ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

Intelligent Fine-Grained Data Access with Attribute Based Re-Encryption Norms over Cloud Platform

V.Saravanan, P.Alagusundaram,

M.E. Computer Science and Engineering, Department of Computer Science and Engineering, Mahath Amma Institute of Engineering and Technology, N.M.Nagar, Ariyur, Sithannavasal Road, Pudukkottai, Tamilnadu, India.

Assistant Professor, Department of Computer Science and Engineering, Mahath Amma Institute of Engineering and Technology, N.M.Nagar, Ariyur, Sithannavasal Road, Pudukkottai, Tamilnadu, India.

ABSTRACT: The main objective of this work is to improve the fine grained security scheme towards cloud storage and improve the privacy by means of two norms such as Attribute-based encryption (ABE) and Advanced Encryption Standard (AES). A new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services has been proposed. In recent years, many users have uploaded data to the cloud for easy storage and sharing with other users at the same time, security and privacy concerns for the data are growing. Attribute-based encryption (ABE) enables both data security and access control by defining users with attributes so that only those users who have matching attributes can decrypt them. In actual implementations, ABE is used in hybrid with a symmetric encryption scheme such as the advanced encryption standard (AES) where data is encrypted with AES and the AES key is encrypted with ABE. The hybrid encryption scheme requires re-encryption of the data upon revocation to ensure that the revoked users can no longer decrypt that data. To re-encrypt the data, the data owner (DO) must download the data from the cloud, then decrypt, encrypt, and upload the data back to the cloud, resulting in both huge communication costs and computational burden on the DO depending on the size of the data to be re-encrypted.

KEYWORDS: Cloud storage, data sharing, access control, revocation, dynamic group.

I. INTRODUCTION

Cloud computing is widely accepted as a new computing paradigm due to its intrinsic resource-sharing and low maintenance characteristics. In cloud computing, the CSPs, such as Amazons EC2 and S3, Google App Engine, and Microsoft Azure, are able to deliver various services, including software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS), to cloud users. By migrating the local data management system into cloud storage, users can enjoy cost savings and productivity enhancements by using cloud-based services to manage projects and establish collaborations. With the increasing development of cloud computing technologies, it is not hard to imagine that in the near future more and more businesses will be moved into the cloud. One of the most fundamental services offered by CSPs is data storage. Despite of the benefits provided by cloud storage, it is facing many challenges that, if not well resolved, may impede its fast growth. Consider a practical application that a company allows its staff or departments to store and share data via the cloud. By utilizing the cloud, the company can be completely released from

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

the local data storage and maintenance burden. However, it also incurs a major security threat towards the data confidentiality.

Specifically, the CSPs are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential. To address this issue, a basic solution is to encrypt data, and then uploads the encrypted data into the cloud. However, the traditional encryption mechanisms are not efficient or flexible for data sharing in the cloud. In order to achieve optimal usage of storage resources, it is desirable to use advanced encryption mechanisms allowing the data to be shared at a finegrained level. One of the promising tools for achieving finegrained access control and sharing of encrypted data is to use attribute-based encryption (ABE). Nevertheless, it is not straightforward to directly apply ABE in real applications due to various practicality concerns. Dynamic User Groups. Dynamic user groups are very common in cloud applications, e.g., due to expiration or change of user membership and user credentials being stolen/compromised/misused. In dynamic user groups, user revocation is a critical security issue that must be properly addressed. However, one challenging problem in handling user revocation in cloud storage is that a revoked user may still be able to decrypt an old ciphertext they were authorized to access before being revoked.

