International Journal of Future Generation Communication and Networking
Vol. 13, No. 2s, (2020), pp. 1131–1138

"Cloud Data Security Authentication And Data Sharing Using Revocable-Storage Identity-Based Encryption"

Monika Ingole , Prof. Nisha Balani and Prof. Amrita Kungwani

Department of CSE , Jhulelal Institute of Technology
*Email Id:-monikaingole04@gmail.com,nisha.balani@jit.org.in,a.kungwani@jit.org.*in

Abstract

Information get upgraded to control by cryptographically. Cryptology is the training and investigation of methods for secure correspondence within the sight of outsiders called enemies. Distributed computing is the conveyance of registering administrations—servers, stockpiling, databases, organizing, programming, investigation, knowledge and then some—over the Internet ("the cloud") to offer quicker development, adaptable assets and economies of scale. Be that as it may, there exists a characteristic opposition for clients to straightforwardly redistribute the common information to the cloud server since the information frequently contain important data. Along these lines, it is important to put cryptographically improved access control on the common information. Personality based encryption is a promising cryptographical crude to manufacture a reasonable information sharing framework[3]. Be that as control To this end, propsse an idea called revocable-capacity personality based encryption (RS-IBE)[11], which isn't static. That is, the point at which some client's approval is lapsed, there component that can expel him/her from the framework. In this manner, the denied customer can't get to both the previously and right now data can give the forward/backward security of ciphertext by introducing the functionalities of customer disavowal and ciphertext update simultaneously.[11]

Index Terms*—Cloud computing, data sharing, revocation, Identity-based encryption, ciphertext update, decryption key exposure*

1. Introduction

Distributed computing gives calculation limit and tremendous memory space at a low cost.Among various administrations gave by distributed computing, distributed storage administration, for example, Apple's iCloud, Microsoft's Azure and Amazon's S3, can offer a progressively flexible and simple approach to share information over the Internet. We can store and share data over cloud. Outsource data usually causes user hesitation it contain valuable and sensitive information. Distributed computing is the conveyance of processing administrations—servers, stockpiling, databases, organizing, programming, investigation, insight and that's just the beginning—over the Internet ("the cloud") to offer quicker development, adaptable assets and economies of scale[5]. You ordinarily pay just for cloud administrations you use, helping bring down your working costs, run your framework all the more productively and scale as your business needs change. Circulated processing gives a versatile and beneficial way for data sharing, which brings various focal points for both the overall population and individuals. Cryptography is the training and investigation of strategies for secure correspondence within the sight of outsiders called foes, But there exists a characteristic obstruction for clients to straightforwardly redistribute the common data to the cloud server since the data much of the time contain significant information. Subsequently, it is important to put cryptographically improved access control on

ISSN: 2233-7857 IJFGCN

the common information. Character based encryption is a promising cryptographical amass down data sharing framework.However, get to control isn't static That is, where some customer's endorsement is ended, there should be an instrument that can oust him/her from the structure. Therefore, the renounced client can't get to both the beforehand and hence shared information. To this end, we propose a notion called revocable-capacity character based encryption (RS-IBE), which can give the forward/in reverse security of cipher text by presenting the functionalities of client denial and cipher text update at the same time. Moreover, we present a solid development of RS-IBE, and demonstrate its security in the characterized security model. The presentation examinations demonstrate that the proposed RS-IBE conspire has preferences regarding usefulness and productivity, and along these lines is possible for a down to earth and savvy information sharing framework. At last, effects of the proposed plan to exhibit its practicability. Further cryptography in validation process to verified individual just could share information. We will use this research for Job Seeker and Job Provider. Job Seeker will upload resume. Similarly, Job provider can view resumes until ID is activated.[8]

Identity-based access control placed on the shared data should meet the following security goals:[11]

1.1Data confidentiality: Unauthorized users should be prevented from accessing he plaintext of the shared data stored in the cloud server.

1.2 Backward secrecy: Backward secrecy means that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data are encrypted under his/her identity.

1.3 Forward secrecy: Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her.

2. Related Work

We have studied following research papers in study of our case study.

1. It is introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party. The scheme assumes the existence of trusted key generation centers, whose sole purpose is to give each user a personalized smart card when he first joins the network. The information embedded in this card enables the user to sign and encrypt the messages he sends and to decrypt and verify the messages he receives in a totally independent way, regardless of the identity of the other party. Previously issued cards do not have to be updated when new users join the network, and the various centers do not have to coordinate their activities or even to keep a user list. The centers can be closed after all the cards are issued, and the network can continue to function in a completely decentralized way for an indefinite period.

