Multi-Stage Security of Shared Cloud Data with Automatic Group User Revocation

Madhurima Sharma[1] , Dr. Rachana Dubey[2]

[1]*M. Tech. Research Scholar,* [2]*Associate Professor*

Department of Computer Science and Engineering, LNCT, Bhopal

Abstract - The security of the information while sharing is very necessary as it is possible to multiple users. The privacy of the content is needed to protect simultaneously maintaining the shared access to authorized users. In this work while managing the privacy as well as security if shared data some added and layers of security is proposed. The group users while accessing the shared information will be blocked on first wrong attempt and need administrator permission to get login access. Even all the data are encrypted with keys so that with wrong keys and authorization credentials no one will be able to access the shared data. These multiple layers increasing the protection of user shared data.

Index Terms—Public integrity auditing, dynamic data, victor commitment, group signature, cloud computing.

I. INTRODUCTION

Cloud concept is nothing but also the storage service, but it can also share across multiple users. We mostly prioritizes privacy preserving mechanism because during auditing data from cloud services it's not a secured while that private information is publicly protected by cloud service. Specifically, the group signature scheme permits the users to anonymously use the cloud resources, and the dynamic broadcast encryption technique concede the data owners to securely share their data files, to others including new joining users which protects the confidentiality from the revoked users in the dynamic broadcast encryption scheme. We propose that when any user is accessing the data from the cloud it must be assured from unauthorized person or hacker. Cloud is un-trusted file storage, so we utilize encryption based access control for sharing document in the cloud storage service. The user's data is encrypted by using cryptographic technique from unauthorized person that can hack the user's private data. In this cryptographic technique we uses different algorithms like signature algorithm, key generation algorithm, ring verify algorithm, etc.. these algorithms are used in the cryptographic technique. Users

can enjoy high-quality services by migrating local data management systems into cloud servers.

The continues development of cloud technique has boasted a number of cloud based application in which data are only persisted in cloud for storage but also a subject to frequent modification from multiple users .Real world examples are cloud based synchronization platforms such as drop box for business [1] ,online data backup services of Amazon and some practical cloud based software Google drive [2].Which enables multiple team members to work in synchronous Accessing and modifying same file on cloud servers anywhere any time. For proper execution of this kind of cloud based collaborative applications one problem is to assure data integration i.e. each data modification operation is simply performed by an authorized member and the data remains intact thereafter. This problem is important given the fact that cloud platforms, even well-known .cloud platforms may experience hard ware software failure human errors and malicious attacks [3][4].

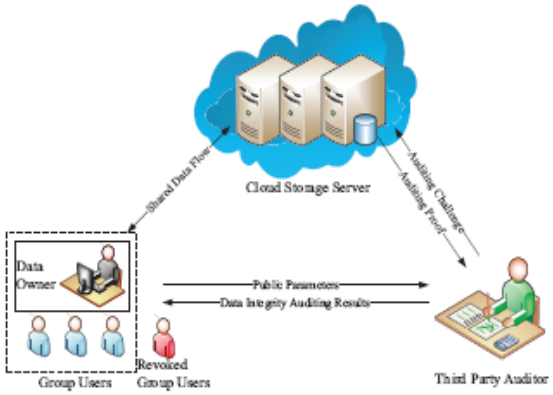


Fig:1.1 the cloud storage model

Service availability, data synchronization between different devices, possibility of data via any devices which includes browser facility makes cloud more interesting. Now since the info gets shared or saved in provider's area, the clientgets worried about privacy of its data, although there are certain accomodation and SLA which are agreed by cloud provider and client. Now although client has a platform to share the info, the charges of securing his/her data or in a nutshell making its data secret gets costlier.

The cloud term is of interest not due to the patient clients but to organizations as well. With organization as a consumer the concern about data security becomes multifold. Keep in mind a typical example of small scale business that has different departments like HR, Finance, etc. We will focus on finance department since finance details of any business/company/organization are

considered to be very sensitive and must be confidential. Therefore if the little scales company thinks of using the cloud services like storage. Storing all account/finance related information in cloud stored makes it prone to leakage of sensitive information tells un-authorized users. Therefore securing this finance data is vital before it gets uploaded to the storage cloud, and just in case the data saved in cloud storage gets tampered there should be a method to cerify the integrity of the data, moving further specific band of people should have access to this data which may be folks from finance department of client company or special auditors. Simply speaking the client should have the ability to save the data securely, certify the integrity of the data, and share the data securely with specific band of people.

