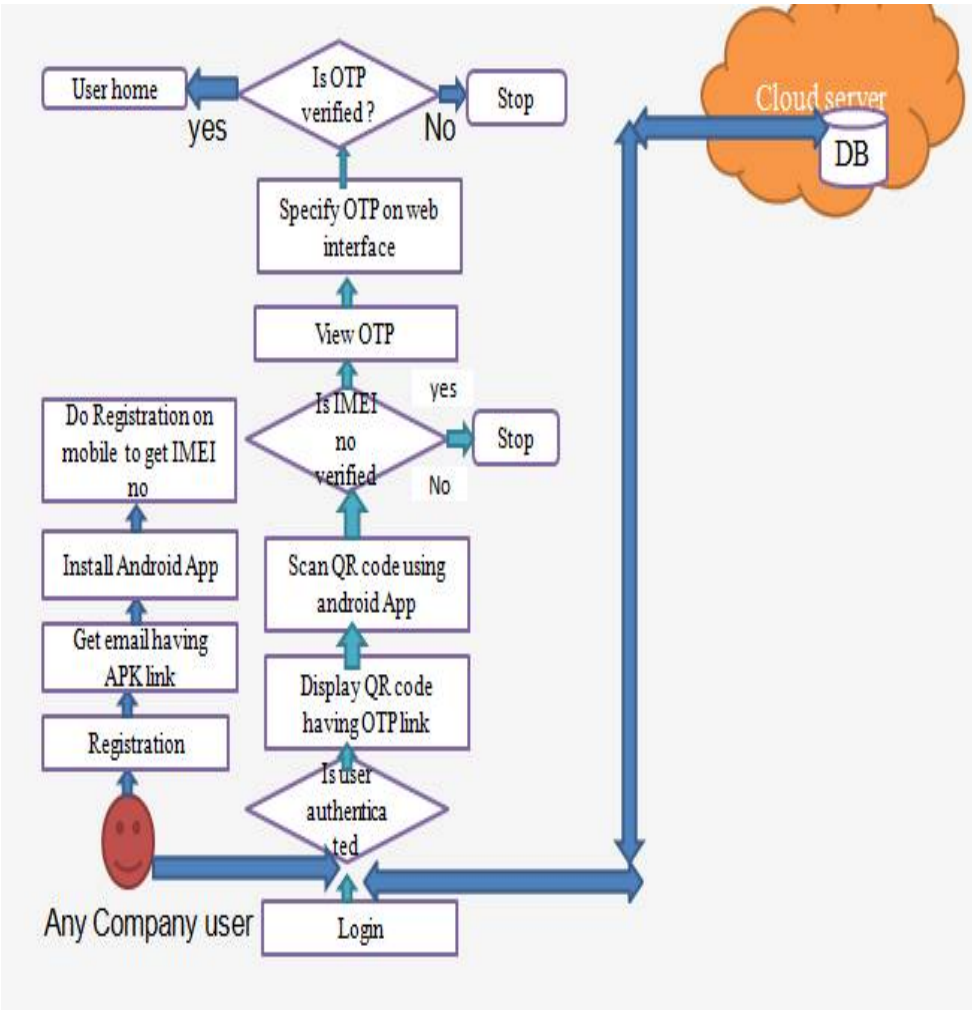

Fig1. Two factor authentication

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

B. Flowchart Of Encrypt And Decrypt Document :

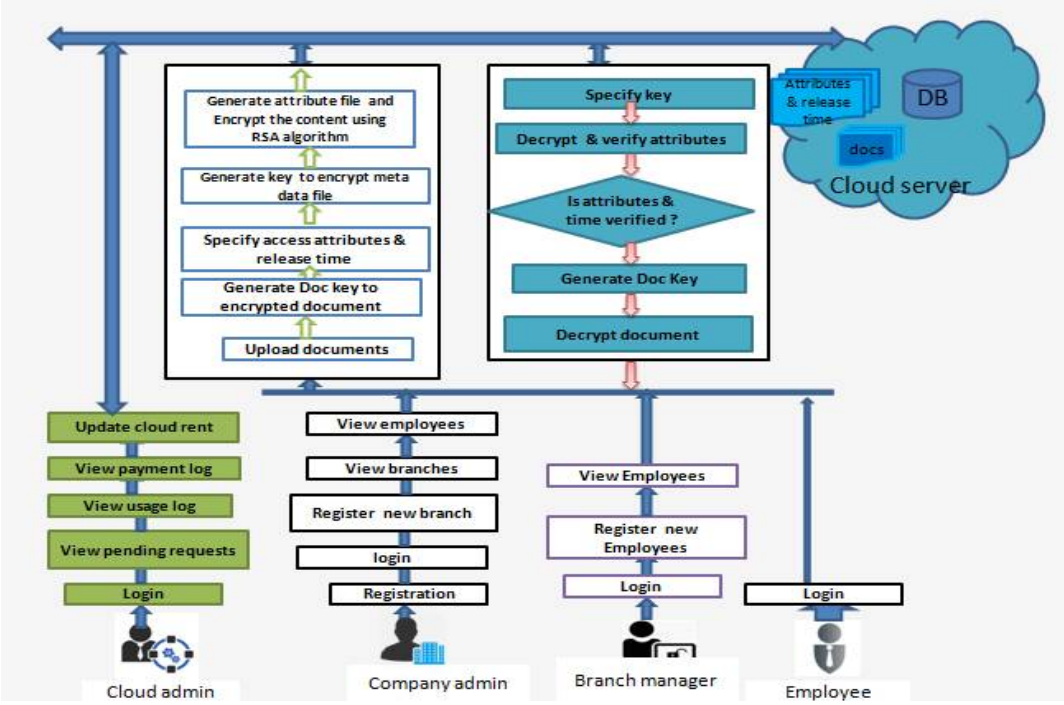

Fig2.Flowchar of Encrypt And Decrypt Document

Fig.2 Shows the flowchart of encrypt and decrypt document. Company admin first login and register branch then Cloud admin login and view pending requests, if the cloud accept the requets of company admin then admin is able to access that cloud services. Company admin get userid and passwords on his mail. Company admin login and register branch after registration he/she able to register new branches and new employee. Users first login his/her userid and passwords after that he/she goes to moblie based authentication. After login user is able to upload the document, view other document and download docment.In this system, propose model which removes the drawback of CP-ABE and maintains the time factor in separte file. In our proposed system, the attributes and release time will be maintained in a separately in meta-data file on server. The attributes of document will be encrypted using secret key. Attributes and time will generate secrete key to encrypt the document using DSA and MD5 algorithms. The RSA algorithm is used to manage access policy management.The attribute will be connected with release time and attribute of the document will be dependent on the document,If user are successfully login then only user can upload or download document. Our proposed model will reduce the time.

Problem Definition:

- In existing system, Time based ABE technique is build to manage time wise document's access permissions easily. While managing/updating the document, Time aware -ABE needs to encrypt document again which requires more computation time and space.
- Therefore to manage access permissions of the documents we modified ABE technique such that it improves the efficiency of the existing ABE technique.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Objectives:

- To develop a cloud based application for secure document sharing.
