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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Security in Cloud using Ciphertext Policy Attribute-Based Encryption with Checkability

Niloufer Rafath[1], Wahaj Ghouri[2], Syed Raziuddin[3]

M.Tech Scholar, Dept. of C.S.E, Deccan College of Engineering and Technology, Osmania University, Hyderabad., India[1]

Associate Professor, Dept. of C.S.E, Deccan College of Engineering and Technology, Osmania University, Hyderabad, India[2]

Professor, Dept. of C.S.E, Deccan College of Engineering and Technology, Osmania University, Hyderabad, India[3]

ABSTRACT: Cipher text-Policy Attribute-based Encryption (CP-ABE) is considered as one of the most suitable scheme for data access control in cloud storage. Despite that the existing Outsourced ABE solutions are able to offload some intensive computing tasks to a third party, the verifiability of results returned from the third party has yet to be addressed. Aiming at tackling the challenge above, a new Secure Outsourced ABE system is proposed, which supports both secure outsourced key-issuing and decryption. This new method offloads all access policy and attribute related operations in the key-issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally. In addition, for the first time, an outsourced ABE construction is proposed which provides checkability of the outsourced computation results in an efficient way.

KEYWORDS: Access Control, Attribute-Based Encryption, CP-ABE, Outsourcing Computation, Key Issuing, Checkability.

I. INTRODUCTION

In ABE system, users' private keys and ciphertextsare labeled with sets of descriptive attributes and access policies respectively, and a particular key can decrypt a particular ciphertext only if associated attributes and policy are matched. Until now, there are two kinds of ABE having been proposed: key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE). In KP-ABE, the access policy is assigned in private key, whereas, in CP-ABE, it is specified in ciphertext.

Recently, as the development of cloud computing, users' concerns about data security are the main obstacles that impede cloud computing from wide adoption. These concerns are originated from the fact that sensitive data resides in public cloud, which is maintained and operated by untrusted Cloud Service Provider (CSP). ABE provides a secure way that allows data owner to share outsourced data on untrusted storage server instead of trusted server with specified group of users. This advantage makes the methodology appealing in cloud storage that requires secure access control for a large number of users belonging to different organizations.

When a large number of users call for their private keys, it may overload the attribute authority. Moreover, key management mechanism, key revocation in particular, is necessary in a secure and scalable ABE system. In most of existing ABE schemes, the revocation of any single private key requires key-update at attribute authority for the remaining unrevoked keys which share common attributes with the one to be revoked. All of these heavy tasks centralized at authority side would make it an efficiency bottleneck in the access control system. Aiming at eliminating the most overhead computation at both the attribute authority and the user sides, an outsourced ABE scheme is proposed that not only supports outsourced decryption but also enables delegating key generation.

In addition, it is observed that when experiencing commercial cloud computing services, the CSPs may be selfish in order to save its computation or bandwidth, which may cause results returned incorrectly. In order to deal with this problem, checkabilityis done on results returned from both KGSP and DSP.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

II. RELATED WORK

Identity-Based Encryption (IBE) allows a sender to encrypt a message to an identity without access to a public key certificate. The ability to do public key encryption without certificates has many practical applications. For example, a user can send an encrypted mail to a recipient, e.g. bobsmith@gmail.com, without requiring either the existence of a Public-Key Infrastructure or that the recipient be on-line at the time of creation.

In this paper a new type of Identity-Based Encryption [1] is proposed that we call Fuzzy Identity-Based Encryption in which we view identities as a set of descriptive attributes. Fuzzy-IBE gives rise to two interesting new applications. The first is an Identity-Based Encryption system that uses biometric identities. Secondly, Fuzzy IBE can be used for an application that is called as "attribute-based encryption".

In this application a party will wish to encrypt a document to all users that have a certain set of attributes. For example, in a computer science department, the chairperson might want to encrypt a document to all of its systems faculty on a hiring committee. In this case it would encrypt to the identity {"hiring-committee","faculty","systems"}. Any user who has an identity that contains all of these attributes could decrypt the document.

Cloud computing is a promising technology, which is transforming the traditional internet computing paradigm and IT industry. With the development of wireless access technologies, cloud computing is expected to expand to mobile environments [4], where mobile devices and sensors are used as the information collection nodes for the cloud. However, users' concerns about data security are the main obstacles that impede cloud computing from being widely adopted. These concerns are originated from the fact that sensitive data resides in public clouds, which are operated by commercial service providers that are not trusted by the data owner. Thus, new secure service architectures are needed to address the security concerns of users for using cloud computing techniques.