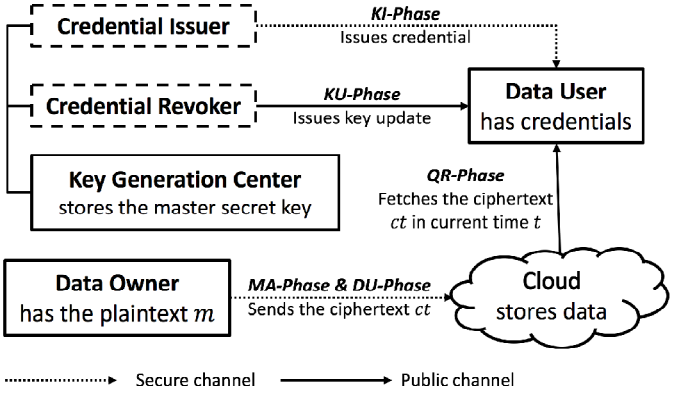

Fig. 1. System Model

In order to address this problem, the ciphertext stored in the cloud storage should be updated, ideally by the (untrusted) cloud server. In the literature, proxy re-encryption has been proposed to enable the change of the authorized decryptor of a ciphertext, and this approach has been incorporated into ABE to allow a ciphertext to be updated by a third party (e.g., the CSP) for revocation purpose. However, the proxy re-encryption approach requires re-encryption/update keys to be issued to the CSP in order to allow the ciphertexts to be updated. From the practicality perspective, it is more desirable that the ciphertext update, which can happen frequently, can be done by the CSP without requiring any delegated key.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

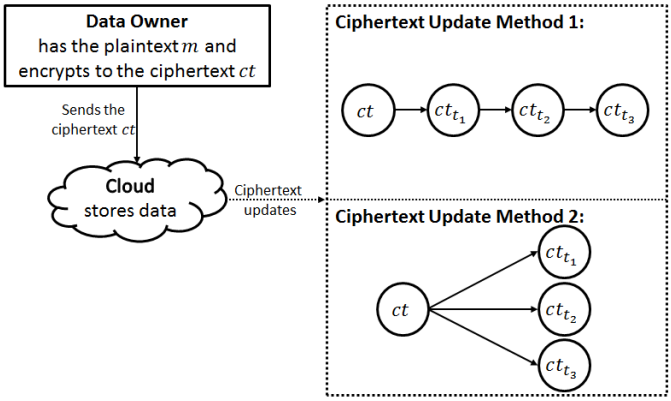

Fig.2. Ciphertext Update

In this work, we aim to develop a secure and practical approach to address the problem. As shown in Fig. 1 and 2, a data owner sends the original ciphertext ct to the cloud storage in revocation epoch t, and a data user can query the cloud storage to access the ciphertext afterwards. Suppose the data user issues a query at t1 t, the CSP then sends the updated ciphertext ctt1 (i.e., ctt1 is transformed from ct by the CSP) to the data user, and this ciphertext can be decrypted by the user if and only if he/she satisfies the access policy specified by the data owner and is not revoked at t1. Different from the proxy re-encryption based approach, here we'd like the transformation to be performed by the CSP without using any re-encryption/update key.

II. SYSTEM IMPLEMENTATION

A. IDENTITY BASED REENCRYPTION MASTER

This module introduces a new scheme called identity based proxy re-encryption system. In the new identity based proxy encryption system, the re-encryption key is generated by the sender S, and the process of agency is controlled by S thoroughly. This method can avoid the flaw of the traditional proxy re-encryption, the sender S can control the people who can get the message and the sharing content of the messages.

B. INTELLIGENT PROXY REENCRYPTION SCHEME

This module can be seen as the dual of the traditional identity based proxy reencryption. In the scheme, the data owner can control sharing capability in a flexible way by using random numbers used in the encryption process. Compared to traditional identity based proxy re-encryption schemes, this scheme has some advantages, and can be more appropriately adapted to some applications for content sharing, such as secure cloud data sharing. Further, it would like to explore other aspects, such as giving formal security proof for our proposal, proposing more efficient schemes and implement the schemes in real Cloud environments, etc.

C. CLOUD MANIPULATION AND SECURITY ESTABLISHMENTS

Cloud storage has emerged as a promising solution for providing ubiquitous, convenient, and on-demand accesses to large amounts of data shared over the Internet. Today, millions of users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a daily basis. Business users are also being attracted by cloud storage due to its numerous benefits, including lower cost, greater agility, and better

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

resource utilization. However, while enjoying the convenience of sharing data via cloud storage, users are also increasingly concerned about inadvertent data leaks in the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business secrets (e.g., the recent high profile incident of celebrity photos being leaked in iCloud).