- To implement Advanced ABE technique for document security.
- Implement two factor authentication factor to enhance security .
- To Secure time-sensitive data from being before release time
- To improve computation time of the system.

Scope of Problem:

- In existing system they maintain only one file for original attribute and other attribute , but in proposed system we used two files one for original file and another one is a meta-data file. so the cipher text size is remain constant.
- In this paper, we embedded timed-release encryption into ABE (Attribute-based Encryption), we propose a new time and attribute factors combined access control on time-sensitive data for public cloud storage, and provide efficient approach to design access policies for time-sensitive data.
- We propose new advanced ABE technique to overcome the drawbacks of CP-ABE and KP-ABE. To make system attacks free, we propose two factor authentication system in which first factor is traditional user id and password authentication and second factor is mobile based authentication.

Implementation:

In proposed system, we combine time and attribute factor and provide the security of time-sensitive data. We implement cloud based application for secure document sharing, using PBE(Password Based Encryption) algorithm its mixture of DES and MD5 algorithm. The DES and MD5 algorithm used for encryption and generating hash value. We also implement Mobile-based application for providing more security to the employee/admin such that we used two factor authentication one is user id and passwords and another is mobile based. For time-sensitive data we manage access permission, for access permission used RSA algorithm. We maintain two files original file and met-data file. The company admin can login with his user id and password, and register branch and uploads document. If the employee or company admin upload the document and give access permission for that document , then that file access only those employee who have permission to access that file. we also evaluate time evaluation and evaluation. cipher text size is constant so its reduce compilation time.