III. PROPOSED SYSTEM

Since some users may change their associate attributes at some time, or some private keys might be compromised, key revocation or update for each attribute is necessary in order to make systems secure. The user revocation can be done via the proxy encryption mechanism together with the CP-ABE algorithm. Attribute group keys are selectively distributed to the valid users in each attribute group, which then are used to re-encrypt the ciphertext encrypted under the CPABE algorithm. In addition, as the user revocation can be done on each attribute level rather than on system level, more fine-grained user access control can be possible. Even if a user is revoked from some attribute groups, he would still be able to decrypt the shared data as long as the other attributes that he holds satisfy the access policy of the ciphertext. Therefore, the proposed scheme is the most suitable for the data sharing scenarios where users encrypt the data only once and upload it to the data-storing centers, and leave the rest of the tasks to the data-storing centers such as re-encryption and revocation.

This new method offloads all access policy and attribute related operations in the key issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally.

Checkability on results returned from both KGSP and DSP is done so that the users obtain the correct results. The idea of appending redundancy and having checksum while sending and receiving the data will fight against the dishonest actions of KGSP and DSP.

The system model for outsourced ABE scheme consists of Data User, Attribute Authority (AA), Key Generation Service Provider (KGSP), Decryption Service Provider (DSP) and Storage Service Provider (SSP).This new method offloads all access policy and attribute related operations in the key issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally.

DATA USER

Data User is he who has successfully registered himself and having his own ID and password using which he can login to the website in order to access the data. If a user possesses a set of attributes satisfying the access policy of the

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

encrypted data, and is not revoked in any of the valid attribute groups, then he will be able to decrypt the cipher-text and obtain the data.

ATTRIBUTE AUTHORITY

Here Attribute Authoritymay also be known asdata owner. He allows to upload it into the external data-storing center for ease of sharing or for cost saving. A data owner is responsible for defining (attribute-based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. The data owner logins to the website using his credentials and then he can upload the file to the Storage Service Provider (SSP). While uploading the file the data owner will define the access policy which is based on attribute. Then the data owner also have the checksum of that file so that the CSP may not return results incorrectly. The redundant data is also attached to the ciphertext to fight against dishonest actions of KGSP and DSP.

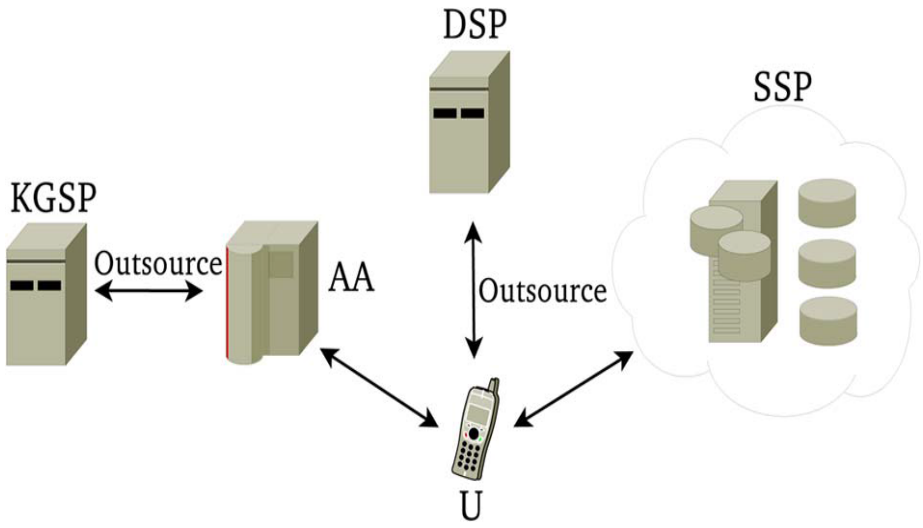

Fig 1: System model for outsourced ABE scheme

KEY GENERATION SERVICE PROVIDER

Aiming at eliminating the most overhead computation at both the attribute authority and the user sides, an outsourced ABE scheme is proposed that not only supports outsourced decryption but also enables delegating key generation. KGSP is to perform aided key-issuing computation to relieve AA load in a scale system when a large number of users make requests on private key generation and key update. It is in charge of issuing, revoking, and updating attribute keys for users. KGSP is in charge of generating the encrypted password and sending it to the mail-ID of the user. At the time of downloading the file, the session password is required which is generated by KGSP.