2. In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing

ISSN: 2233-7857 IJFGCN

service to check the data integrity in the cloud. Some existing remote integrity checking methods can only serve for static archive data and, thus, cannot be applied to the auditing service since the data in the cloud can be dynamically updated. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. In this paper, we first design an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. It further extend our auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. The analysis and simulation results show that our proposed auditing protocols are secure and efficient, especially it reduce the computation cost of the auditor.

3. iCloud also provides the means to wirelessly back up iOS devices directly to iCloud, instead of being reliant on manual backups to a host Mac or Windows computer using iTunes. Service users are also able to share photos, music, and games instantly by linking accounts via Airdrop wireless.

4. With data services in the cloud, users can easily modify and share data as a group. To ensure data integrity can be audited publicly, users need to compute signatures on all the blocks in shared data. Different blocks are signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks, which were previously signed by this revoked user must be re-signed by an existing user. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this paper, it propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing proxy re-signatures, we allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Experimental results show that our mechanism can significantly improve the efficiency of user revocation.

5. This deal with the problem of a center sending a message to a group of users such that some subset of the users is considered revoked and should not be able to obtain the content of the message. It concentrate on the *stateless receiver* case, where the users do not (necessarily) update their state from session to session. We present a framework called the *Subset-Cover* framework, which abstracts a variety of revocation schemes including some previously known ones. It provide sufficient conditions that guarantees the security of a revocation algorithm in this class.

6.This introduce the notion of certificate-based encryption. In this model, a certificate or, more generally, a signature — acts not only as a certificate but also as a decryption key. To decrypt a message, a keyholder needs both its secret key and an up-to-date certificate from its CA (or a signature from an authorizer). Certificate-based encryption combines the best aspects of identity-based encryption (implicit certification) and public key encryption (no escrow). It demonstrate how certificate-based encryption can be used to construct an efficient PKI requiring less infrastructure than previous proposals.

ISSN: 2233-7857 IJFGCN

3. **Target**

Data confidentiality: Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data.

Backward secrecy: Backward secrecy means that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity.

Forward secrecy: Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her. [11]

4. Sentiment analysis' techniques

4.1 Identity-based encryption **:- .**1 Identity-based encryption :- Identity-based encryption (IBE) is a public key encryption that any values, e.g., mail address, name, and so on, can be public keys. Though public key certificates are required in conventional public key encryption schemes since public keys are random values, no such a certificate is required in IBE. An authority called key generation center (KGC) issues a secret key for each identity ID, and the secret key can decrypt ciphertexts generated by ID as the public key. The first IBE scheme was proposed by Boneh and Franklin[1]. They considered how to revoke secret keys, where, for a time period T, KGC issues secret keys of identitiy ID||T if a user who has ID is not revoked on time T. This system, T indicate as a part of public key and user who donot have secret key at time T the cost of KGC is the drawback since secret key for each T where N is the number of users and R isthe number of revoked users. Thus, this scheme is not scalable.[11]

4.2 Decryption key exposer resistance:-security model of Boldyreva et al. In this section, we introduce decryption key exposure resistance. As a remark, the Boneh-Franklin paper does not mention decryption exposer resistance. blic keys are random values, no such a certificate is required in IBE. An authority called key generation center (KGC) issues a secret key for each identity ID, and the secret key can decrypt ciphertexts generated by ID as the public key. The first IBE scheme was proposed by Boneh and Franklin[1]. They considered how to revoke secret keys, where, for a time period T, KGC issues secret keys of identitiy ID||T if a user who has ID is not revoked on time T. In this system, a time T is also indicated as a part of a public key, and users who do not have legitimate secret keys on time T can be revoked. On drawback is the cost of KGC since KGC needs to re-issue O(N-R) size secret keys for each T where N is the number of users and R is the number of revoked users. Thus, this scheme is not scalable. Each user is issued a (long-term) secret key sk★↓ID KGC as in IBE. A cipher text is generated by using not only the corresponding ID but also a time period T. KGC generates key update information time T, and broadcast it (i.e., no secure channel is required). If a user is not revoked, then the user can compute a decry the adversary obtains skID* but ID* is revoked on time T*. In the security model of Boldyreva et al., the foe isn't permitted to acquire an unscrambling key dkID,T (ID,T)≠(ID*,T*). Boneh-Franklin plot is as yet secure regardless of whether the enemy is permitted to acquire dkID,T (ID,T)≠(ID*,T*) yet the Boldyreva et al. plot gets unreliable. Since the Boneh-Franklin conspire isn't adaptable, we likewise proposed the main versatile RIBE plot with decoding key introduction obstruction. [11]

