ISSN:0975-9646

User Anonymous Authentication Scheme for Decentralized Access Control in Clouds

Pooja R. Vyawhare, Prof.Namrata D. Ghuse

Department of Computer Science & Engineering,
P.R.Pote CET, Amravati, Maharashtra, India

***Abstract*— Cloud Computing is the emerging technology where we can get platform as a service, software as a service and infrastructure as a service. When it comes to storage as a service, data privacy and data utilization are the primary issues to be deal with. Security and privacy are very important issues in cloud computing. Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. Users are authenticated who store and modify their data on the cloud. The identity of the user is protected from the cloud during authentication. The architecture is decentralized, meaning that there can be several KDCs for key management. Revoked users cannot access data after they have been revoked. The proposed scheme is resilient to replay attacks. The protocol supports multiple read and writes on the data stored in the cloud. It proposing privacy preserving authenticated access control scheme. According to the scheme a user can create a file and store it securely in the cloud. The cloud verifies the authenticity of the user without knowing the user's identity before storing data. The scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. The work proposes a new decentralized access control scheme for secure data storage in clouds, which supports anonymous authentication .Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized.**

***Keywords*— Cloud Storage, Decentralised Access, Key Distribution Center, Attribute Based Encryption, Access Control, Anonymity Authentication, Key Management**

I. INTRODUCTION

Cloud computing is a promising computing model which currently has drawn far reaching consideration from both the educational community and industry. By joining a set of existing and new procedures from research areas, for example, Service-Oriented Architectures (SOA) and virtualization, cloud computing is viewed all things considered a computing model in which assets in the computing infrastructure are given as services over the Internet. . Numerous services like email, Net banking and so forth are given on the Internet such that customers can utilize them from anyplace at any time. Indeed cloud storage is more adaptable, how the security and protection are accessible for the outsourced data turns into a genuine concern. The three points of this issue are availability, confidentiality and integrity. The data possessor must encrypt the record and then store the record to the cloud. Assuming that a third person downloads the record, they may see the record if they had the key which is utilized to decrypt the encrypted record. Once in a while this may be failure because of the technology improvement and the programmers. To overcome the issue there is lot of procedures and techniques to make secure transaction and storage.

Recently experts addressed Anonymous authentication for data archiving to clouds[2]. Anonymous authentication is the procedure of accepting the client without the details of the client. So the cloud server doesn't know the details of the client, which gives security to the clients to conceal their details from other clients of that cloud. Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often related to health, important documents (as in Google Docs or Dropbox) or even personal information (as in social networking).Access control is also gaining importance in online social networking where users (members) store their personal information, pictures, videos and share them with selected groups of users or communities they belong to. It is not just enough to store the contents securely in the cloud but it might also be necessary to ensure anonymity of the user. For example, a user would like to store some sensitive information but does not want to be recognized. The user might want to post a comment on an article, but does not want his/her identity to be disclosed. However, the user should be able to prove to the other users that he/she is a valid user who stored the information without revealing the identity.

A. Motivation

Existing methods works on access control in cloud are centralized in nature. Except some all other schemes use ABE. The schemes use a symmetric key approach and does not support authentication. The most previous schemes do not support authentication as well. Much of the previous work takes a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. Therefore, the expert emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world.

B. Objective

1.Distributed access control of data stored in cloud so only authorized users with valid attributes can access them.
2. Authentication of users who store and modify their data on the cloud.
3. The identity of the user is protected from the cloud during authentication.
4. The architecture is decentralized, meaning that there can be several KDCs for key management.
5. Revoked users cannot access data after they have been revoked.
6. The proposed scheme is resilient to replay attacks.
7. The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud.

II. LITERATURE REVIEW

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters[27]introduced the concept of Attribute-Based Encryption for Fine Grained Access Control of Encrypted Data in 2006. He introduces the new cryptosystem for fine grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KPABE). In cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. Matthew Pirretti and Brent Waters[31]introduce a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives also they propose cryptographic optimizations in Secure Attribute Based Systems in 2007. Decryption decrypts a ciphertext encrypted by the Encryption. This process begins with the decrypting party verifying that they have the required attributes. The party performing decryption will then use their attributes to decrypt the decrypt the ciphertext in order to obtain the AES and HMAC key.

John Bethencourt, Amit Sahai, Brent Waters[26]introduces Ciphertext-Policy Attribute-Based Encryption in 2008. The expert employ a trusted server to store the data and mediate access control. In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any serverstoring the data is compromised, then the confidentiality of the data will be compromised. In addition, they provide an implementation of our system and give performance measurements.

Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati describes combination of access control and cryptography in 2010. It illustrate the basic principles on which an architecture for combining access control and cryptography can be built. then illustrate an approach for enforcing authorization policies and supporting dynamic authorizations, allowing policy changes and data updates at a limited cost in terms of bandwidth and computational power. Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Bjorn Tackmann, Daniele Venturi[9]introduced Anonymity-preserving Public-Key Encryption:A Constructive Approach where public-key cryptosystems with enhanced security properties have been proposed. it investigate constructions as well as limitations for preserving receiver anonymity when using public-key encryption (PKE). Junbeom Hur, Dong Kun Noh[23] introduces the concept of Attribute-Based Access Control with Effcient Revocation in Data Outsourcing Systems in May 16, 2012. The attribute based crypto-systems were introduced such as Ciphertext-Policy Attribute-Base Encryption (CP-ABE) with an addition of two new functions. The first function is KEKGen(U)) which is used to generate keys to encrypt attributes for groups. The other extra function is the ReEncrypt(CT;G) which is a re-encryption that takes the ciphertext and re-encrypt it so that a user in Group G can only access it.

R.Ranjith and D.Kayathri Devi[16] describes the concept of Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication in 2013. The scheme implemented secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination. Private Key is the combination of the user's credentials. So that high security will be achieved. The Renewal can be done by providing the new key to the existing file, will remains the file until the new time limit reaches. Mr. Parjanya C.A and Mr. Prasanna Kumar M[15]describes the concept of Advance Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud in march 2014. They were presented the new framework for MONA. In this method further presented how to manage the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability. S Divya Bharathy and T Ramesh[14] intrdused the concept of privacy preserving access control scheme for data storage, which supports anonymous authentication and performs decentralized key management in Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control in April 2014. In the proposed scheme, the cloud adopts an access control policy and attributes hiding strategy to enhance security. This new scheme supports secure and efficient dynamic operation on data blocks, including: data update, creation, modification and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized.

Sushmita Ruj, Milos Stojmenovic, AmiyaNayak[1]-[17] introduces Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds in 2014. They propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. We have presented a decentralized access

control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials.

III. PROPOSED SYSTEM

The proposed scheme consists of four algorithms which is defined as follows

- Setup:
  This algorithm takes as input security parameters and attribute universe of cardinality N. It then defines a bilinear group of prime number. It returns a public key and the master key which is kept secret by the authority party.
- Encryption:
  It takes a message, public key and set of attributes. It outputs a cipher text.
- Key Generation:
  It takes as input an access tree, master key and public key. It outputs user secret key.
- Decryption:
  It takes as input cipher text, user secret key and public key. It first computes a key for each leaf node. Then it aggregates the results using polynomial interpolation technique and returns the message.

IV. REQUIREMENT ANALYSIS

- Software Requirements

Operating system : Windows XP, Windows 7
Browser : Mozilla firefox, Internet Explorer
Data Base : My Sql / MS Access.
Server : WAMP Server

- Hardware Requirement
  System : Pentium IV 3.5 GHz.
  Hard Disk : 40 GB

V. SYSTEM DESIGN

a. Key Management

In our project following are the cryptographic keys to protect data files stored on the cloud.

- Public Key: The Public key is a random generated binary key, generated and maintained by the Key manager itself. Particularly used for encryption/ decryption.
- Private Key: It is the combination of the username, password and two security question of user's choice. The private key is maintained by client itself. Used for encrypt / decrypt the file.
- Access key: It is associated with a policy. Private access key is maintained by the client. The access key is built on attribute based encryption. File access is of read or write.
- Renew key: Maintained by the client itself. Each has its own renew key. The renew key is used to renew the policy of each necessary file at easy method.

b. Encryption / Decryption

We used RSA algorithm for encryption/Decryption. This algorithm is the proven mechanism for secure transaction. Here we are using the RSA algorithm with key size of 2048 bits. The keys are split up and stored in four different places. If a user wants to access the file he/she may need to provide the four set of data to produce the single private key to manage encryption/decryption.

