International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

An Enhanced Cloud Based Attribute Cryptography Technique for Hierarchy Shared Files

Md Ateeq Ur Rahman[1] and Sayeed Bin abdullah[2],
[1]Professor and Head, Dept. of Computer Science & Engineering,
SCET, Hyderabad
mail_to_ateeq@yahoo.com
[2]Research Scholar, Dept. of Computer Science & Engineering,
SCET, Hyderabad
sayeed.binabdullah@yahoo.com

Abstract- Ciphertext-policy attribute-based Cryptography (CP-ABC) has been a preferred cryptography technology to unravel the tough drawback of secure information sharing in cloud computing. The shared info files generally have the characteristic of structure hierarchy, notably at intervals the house of care and so the military. However, the hierarchy structure of shared files has not been explored in CP-ABC. Throughout this paper, degree economical file hierarchy attribute-based Cryptography theme is projected in cloud computing. The stratified access structures unit integrated into one access structure, and then, the stratified files unit encrypted with the integrated access structure. The ciphertext components related to attributes might be shared by the files. Therefore, every ciphertext storage and time worth of cryptography unit saved. Moreover, the projected theme is proved to be secure beneath the standard assumption. Experimental simulation shows that the projected theme is incredibly economical in terms of cryptography and coding. With the number of the files increasing, the advantages of our theme become a lot of and a lot of conspicuous.

I. INTRODUCTION

With the quickly increasing network and mobile technologies, on-line data sharing has become a fresh “pet”, like Facebook, MySpace, and Badoo. Meanwhile, cloud computing [1]–[5] is one of the foremost promising application platforms to unravel the explosive increasing of information sharing. In cloud computing, to safeguard data from leaky, users need to be compelled to write in code their data before being shared. Access management [6]-[7] is dominant as a result of it's that the initial line of defense that forestalls unauthorized access to the shared data. Recently, attribute-based cryptography (ABC) [8] – [10] has been attracted way more attentions since it'll keep data privacy and perceive fine-grained, one-to-many, and non-interactive access management. Ciphertext-policy attribute based cryptography (CP-ABC) is one of potential schemes that has additional flexibility and is more applicable for general applications.

In cloud computing, as illustrated in Fig. 1, authority accepts the user enrollment and creates some parameters. Cloud service supplier (CSP) is that the manager of cloud servers and provides multiple services for shopper. info owner encrypts and uploads the generated ciphertext to CSP.

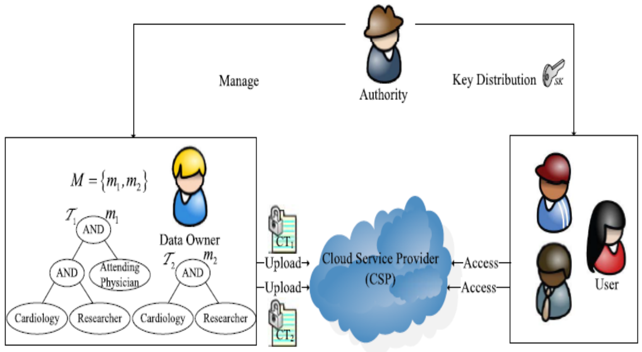


Figure 1: An example of secure data sharing in cloud computing

User downloads and decrypts the interested ciphertext from CSP. The shared files generally have hierarchical data structure. That is, a bunch of files area unit divided into style of hierarchy subgroups placed at all totally different access levels. If the files at intervals constant system may be encrypted by associate integrated access structure, the storage value of ciphertext and time value of cryptography may be saved.

In this study, a cost-effective cryptography theme supported stratified model of the access structure is projected in cloud computing, that's referred to as file hierarchy CP-fundamentals theme (or FH-CP- fundamentals, for short. FH-CP- fundamentals extends typical CP- fundamentals with an information structure of access policy, thus on reach easy, versatile and fine-grained access management. The contributions of our theme area unit 3 aspects:

1) Firstly, we have a tendency to tend to propose the stratified model of access structure to unravel the matter of multiple gradable files sharing. The files area unit encrypted with one integrated access structure.

2) Secondly, we have a tendency to tend to jointly formally prove the protection of FH-CP- fundamentals theme which can successfully resist chosen plaintext attacks (CPA)

below the Decisional additive Diffie-Hellman (DBDH) assumption.