ISSN: 2233-7857 IJFGCN

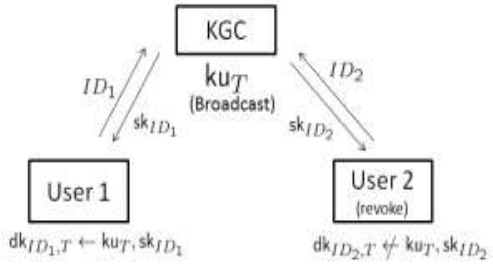


Fig. 1 A framework of RIBE

adversary is required either the adversary does not obtain skID* or the adversary obtains skID* but ID* is revoked on time T*. In the security model of Boldyreva et al., the adversary is not allowed to obtain a decryption key dkID,T (ID,T)≠(ID*,T*). We pointed out that the Boneh-Franklin scheme is still secure even if the adversary is allowed to obtain dkID,T (ID,T)≠(ID*,T*) but the Boldyreva et al. scheme becomes insecure. Since the Boneh-Franklin scheme is not scalable, we also proposed the first scalable RIBE scheme with decryption key exposure resistance.

5. Methodology

5.1 GUI

a.)In this module we will design GUI for cloud data sharing and authentication.
b.)Users will develop data sharing GUI's on cloud

5.2 Microsoft Windows Azure

a) Microsoft Azure is created for building, testing, deploying, and managing applications and services through Microsoft-manager data center.it is Microsoft cloud computing service.[3]
b) It support many different programming languages,tools,frame work and provide service as software(Saas) platform as a service(Paas) Infrastructure as a service (Iaas) Microsoft-specific and third-party software and systems
c) It is Microsoft cloud operating system where we will share data
d) SQL Azure for database management system
e) Azure security for user management

5.3 Authentication Cryptography

A) Encrytion protects data by scrambling it with a randomly generated password, called an encryption key.

B) Third party are not able to access the data without secret key Hackers can attempt to steal access by impersonating an authorized user. Encryption protects the key from bad actors

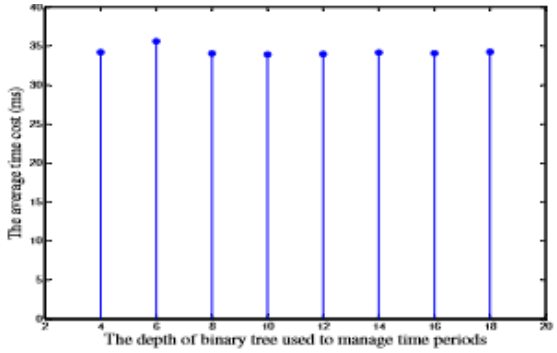
C) User's Profile Data will be stored in encrypted format to improve data security. User can share and receive the data with proper encryption and decryption. Maintain key to share and receive data.

6. Performance discussions

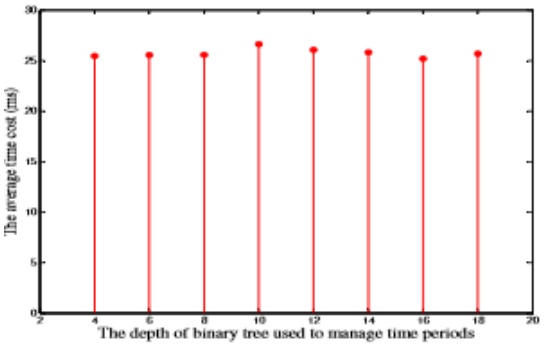
In this section, we discuss the performance of the proposed RS-IBE scheme by comparing it with previous works in terms of communication and storage cost, time complexity and functionalities,

