International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume – 3, ISSUE – 3 **ISSN (Online):2454- 1966**

Research Manuscript Title

SURVEY ON ATTRIBUTE-BASED ACCESS CONTROL WITH USER REVOCATION IN CLOUD DATA STORAGE

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

[1]PG Student, Vivekanandha College of Engineering for Women, Namakkal

[2]Assistant Professor, Vivekanandha College of Engineering for Women, Namakkal

E-Mail-ID: lavancse21@gmail.com

Sep - 2017

www.istpublications.com

SURVEY ON ATTRIBUTE-BASED ACCESS CONTROL WITH USER REVOCATION IN CLOUD DATA STORAGE

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

[1]PG Student, Vivekanandha College of Engineering for Women, Namakkal

[2]Assistant Professor, Vivekanandha College of Engineering for Women, Namakkal

E-Mail-ID:lavancse21@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. Though there were many studies deal with fine grained data access control, there is no study proposed for both fine-grained access control and time-sensitive data publishing. Ciphertext-Policy Attribute-based Encryption is used for data security in cloud. A time and attribute factors combined access control is necessary to handle time-sensitive data in public cloud storage. 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 secure access control problem has become a challenging issue in public cloud storage.

Ciphertext-policy attribute-based encryption (CP-ABE) is used for secure data access control in cloud storage. CP-ABE based schemes enable data owners to realize fine-grained and flexible access control on their own data. CP-ABE determines users' access privilege based only on their inherent attributes without any other critical factors, such as the time factor. 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.
Timed releasing data application is used in scenario, where a company usually prepares some important files for different intended users, and these users can gain their access privilege at different time points, students result announcement by government etc.

Timed release encryption is a kind of encryption scheme that a recipient can decrypt only after a specified amount of time. A revocable timed release encryption, provably loosing all access to the data. The definition TRE came in two flavors: one way revocable TREs and revocable hiding TREs. The construction of one-way revocable TREs is too weak a property for almost all purpose, the construction and its proof are useful as a warm up for the hiding construction, and also useful on their own for the random oracle based constructions. The following step is to build revocably hiding TREs.The building labelled already is not hiding, because if the adversary guesses a few bits of B correctly, we will learn some of bits of m while still passing revocation. A natural idea would be to use secrecy plaintext is XORed with f (m) and transmitted.

2. LITERATURE REVIEW

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 frees data owners 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. However, till now, no schemes can support both fine-grained access control and time-sensitive data publishing. An efficient approach to design access policies faced with various access requirements for time-sensitive data. Extensive security and performance analysis shows that scheme is extremely efficient and satisfies the security requirements for time sensitive data storage in public cloud. 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. It can be placed upon any node in the structure, arbitrarily describing access privilege releasing time for different users. The accessing time, together with user’s attribute set, decides whether the user satisfies the policy. In TAFC, an access policy is over some attributes and one or more releasing time points. Access policy design for all potential access requirements of time sensitive, through suitable placement of time trapdoors. The analysis shows that our scheme can preserve the confidentiality of time-sensitive data, with a lightweight overhead on both *CA* and data owners.

In [2] authorsKan Yang, Xiaohua Jia, Kui Ren, Bo Zhangin the paper **“DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems”** DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, build a new multi-authority CP-ABE scheme with efficient decryption and also design an efficient attribute revocation method that can succeed both forward security and backward security. Design an efficient immediate attribute revocation technique for multi-authority CP-ABE scheme that succeeds both forward security and backward security. 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. Thus, the main task is to design a new underlying multi-authority CP-ABE scheme with efficient decryption and revocation. The DAC-MACS consists of five phases: System Initialization, Secret Key Generation by *AA*s, Data Encryption by Owners, Data Decryption by Users and Attribute 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). The original HABE permits an allocation mechanism in the generation of keys, as that in hierarchical identity-based encryption (HIBE). Without the master key, the adversary is not able to derive the data encryption keys due to the one-wayness of the key chain, which can be guaranteed by choosing a secure one-way hash function such as SHA-1. KP-ABE when encrypting the master key. The enhanced KP-ABE is provably secure under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.

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. Tag-based non-flexibility as defined in the random oracle model, under the Strong Diffie-Hellman assumption (SDH). The user should be able to access the file only if her identity, location(s) and time of interaction with the location server(s) are compliant with the access policy of the file.