3) Thirdly, we have a tendency to tend to conduct and implement comprehensive experiment for FH-CP-fundamentals theme, and thus the simulation results show that FH-CP- fundamentals has low storage value and computation quality in terms of cryptography and cryptography.

It got to be detected that the projected theme differs from the following CP- fundamentals schemes, that utilize the user stratified model to distribute the work of key creation on multiple domain authorizations and lighten the burden of key authority

II. RELATED WORKS

Existing System

Sahai and Waters planned fuzzy Identity-Based Cryptography (IBE) in 2005 that was the model of fundamental principle. Latterly, a variant of fundamental principle named CP-ABC was planned. Since aristocracy and Silverberg planned the first notion of stratified cryptography theme, many stratified CP-ABC schemes area unit planned. as associate example, Wang et al. planned a stratified fundamental principle theme by combining the stratified IBE and CP-ABC. Wan et al. planned stratified fundamental principle theme. Later, Zou gave a stratified fundamental principle theme, whereas the length of secret secret's linear with the order of the attribute set. A ciphertext policy stratified fundamental principle theme with short ciphertext is to boot studied. In these schemes, the parent authorization domain governs its child authorization domains and a ranking authorization domain creates secret key of the next-level domain. The work of key creation is distributed on multiple authorization domains and conjointly the burden of key authority center is lightened.

At present, there area unit three types of access structures gate, access tree, and linear secret sharing theme (LSSS) utilized in existing CP-ABC schemes. Cheung and Newport initial used gate access structure to achieve CP-ABC theme. Later, some improved schemes area unit planned. Meanwhile, there area unit CP-ABC schemes supported access tree that support AND, OR, and threshold, and supported LSSS, where and area unit the quality schemes of access tree and LSSS.

Other CP-ABC schemes with specific choices area unit presented. as associate example, Hur planned associate data sharing theme to unravel the matter of key agreement by exploitation associate written agreement free key supply protocol between the key generation center and conjointly the information storing center. inexperienced et al. and Lai et al. planned CP-ABC schemes with outsourced decryption to chop back the work of the decryption user. And Fan et al. planned associate arbitrary-state fundamental principle theme to resolve the matter of the dynamic membership management. to boot, Guo et al. planned a singular constant-size decryption key CP-ABC theme for storage-constrained devices. Hohenberger associated Waters planned associate online/offline fundamental principle theme to reinforce the speed of key generation and cryptography, where each computation processes is split into 2 halfs: offline part (a preparation section) and on-line phase.

Disadvantages of Existing System

In Existing System

Time and cost for encryption is high.

No any special multiple hierarchical files are used.

Decryption system time and computation cost are very high.

III. PROPOSED SYSTEM

In this study, associate economical cryptography theme supported superimposed model of the access structure is planned in cloud computing, that's referred to as file hierarchy CP-ABC theme (or FH-CP-ABC, for short). FH-CP-ABC extends typical CP-ABC with a knowledge structure of access policy, so on succeed simple, versatile and fine-grained access management. The contributions of our theme unit of measurement three aspects. Firstly, we tend to tend to propose the superimposed model of access structure to unravel the matter of multiple graded files sharing. The files unit of measurement encrypted with one integrated access structure. Secondly, we tend to tend to in addition formally prove the protection of FH-CP-ABC theme which is able to successfully resist chosen plaintext attacks (CPA) below the Decisional linear Diffie-Hellman (DBDH) assumption. Thirdly, we tend to tend to conduct and implement comprehensive experiment for FH-CP-ABC theme, and conjointly the simulation results show that FH-CP-ABC has low storage worth and computation complexity in terms of cryptography and coding.

Advantages of Proposed System

CP-ABC attainable schemes that incorporates a heap offlexibility and is additional applicable for general applications Multiple hierarchic files sharing unit resolved pattern superimposed model of access structure. In planned system every ciphertext storage and continuance of coding unit saved. The planned theme incorporates a bonus that users can decipher all authorization files by computing secret key once. Thus, the continuance of decryption is to boot saved if the user needs to decipher multiple files. The computation worth of decryption may be reduced if users ought to be compelled to decipher multiple files at an identical time.

