Innovative Science and Technology Publications

International Journal of Future Innovative Science and Technology,
ISSN: 2454- 194X Volume-4, Issue-2, May - 2018

EFFICIENT USER REVOCATION AND TIME SENSITIVE DATA ACCESS IN CLOUD

P.Brindha [1]*, P.Lavanya [2]

[1]Professor, Vivekanandha college of Engineering for Women, India
[2]PG Scholar, Vivekanandha college of Engineering for Women, India

Email-ID: lavancse21@gmail.com,brindhassk@gmail.com

May – 2018

www.istpublications.com

Journal of Future Innovative Science and Technology, ISSN: 2454- 194X, Volume-4, Issue-2, MAY - 2018

EFFICIENT USER REVOCATION AND TIME SENSITIVE DATA ACCESS IN CLOUD

P.Brindha[1]*, P.Lavanya[2]

[1]Professor, Vivekanandha college of Engineering for Women, India
[2]PG Scholar, Vivekanandha college of Engineering for Women, India

Email-ID: *lavancse21@gmail.com, brindhassk@gmail.com*

ABSTRACT: Outsourcing data to cloud faces many challenges on security and privacy. Cloud computing is preferred as it reduces cost of data management and its available resources. To protect data from third party cloud server, it is necessary to have an efficient data access control. Timed release encryption is a kind of encryption in which owner encrypts a message for the purpose that intended users can decrypt it after a designated time. Apart from access control, it is also necessary for user revocation, this provides more efficient system for access control.

Keywords: *Cloud Storage, Time Sensitive data, fine Grained access control, User revocation*

1. Introduction

Enterprises and individual seeks the advantages of convenient data sharing and cost reduction of cloud computing services. Whereas the storage and data sharing poses new challenges on data confidentiality preservation. As the cloud serve is third party server, the data owner cannot trust the cloud server to conduct secure data access control. Therefore, the safe and sound right to use governor badly behaved has become an inspiring concern in communal cloud putting a way. Time factor is important while dealing with time sensitive data. Providing access privilege on time sensitive data is proposed here. As the time sensitive data is handled, there is more security need in access control, thus user revocation is checked with access policy.

2. **Literature Survey**:

In [1] authors Jianan Hong, Kaiping Xue, Yingjie Xue, Weikeng Chen, David S.L. Wei, Nenghai Yu and Peilin Hong in the paper **"TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud"** it discharge records title holders from the technical management, and is easier for data owners to share their data with planned users and also it poses new tasks on privacy and security protection. Nonetheless, cash register at this moment, no chaos can maintenance both fine-grained right to use resistor and time-sensitive records broad casting. An efficient approach to design access policies faced with various access requirements for time-sensitive data. TRE satisfies that except the planned users, no one is able to get any data of the message and even the planned user cannot get the plaintext of the message before the designated releasing time. To build a scalable and fine-grained access control system for outsourced time-sensitive data, we trust two advanced cryptographic techniques, namely CP-ABE and TRE. The general idea of our unique mechanism is to understand access structures in a new form. Apart from attributes and logic gates defined in existing CP-ABE, the access structure in our scheme contains one or more time trapdoors (*TS*), each of which denotes a time point. The trapdoor is implemented for the timed release function in CP-ABE algorithm.

In [2] authorsKan Yang, Xiaohua Jia, Kui Ren, Bo Zhang in the paper **"DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems"** Data Access Control for Multi-Authority Cloud Storage and lively and protected histories communication controller assembly with operative decryption and revocation. Specifically, build a new multi-authority CP-ABE scheme with efficient decryption and also design an effective attribute cancellation method that can flourish both forward safety and hesitant retreat.

Strategy and competent immediate feature with drawl skill for multi-authority CP-ABE pattern that flourishes both head first safekeeping and regressive safekeeping. It is efficient in the sense that it incurs less communication price and computation price of the revocation. DAC-MACS is a group of algorithms that combines a set of CP-ABE algorithms and a set of attribute revocation algorithms: DAC-MACS is protected against static corruption of authorities if all polynomial time adversaries have at most a negligible benefit in the safety game. Multi-authority CP-ABE scheme has been extended to support attribute revocation in, it still cannot be efficient to access control for multi-authority cloud storage systems due to the insufficiency of decryption and revocation.

