# Fine-Grained Access Control and Secured Data Sharing in Cloud Computing


**Neha Agarwal, Ajay Rana and J. P. Pandey**

**Abstract** In cloud computing data, outsourcing is one of the most convenient, cost–efficient, and cheapest ways for users to share their data with remote clients. However, the main problem is that the owner loses its physical control on data and so the main challenge is how to secure and share the data efficiently and maintaining fine-grained access control on it. Several approaches have been proposed including attribute-based encryption and proxy re-encryption for secured data sharing through cloud service providers. In this paper, we have given a survey and comparison of different attribute-based encryption and proxy re-encryption techniques. We have also proposed that threshold cyptosystem can be used for secured and efficient data sharing in cloud.

**Keywords** Cloud computing · Fine-grained access control · Confidentiality Attribute-based encryption · Proxy re-encryption

## 1 Introduction

Cloud computing is a new computer science paradigm which provides access to shared pool of resources in an efficient and scalable manner over Internet on demand basis. These services may involve application, network, data, computation, infrastructure, and so on [1–5]. The customer pays for the services as per usage which leads to great advantage to customers as well as service providers (Fig. 1).

N. Agarwal (✉) · A. Rana
Amity University, Noida, Uttar Pradesh, India
e-mail: agarwalnehajain@gmail.com

A. Rana
e-mail: ajay_rana@amity.edu

J. P. Pandey
KNIT Sultanpur, Sultanpur, India
e-mail: tojppandey@rediffmail.com



M. U. Bokhari et al. (eds.), *Cyber Security*, Advances in Intelligent Systems and Computing 729, https://doi.org/10.1007/978-981-10-8536-9_20

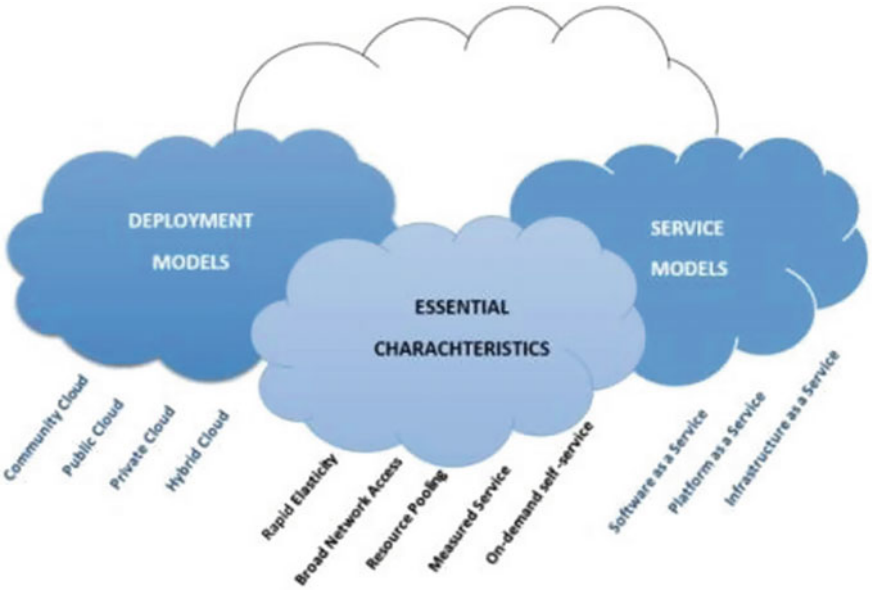


**Fig. 1** Model of cloud computing

The main deployment models in cloud are public cloud, private cloud and hybrid cloud. Public cloud is cheapest of all deployment models and is owned by third party; however, they are highly insecure, for example, AWS. Private cloud is owned by individual party and so is highly secure but at the same time they are costliest, for example, Badaal Cloud. Hybrid cloud is owned partially by service providers and partially by individual party and so are partially secured and is used in mainly critical places like they are used in Union Bank of India.

Cloud computing several services are mainly categorized into three main types: Infrastructure as a Service (IaaS), Platform as a Service (Paas), and Software as a Service (SaaS). However, recently several types of service XaaS models are defined; one of the such models is Data as a Service (DaaS) [6].