System Architecture

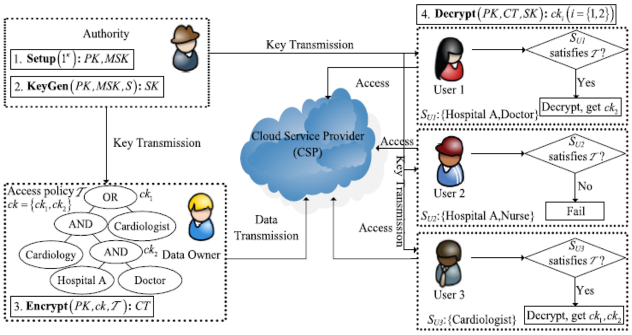

Authority
1. **Setup**(1^κ): PK, MSK
2. **KeyGen**(PK, MSK, S): SK
Key Transmission
Key Transmission
Access
Cloud Service Provider (CSP)
Access
Key Transmission
Data Transmission
Access
Access policy $\mathcal{T}$
$ck = \{ck_1, ck_2\}$
OR
ck_1
AND
Cardiologist
Cardiology
AND
ck_2
Data Owner
Hospital A
Doctor
3. **Encrypt**$(PK, ck, \mathcal{T})$: CT
4. **Decrypt**(PK, CT, SK): $ck_i\,(i=\{1,2\})$
User 1
S_{U1} satisfies $\mathcal{T}$?
Yes
Decrypt, get ck_2
S_{U1}:{Hospital A,Doctor}
User 2
S_{U2} satisfies $\mathcal{T}$?
No
Fail
S_{U2}:{Hospital A,Nurse}
User 3
S_{U3} satisfies $\mathcal{T}$?
Yes
Decrypt, get ck_1, ck_2
S_{U3}:{Cardiologist}

Figure 2: Proposed System Architecture

System Design

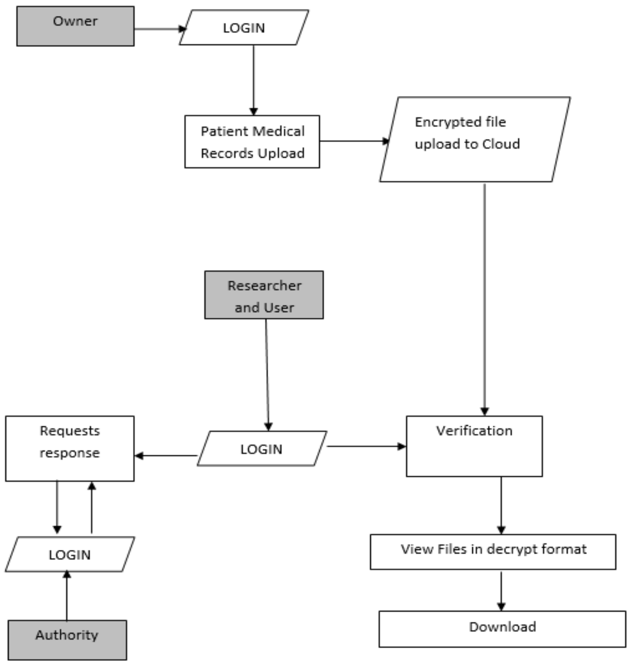

Owner
LOGIN
Patient Medical Records Upload
Encrypted file upload to Cloud
Researcher and User
Requests response
LOGIN
Verification
LOGIN
View Files in decrypt format
Authority
Download