IV. PROPOSED ALGORITHM

This proposed system perform encryption and decryption using DSA and MD5 algorithm. Using this algorithm our system is more secure. Therefore following algorithm is used to provide security of time-sensitive data.

Advanced ABE encryption algorithm using DES and MD5:

1. **File Encryption: Steps**
   - Initialize FileInputStream with input file
   - Generate key using Random() class in text format eg. Seckey@3412.
   - Convert key into message Digest using MD5.
   - Set salt [] = Random(8) byte.
   - Initialize parameter specification that takes hash value of 8 byte random number.
   - Initialize cipher with hashed key and salt to generate cipher text.
   - Initialize input[]
     - Byte [] input = new byte [64]
     - Initialize int byteread=0;

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

- While (bytesRead!= -1)
    - Set bytesRead = inFile.read(input)
    - Set byte[] output = cipher update(output)

  End while.
- Store encrypted file on server and delete original file from server.

2. File Decryption algorithm: steps

- Initialize FileInputStream with input file
- Generate key using Random() class in text format eg. Seckey@3412.
- Convert key into message Digest using MD5.
- Set salt [] = Random(8) byte.
- Initialize parameter specification that takes hash value of 8 byte random munber.
- Initialize cipher with hashed key and salt to generate cipher text.
- Initialize input []
    - Byte [] input = new byte [64]
    - Initialize int byteread=0;
- While (bytesRead!= -1)
    - Set bytesRead = inFile.read(input)
    - Set byte[] out = cipher update(output)
    - End while.
- Store decrypted file on server and delete original file from server.

Access Permission Management Steps:

1) Specify branch, designnation, release date and release time.
2) Combine the attribute to form one string, arrange attribute in following format.
   Designation + '|' + branch + '|' + date + '|' + time.
3) Findout whether the meta-data file is already exist or not. If meta-data file not exits then create meta-data file i.e XML file

    1. Create parent Node
    2. Create child node having name document.
    3. Create sub-child node having name parent.
    4. Generate RSA keys.
    5. Encrypt access permission string using RSA.
    6. Save the encrypted string in XML.

   Else

    1. Read XML from server.
    2. Get content in list
    3. Add new content in list.
    4. Encrypt new content using existing RSA keys.
    5. Generate meta-data file again.
    6. Store XML file on server.

   End if

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

V. EXPERIMENTAL EVALUATION:

In this section, we describe the experimental evaluation of the proposed scheme. We implemented the success of our scheme in the context of encryption and decryption. In the evaluation of our proposed scheme, we use result of existing and proposed scheme In existing system user want to some changes in existing document, then he/she first encrypt the document and then decrypt the document and again encrypt the same document again, for this more computation time is required, and also increase the size of cipher-text. Fig .3 shows that time evaluation of proposed system. so that we evaluate the encryption time and decryption time in terms of size KB. In this require less computation time, and cipher text size remain constant. so we evaluate after encryption size in kb, document decryption time and document encryption time, access permission file for encrypted and decrypted document in the proposed system. The evaluation Result will show how existing and proposed system reduced the computation time, and also shows the cipher text size will be remain constant.

Example:

If the user upload the document on the server, then the proposed scheme calculate encryption size in kb, document decryption time and document encryption time, access permission file. Then evaluation will gives result for that document that how much computation time is reduced in existing and proposed scheme. Graphical representation is given below.