## 2 Security Issues in Cloud Computing

Among the several services, cloud storage service enables the owner of data to store and share his important data with trusted clients which has freed the owner from worry of storage and resource management. But at the same time since the owner looses the physical control on stored data there are several security concerns related

to confidentiality, security, and privacy of data-like authentication [7]. These security issues [8] are preventing the companies or people from adopting cloud which are mainly classified as follows [9]:

(i) Traditional security—There are several number of traditional risks [6, 10–13]. Gartner [14] suggested few of them which data owner should discuss with vendor beforehand. Some of the general issues and attacks include security issues like cloud malware injection attack, related to virtual machines VM-level attacks [15], cloud provider vulnerabilities [16], malicious insider, cookie poisoning, phishing attack on cloud provider such as the Salesforce phishing incident [17], SQL injection attack, authentication and authorization [18], sniffer attack, man-in-middle attack, and forensics in the cloud [19]. There are number of guidelines provided to ensure security of data to the user while storing and sharing it in cloud [20–23]; however, the data owners may not completely trust the cloud service provider. Availability of critical data is another main concern [24]. There are several issues like single-point failure, server down issues, and owner is unable to ensure that cloud service provider will not be colluding with unauthorized users and results are valid. A real-life example is an incidence in which cloud outage of Amazon S3 was down for 7 h on July 20, 2008 [25].

(ii) Third-party data control—In order to optimize the utilization of available resources in cloud, the data owner stores their data at remote site. However, security of data is a major concern since the data can reside anywhere in cloud. At the same time, the owner needs to ensure that he should have a complete control on its outsourced data rather than it being controlled by service provider [9].

As mentioned above, the major security concern of data owner is how the third service provider handles his data since architecture of storage services in cloud is bit complex so it becomes difficult for him to understand it [15, 26]. Researchers and industry people are working to address security models [7, 12, 27] by developing standards but there is still lots of work need to be done [28]. However, trusted computing and applied cryptographic techniques may offer new tools to solve these problems [29, 30].

Cryptography helps in maintaining the confidentiality of critical data by encrypting the data; yet, there are certain issues like revoking users privileges without re-encrypting data and re-distributing the new keys to the authorized users, handling collusion between users and revoked users, handling collusion between revoked users, and cloud service providers. In addition, there are several issues related to secure query processing over encrypted data [31].

## 3 Main Features Required for Secure Data Sharing in Cloud Computing

The main features to be achieved for securing data while outsourcing it on cloud are as follows:

1. Data Confidentiality: Any unauthorized user or even the service provider must not have an access to the data. Even if they steal the data, they must not be able to decrypt it.
2. Fine-Grained Access Control: Each and every authorized user will be associated with some access rights. This enhances the efficiency and reliability in system.
3. Improved Scalability: The system must be able to work efficiently with increased number of users.
4. User Accountability: It should be maintained so that he can be charged accordingly.
5. Efficient User Revocation: If the user is revoked, then the data owner need not have to redistribute the keys to authorized user.
6. Efficient and Secure User Rejoin: If a revoked user rejoins with same or different access rights, then he must rejoin without affecting the system or users.
7. Collusion Resistant: There must be no collusion between the revoke user and other authorized user or cloud service provider.
8. Ciphertext Size: The size of encrypted file must not be too big.
9. Support for Secured Query Processing: The encrypted query of authorized user can be executed over an encrypted data and only the result of executed query must be sent to authorized user.
10. Stateless Cloud: The cloud should not be in need to retain the state of revoked and active users.

## 4 Related Work

For secured data sharing in cloud through CSP, many encryption schemes have been introduced. The owner encrypts his data and sends it to third party called cloud service provider. Along with encrypted data, owner also sends the access control list specifying the authorization for accessing the attributes corresponding to users. The cloud service provider converts the ciphertext of one authorized user to another authorized user and provides it to him. In this way, data is securely shared among authorized users using concept called fine-grained access control in order to limit the access of encrypted data in cloud.

## 4.1 Attribute-Based Encryption (ABE)

In the traditional approach, if the owner wants to share some messages with others, he should know public key authorized user in order to encrypt the data. Identity-based encryption has changed the concept and allowed the public key to be of random string, e.g., email id of recipient. One of the main issues arises from sharing keys is user revocation where a user is needed to be revoked from accessing his data. The usual solution followed by owners is to re-encrypt the whole dataset with new generated key and redistribute the re-encrypted data to all authorized users.