Figure 3: Process flow of the proposed System

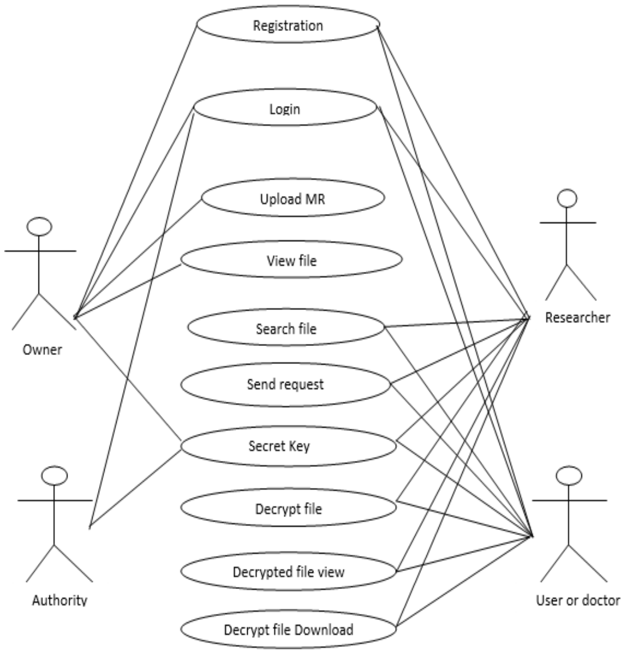


Figure 4: UML diagram of the proposed system

IV. MODULES

Registration

In this module ancient registration for the multiple users. There square measure multiple house owners, multiple AAs, and multiple users. The attribute hierarchy of files – leaf nodes is atomic file categories whereas internal nodes square measure compound categories. Dark boxes ar the categories that a PSD's data reader have access to Encrypted data. Ciphertext-policy attribute-based cryptography (CP-ABC) has been a most well liked cryptography technology to resolve the troublesome disadvantage of secure information sharing in cloud computing

Upload files

In this module, users transfer their files with secure key prospects. The house owners transfer ABE-encrypted PHR files to the server. each owner's PHR file encrypted every beneath a particular fine grained model.

ABE for Fine-grained Data Access Control

In this module ABE to grasp fine-grained access management for outsourced info notably, there has been Associate in Nursing increasing interest in applying ABE to secure electronic health care records (EHRs). Associate in Nursing attribute-based infrastructure for EHR(Electronic Health Records) systems, where each patient's EHR files ar encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the quantity of worldwide organization revoked user in an exceedingly very variant of ABE that allows delegation of access rights is projected for encrypted EHRs(Electronic Health Records) applied cipher text policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the conception of social/professional domains investigated exploitation ABE to induce self-protecting EMRs, which can either be hold on on cloud servers or cell phones therefore EMR could also be accessed once the health supplier is offline.

Setup and Key Distribution

In this module the system first defines a typical universe of data attributes shared by every PSD, like "basic profile", "medical history", "allergies", and "prescriptions". Associate in nursing emergency attribute is to boot printed for break-glass access.

Every PHR owner's shopper application generates its corresponding public/master keys. the final public keys could also be discovered via user's profile in an online health care social-network (HSN)
There square measure two ways in which during which for distributing secret keys.

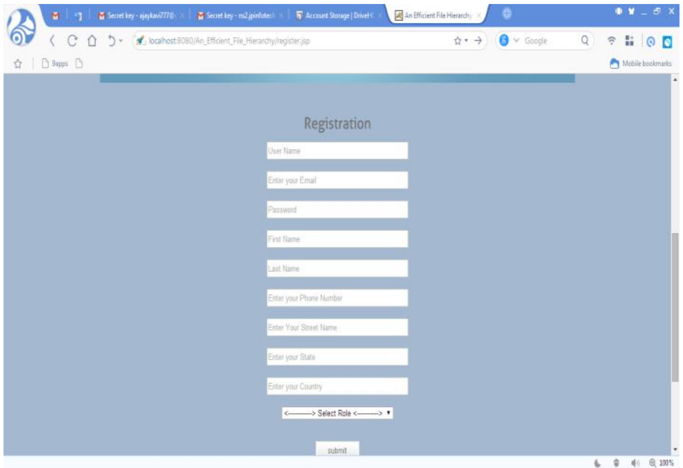
1) First, once initial exploitation the PHR service, a PHR owner can specify the access privilege of Associate in Nursing info reader in her PSD, and let her application generate and distribute corresponding key to the latter, in an exceedingly very technique resembling invitations in GoogleDoc.
2) Second, a reader in PSD could acquire the key key by inflicting document of invite (indicating that forms of files she needs to access) to the PHR owner via HSN, and so the owner will grant her a group of requested info varieties. Supported that, the policy engine of the appliance automatically derives Associate in Nursing access structure, and runs keygen of KP-