c. File Upload / Download

i. File Upload

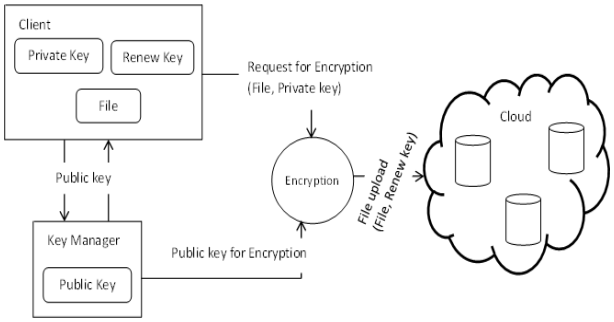


Fig.1: File uploading process

The client made request to the key manager for the public key, which will be generated according to the policy associated with the file. Different policies for files, public key also differs. But for same public key for same policy will be generated. Then the client generates a private key by combining the username, password and security credentials. Then the file is encrypted with the public key and private key and forwarded to the cloud.

ii. File Download

The client can download the file after completion of the authentication process. As the public key maintained by the key manager, the client request the key manager for public key. The authenticated client can get the public key. Then the client can decrypt the file with the public key and the private key. The users credentials were stored in the client itself. During download the file the cloud will authenticate the user whether the user is valid to download the file. But the cloud doesn't have any attributes or the details of the user.

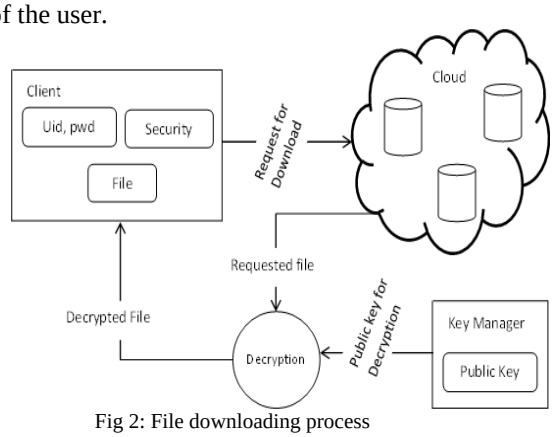


Fig 2: File downloading process

d. Policy Revocation for File Assured Deletion

The policy of a file may be revoked [8] under the request by the client, when expiring the time period of the contract or completely move the files from one cloud to another cloud environment. When any of the above criteria exists the policy will be revoked and the key manager will completely removes the public key of the associated file. So no one recover the control key of a revoked file in future. For this reason we can say the file is assuredly deleted. Automatic file revocation [12] scheme is also introduced to revoke the file from the cloud when the file reaches the expiry and the client didn't renew the files duration.

e. File Access Control

Ability to limit and control the access to host systems and applications via communication links. To achieve, access must be identified or authenticated. After achieved the authentication process the users must associate with correct policies with the files. To recover the file, the client must request the key manager to generate the public key. For that the client must be authenticated. The attribute based encryption standard is used for file access which is authenticated via an attribute associated with the file. With file access control the file downloaded from the cloud will be in the format of read only or write supported. Each user has associated with policies for each file. So the right user will access the right file. For making file access the attribute based encryption scheme is utilized.

f. Policy Renewal

Policy renewal is a tedious process to handle the renewal of the policy of a file stored on the cloud. Here we implement one additional key called as renew key, which is used to renew the policy of the file stored on the cloud. The renew key is stored in the client itself.

VI. DETAIL DESIGN

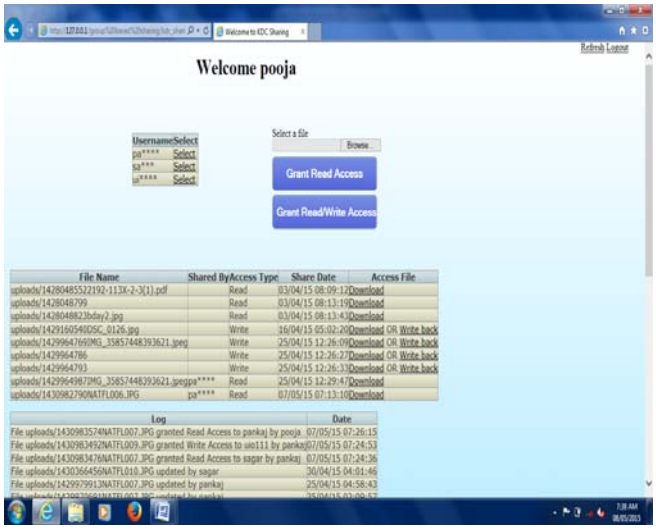
1. System Initialization
   The System Initialisation is the initial process for the system. The system get initialised for the user. The single user or the group of user can register within the system.
2. User Registration
   The User have to register themselves under the registration module. According to the user credentials, which will be provided by the users,the user will get the private key. And by using that private key the user can then upload or download the required data in the future.
3. KDC setup
   We emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. The architecture is decentralized, meaning that there can be several KDCs for key management.
4. Attribute generation
   The token verification algorithm verifies the signature contained using the signature verification. This key can be checked for the consistency. There are two types of access permissions are given to the user. Read and read write access. The user will allow the another user to only read the content of the sent file or they can permit to read and make some required modification and write it back again.
5. Sign
   The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim. The ciphertext C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the ciphertext C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message.
6. Verify
   The verification process to the cloud, it relieves the individual users from time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs.