Sahai and waters presented attribute-based encryption in 2005 [32] for secured data sharing based on the concept of public-key cryptography in which authorized users are allowed to decrypt the data only if they satisfy certain attributes. The main feature of this approach is that it is collusion resistant but since it uses access of monotonic attributes in order to control users access, it is restricted in real environment. Attribute-Based Encryption (ABE) was further classified as KP-ABE and CP-ABE.

In 2006, Goyal [33] proposed KP-ABE in which users' private key is used to store access control policy and encrypted data stores additional attributes. An authorized user can decrypt data if the access policy defined in users' private key satisfies attribute of data. However, the main issue with KP-ABE is owner (one who has encrypted data) cannot take a decision on who can decrypt the data.

In 2007, Bethencourt et al. [31] introduced CP-ABE in which the access policy is stored with encrypted data and attributes are stored in users' secret key; as a result, the user can access only the attributes associated with his private key. The concept supports access control in real-time environment; however, it requires flexibility and efficiency and its decryption key only supports user attributes that are logically organized as a single set; as a result, user has to use a combination of all attributes. To overcome this problem, ciphertext-policy attribute-set-based encryption is introduced. It organizes user attributes into a recursive set-based structure and user combines these attributes dynamically in order to satisfy a policy without sacrificing the flexibility. The main challenge is allowing users to combine attributes dynamically within a given key and avoiding collusion at the same time.

Earlier, ABE was based on monotonic access structure. Ostrovsky et al. in 2007 [34] proposed ABE that supports non-monotonic formulas on access policies to express any access formula. Tang et al. in 2008 [35] put forward verifiable ABE.

Muller in 2009 [36] proposed an extension of CPABE, DABE (Distributed Attribute-Based Encryption) that supports random number of parties to maintain the attributes along with their corresponding secret keys; however, the access policy has to be in DNF form.

Boneh and Franklin [37] proposed an identity-based encryption scheme, in which data is encrypted using a random string as the key and for decryption; a decryption key is mapped to the random encryption key-by-key authority.

Hierarchical Identity-Based Encryption (HIBE) [38] is the tree-like form of a single IBE; the main disadvantage of this system is key management overhead. Wang et al. [39] embedded a hierarchical structure in the CPABE. They delegated most of the computation workloads to the cloud and provided compatibility with complex applications. But the scheme does not support compound attributes.

Wan et al. [40] in 2012 proposed scalable and flexible HASBE scheme and considered that root level authority is responsible for managing top-level domain authorities. It supports flexible compound attribute set combinations and achieves efficient user revocation because of multiple values assigned to attributes (Table 1).

## *4.2 Proxy Re-encryption*

The main security concern while sharing the data using cloud is to prevent it from semi-trusted cloud service providers. In order to maintain confidentiality, several proxy re-encryption techniques are available. Proxy encryption is a primitive which helps in translating ciphertext from one encryption form to another encryption form without any information leaked to third party or cloud service provider. Application of proxy re-encryption is sharing public health records online, social media, and email forwarding.

### 4.2.1 Type-Based Proxy Re-encryption

The scheme proposed by Tang [41] enables owner to categorize ciphertext into subsets and uses one key pair in order to simplify key management problem. These subsets are re-encrypted to ciphertext using public key of specified authorized user. The main advantage of this scheme is that every authorized user can use a particular proxy.

### 4.2.2 Key Private Proxy Re-encryption

It was introduced by Ateniese [42] in 2009 under this scheme that it is impossible for proxy server to identify the recipient of the message.

### 4.2.3 Identity-Based Proxy Re-encryption

Identity-based proposed by Shamir [43] uses string of arbitrary length such as email id for creating public key of authorized users. The proxy server will translate the ciphertext of Alice to ciphertext of Bob without being able to retrieve any information.