DECRYPTION SERVICE PROVIDER

DSP is used for generating the decrypted key when the user requests for the decryption of the encrypted key. Then the DSP asks for the ID and encrypted key of the user and then sends the decrypted key to the user. It is used for decrypting the ciphertext which is obtained from the user. When the data owner uploads the file which is in encrypted format, then the DSP will decrypt it when the authorized user who satisfies the access policy and who have suitable attributes requests for downloading the file. The DSP will then send the file in the decrypted format to the authorized user so that the user can gain access to that data.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

STORAGE SERVICE PROVIDER

SSP is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. All the uploaded data will be stored in Storage service provider. SSP will be in charge of controlling the access to that data from outside users. It will be storing all the data and provides the data only to authorized users.The files which are uploaded by the Data Owner will be stored in the SSP. When the authorized user wants to access that file, the SSP will then sends the file to the user so that user can download it by entering session password (OTP).

A. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Using Elliptic Curve Cryptography (ECC) algorithm data is encrypted and decrypted. Elliptic curve cryptography is a set of algorithms for encrypting and decrypting data and exchanging cryptographic keys. ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography is the same level of security provided by keys of smaller size. ECC is based on properties of a particular type of equation created from the mathematical group (a set of values for which operations can be performed on any two members of the group to produce a third member) derived from points where the line intersects the axes.

Equations based on elliptic curves have a characteristic that is very valuable for cryptography purposes: they are relatively easy to perform, and extremely difficult to reverse. An elliptic curve is the set of points that satisfy a specific mathematical equation.
The equation for an elliptic curve looks something like this:
$y^2 = x^3 + ax + b$

B. ALGORITHM OF ECC DIFFIE-HELLMAN KEY EXCHANGE

1. Users select an elliptic curve $E_q(a, b)$with parameters a, b and q, where q is a prime and G is a point on Elliptic curvewhose order is large value n.
2. Users A and B select private keys n_A<n, n_B<n.
3. They compute public keys: P_A=n_A×G, P_B=n_B×G.
4. They calculate shared secret key: K=n_A×P_B, K=n_B×P_A
The two calculations in step 4 produce the same result because
$n_A \times P_B = n_A \times (n_B \times G) = n_B \times (n_A \times G) = n_B \times P_A$
To break this scheme, an attacker would need to be able

$$C_m = \{ kG, P_m + kP_B \}$$

Note that A has used B's public key P_B. To decrypt the ciphertext, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point:
$P_m + kP_B - n_B(kG) = P_m + k(n_B G) - n_B (kG) = P_m$

C. PROPOSED ALGORITHM

The following algorithm is used in the proposed system
Step-1 The data owner logins the system using his ID and password.
Step-2 The data owner defines the access policy for the data which is to be placed on the public cloud.
Step-3 The data owner chooses the file to be uploaded and define the access policy for that file.
Step-4 The data owner defines the access policy using Attribute Based Encryption.
Step-5 The file gets encrypted using ECDH algorithm.
Step-6 The owner then finds out the checksum of the data which is being uploaded in order to provide checkability.
Step-7 The file then finally gets uploaded to the database on the cloud and the data owner gets the message after the file gets uploaded.
Step-8 The registered user logins to the system with the valid ID and key.
Step-9 The user then search for the file he wants to download.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Step-10 The file will be displayed to the user only if he is having suitable attributes that satisfy the access policy, otherwisethe file will not be displayed.
Step-11 Then in order to download the file the user search for the key.
Step-12 The session key will be generated by KGSP to the user only if he is having suitable attributes.
Step-13 Then using the session key, the user requests for downloading of the file.
Step-14 Then DSP will decrypt the encrypted file which is placed on the database and returns the decrypted file to the user.
Step-15 Then the user will be able to download the file on the local machine.