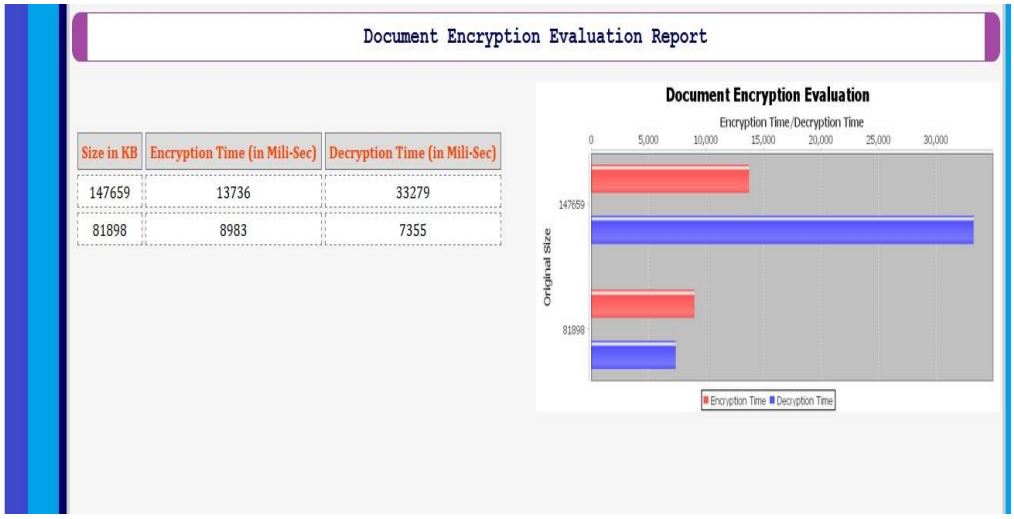

Fig No. 3 Time Evaluation Report

VI. CONCLUSIONS AND FUTURE WORK

In this system, we implement advances ABE technique that maintain access policy attributes separately in file. The employee call any time update / add new changes in existing encrypted document. We give access permission to the user for release date and time, and also delete the previous access permission that give to the employee. For access permission we used RSA algorithm. And for encryption and decryption used PBE algorithm that mixture a DES and MD5 algorithm. Therefore our system is more reduced compilation time compare to existing system. The advantage of this system is used two factor authentication Factor for fine-grained access control. This paper shows implementation and evaluation of document security on cloud server with the help of advanced ABE techniques. Here

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

we give the security of time-sensitive data. Our system shows that its more efficient than the existing system. In future we also try to reduce more compilation time and security of time-sensitive data and fine-gained access control.

REFERENCES

[1] K.YANG,X.JIA,K.REN, B.ZHANG AND R.XIE, "DAC-MACS: Effective data access control for multi authority cloud storage systems, "IEEE transactions on information Forensics & Security, vol. 7,2012
[2] Ming Li,Shucheng Yu,Yao Zheng,Kui Ren,Wenjing Lou, "Scalable and secure sharing of personal heath records in cloud computing using attribute based encryption,"IEEE transactions on parallel and distributed systems, vol 24, 2013
[3] Baishuang Hu, Qin Liu,Xuhui Liu,Tao Peng,Guojun Wang & Jie wu, "DABKS:Dynamic attribute based Keyword search in cloud computing",IEEE communication and information systems security symposium,2017
[4] Quin Liu, Guojun Wang, & Jie wu,"Clock based proxy Re-encryption scheme in unreliable cloud,"IEEE 41st international conference on parallel processing workshops, 2012
[5] Joseph K. Liu, Man Ho Au_, Xinyi Huang, Rongxing Lu, Jin Li, "Fine-grained Two-factor Access Control for
Web-based Cloud Computing Services" , IEEE Transactions on Information Forensics and Security,2015
[6] Jianan Hong, Kaiping Xue, Yingjie Xue, Weikeng Chen, David S.L. Wei, Nenghai Yu and Peilin Hong, "TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud", IEEE Transactions on Services Computing 2017
[7] Ke Yuan, Zheli Liu, Chunfu Jia*, Jun Yang, "Public Key Timed-Release Searchable Encryption", 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies 16] E. Androulaki, C. Soriente, L. Malisa, and S. Capkun,"Enforcing location and time-based access control oncloud-stored data," in *Proceedings of the 2014 IEEE 34th International Distributed Computing Systems (ICDCS'14)*, pp. 637–648, IEEE, 2014.
[8] C.-I. Fan and S.-Y. Huang, "Timed-release predicate encryptionand its extensions in cloud computing," *Journalof Internet Technology*, vol. 15, no. 3, pp. 413–426, 2014.
[9] J. Hong, K. Xue,W. Li, and Y. Xue, "TAFC: Time and attributefactors combined access control on time-sensitivedata in public cloud," in *Proceedings of the 2015 IEEEGlobal Communications Conference (GLOBECOM '15)*,pp. 1–6, IEEE, 2015.
[10] H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang,Y. Chen, and J. Liu, "Dynamic-hash-table based publicauditing for secure cloud storage," *IEEE Transactions onServices Computing, Avaliable online*, 2016.
[11] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou,"Toward secure and dependable storage services in cloudcomputing," *IEEE Transactions on Services Computing*,vol. 5, no. 2, pp. 220–232, 2012.
[12] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 743–754,2012.