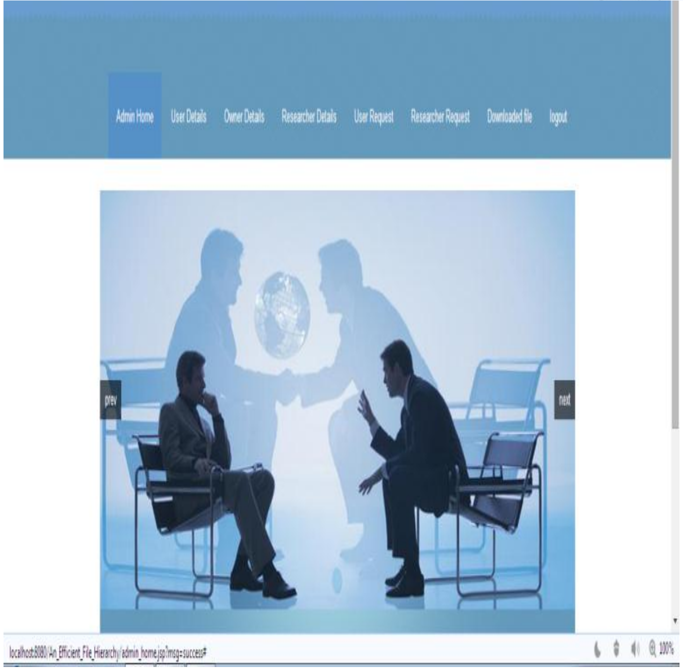
ABC to induce the user secret key that embeds her access structure.

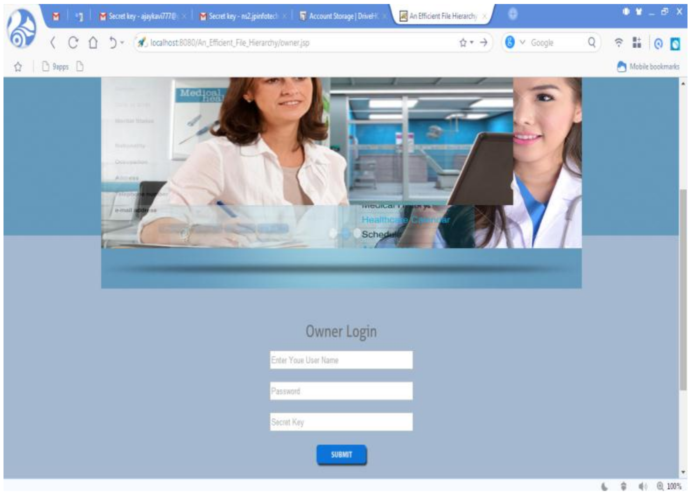
Break-glass module

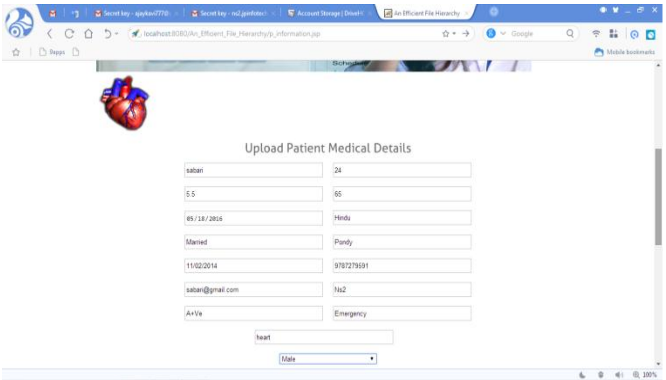
In this module once associate degree emergency happens, the regular access policies couldn't be applicable. To handle this instance, break-glass access is needed to access the victim's PHR. In our framework, each owner's PHR's access right is to boot delegated to associate degree emergency department erectile dysfunction to stop from abuse of break-glass chance, the emergency workers must contact the erectile dysfunction to verify her identity and thus the emergency state of affairs, and acquire temporary browse keys. Once the emergency is over, the patient can revoke the emergent access via the erectile dysfunction.