**Table 1** Comparison of attribute-based encryption

| Techniques | ABE | KP-ABE | CP-ABE | IBE | HABE | DABE | MA-ABE |
|---|---|---|---|---|---|---|---|
| Fine-grained access control | Low | High if there is re-encryption, low | Avg, high if there is re-encryption | Avg | Good | Good | Good |
| Efficiency | Avg | High for broadcast type system average | Avg | Low | Flexible | Avg | High |
| Confidentiality | Low | High | High | High | High | High | High |
| User accountability | Not maintain | Not maintain | Well maintain | Well maintain | Well maintain | Well maintain | Well maintain |
| Computation overhead | High | High | Avg | Low | Low | Avg | Avg |
| Collusion resistant | Avg | Good | Good | Low | Good | Good | High |

### 4.2.4 Conditional Proxy Re-encryption

Under this scheme, the owner specifies the conditions along with ciphertext and the proxy can transform the ciphertext of data owner to encrypted form of recipient if and only if ciphertext satisfies the condition specified by the owner. This scheme is not sufficient to implement fine-grained access control [44].

### 4.2.5 Time-Based Proxy Re-encryption

The scheme introduced by Liu [45] has achieved user revocation and fine-grained access control in the absence of data owner. In it, each user is associated with time period for validity of user access rights so if he wants to access the data he needs to have the access rights on attributes as well as access time must satisfy the validity. Major limitation in it is for a user; the access time for all the attributes is same.

### 4.2.6 Threshold Proxy Re-encryption

This scheme integrates encrypting, encoding, and forwarding [46] and exhibits homomorphism, proxy re-encryption, and threshold decryption properties. Homomorphism states that for ciphertexts c1 and c2 defined on plain text p1 and p2, one can use c1 and c2 to obtain ciphertext on the plain text $p1 \cdot p2$ or $p1 + p2$. Proxy re-encryption allows encrypted form of data of user1 to be transformed into encrypted for another user without any information leaked to third party. Threshold encryption lets the private keys to be divided into several pieces and distributed to clients and all clients must together decrypt the file.

## *4.3 Hybrid Approach of Attribute-Based Encryption and Proxy Re-encryption*

Yu et al. [47] proposed a technique by combining KP-ABE, proxy re-encryption, and lazy re-encryption; he managed to push the task of data re-encryption and decryption to cloud. The main issue is cloud has to be stateful to retain history of user revocation.

Blaze et al. [48] proposed a proxy re-encryption which allows the encrypter to ask a third party to re-encrypt his encrypted message and deliver it to the decrypter.

Yang et al. [49] proposed a generic solution for implementing fine-grained data sharing. His technique enables cloud to be stateless and need not have to maintain state of user revocation. However, the scheme is not able to handle scenarios when a revoked user rejoins the system and is authorized with different access privileges.

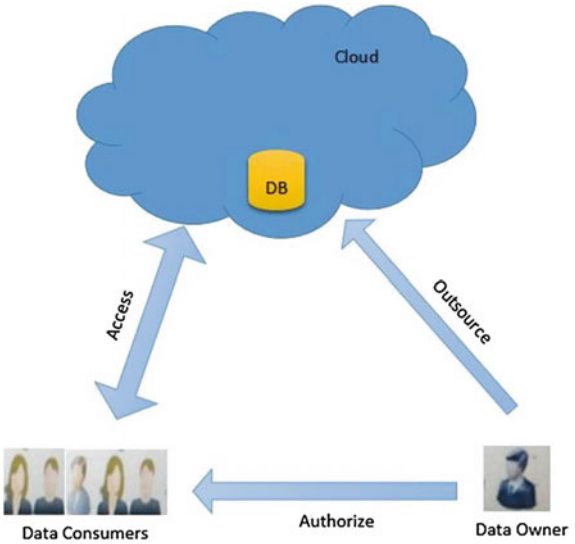


**Fig. 2** Data sharing between owner and clients

The scheme also fails to handle collusion between revoked and authorized user and revoked user and untrusty cloud service provider.

Bharath et al. [50] proposed framework using proxy re-encryption and additive homomorphic encryption in order to give a solution. He has implemented the concept of federation of clouds in order to prevent collusion. However, there is a limitation in their work that they have assumed that if revoked user colludes with authorized user; then, the revoked user shares information available to authorized user only (Figure 2).