Cloud service workers manage an enterprise-class infrastructure that offers a scalable, secure and reliable environment for users, at a much reduce marginal cost due to the sharing nature of resources. It is routine for users to use cloud storage services to share data with others in a team, as data sharing becomes a standard feature in most cloud storage offerings, including Dropbox and Google Docs. The integrity of data in cloud storage, however, is a subject to skepticism and scrutiny, as data saved in an un-trusted cloud that can easily be lost or corrupted, due to hardware failing and human errors. To protect the integrity of cloud data, by perform public auditing through introducing to a third party auditor (TPA), who offers its auditing service with more powerful computation and delivery abilities than regular users.

II. LITERATURE SURVEY

Tao Jiang, Xiaofeng Chen, and Jianfeng Ma [1], proposed a scheme to realize efficient and secure data integrity auditing for share dynamic data with multi-user modification. The scheme vector commitment, Asymmetric Group Key Agreement (AGKA) and group signatures along with user revocation are adopt to achieve the data integrity auditing of remote data. Beside the public data auditing, the combining of the three primitive enable our scheme to outsource cipher-text database to remote cloud and support secure group users revocation to shared dynamic data.

Provable data possession (PDP), first proposed by Ateniese et al. [2], allows a verifier to check the accuracy of a client's data saved at an un-trusted server. By utilizing the RSA-based homomorphic authenticators and sampling strategies, the auditor is able to publicly audit the integrity of data without retrieving the entire data, which is referred to as public verifiability or public auditing. Unfortunately, their scheme is only suitable for auditing the integrity of static data.

Juels and Kaliski [3] defined another identical model called proofs of Retrievability (POR), which is also able to check the correctness of data on an un trusted server. The main file is added with a set of randomly-valued audit blocks called sentinels. The verifier challenges the un-trusted server by describing the locations of a collection of sentinels and asking the un trusted server to return the associated sentinel values.

To support dynamic operations on data, Ateniese et al. [4] presented an correct PDP mechanism based on symmetric keys. This mechanism can support update and remove the operations on data, however, insert operations are not available in this mechanism. Because it the accomplishment of symmetric keys to verify the integrity of data, it is not publicly verifiable and only provides a user with a finite numbers of verification requests.

Shacham and Waters [6] designed to improved POR schemes. The first scheme is built from BLS signatures, and the second one is based on pseudorandom functions. Wang et al. [3] is able to preserve users' private data from the TPA by using random maskings. In addition, to operate the multiple auditing tasks from different users efficiently, they continued their mechanism to enable batch auditing by leveraging aggregate signatures [5].

The public mechanism proposed by Wang et al. [6] leveraged homomorphic tokens to assure the efficient of erasure codes-based data assigned on multiple servers. This mechanism is adept not only to backing dynamic operations on data, but also to identify misbehaved servers. To minimize communication over in the phase of data repair, Chen et al. [7] also introduced a mechanism for verifying the correctness of data with the multi-server scenario, where these data are encoded through network coding instead of using erasure codes. More recently, Cao et al. [8] composed an LT codes-based secure and reliable cloud storage mechanism. Examine the previous work [6], [7], this structure can avoid high decoding computation charge for data users and save computation resource for online data owners during data repair.

Wang et al. utilized Merkle Hash Tree and BLS signatures [9] to support fully dynamic operations in a public verifying mechanism. Erway et al. [8] introduced dynamic provable data possession (DPDP) by using authenticated dictionaries, which are depend on rank information. Zhu et al. exploited the fragment system to reduce the storage of signatures in their public auditing mechanism. In addition, they also used index hash tables to provide dynamic operations for users.

To avoid special attacks exist in remote data storage system with deduplication, Halevi et al. [9] introduced the notation of proofs-of-ownership (POWs), which allows a

client to prove to a server that she actually holds a data file, alternatively just some hash values of the data file. Zheng et al. [10] further discussed that POW and PDP can co-exist under the same framework. Recently, Franz et al. [11] proposed an oblivious outsourced storage scheme based on Oblivious RAM techniques, which is able to hide users' access patterns on outsourced data from an un trusted cloud. Vimercati et al. [2] utilize shuffle index structure to protect users' access patterns on outsourced data.