ISSN: 2233-7857 IJFGCN

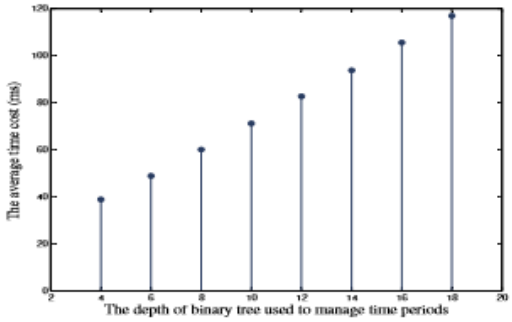
that the sizes of private key and update key in schemes and our scheme are all upper bounded by O(rlogN/r), since these schemes all utilize binary data structure to achieve revocation. On the other hand, Liang et al.'s scheme involves a broadcast encryption scheme to distribute update key such that their scheme has constant sizes of private key and update key. Furthermore, by delegating the generation of re-encryption key to the key authority, the ciphertext size of their scheme also achieves constant. However, to this end, the key authority has to maintain a data table for each user to store the user's secret key for all time periods, which brings O(T)τG1



(a) PKGen

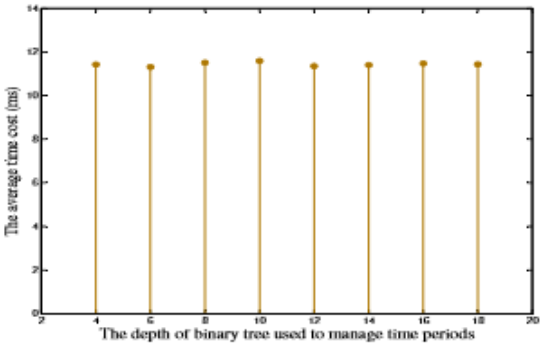


(b) KeyUpdate

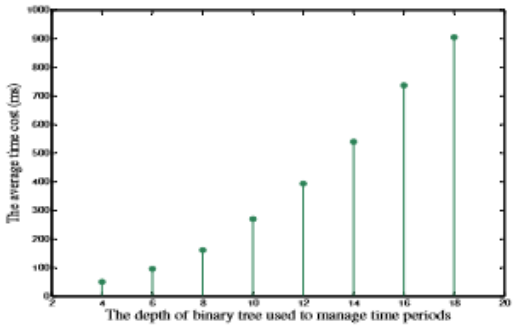


(a) Encrypt

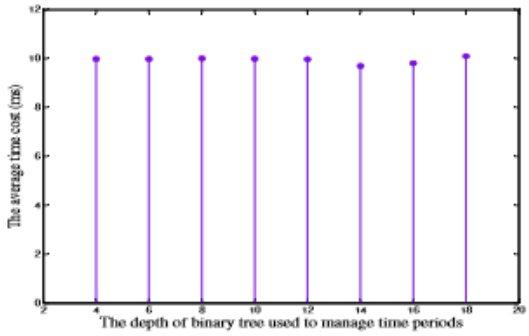
ISSN: 2233-7857 IJFGCN



(b) DKGen



(a) CTUpdate



(b) Decrypt

7. CONCLUSIONS AND FUTURE WORK

Cloud computing brings great convenience for people especially, it splendidly coordinates the expanded need of sharing information over the Internet. In this paper, to manufacture a practical and secure information sharing framework in distributed computing, we proposed an idea called RS-IBE, which underpins character disavowal and figure content update simultaneously such that are voted user is prevented from accessing previously shared data, as well as subsequently shared data. Furthermore, concrete construction of RS-IBE is presented.The proposed RS-IBE is shown adaptable secure in the

ISSN: 2233-7857 IJFGCN

standard model, under the decisional ℓ-DBHE assumption. The examination results show that our plan has favorable circumstances as far as proficiency and usefulness, and along these lines is increasingly achievable for viable applications.

References

1. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*. Springer, 1985, pp. 47–53.
2. Azure.(2014) Azure service. Available: http://www.windowsazure.com
3. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 9, pp. 1717–1726, 2013
4. iCloud.(2014) Apple storage service. Available: https://www.icloud.com
5. B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013*Proceedings IEEE*. IEEE, 2013
6. Boneh and M. Franklin, "Identity-based encryption from the eil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.
7. S.Micali, "Efficient certificate revocation," Tech. Rep., 1996.
8. D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Advances in Cryptology–CRYPTO 2001*. Springer, 2001, pp. 41–62.
9. C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Advances in Cryptology–EUROCRYPT 2003*.Springer, 2003, pp. 272–293.
10. B. Libert and D. Vergnaud, "Adaptive-id secure revocable identity based encryption," in Topics in Cryptology–CT-RSA 2009. Springer, 2009, pp. 1–15
11. Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption Jianghong Wei, Wenfen Liu, Xuexian Hu

ISSN: 2233-7857 IJFGCN