VII. SCREENSHOT

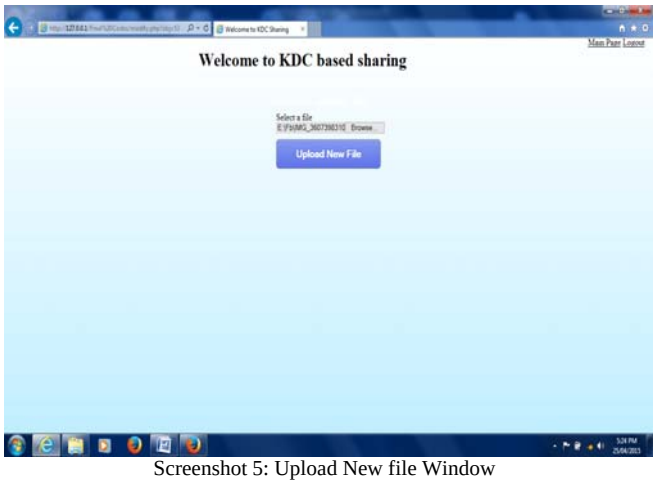
Screenshot 1: Homepage of the system

Screenshot 2: Login Page

Screenshot 4: KDC User Login



Screenshot 4: Select user and file to grant access



Screenshot 5: Upload New file Window

VIII. Result Analysis

In this sections result analysis is discuss in detail. Cloud is the virtual storage area where the user can store the data securely. The data storage is mainly consist of the security. The user must be ensure that the stored data is securely stored on the cloud. For this the user must be sure that only autherized used can access the data. Privacy and the security are the two mentioned factor for the data stored on the cloud. User authentication ensures the security. Hence the data can be only visible to the user who are successfully authenticated to the system. The user may permit the another user to access data by granting the access permission according to the choice. User Anonymity ensures the privacy of the data. The decentralized nature of the system relaxed it from the burdon of maintaining the eys abd attributes of all the user. Hence the analysis can be done according to the Authentication scheme, granting the access permission and Anonymity scheme and the decentralized enviornment.

a. Analysis with respect to the distribution of the key

In the single key distribution environment, the public key of all the users is maintained by the single KDC. The single KDC is responsible for all the encryption and decryption. Hence the load on the center is too much too handle such a large amount of key as the users of cloud are increasing day by day.Hence the burdon of one KDC is divided into more than one KDC. The distributed environment have more than one KDC where the keys and the user attributes are distributed.As the one KDC is the single point of failure may breakdown the transaction hence the keys are distributed all over the KDCs.

Scheme	Approach
Secure and efficient access to outsoursed data	Centralised
Effective Data Access Control for Multiauthority Attributebased encryption	Decentralised
Realising Fine Grained and access control to outersoursed data with attributebase cryptosystem	Centralised
Proposed System	Decentralised

Table 1: Comparison between the Number of KDC (Centralised/Decentralised)

b. Analysis with respect to the privacy preserving Authentication

The Authentication is to verify the user among the various users.Only Autherised user can access the data. The authentication process exceeds authorization. The authentication can be provide by obtaining the userid, username or password etc. According to the credentials that are received by the user can get verified uniquely. The authentication scheme is privacy preserving that it prevent the data to be access by any unauthorized user.

Scheme	Authentication
Securing Personal Health Records in Cloud Computing	No Authentication
“Attribute Based Data Sharing with Attribute Revocation,	No Authentication
“Outsourcing the Decryption of ABE Ciphertexts	No Authentication
Decentralizing Attribute-Based Encryption	No Authentication
Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems,”	Authentication
Proposed System	Authentication

Table 2:Comparison between the Authentication schemes of the various systems.

c. Analysis with respect to the Access Policy

The user can decide that which user can access his data, and which user can only read the data or can modify it and write back. There are 2 types of access policies, the only read policy permits user to only read the file and can only downloads the file. User cant make any changes through it.