Difference:-

Existing System:-

This paper, we figure out the collusion attack in the exiting scheme and provide an efficient public integrity auditing scheme with secure group user revocation based on vector commitment and the verifier-local revocation group signature. We design a concrete scheme based on the scheme definition. Our scheme supports the public checking and efficient user revocation and also few nice properties, such as confidently, correctness, accountability and traceability of secure group user revocation.

III. SYSTEM MODEL

The users are able to access and to share resources offered by cloud service providers at a lower marginal expenditure. It is routine for users to leverage cloud storage services to share data which remains in a group, as data sharing becomes standard feature in most cloud storage offerings, including Dropbox, iCloud and Google Drive. A system model composed of three major entities

1. The Cloud server
2. The Third party auditor [TPA]
3. Users

There are two category of users in a groups

1. The original user (master user)
2. The no. of group users

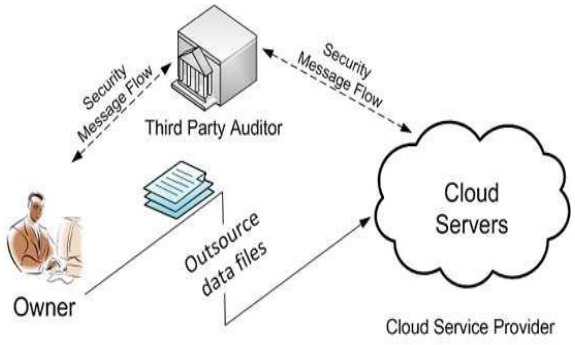


Fig:3.1 System Model Includes The Cloud Server, The Third Party Auditor And Users.

The original user and the no. of group user are both associate of the group. The group associate can modify shared data created by the original user based on the controlled policy. Shared data and its verification information (i.e. signature) are both stored in the cloud server. The TPA refers to any party that check that integrity of data which is stored on the cloud.

The traditional form for checking data correctness is to retrieve the full data from the cloud, and then certify the data integrity by checking the correctness of signatures (e.g., RSA) or hash values (e.g., MD5) of the entire data. Certainly, this conventional approach able to successfully analysis the accurate of the cloud data. However, the efficiency of using this traditional approach on cloud data is in doubt.

IV. PROBLEM IDENTIFICATION

In this work, focusing on the serious issues of identity revocation, we introduce public verification which check data integrity not only by data owners, but also by any third party auditor. However dynamic schemes focus on data owner and data owner can modify the data. To protect the confidential data, it is essential and critical top reserve status of privacy from public verifiers during public auditing. In our protypical, privacy is accomplished by allowing the parties to upload their information in multi clouds and information is split into multiple parts so it gives more protection. The critical reasons due to which our above system is beneficial as:

1. Current working scenario involves Data analysis and verification.

2. Data Storage is path to mitigate the privacy concern.

3. Unauthorized users can leak or misuse the data, this problem still remains due to the based work.

The cloud service providers manage an enterprise-classinfrastructure that offers a scalable, secure and reliableenvironment for users, at a much lower marginal charge due to the sharing nature of resources.

V. PROPOSED METHODOLOGY

In proposed methodology, mainly focused on security enhancement using Identity-Based Encryption with added a secret Data key & Owner key to improve the user security, in demand to provide privacy in accessing the user data stored on cloud. In this proposed system, work and improvement done in two areas:

- Security Enhancement:
- Encryption Algorithm:

File Auditing

If an user edited an data then the auditor will monitor the user and report to the owner about the edited data . the group manager will monitored the changes in the file and if he found any discrepancy auditor has right to evocate from his particular group public auditor can audit the integrating of shared data without retrieving full data from a cloud even if some blocks in shared data have been resigned by a cloud.

Re-Assigning

On one hand, once our user is revoked from the group the block signed by the revoked user can be effectively resigned. The proxy is easy to convert a signature of Alice in to a signature of bob on the same block .

Mean while the proxy is not able to learn any private keys of the two users which mean any can not sign any block on favor of either Alice or bob .