In [3] authors Dayananda RB, Prof. Dr. G.Manoj Someswar in the paper **"Time-Based Proxy Re-encryption Scheme for Secure Data Sharing in a Cloud Environment"** The data owner is responsible for defining the access building for each data, and issuing user attribute secret keys (UAKs) corresponding to user attributes to each user. When a user wishes to access information, he will first request appropriate keys from the data vendor, and then request the CSP to download the cipher text. The main policy aim is to succeed fine-grained access control and scalable user revocation while protecting data security in cloud computing. PRE system by the following example: Alice receives emails encrypted below her public key PKA via a semi trusted mail server. When she leaves for holiday, she wants to representative her email to Bob whose public key is PKB, but does not need to share her secret key SKA with him. The PRE system allows Alice to deliver a PRE key$_{RK\ A \rightarrow B}$ to the mail server, with which the mail server can convert a ciphertext that is encrypted below Alice's public key PKA into extra ciphertext that can be decrypted by Bob's secret key SKB, without seeing the underlying plaintext, SKA, and SKB. HABE which is built based on the bilinear map. The access structure in HABE is expressed as disjunctive normal form (DNF).

In [4] authors Elli Androulaki, Claudio Soriente, Luka Malisaand Srdjan Capkun in the paper **"Enforcing Location and Time-based Access Control on Cloud-stored Data"** Enforce location and time-based access control has two entities. These two things operate independently and are only important to offer their basic services: the cloud provider is used and reliable only to reliably store data, the localization infrastructure is used and reliable only to accurately locate users. Protocols in LoTAC leverage ElGamal encryption and a novel tag-based encryption system, what kinds proposed protocols suitable for resource-constrained user devices. LoTAC over a prototype enactment where the localization infrastructure is instantiated as a cellular network and display that our protocols can be executed with low communication and computation costs and scale well with large numbers of users and policies. In tag-based encryption schemes, encryption and decryption algorithms take an added (public) input referred to as tag. The latter is simply a binary string of appropriate length, and want not have any particular internal structure. Another option is to leverage ciphertext-policy attribute based encryption (CP-ABE). CP-ABE allows to encrypt a message below a policy distinct over arbitrary attributes, such that only users who satisfy the policy (i.e., hold the right set of attributes) can decrypt the ciphertext.

In [5] authors Cong Wang, Qian Wang, Kui Ren, Wenjing Lou in the paper **"Toward Secure and Dependable Storage Services in Cloud Computing"** In this plastic distributed stowage honor inspecting apparatus, overriding the homomorphic empty and circulated deletion-implied records. The future plan allows users to audit the cloud storage with very lightweight communication and computation cost. The examining product not only certifies tough cloud loading truth surety, but also instantaneously achieves fast data inaccuracy localization, i.e., the identification of misbehaving server. Since the cloud figures are energetic in nature, the coming design extra cares secure and competent active maneuvers on subcontracted data, including lump change, erasure, and join. Investigation demonstrations the planned system is really effectual and strong in contradiction of Scheming bomb, malicious information adjustment occurrence, and even head waiter plotting rounds. Demonstration age band, the consumer has the special of either protection the pre computed

demonstrations in the vicinity or putting away them in express in code form on the cloud servers. In our instance here, the employer provisions them nearby to preclude the want for encryption and lesser the bandwidth above during self-motivated figures procedure which will be debated presently. Fault localization is a main condition for eliminating faults in packing arrangements. It is also of perilous standing to categorize budding coercions from exterior outbreaks. Nevertheless, various former coordination do not unambiguously cogitate the challenging of numbers blunder localization, thus only provided that double domino effect for the putting away authentication. In the meantime our arrangement of heading conditions is efficient, the manipulator can re fabricate the inventive file by moving the records flight path from the first m servers, high and mighty that they coming back the truthful comeback values. Notice that our verification scheme is based on casual spot-checking, so the storage correctness declaration is a probabilistic one.