## *4.4 Secured Query Processing*

One of the problems while outsourcing the data to cloud is that the query must be executed and output should be given to only authorized users who have initiated the query. While the query is being sent and processed and output generated, the process should not be accessible to any unauthorized user or cloud service provider. Boneh et al. [51] have presented a general framework for analyzing security of searching on encrypted data systems. Under this framework, they have constructed public-key systems that support comparison queries on encrypted data as well as more general queries such as subset queries.

Hakan et al. [52] have introduced an algebraic framework in which they have deployed coarse index which allows query to be partially executed on encrypted data at providers end and then decrypted at client end and remaining query executes.

Hore et al. [53] have developed a bucketization procedure for answering multidimensional range queries on multidimensional data and allow the data owner to control the tradeoff between risk and cost.

Wang et al. [54] have ensured data confidentiality both at storage and at access time and also supports different queries and data updates.

## 5 Conclusion and Future Work

Sharing data on cloud is widely accepted and is increasing rapidly. The data owners are interested in outsourcing the data on cloud in order to avoid storage management and capital expenditure in infrastructure but there are several issues associated with it and one of the major issues is confidentiality and security. In this paper, we have discussed on how to increase confidentiality and maintain privacy and security while sharing the critical data through third party named cloud service providers. We have explained encryption technique like ABE and PRE, when combined altogether enable us to share the data securely maintaining confidentiality along with fine-grained access control. However, the information can be leaked if there exists collusion between cloud service provider and revoked user or between authorized user and revoked users. Our proposed approach is to implement multi-party computation-based homomorphic threshold cryptosystem under this approach; private key of authorized user will be shared among n number of clouds and the secret can be revealed if x out of total n participants work together. This approach will prevent the data as the revoked user cannot collude with x number of users altogether.

## References

1. Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M (2010) A view of cloud computing. Commun ACM 53:50–58
2. Mell P, Grance T (2009) The NIST definition of cloud computing. Technical report, National Institute of Standards and Technology, Information Technology Laboratory, July 2009. http://www.csrc.nist.gov/groups/sns/cloud-computing/
3. Qian L, Luo Z, Du Y, Guo L (2009) Cloud computing: an overview. In: Proceedings of the 1st international conference on cloud computing, CLOUDCOM'09. Springer, Berlin, pp 626–631
4. Rimal B, Choi E, Lumb I (2009) A taxonomy and survey of cloud computing systems. In: IEEE fifth international joint conference on INC, IMS and IDC, pp 44 –51, Aug 2009
5. Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl 1(1):7–18
6. Hanna S. Cloud computing: finding the silver lining. http://www.ists.dartmouth.edu/events/abstract-hanna.html