File Upload

File owner allowed uploading data on the cloud either for their private or public use they act as a group manager for the file they upload in cloud.

Both the original user and group user are easy to access download and modify shared data. Shared data is divided in to a no of blocks a user in the group can modify a block s. in shared data can performed and insert, delete or update operation on the block.

Group Sharing

data owner will save their data in a cloud and share the data among the group members . to upload the data have rights to modify and download their data in the cloud .

Access Control

The cloud server allowed only the certified group member to save the data in the cloud offer by cloud service provider.

User Revocation

The user revocation is secure because only existing users are easy to sign the blocks in shared data. even with a resigning key a cloud which cannot generate a valid signature for arbitrary block on favor of an existing user.

VI. PROPOSED BLOCK DIAGRAM

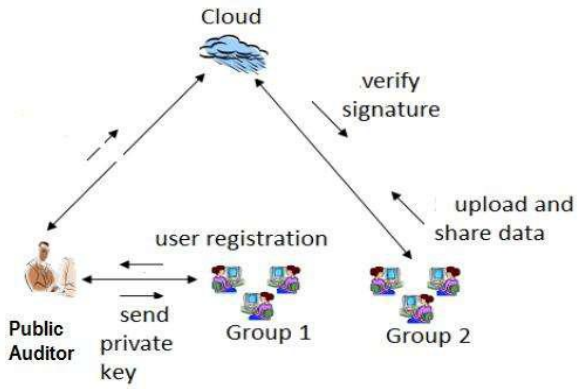


Fig:6.1 cloud proposed model

Group user upload his data on cloud and shared it within group and another group , than public verifier is nothing but the group admin who can provide verification services to maintain integrity of data on cloud.

1. Current working scenario involves Data analysis and verification.

2. Data Storage is path to mitigate the privacy concern.

3. Unauthorized users can disclosed or misuse the data, this problem still remains due to the based work.

User has to registered in user registration, after that user login and can upload file and can check upload by checking in view data which required Data key.

VII. PROPOSED FLOW DIAGRAM

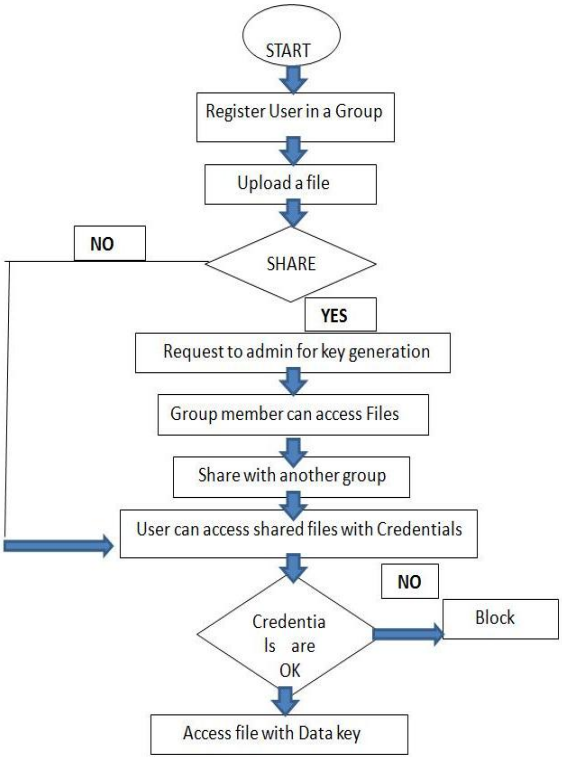


Fig:7.1 Flow diagram

VII. RESULTS

1. Install jdk 1.7 and above version

2. Install myself with ***admin*** password

3. Install net beans 8.0 with tomcat

4. Established connection through JDBC.

5.Open the source code find filename db.sql

6. Open in wordpad

7. Copy the file data and paste into mysql command prompt

8. In net beans then go for file->open project->then move to your project location->globe symbol appear->select it ->and click on open button.

9. Right tick on the project in net beans project explorer->properties->libraris->rmove the red colored libraries

10. Import all those packets which is required for our project.

11.And click on button leftside->add externel jars->in each and every project having its own li folder open it.