In [6] authors Qin Liu, Chiu C. Tan, Jie Wu, Guojun Wangin the paper **"Reliable Re-encryption in Unreliable Clouds"** A key method to secure cloud computing is for the data owner to store encrypted data in the puff, and issue decryption keys to authorized users. Then, when a user is retracted, the records titleholder will difference of opinion re-encryption directions to the puff to re-encrypt the records, to check the retracted consumer from decrypting the records, and to generate new decryption keys to valid users, so that they can remain to access the data. An interval-constructed re-encryption classification, which authorizations the cloud member of staff serving at table to inevitably re-encrypt records based on their heart clocks. Our clarifications is assembled on best of an innovative encryption pattern, attribute *based encryption*, to authority fine-grain contact resistor, and does not need unspoiled clock harmonization for perfection. ABE countenances numbers to be scrambled using an *access structure* comprised of different *attributes*. Instead of explicit decryption sources for unambiguous files, managers are conveyed point explanations. Users must have the necessary attributes that fulfill the access structure in order to decrypt a file. The vital delinquent of putting away encrypted records in the cloud fabrications in *withdrawing* contact rights from consumers. A user whose permission is revoked will still recollect the keys distributed earlier, and thus can still decrypt data in the cloud. *Reliable re-encryption scheme in unreliable clouds* (R3 system for short). R3 is an interlude-constructed re-encryption organization, which tolerates for per capitapuff attendant to inevitably re-encrypt records constructed on its heart chronometer. The basic idea of the R3 system is to associate the data with an *access control* and an *access time*.

In [7] authors Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang, and Shanbiao Wangin the paper **"Towards Temporal Access Control in Cloud Computing"** Attribute-based access control delivers a flexible approach that permits data owners to integrate data access policies within the encrypted data. However, little work has been done to explore temporal attributes in requiring and enforcing the data owner's policy and the data user's privileges in cloud-based environments. Here, an efficient temporal access controls encryption coordination for cloud service station with the help of cryptographic whole number evaluations and a proxy-based re-encryption appliance on the contemporary time. Entrance resistor is well thought-out as one of precarious safe keeping appliances for evidence shelter in cloud presentations. Unfortunately, traditional data access control systems usually accept that information is stored on trusted data servers for all users. This assumption however no longer holds in cloud computing then the data owner and cloud servers are very likely to be in two different domains.

In [8] authors Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou in the paper **"Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing"** Cloud computing is an evolving subtracting archetype in which funds of the figuring arrangement are as long as filling station terminated the Internet. As capable as it is, this archetype also conveys into the open sundry new contests for records safe keeping and right to use mechanism when customers farm out profound data for partaking on cloud headwaiters, which are not in the interior the same confidential territory as data

owners. To keep multifarious user data stable touching un trusted attendants, remaining solutions generally spread on cryptographic methods by releasing records decryption keys only to accredited users. The knotty of all together triumph fine-graininess, scalability, and records concealment of contact governor essentially still vestige sun certain. In this structure also had prominent assets of handler contact license concealment and handler secret key liability. All-embracing breakdown confirmations that coordination is particularly proficient and provably safe and sound under surviving safekeeping models.

In [9] authors M. Jothirmyi, Karpurapu Sudhakar Babuin the paper **"Flexible and Fine-Grained Attribute Based Data Storage in Cloud Computing"** Various layouts based on the attribute-based encryption used to secure the cloud storage. However, most effort goals on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity secrecy. A semi-unidentified pleasure hemostat arrangement AnonyControl to discourse not only the documents confidentiality, but also the manipulator distinctiveness confidentiality in contemporary right of entry mechanism organizations. AnonyControl spread out the fundamental expert witness to bind the personality beginning and thus apprehends semi anonymity. Both AnonyControl and AnonyControl-F are sheltered lower than the Diffie Hellman postulation, and our confirmation guesstimate revelations the practicability of our arrangements. In addition, it also take a broad view the file access governor to the source of pride controller, which constitutional rights of all procedures on the cloud records can be bring about in a compacted prearranged manner. By using the compound powers that be in the cloud computing organization, this systems accomplish not only fine-grained source of pride governor but also distinctiveness concealment while monitoring source of pride controller constructed on manipulators" distinctiveness statistics. More importantly, our system can accept up to N −2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also direct detailed security and performance analysis which displays that AnonyControl both efficient and secure for cloud storage system.