7. Kantarcioglu M, Clifton C (2005) Security issues in querying encrypted data. In: Proceedings of the 19th annual working conference on data and applications security, DBSEC'05. Springer, Berlin, pp 325–337
8. Cantor S, Sigaba JM, Philpott R, Maler E (2005) Metadata for the OASIS security assertion markup language (SAML) v2.0", copyright © OASIS open
9. Chow R, Golle P, Jakobsson M, Shi E, Staddon J, Masuoka R, Molina J (2009) Controlling data in the cloud: Outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on cloud computing security (CCSW), pp 85–90
10. Dahbur K, Mohammad B, Tarakji AB (2011) Security issues in cloud computing: a survey of risks, threats and vulnerabilities. Int J Cloud Appl Comput (IJCAC) 1
11. Dhage SN, Meshram BB, Rawat R, Padawe S, Paingaokar M, Misra A (2011) Intrusion detection system in cloud computing environment. In: Proceedings of the international conference & workshop on emerging trends in technology, ICWET'11, pp 235–239
12. Kandukuri B, Paturi V, Rakshit A (2009) Cloud security issues. In: IEEE International conference on services computing, pp 517–520
13. Singh G, Sharma A, Lehal MS (2011) Security apprehensions in different regions of cloud captious grounds. Int J Network Secur Its Appl (IJNSA) 3
14. Brodkin J. Gartner: seven cloud-computing security risks. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853
15. Ristenpart T, Tromer E, Shacham H, Savage S (2009) Hey, you, get off of my cloud: exploring information leakage in third—party compute clouds. In: Proceedings of the 16th ACM conference on computer and communications security, CCS'09. ACM, New York, pp 199–212
16. Wang C, Wang Q, Ren K, Lou W (2009) Ensuring data storage security in cloud computing. In: International workshop on quality of service, pp 1 –9, July 2009
17. Salesforce.com. warns customers of phishing scam. http://www.pcworld.com/article/139353/article.html
18. Yan L, Rong C, Zhao G (2009) Strengthen cloud computing security with federal identity management using ierarchical identity-based cryptography. In: Proceedings of the 1st international conference on cloud computing, CLOUDCOM'09. Springer, Berlin, pp 167–177
19. Lu R, Lin X, Liang X, Shen XS (2010) Secure provenance: the essential of bread and butter of data forensics in cloud computing. In: Proceedings of the 5th ACM symposium on information, computer and communications security, ASIACCS'10. ACM, New York
20. Lin D, Squicciarini A (2010) Data protection models for service provisioning in the cloud. In: Proceeding of the 15th ACM symposium on access control models and technologies, SACMAT'10, pp 183–192
21. Nyre AA, Jaatun M (2009) Privacy in a semantic cloud: whats trust got to do with it? In: Cloud computing, volume 5931 of lecture notes in computer science. Springer, Berlin, pp 107–118
22. Pearson S, Shen Y, Mowbray M (2009) A privacy manager for cloud computing. In: Proceedings of the 1st international conference on cloud computing, CLOUDCOM'09. Springer, Berlin, pp 90–106
23. Thuraisingham B, Khadilkar V, Gupta A, Kantarcioglu M, Khan L (2010) Secure data storage and retrieval in the cloud. In: Collaborative computing: networking, applications and worksharing (collaboratecom), pp 1–8, Oct 2010
24. Uemura T, Dohi T, Kaio N (2009) Availability analysis of a scalable intrusion tolerant architecture with two detection modes. In: Proceedings of the 1st international conference on cloud computing, CLOUDCOM'09. Springer, Berlin, pp 178–189
25. A. S. A. event. July 20, 2008. http://status.aws.amazon.com/s3-0080720.html
26. Takabi H, Joshi J, Ahn G (2010) Security and privacy challenges in cloud computing environments. IEEE Secur Privacy 8(6):24–31
27. Jansen W, Grance T (2011) Draft special publication 800-144: guidelines on security and privacy in public cloud computing. National Institute of Standards and Technology, U.S. Department of Commerce