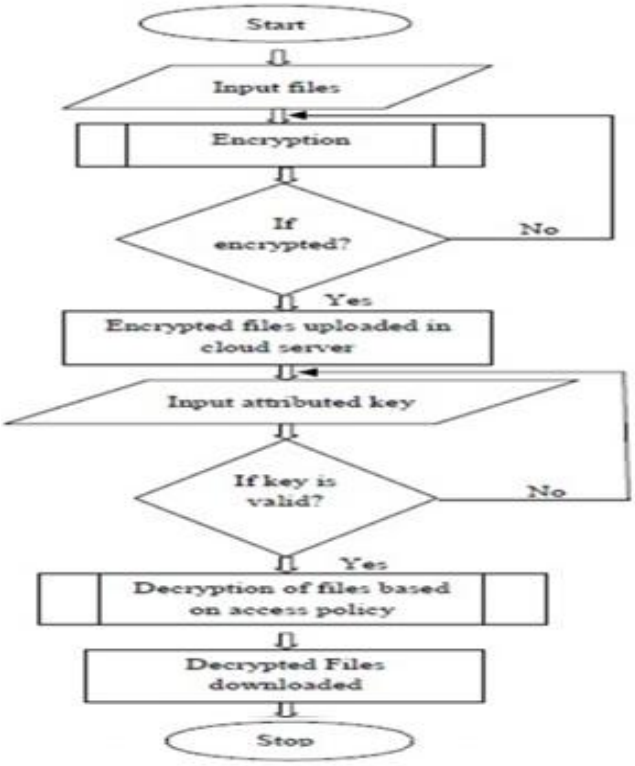

Fig 2: Flow Chart of Proposed System

IV. PERFORMANCE ANALYSIS

To evaluate the performance of CP-ABE outsourcing scheme, encryption time, key generation time and decryption time are calculated. The time taken by CP-ABE outsourcing scheme is calculated on Integrated Development Environment (IDE) Visual Studio (C#.Net) while the database is kept in Microsoft Azure Database.

Performance analysis is done by calculating Encryption and upload time, Decryption and download time and key generation time. Performance analysis is done using different file sizes and the results are obtained by noting down the time taken for encrypting those files with different sizes, time taken for decrypting those files and time taken for key generation.

A. ENCRYPTION AND UPLOAD TIME

To evaluate CPABE performance, I have measured time taken to encrypt and upload the file on the SQL Azure Database by using different file sizes—1 KB, 2 KB, 5 KB, 50 KB, 100 KB.
To capture time used for encryption and uploading the file, i have used the following code.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

```
stringst, et;
et = DateTime.Now.Millisecond.ToString();
// Here the module code and the query will run which will connect with the Microsoft Azure database
intiet = Convert.ToInt16(et);
intist = Convert.ToInt16(st);
intft = iet - ist;
Label1.Text = ft.ToString();
```

I have written this code in the essential class files of my project and then execute it. This code will take the current system time and then run the code and the query in it and then captures the time which it takes for doing so. Then it subtracts that system time from the time it captures and returns the result in the label which is placed for that purpose
Fig 3 shows the encryption time taken by the proposed system i.e. outsourcing ABE. It is clear from the figure that as the file size increases, the encryption time also increases.
Here the encryption time indicates the time to encrypt and upload the file on the Microsoft Azure.

B. KEY GENERATION TIME

The Key generation time returns the time to generate the keys. I have used same files for performing tests in order to capture the time taken to generate the secret key. Using this key only the users will be able to download the files. The file sizes which I have used for testing are 1KB, 2KB, 5KB, 50KB, 100KB. Fig 4 shows the key generation time taken by the proposed scheme.

C. DOWNLOAD AND DECRYPTION TIME

Same files were used for performing tests for capturing time taken to download and decrypt these files using both proposed system (CPABE) and existing system (IBE).
These files were staged on SQL Azure Database file repository. Following operations are performed when a user requests to download a file:-
-Encrypted file is downloaded from file storage service to local machine.
-Requested file is decrypted using private key of the user.
It is shown in Fig 5 that the decryption time of Outsourcing ABE increases as the file size increases.