In [10] authors Hui Tian, Yuxiang Chen, Chin-Chen Chang,Hong Jiang, Yongfeng Huang, Yonghong Chen,Jin Liu, in the paper **"Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage"** Cloud storage is an increasingly popular application of cloud computing, which can carry on-demand outsourcing data facilities for both organizations and individuals. A innovative unrestricted glance organization for safe as houses cloud putting away constructed on self-motivated hash table , which is a innovative two-dimensional records arrangement to be found at a third uniformity inspector to best ever the records belonging statistics for self-motivated testing. In this system migrates the authorized information from the CSP to the TPA, and thereby significantly diminishes the computational cost and communication overhead. However, one of the most grave difficulties to its development is that users may not fully trust the CSPs in that it is difficult to decide whether the CSPs meet their legal expectations for data security. Therefore, it is critical and significant to develop efficient auditing methods to strengthen data owners' trust and assurance in cloud storage. For secrecy preservation, our system introduces a random masking provided by the TPA into the process of generating proof to blind the data information. Moreover, our system further activities the aggregate BLS signature practice from bilinear maps to achieve multiple checking tasks simultaneously, of which the principle is to cumulative all the signatures by unrelated users on numerous data blocks into a single short one and prove it for only one time to decrease the communication cost in the verification procedure. While exercising the same security strength (e.g. 80-bit security), a BLS-based signature (160 bit) is much shorter than an RSA-based signature (1024 bit).

3. Problem statements:

As the timed release data is considered to be time sensitive data, it is necessary to introduce an effective scheme, which will not release the data access privilege to intended users until reaching predefined time points. An efficient solution is

needed to let data owners manually release the time-sensitive data: The owner uploads the encrypted data under different policies at each releasing time such that the intended users cannot access the data until the corresponding time arrives. The user revocation is added to the proposed scheme to improve the security of access policies. The users who got block listed cannot get data from data owner.

4. Proposed system:

An well-organized pattern, which take part TRE and CP-ABE in unrestricted cloud putting away is carry out, to comprehend safe as houses reasonable grained right of entry rheostat for time-penetrating records. Data owner can in competition in waiting anticipated manipulators and their appropriate right to use source of pride leave go of stretch arguments. User revocation is added to give more effectiveness to access policy. Data owner can check the revocation list and it is avoided sharing data to blocked users. In this scheme is secure and effective.

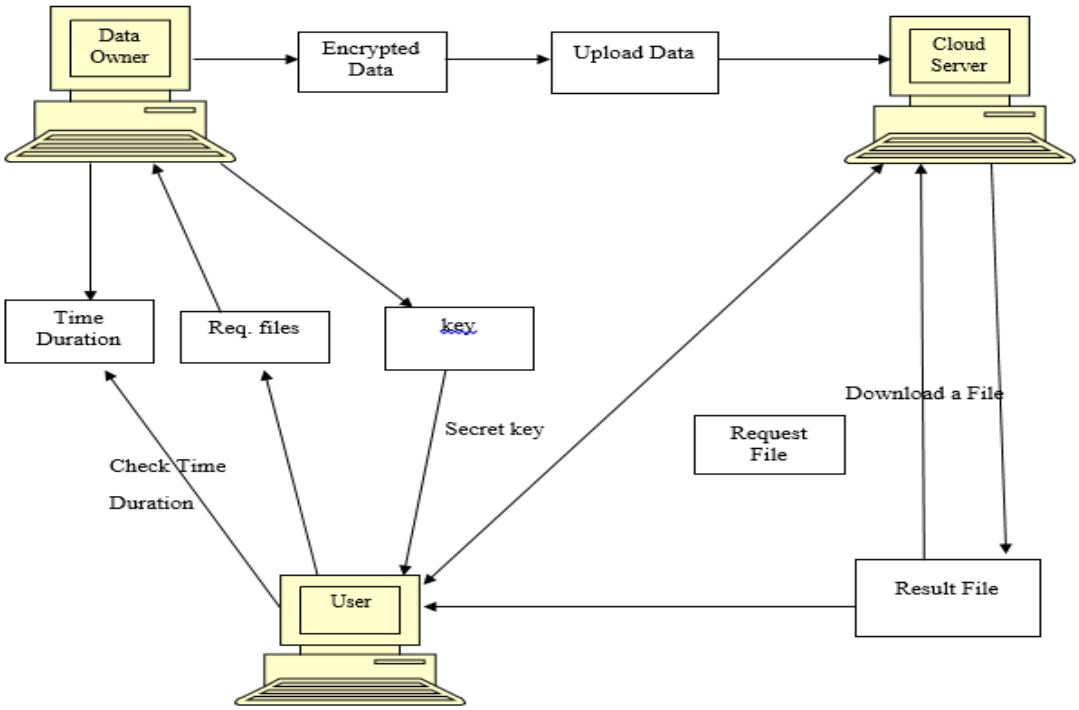

Figure 1: System Architecture

5. Modules Description

5.1. Cloud Server:

Cloud service provider (Cloud) includes the administrator of the cloud and cloud servers. The cloud undertakes the storage task for other entities, and executes access privilege releasing algorithm under the control of CA. Manipulators rely on the CS for haze records putting away and looking after. They may perhaps also with passion act together with the CS to right to use and keep informed their put in storage records for a number of presentation commitments.