28. Andrei T (2009) Cloud computing challenges and related security issues
29. Agudo I, Nuez D, Giammatteo G, Rizomiliotis P, Lambrinoudakis C (2011) Cryptography goes to the cloud. in secure and trust computing, data management, and applications, vol 187 of communications in computer and information science. Springer, Berlin, pp 190–197
30. Santos N, Gummadi KP, Rodrigues R (2009) Towards trusted cloud computing. In: Proceedings of the 2009 conference on hot topics in cloud computing, HOTCLOUD'09, Berkeley, CA, USA. Usenix Association
31. Bethencourt J, Sahai A, Waters B (2007 )Ciphertext-policy attribute-based encryption. In: Proceedings of IEEE symposium on security and privacy
32. Sahai A, Waters B (2005) Fuzzy identity-based encryption. In: Cramer R (ed) Advances in cryptology—EUROCRYPT 2005. Springer, Berlin, pp 457–473
33. Goyal V, Pandy O, Sahai A, Waters B (2006) Attribute based encryption for fine-grained access control of encrypted data. In: Proceedings of ACM computer and communications security conference, CCS'06
34. Ostrovsky R, Sahai A, Waters B (2007) Attribute-based encryption with non-monotonic access structures. In: Proceeding of ACM conference on computer and communications security, pp 195–203
35. Tang Q, Ji D (2010) Verifiable attribute-based encryption. Int J Network Secur 10(2):114–120
36. Müller S, Katzenbeisser S, Eckert C (2009) Distributed attribute-based encryption. In: Proceedings of 11th international conference on information security and cryptology (ICISC 08), pp 20–36
37. Boneh D, Franklin MK (2003) Identity-based encryption from the weil pairing. SIAM J Comput 32(3):586–615
38. Boneh D, Boyen X, Goh E-J (2005) Hierarchical identity based encryption with constant size ciphertext. In: Cramer R (ed) Eurocrypt, volume 3494 of lecture notes in computer science. Springer, Berlin, pp 440–456
39. Wang G, Liu Q, Wu J (2010) Hierarhical attribute-based encryption for fine-grained access control in cloud storage services. In: Proceedings of ACM conference on computer and communications security, CCS' 10
40. Wan Z, Liu J, Deng RH (2012) HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Trans Inf Forensics Secur 7(2):743–754
41. Tang Q (2008) Type-based proxy re-encryption and its construction. In: Proceedings of ninth international conference on cryptology in India, pp 130–144
42. Ateniese G, Benson K, Hohenberger S (2009) Key-private proxy re-encryption. In: Proceedings topics in cryptology, pp 279–294
43. Shamir A (1984) Identity-based cryptosystems and signatures schemes. Adv Cryptol 47–53
44. Libert B, Vergnaud D (2008) Tracing malicious proxies in proxy re-encryption. In: Proceedings of PAIRING'08. LNCS 5209. Springer, Berlin, pp 332–353
45. Liu Q, Wang G, Wu J (2012) Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Information sciences (in press)
46. Asharov G, Jain A, Lopez-Alt A, Tromer E, Vaikuntanathan V, Wichs D (2012) Multiparty computation with low communication, computation and interaction via threshold FHE. In: Proceeding of eurocrypt'12. Springer, Berlin, pp 483–501
47. Yu S, Wang C, Ren K, Lou W (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. In: Proceedings of IEEE international conference on computer communications, INFOCOM'10
48. Blaze M, Bleumer G, Strauss M (1998) Divertible protocols and atomic proxy cryptography. In: Proceedings of advances in cryptology, eurocrypt'98
49. Yang Y, Zhang Y (2011) A generic scheme for secure data sharing in cloud. In: 40th international conference on parallel processing workshops, pp 145–153, Sept 2011
50. Samanthula BK et al (2015) A secure data sharing and query processing framework via federation of cloud computing. Inf Syst 48:196–212

51. Boneh D, Waters B (2007) Conjunctive, subset, and range queries on encrypted data. In: Proceedings of the 4th conference on theory of cryptography, TCC'07. Springer, Berlin, pp 535–554
52. Hakan H, Iyer B, Li C, Mehrotra S (2002) Executing Sql over encrypted data in the database-service provider model. In: Proceedings of the 2002 ACM sigmod international conference on management of data, SIGMOD'02. ACM, pp 216–227
53. Hore B, Mehrotra S, Canim M, Kantarcioglu M (2012) Secure multidimensional range queries over outsourced data. VLDB J 21(3):333–358
54. Wang S, Agrawal D, El Abbadi A (2011) A comprehensive framework for secure query processing on relational data in the cloud. In: Proceedings of the 8th VLDB international conference on secure data management, SDM'11. Springer, Berlin, pp 52–69

## Author Biographies

**Neha Agarwal** is currently working as an Assistant Professor in Amity School of Engineering and Technology, Amity University, Uttar Pradesh. She is pursuing her Ph.D. from Dr. A. P.J. Abdul Kalam Technical University (APJAKTU) (UP) in the area of Cloud Computing. She received her M.Tech in Computer Science Engineering from Amity University Noida, Uttar Pradesh.

**Ajay Rana** is a director at Amity University. He received his M.Tech degree in Computer Science Engineering from Kurukshetra University, Haryana, India. He obtained his Ph.D. from UP Technical University, Lucknow (UP) India. He has published more than 200 Research Papers in reputed Journals and Proceedings of International and National Conferences. He has co-authored 06 Books and co-edited 36 Conference Proceedings. He is Editor in Chief, Technical Committee Member, Advisory Board Member for 18 Plus Technical Journals and Conferences at National and International Levels.

**Jai Prakash Pandey** is currently working as Professor and Director in the Department of Electrical Engineering at Kamala Nehru Institute of Technology, Sultanpur, (UP), India. He has received his B. Tech and M. Tech in Electrical Engineering from Kamala Nehru Institute of Technology, Sultanpur (UP), India. He obtained his Ph.D. degree from UP Technical University, Lucknow (UP) India. His research interests include applications of artificial techniques to electrical engineering problems in power system, estate estimation and power quality.