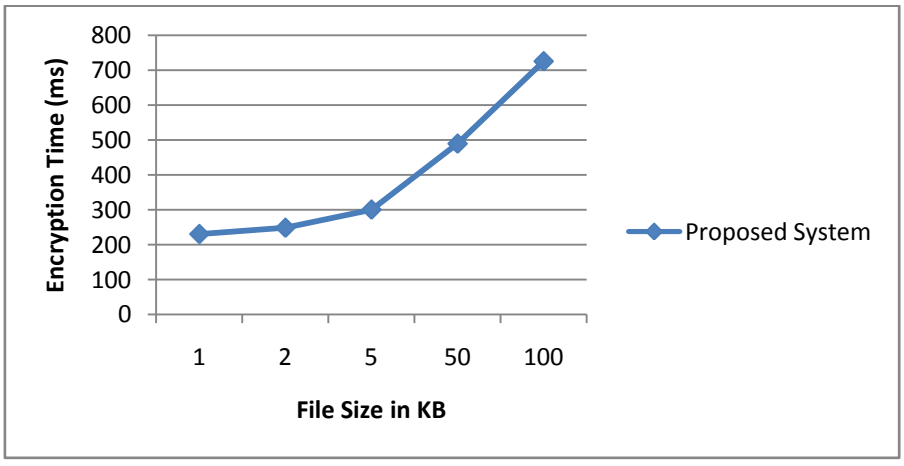

Fig 3: Encryption time taken by the proposed scheme

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

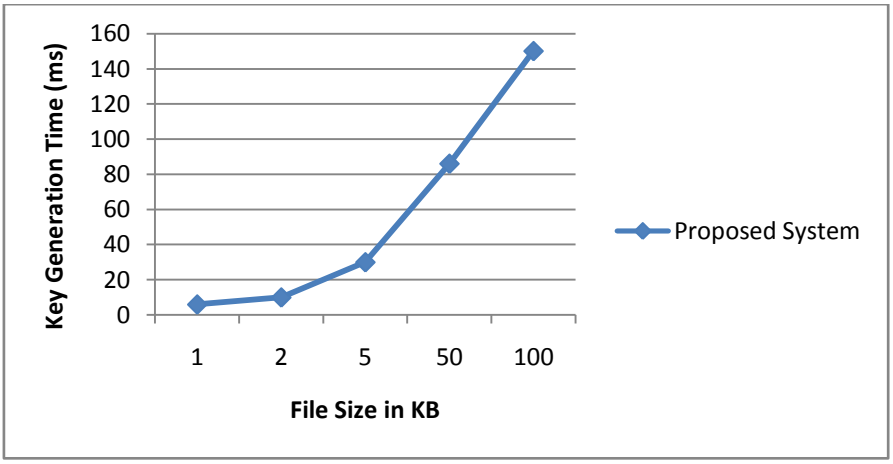

Fig 4: Key Generation time taken by the proposed scheme

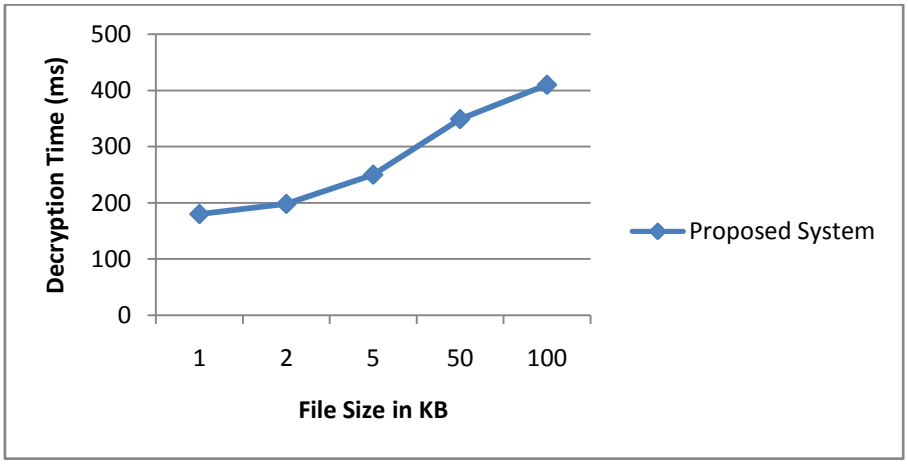

Fig 5: Decryption time taken by the proposed scheme

VI. CONCLUSION AND FUTURE WORK

A new outsourced ABE scheme is proposed that simultaneously supports outsourced key-issuing and decryption. With the aid of KGSP and DSP, this scheme achieves constant efficiency at both authority and user sides. Performance analysis shows that the proposed system i.e. outsourced ABE takes less encryption time and decryption time and the time increases as the file size increases. The time taken by the proposed scheme for encryption and decryption and key generation is in milliseconds.To sum up, this outsourced ABE scheme achieves efficiency at both attribute authority and user sides during key-issuing and decryption without introducing significant overhead compared to the original approach.

In this paper, the data owner acts as the only authority in every cryptosystem. In large-scale systems, it is desirable to provide decentralized access control in the sense that the existence of multiple authorities in an application is allowed.