12. Click on ok

13. Right click on the project run

14. Then execute the project...

Comparison Table

Particulars	Existing System	Proposed System
Security of Data	Single Level Security	Multi-Level Security with Cloud Key and Owner Key
User Revocation	Revoke Manually (By Admin)	Automatic Revocation on Wrong Credentials
Data Confidentiality	User can see shared data only	Shared Data/File Accessible with Security Credentials only
Access Permission	On Request of Group User	On Request of Group User
Accessibility of Shared Data/File	Data Key will be Required	Owner Key as well as Cloud Key will be required
Auditor Role	Third Party	Third Party
	Auditor for Data	Auditor for Data having Editing Rights for Documents
Admin Control	Block and Activate User	Activate User, Blocking will be done Automatically
User Control	Send request for files access and upload own files/data, Share it, View Group Files	Send request for files access and upload own files/data, Share it, View Group Files

The time analysis of the proposed system is carried out with different data items or blocks to calculate the time cost.

The comparison of time cost of query, verify time and update time is shown in the figures 10.1, 10.2 and 10.3. respectively. From the time cost analysis it can be analyzed that the proposed (our scheme) has lower cost than the previous[1] scheme.

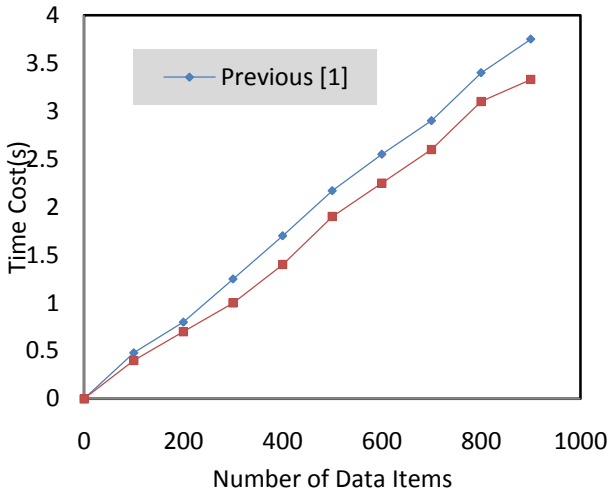


Figure 8.1 Query Time Cost

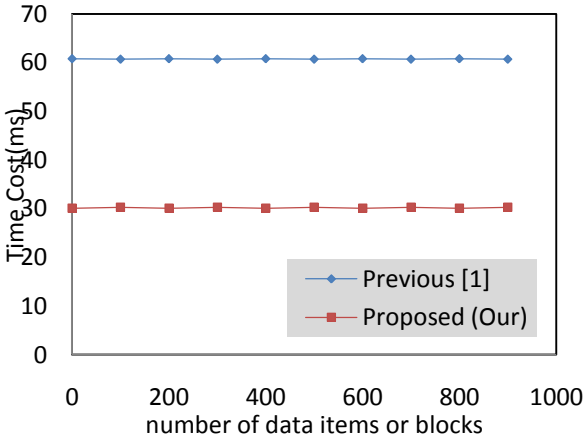


Figure 8.2. Verify Time Cost

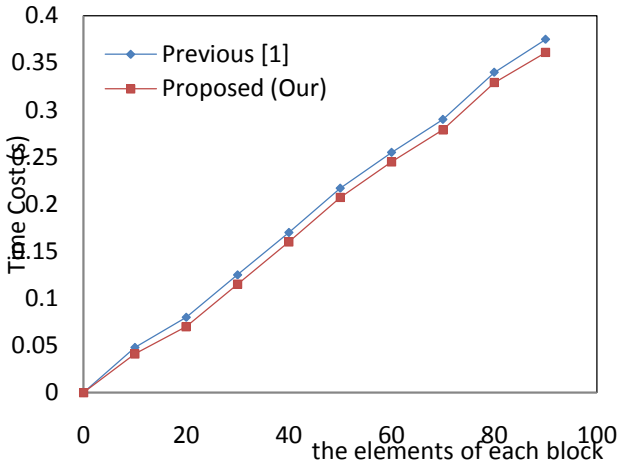
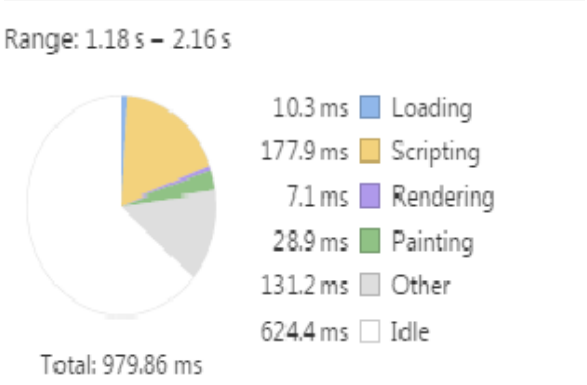