III. LITERATURE SURVEY

Achieving Secure, Scalable, And Fine-Grained Data Access Control In Cloud Computing - S. Yu, C. Wang, K. Ren. [1] 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 sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

Secure Provenance: The Essential Of Bread And Butter Of Data Forensics In Cloud Computing - R. Lu, X. Lin. [2] Secure provenance that records ownership and process history of data objects is vital to the success of data forensics in cloud computing, yet it is still a challenging issue today. In this paper, to tackle this unexplored area in cloud computing, we proposed a new secure provenance scheme based on the bilinear pairing techniques. As the essential bread and butter of data forensics and post investigation in cloud computing, the proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model.

Mona: Secure Multiowner Data Sharing For Dynamic Groups In The Cloud - X. Liu, Y. Zhang. [3] With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a secure multi-owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

Practical Techniques For Searches On Encrypted Data - X. Song, D.Wagner. [4] It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms presented are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

Searchable Symmetric Encryption: Improved Definitions And Efficient Constructions - R. Curtmola, J. Garay. [5] Searchable symmetric encryption (SSE) allows a party to outsource the storage of its data to another party (a server) in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research in recent years. In this paper we show two solutions to SSE that simultaneously enjoy the following properties: Both solutions are more efficient than all previous constant-round schemes. In particular, the work performed by the server per returned document is constant as opposed to linear in the size of the data. Both solutions enjoy stronger security guarantees than previous constant-round schemes. In fact, we point out subtle but serious problems with previous notions of security for SSE, and show how to design constructions which avoid these pitfalls. Further, our second solution also achieves what we call adaptive SSE security, where queries to the server can be chosen adaptively (by the adversary) during the execution of the search; this notion is both important in practice and has not been previously considered. Surprisingly, despite being more secure and more efficient, our SSE schemes are remarkably simple. We consider the simplicity of both solutions as an important step towards the deployment of SSE technologies. As an additional contribution, we also consider multi-user SSE. All prior work on SSE studied the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in the multi-user setting, and present an efficient construction that achieves better performance than simply using access control mechanisms.

Computationally Efficient Searchable Symmetric Encryption - P. Van,S. Sedghi. [6] Searchable encryption is a technique that allows a client to store documents on a server in encrypted form. Stored documents can be retrieved selectively while revealing as little information as possible to the server. In the symmetric searchable encryption domain, the storage and the retrieval are performed by the same client. Most conventional searchable encryption schemes suffer from two disadvantages. First, searching the stored documents takes time linear in the size of the database, and/or uses heavy arithmetic operations. Secondly, the existing schemes do not consider adaptive attackers; a search-query will reveal information even about documents stored in the future. If they do consider this, it is at a significant cost to the performance of updates. In this paper we propose a novel symmetric searchable encryption scheme that offers searching at constant time in the number of unique keywords stored on the server. We present two variants of the basic scheme which differ in the efficiency of search and storage. We show how each scheme could be used in a personal health record system.

IV. SYSTEM ANALYSIS

A. Existing System

Revocation of users or their attributes is an indispensable feature of ABE for real-world applications. In real-world situations, users and their attributes change over time within the system. For example, users may be found to be malicious, may simply leave the system, or their attributes may change. Therefore, revoking users or their attributes accordingly so that they can no longer decrypt data is important. Existing revocation methods of ABE are proposed based on the notion of using ABE to encrypt the data entirely, whereas in actual implementations, hybrid encryption of ABE and symmetric encryption, specifically the advanced encryption standard (AES), are used for efficiency. In hybrid encryption, data is encrypted with AES and the AES key is encrypted with ABE. Because existing revocation methods affect only ABE ciphertext, this fact introduces a problem in which users can keep the AES key prior to revocation and use it to decrypt data even after the users are revoked. Therefore, although existing revocation methods can be applied

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

to revoke users from ABE, re-encrypting data with a new AES key is necessary so that the old AES key can no longer be used.

DISADVANTAGES OF EXISTING SYSTEM

(a) Poor Security by means of Standard Password Generation technique for Encryption and Decryption.
(b) Insecure Authentication Principles.
(c) Easy to guess passwords.