When encryption provides data confidentiality, it also greatly limits the flexibility of data operation. To address this issue, it is needed to combine ABE with cryptographic primitives such as searchable encryption, private information retrieval and homomorphic encryption to enable computations on encrypted data without decrypting.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

REFERENCES

1. A. Sahai and B. Waters, ''Fuzzy Identity-Based Encryption,'' in Proc. Adv. Cryptol. EUROCRYPT, LNCS 3494, R. Cramer, Ed., Berlin, Germany, 2005, pp. 457-473, Springer
2. M. Green, S. Hohenberger, and B. Waters, ''Outsourcing the Decryption of ABE Ciphertexts,'' in Proc. 20th USENIX Conf. SEC, 2011, p. 34.
3. J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, ''Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryption,'' in Proc. 18th ESORICS, 2013
4. Z. Zhou and D. Huang, ''Efficient and Secure Data Storage Operations for Mobile Cloud Computing,'' in Cryptology ePrint Archive, Report 2011/185, 2011.
5. S.Yu,C. Wang,K.Ren, andW. Lou, ''Achieving Secure, Scalable, Fine-Grained Data Access Control in Cloud Computing,'' in Proc. IEEE 29th INFOCOM, 2010, pp. 534-542.
6. 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.
7. L. Cheung and C. Newport, ''Provably Secure Ciphertext Policy ABE,'' in Proc. 14th ACM Conf. CCS, 2007, pp. 456-465.
8. J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-Policy Attribute-Based Encryption,'' in Proc. IEEE Symp. Security Privacy, May 2007, pp. 321-334.
9. A. Beimel. "Secure Schemes for Secret Sharing and Key Distribution". PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
10. S. Hohenberger and A. Lysyanskaya, ''How to Securely Outsource Cryptographic Computations,'' in Proc. Theory Cryptogr., LNCS 3378, J. Kilian, Ed., Berlin, Germany, pp. 264-282, Springer-Verlag.
11. J. Lai, R. Deng, C. Guan, and J. Weng, ''Attribute-basedEncryption with Verifiable Outsourced Decryption,'' IEEE Trans.Inf. Forensics Security, vol. 8, no. 8, pp. 1343-1354, Aug. 2013.
12. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski,G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"Above the clouds: A berkeley view of cloud computing," University ofCalifornia, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.
13. R. Canetti, B. Riva, and G. Rothblum, ''Two Protocols for Delegationof Computation,'' in Proc. Inf. Theor.Security, LNCS 7412, A. Smith,Ed., Berlin, Germany, 2012, pp. 37-61, Springer-Verlag.
14. R. Canetti, B. Riva, and G.N. Rothblum, ''Practical Delegation ofComputation Using Multiple Servers,'' in Proc. 18th ACM Conf.CCS, 2011, pp. 445-454.
15. N. P. Smart. Access control using pairing based cryptography. In CT-RSA, pages 111–121, 2003.
16. A. Shamir. How to share a secret.Commun. ACM,22(11):612–613, 1979.
17. A. Shamir. Identity Based Cryptosystems and Signature Schemes. In Advances in Cryptology – CRYPTO,volume 196 of LNCS, pages 37–53. Springer, 1984.
18. R. Canetti, S. Halevi, and J. Katz.Chosen Cipher-text Security from Identity Based Encryption. InAdvances in Cryptology – Eurocrypt, volume 3027 ofLNCS, pages 207–222. Springer, 2004.
19. Microsoft Azure, http://www.microsoft.com/azure/.

BIOGRAPHY

Niloufer Rafath is anM.Tech Scholar in the Computer Science Department, Deccan College of Engineering and Technology, Osmania University, Hyderabad,India. She received Bachelor of Engineering (B.E) degree in 2010 from Deccan College of Engineering and Technology, Hyderabad, India. Her research interests are Cloud Computing, Network Security and Mobile Computing.

WahajGhouriis an Associate professor in the Computer Science Department, Deccan College of Engineering and Technology, Osmania University, INDIA.He is pursuing Ph.D. in C.S.E from GITAM University,Hyderabad, India.He received Master of Technology from JawaharlalNehru Technological University, Hyderabad, India.His research interests are Mobile Cloud Computing and Mobile Web Services.

Syed Raziuddinis a Professor and Head of the Computer Science Department, Deccan College of Engineering and Technology, Osmania University, Hyderabad, India. He received Ph.D. in C.S.E in the year 2012 from GITAM University, Hyderabad, India. His research areas include Computer Networks and Soft Computing.