Table 3: Comparison of granting the access i.e., read or read/write access to the user.

	read	read/write
rahul	12	22
sumit	10	4
amar	0	15
ramesh	9	6

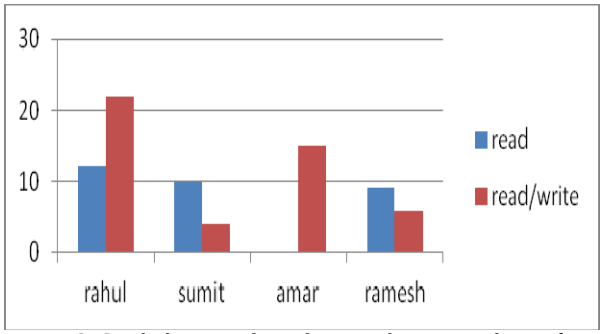


Figure 3: Graph showing relation between the access policies of various users.

Scheme	**Read/write Access**
Secure and efficient access to outsoursed data	1-W-M-R
Securing Personal Health Records in Cloud Computing	1-W-M-R
DACC: Distributed Access Control in Clouds	1-W-M-R
Outsourcing the Decryption of ABE Ciphertexts	1-W-M-R
Decentralizing Attribute-Based Encryption	1-W-M-R
Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems	M-W-M-R
Proposed System	M-W-M-R

Table 4: Comparison between the access policy between the schemes

The read/write access permits the user to read the content of the file and if the user feels to change it then the file can be modify and user may write it back. These policy granting facility is depend upon the user itself. Its depend wholely on the user to grant the access permission to the another user.the single write and single read permissions are granted by the many users. but the system proposes the many read and many write permission to the user.

d. Analysis of time required for transaction on cloud

File Size	Upload (Sec)	Download (Sec)
10 Bytes	15	0
1 KB	17	3
10 KB	19	0
100KB	20	7
1 MB	22	7

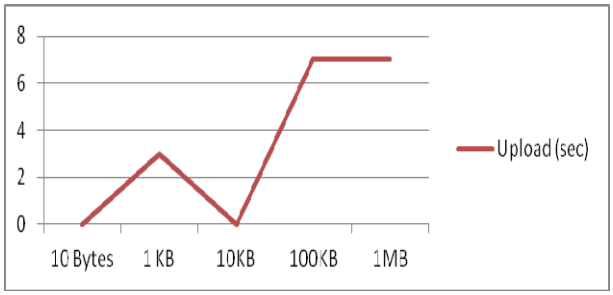


Figure 4: Graph showing time required for uploading the file on cloud

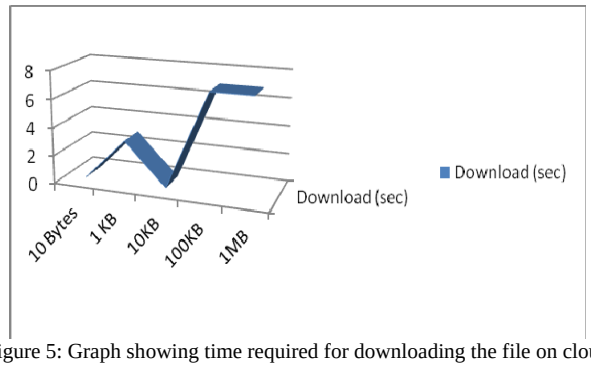


Figure 5: Graph showing time required for downloading the file on cloud

IX. Conclusions

We have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.

References

[1] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556- 563, 2012.

[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.

[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, pp. 441-445, 2010.

[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136- 149, 2010.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.

[6] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009.

[7] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.

[8] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/ 2011/HPL-2011-38.html, 2013.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[10] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., 1992.
[11] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role-Based Access Control," IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.
[12] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.
[13] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.
[14] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.
[15] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.
[16] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.
[17] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.
[18] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A View of Cloud Computing. *Comm. of the ACM, 53(4):50–58, Apr 2010*.
[19] M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in *ACM Conference on Computer and Communications Security, pp. 121–130, 2009*.
[20] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 552-565, 2001.
[21] X. Boyen, "Mesh Signatures," Proc. 26th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 210-227, 2007.
[22] D. Chaum and E.V. Heyst, "Group Signatures," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 257-265, 1991.
[23] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.
[24] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.
[25] A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," PhD thesis, Technion, Haifa, 1996.
[26] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.
[27] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.