B. Proposed System

In this proposed approach, we propose an attribute-based proxy Reencryption method for revocation in which the DO is no longer required to download any data for re-encryption. By using a symmetric encryption scheme that supports proxy Reencryption in hybrid with RABE, we can perform revocation in the cloud so that a revoked user will no longer be able to decrypt data after revocation. Specifically, we implement a symmetric encryption scheme proposed by Syalim et al. in hybrid with RABE, encrypt data with Syalim's scheme, and encrypt Syalim scheme's keys with RABE. By using a symmetric proxy re-encryption scheme, the data can be reencrypted in the cloud without revealing any data to the cloud. In addition, the Data Owner only has to generate a set of Reencryption keys and a new ABE ciphertext that encrypts the new Syalim scheme's keys, and then send both to the cloud for re-encryption. Therefore, in the revocation step, sending only the re-encryption keys and RABE ciphertext to the cloud is required, thus reducing the communication cost between the DO and cloud. Because the re-encrypted ciphertext is encrypted under a completely new set of keys, users cannot decrypt data even if they keep the old symmetric keys or parts of the old ciphertext.

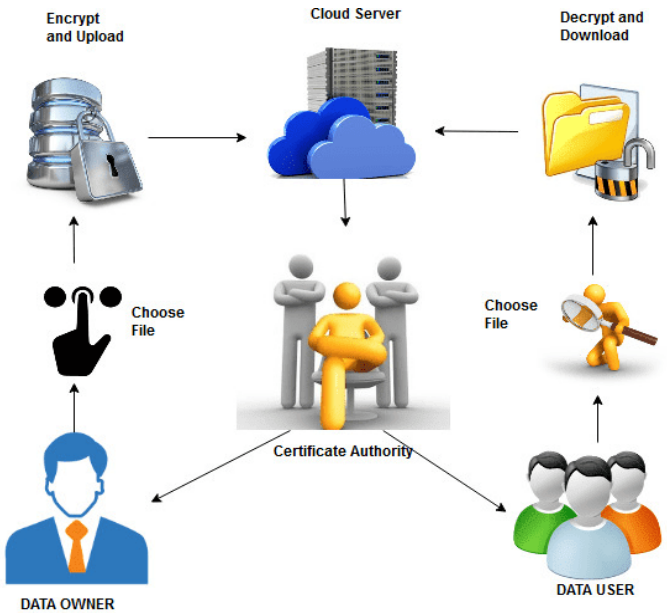

Fig.3 Proposed System Architecture Design

ADVANTAGES OF PROPOSED SYSTEM

(a) High Security establishments by means of Identity based Proxy Encryption Methodology as well as Password Generation technique is based on IBE principles for Encryption and Decryption, so it is highly secured compare to other classical schemes.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

(b) Secure Authentication Principles, which generates the password systematically and send to users for precedence, so it is non-guessable.

V. RESULTS AND DISCUSSION

In this section, we provided the simulated results of entire project with its practical proofs. The following figure shows the Home Page of the Proposed System.

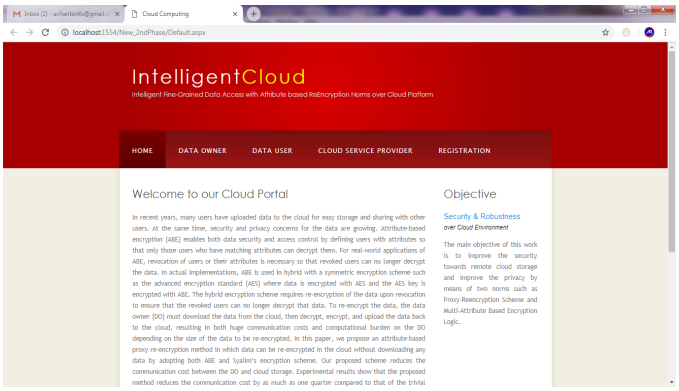

Fig.4 Home Page

The following figure illustrates the Registration view of the proposed system.