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 flexible scattered storage integrity auditing mechanism, consuming the homomorphic token and distributed erasure-coded data. The future plan allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Since the cloud data are active in nature, the future design further supports secure and efficient active operations on outsourced data, including block modification, deletion, and append. Analysis displays the proposed scheme is extremely efficient and resilient against Byzantine failure, malicious information modification attack, and even server colluding attacks. Token generation, the user has the choice of either keeping the precomputed tokens locally or storing them in encrypted form on the cloud servers. In our case here, the user stores them locally to obviate the need for encryption and lower the bandwidth above during dynamic data operation which will be discussed shortly. Error localization is a key prerequisite for removing errors in storage systems. It is also of critical status to identify potential threats from external attacks. However, many previous systems do not explicitly consider the difficult of data error localization, thus only providing binary results for the storage verification.Since our layout of file matrix is systematic, the user can recreate the original file by downloading the data vectors from the first m servers, assuming that they return the accurate response values. Notice that our verification scheme is based on casual spot-checking, so the storage correctness declaration is a probabilistic one. The declarations of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, we suggest an effective and flexible distributed system with explicit active data support, including block update, delete, and append. We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. Whenever data corruption has been detected during the storage correctness verification across the distributed servers, we can almost guarantee the simultaneous identification of the mischievous server(s). Considering the time, computation resources, and even the linked online burden of users, we also deliver the extension of the future main system to support third-party auditing, where users can safely delegate the integrity checking tasks to third party auditors and be worry-free to use the cloud storage facilities.

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 cloud, and issue decryption keys to authorized users. Then, when a user is revoked, the data owner will dispute re-encryption commands to the cloud to re-encrypt the data, to prevent the revoked user from decrypting the data, and to generate new decryption keys to valid users, so that they can remain to access the data. A time-based re-encryption system, which permits the cloud servers to automatically re-encrypt data based on their internal clocks. Our solution is built on top of a new encryption scheme, *attribute based encryption*, to permit fine-grain access control, and does not need perfect clock synchronization for correctness. ABE allows data to be encrypted using an *access structure* comprised of different *attributes*. Instead of specific decryption keys for specific files, users are delivered attribute keys. Users must have the necessary attributes that fulfill the access structure in order to decrypt a file. The key problem of storing encrypted data in the cloud lies in *revoking* access rights from users. 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 a time-based re-encryption system, which allows each cloud server to automatically re-encrypt data based on its internal clock. The basic idea of the R3 system is to associate the data with an *access control* and an *access time*. Each user is distributed keys associated with *attributes* and *attribute effective times*. The data can be decrypted by the users using the keys with attributes satisfying the access control, and attribute effective times sufficient the access time. Unlike the command-driven re-encryption scheme, the data owner and the CSP share a secret key, with which each cloud server can reencrypt data by informing the data access time according to its own internal clock. Our technique does not rely on the cloud to reliably propagate re-encryption commands to all servers to ensure access control correctness.

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 control encryption system for cloud services with the help of cryptographic integer comparisons and a proxy-based re-encryption mechanism on the current time. Access control is considered as one of critical security mechanisms for information protection in cloud applications. 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. Hence, attribute-based access control had been introduced into cloud computing to encrypt outsourced sensitive data in terms of access rule on attributes labelling the outsourced data, and only authorized users can decrypt and access the information. Since the access control rule of every object is embedded within it, the enforcement of rule becomes an inseparable characteristic of the data itself. This originated from the needs of practical cloud applications, in which each outsourced resource can be associated with an access rule on a set of temporal attributes, e.g., period-of-validity, opening hours, or hours of service. Each user can also be assigned a license with several privileges based on the comparative attributes.

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 emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep complex user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users.The problematic of simultaneously reaching fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. In this scheme also had salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that system is extremely efficient and provably secure under existing security models. This system to realize this goal by exploiting KPABE and uniquely combining it with techniques of proxy re-encryption and lazy re-encryption. Moreover, that system can enable the data owner to delegate most of computation overhead to powerful cloud servers. Confidentiality of user access privilege and user secret key accountability can be reached.

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-anonymous privilege control system AnonyControl to address not only the data secrecy, but also the user identity secrecy in present access control schemes. AnonyControl decentralizes the central authority to bound the identity origin and thus realizes semi anonymity. Both AnonyControl and AnonyControl-F are secure under the Diffie Hellman assumption, and our show estimation exhibits the feasibility of our systems. Besides, it also generalizes the file access control to the privilege control, which privileges of all operations on the cloud data can be managed in a compact planned manner. By using the multiple authorities in the cloud computing system, this systems achieve not only fine-grained privilege control but also identity anonymity while controlling privilege control based on users‟ identity information. 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. The AnonyControl-F directly inherits the security of the AnonyControl and thus is equivalently secure as it. Supporting user repudiation is an important dispute in the real application, and this is a great challenge in the application of ABE schemes.