V. SCREENSHOTS

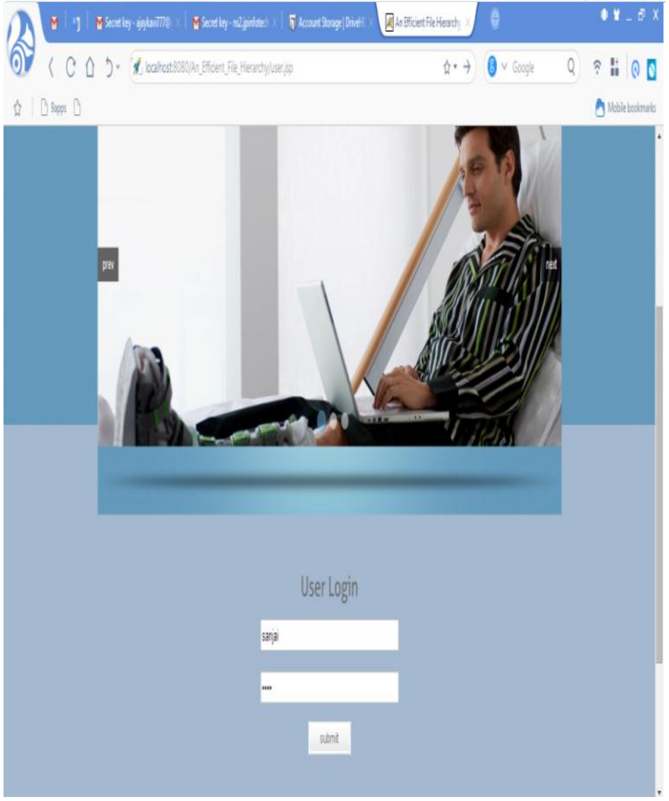




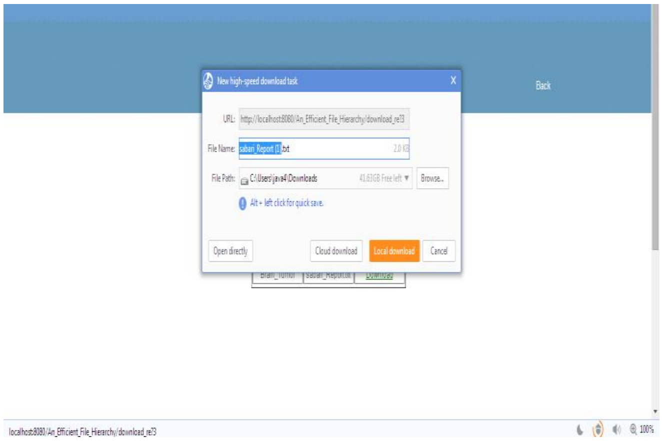

Secret key - ajaykavi777@
Secret key - ns2.jpinfotech
Account Storage | DriveH
An Efficient File Hierarchy
localhost:8080/An_Efficient_File_Hierarchy/owner.jsp
Mobile bookmarks
Medical
Healthcare Calendar
Schedule
Owner Login
Enter Youe User Name
Password
Secret Key
SUBMIT


Secret key - ajaykavi777@
Secret key - ns2.jpinfotech
Account Storage | DriveH
An Efficient File Hierarchy
localhost:8080/An_Efficient_File_Hierarchy/p_information.jsp
Mobile bookmarks
Upload Patient Medical Details

sabari
24
5.5
65
05/18/2016
Hindu
Married
Pondy
11/02/2014
9787279591
sabari@gmail.com
Ns2
A+Ve
Emergency
heart
Male


Secret key - ajaykavi777@
Secret key - ns2.jpinfotech
Account Storage | DriveH
An Efficient File Hierarchy
localhost:8080/An_Efficient_File_Hierarchy/user.jsp
Mobile bookmarks
prev
next
User Login
submit

sanjai
••••



New high-speed download task

URL: http://localhost:8080/An_Efficient_File_Hierarchy/download_re?3

File Name: sabari_Report (1).txt 2.0 KB

File Path: C:\Users\java4\Downloads 41.63GB Free left

Alt + left click for quick save.

VI. CONCLUSION

In this paper, we tend to planned a variant of CP-ABC to with efficiency share the hierarchical files in cloud computing. The hierarchical files are encrypted with AN(Authorized) integrated access structure and additionally the ciphertext components related to attributes could be shared by the files. Therefore, every ciphertext storage and note value of cryptography are saved. The planned theme encompasses a bonus that users can rewrite all authorization files by computing secret key once. Thus, the note value of secret writing is to boot saved if the user needs to rewrite multiple files. Moreover, the planned theme is verified to be secure below DBDH assumption.

REFERENCES

[1] 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.

[2] 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.

[3] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, “An efficient cloudbased 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.

[4] 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.

[5] 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.

[6] An Efficient File Hierarchy Attribute-BasedEncryption Scheme in Cloud Computing, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 6, JUNE 2016

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

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

[9] 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.

[10] 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.