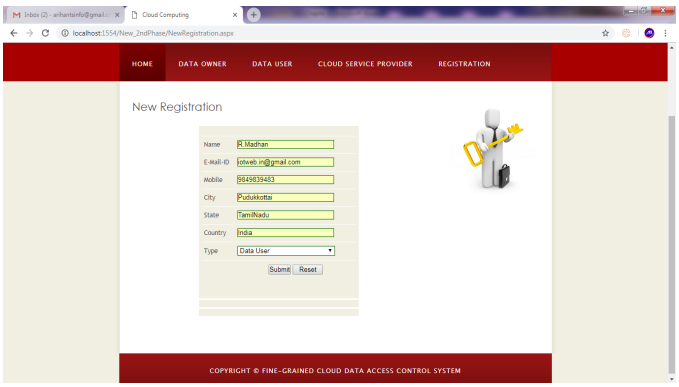

Fig.5 Registration

The following figure illustrates the CSP Authentication view of the proposed system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

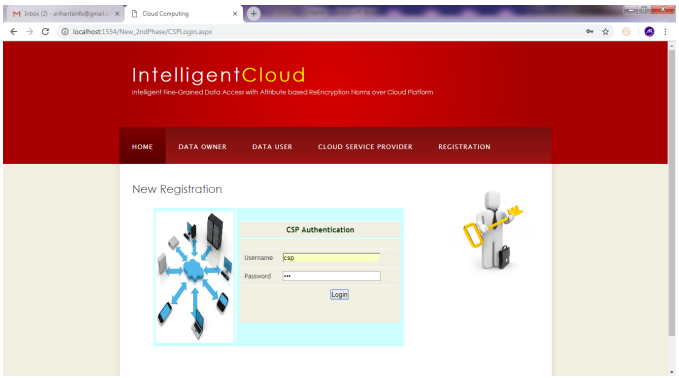

Fig.6 CSP Authentication

VI. CONCLUSION

Revocable attribute-based encryption (RABE) supporting ciphertext delegation is a useful primitive for enabling secure data sharing via a third-party storage service provider such as cloud storage. In this system, we revisited the state-of-the-art RABE scheme supporting ciphertext delegation and proposed a new construction paradigm that gives more efficient schemes compared with the previous solution. We provided formal security proofs for our proposed schemes and performed experiments to demonstrate that our new schemes are indeed more efficient than the previous solution. We also presented a fine-grained access control and data sharing system for ondemand services based on the proposed RABE scheme.

REFERENCES

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in EUROCRYPT, 2005, pp. 457–473.
[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in ACM CCS, 2006, pp. 89–98.
[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” in NDSS, 2005.
[4] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in INFOCOM, 2010, pp. 534–542.
[5] “Attribute based data sharing with attribute revocation,” in ASIACCS, 2010, pp. 261–270.
[6] K. Yang, X. Jia, and K. Ren, “Attribute-based fine-grained access control with efficient revocation in cloud storage systems,” in ASIACCS, 2013, pp. 523–528.
[7] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute based encryption,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, 2013.
[8] A. Sahai, H. Seyalioglu, and B. Waters, “Dynamic credentials and ciphertext delegation for attribute-based encryption,” in CRYPTO, 2012, pp. 199–217.
[9] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,” in EUROCRYPT, 2010, pp. 62–91.
[10] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” in IEEE S&P, 2007, pp. 321–334.
[11] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. R`afols, “Attribute-based encryption schemes with constant-size ciphertexts,” Theor. Comput. Sci., vol. 422, pp. 15–38, 2012.
[12] B. Waters, “Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions,” in CRYPTO, 2009, pp. 619–636.
[13] M. Pirretti, P. Traynor, P. D. McDaniel, and B. Waters, “Secure attribute based systems,” in ACM CCS, 2006, pp. 99–112.
[14] D. Boneh and M. K. Franklin, “Identity-based encryption from the weil pairing,” in CRYPTO, 2001, pp. 213–229.
[15] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in ACM CCS, 2008, pp. 417–426.
[16] N. Attrapadung and H. Imai, “Attribute-based encryption supporting direct/indirect revocation modes,” in IMA, 2009, pp. 278–300.
[17] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in PKC, 2011, pp. 53–70.
[18] D. Naor, M. Naor, and J. Lotspiech, “Revocation and tracing schemes for stateless receivers,” in CRYPTO, 2001, pp. 41–62.
[19] B. Waters, “Efficient identity-based encryption without random oracles,” in EUROCRYPT, 2005, pp. 114–127.