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 novel public checking scheme for secure cloud storage based on dynamic hash table (DHT), which is a new two-dimensional data structure situated at a third parity auditor (TPA) to record the data property information for dynamic 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). Therefore, BLS-based homomorphic verifiable authenticators (BLSHVA) are more generally accepted in the recent public structures. Here, to point out that no single method can succeed perfect audits for all types of cloud data, just as no standard has a universal validity. Thus, it may be a new trend to design a more effective system, including different audit strategies for various types of cloud data, which is also the direction disadvantage.

3. ANALYSIS

S.NO	TITLE	PARAMETER	ALGORITHM	MERITS	DEMERITS
1	TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud	Setup, Key Generation, encryption, Token generation, Trapdoor exposure Decryption	Ciphertext-Policy Attribute-based Encryption Timed-Release Encryption	Can Support both fine-grained access control and time-sensitive data	Each file can be labeled with only one time point, which cannot release the access privilege of one file to different intended users at different time.
2	DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems	Setup Encryption Key generation Token generation Decryption	Ciphertext-Policy Attribute-based Encryption attribute revocation	Achieve both forward Security and Backward Security	Security weakness
3	Time-Based Proxy Re-encryption Scheme for Secure Data Sharing in a Cloud Environment	Disjunctive normal form, Conjunctive normal form, One-way hash Function	Hierarchical Attribute-Based Encryption Proxy Re-Encryption Decisional Bilinear Diffie-Hellman	Using the revocable KP-ABE is its enhanced security against user collusion	Security level is reduced
4	Enforcing Location and Time-based Access Control on Cloud-stored Data	Setup Encryption Key Generation Decryption	ElGamal, Ciphertext-Policy Attribute Based Encryption Strong Diffie-Hellman	Low Communication, Low Computation Costs	It does not improving localization mechanisms.
5	Toward Secure and Dependable Storage Services in Cloud Computing	Matrix, Permutation	Token Precomputation. Correctness Verification and Error Localization Error Recovery	very lightweight communication and computation cost, highly efficient	malicious data modification attack, server colluding attacks

6	Reliable Re-encryption in Unreliable Clouds	Setup GenKey Encrypt ReEncrypt Decrypt	Synchronized clock with no delays Asynchronized clock with delays	Does not require perfect clock synchronization for correctness	Security Level is low
7	Towards Temporal Access Control in Cloud Computing	Setup GenKey Encrypt ReEncrypt Decrypt	Temporal Access control encryption (TACE) Rivest Shamir Adleman (RSA) Gap Diffie-Hellman	Privacy Protection Supervisory Flexibility	In the forward and backward derivation processes is kind of "one-way" property can be guaranteed because the inverse cannot be computed.
8	Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing	Setup Encryption Key Generation Decryption	Key Policy Attribute-Based Encryption	Highly efficient and provably secure	No longer dependent to the number of users.
9	Flexible and Fine-Grained Attribute Based Data Storage in Cloud Computing	Setup Encryption Key Generation Decryption	Diffie Hellman cipher text-policy attribute-based encryption Attribute Encryption Standard (AES)	A semi-anonymous privilege control scheme anonycontrol to address not only the data privacy, but also the user identity privacy in current access control schemes.	Does not support user revocation
10	Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage	Dynamic Hash Table Merkle Hash Tree index-hash table	BLS (Boneh-Lynn-Shacham) signature RSA (Rivest Shamir Adleman)Signature Computational Diffe-Hellman	Communication cost is low and communication overhead is low	No single Method can achieve perfect audits for all types of cloud Data, just as no standard has a universal validity.

4. POSSIBLE SOLUTION

Cloud computing introduces risks to any sensitive data it touches. These risks largely arise from the need to entrust data protection to a third party cloud provider. Different nodes in the environment may be controlled or administered by different untrusted parties, and could be vulnerable to attacks fromother cloud tenants, malicious insiders or external adversaries. When data owners release control of their data to a cloud environment, they require guarantees that their data remains appropriately protected.

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.

An efficient scheme, which integrates TRE and CP-ABE in public cloud storage is implemented, to realize secure fine grained access control for time-sensitive data. Data owner can autonomously designate intended users and their relevant access privilege releasing time points. 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.

5. CONCLUSION

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 finegrained 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.