5.2. Data owner:

The data owner decides the access policy based on a specific attribute set and one or more releasing time points for each file, and then encrypts the file under the decided policy before uploading it. Data owner upload and store the files in cloud server. Data owners are in charge of

encrypting the data before uploading them on the cloud. While uploading the data, it should be encrypted and stored in cloud to ensure the data security.

5.3. Security Model:

The data owner generates a session key K and encrypts the message M with K and stores the encrypted data in the cloud server. The key will be shared to the user who wants to download data from the server. The decryption key will be sent to user email id. After getting the decryption key from the data owner, user can able to decrypt the data. There are two file generated .enc and .key files stored in the cloud. The user must choose the encrypted file and key file to download the data from the server.

5.4. User Revocation:

The malicious user is block listed by the central authority. The time sensitive data cannot be accessed by the revocated users. The data owner can have more effective access policy scheme by not sharing data to blocked users.

6. Output:

This section contains the screenshots of efficient user revocation and time sensitive data access control. Initially admin has to enter username and password to login the system which is shown in fig 2. In fig 3 view the data user details. A new user register her details which is shown fig 4 and that user will be added to the system which is shown in fig 5.In fig 6 has user details and also user file opening and closing time. After closing time finished user doesn't open the file. In fig 2 data owner to enter user id and password and then entering into system. After that login data owner upload their data to their intended user. Data user register their details shown in fig 4.after registration of data user the data will confirm data user which is shown in fig 3 and also this called the user revocation. Data owner upload their data which is shown in fig 5.In fig 6 have the parameter user name, email-id, file name, file opening time, file closing time and file action and also user can request for file to data owner. The data owner verifies the user revocation list and then sends their file and also sends file opening time and file closing time.

6.1. User Login

In fig 2 data owner enter username and password if it's correct data owner entering into system. After that data owner update their details.

Figure 2: User Login

6.2. View Data User

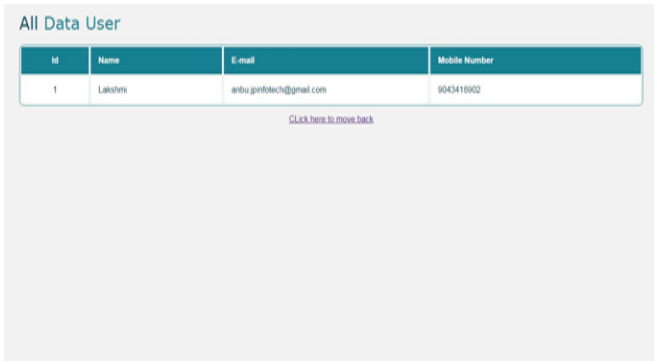

Figure 3: View data user

In fig 3 is view data user and also its contain user name, e-mail, mobile number. And also these data user called the revocated user. This called user revocation.

6.3. User Registration

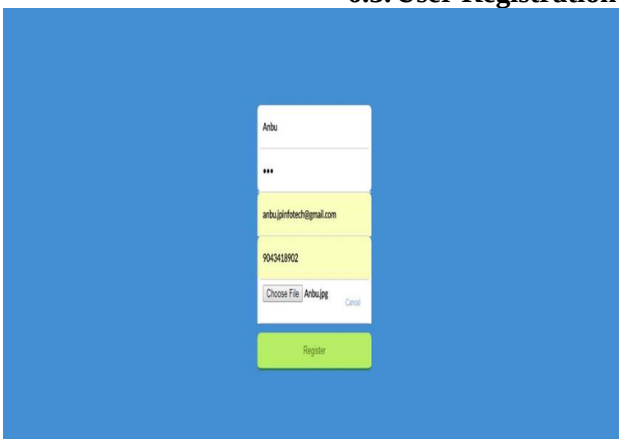

Figure 4: User Registration

In fig 4 is the user registration they have username, password, mail-id, mobile number and also update their file.

6.4. View File

Fig 5: View file

In fig 5 they have file information. That is file name, size, key, updated date.

6.5. Time Key

Data Owner Name	User Name	E-Mail	File Key	File Name	Open Date	Close Date	Action
Anbu	Lakshmi	anbu.jpinfotech@gmail.com	74054727	Java.txt	18.09.2017 at 16:35:40	17.09.2017 at 16:35:40	Send Time Key
Anbu	Lakshmi	anbu.jpinfotech@gmail.com	74054727	Java.txt	18.09.2017 at 16:35:40	19.09.2017 at 16:35:40	Send Time Key

Click Back

Fig 6: Time key

In fig 6 is time key they have username, e-mail, file key, and file name open date time, close date time. If user can use file during the opening date time and close date time. After that closing date time they can't use file.

7. Performance analysis

This section illustrates the comparison between cost of data owner and number of intended user. Here cost of data owner increase the number of intended user will also increase in LoTAC. In TAFC cost of data owner is constant but number of intended user will increase and also same as in TaSA when cost of data owner is constant but number of intended user will increase.TAFC and TasA significantly reduce the communication complexity of data owner when access privilege should be released to quite a number of users. Efficient user revocation and time sensitive data access well tolerates the increasing number of users and shared data. This can provide a lightweight, flexible, and fine-grained access control system for time-sensitive data in cloud storage.

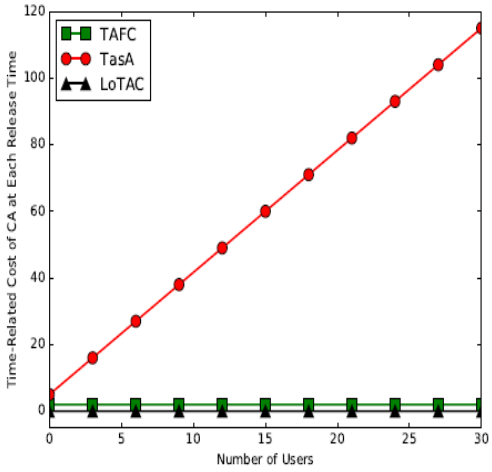

Fig 7: cost of CA versus number of users

8. Conclusion and Future Enhancement

Fine-grained access control scheme is proposed with user revocation for time sensitive data in cloud storage. One challenge is to simultaneously achieve both flexible timed release and fine granularity with lightweight overhead, which was not explored in existing works. Proposed scheme achieves this goal. The concept of timed-release encryption is incorporated to the architecture of ciphertext policy attribute-based encryption. With a suit of proposed mechanisms, this scheme provides data owners with the capability to flexibly release the access privilege to different users at different time, according to a well-defined access policy over attributes and release time. The data can be shared only to valid users, revocation list is maintained to avoid illegitimate data sharing.

REFERENCES

[1] . Jianan Hong, Kaiping Xue, Yingjie Xue, Weikeng Chen, David S.L. Wei, Nenghai Yu and Peilin Hong," TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud", *IEEE Transactions on Services Computing*,2017.

[2] . K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DACMACS: Effective data access control for multi-authority cloud storage systems," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1790–1801, 2013.

[3] . Q. Liu, G. Wang, and J. Wu, "Time-based proxy reencryption scheme for secure data sharing in a cloud environment," *Information Sciences*, vol. 258, no. 3, pp. 355–370, 2014.

[4] . E. Androulaki, C. Soriente, L. Malisa, and S. Capkun, "Enforcing location and time-based access control on cloud-stored data," in *Proceedings of the 2014 IEEE 34th International Distributed Computing Systems (ICDCS '14)*, pp. 637–648, IEEE, 2014.

[5] . C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.

[6] . Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Reliable re-encryption in unreliable clouds," in *Proceedings of the 2011 IEEE Global Communications Conference (GLOBECOM '11)*, pp. 1–5, IEEE, 2011.

[7] . Y. Zhu, H. Hu, G.-J. Ahn, D. Huang, and S. Wang, "Towards temporal access control in cloud computing," in *Proceedings of the 31st IEEE International Conference on Computer Communications (INFOCOM '12)*, pp. 2576–2580, IEEE, 2012.

[8] . S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in

cloud computing," in *Proceedings of the 29th IEEE International Conference on Computer Communications (INFOCOM '10)*, pp. 1–9, IEEE, 2010.

[9] . J. Li, W. Yao, Y. Zhang, and H. Qian, "Flexible and fine grained attribute-based data storage in cloud computing," *IEEE Transactions on Services Computing, Avaliable online*, 2016.

[10] . H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang,Y. Chen, and J. Liu, "Dynamic-hash-table based public auditing for secure cloud storage," *IEEE Transactions on Services Computing, Avaliable online*, 2016.