Figure 8.3. Update Time Cost

No. of Data Items	Previous Time	Proposed Time
0	0	0
100	0.48	0.4
200	0.8	0.7
300	1.25	1
400	1.7	1.4
500	2.17	1.9
600	2.55	2.25
700	2.9	2.6
800	3.4	3.1
900	3.75	3.33

Query Time Cost



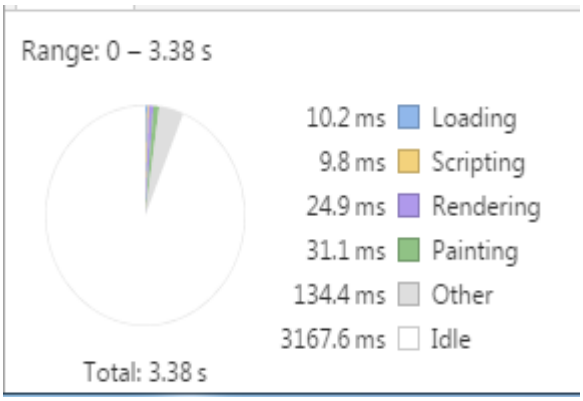
Query Time Cost

No. of Data Items	Previous Time	Proposed Time
0	60.8	30.1
100	60.7	30.3
200	60.8	30.1
300	60.7	30.3
400	60.8	30.1
500	60.7	30.3
600	60.8	30.1
700	60.7	30.3
800	60.8	30.1
900	60.7	30.3

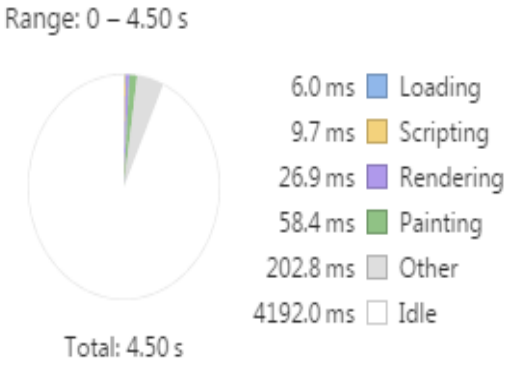
Verify Time Cost

No. of Data Items	Previous Time	Proposed Time
0	0	0
10	0.048	0.041
20	0.08	0.07
30	0.125	0.115
40	0.17	0.16
50	0.217	0.207
60	0.255	0.245
70	0.29	0.279
80	0.34	0.329
90	0.375	0.361

Update Time Cost



Verify Time Cost



Update Time Cost

XI. CONCLUSION AND FUTURE WORK

In this research study the multiple layers has been analyzed through the system design. Security of user shared data has been increased the above results shows the system performance reached to the optimum value and the comparison table has been presented. We utilizing, the privacy preserving which shared the data in the cloud storage service that support the ring signature and Homomorphic authentication ring signature. It will easily

audit the integrity of shared data. Our future work is how to audit shared data with dynamic members although users sharing the data it will be safe. Utilizing privacy preserving who shared the data in the cloud storage service with the aid of rising signature it will easily audit the integrity of shared data. In future shared data can audit with dynamic members while the users sharing the data. It also provides the privacy to users for saving their confidential file on a cloud and using ownercloud key and owner key after that user can access the file. In this disquistion, stages of security are increased.

In observance of all the parameters, in future we can add other security to improve this system by adding various new techniques to enhance more stages of security. Some another algorithms can further be used to provide more perfection and security to the system.

REFERENCES

[1] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation" 10.1109/TC.2015.2389955, IEEE.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2007, pp. 598–610.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, 2010, pp. 525–533.

[4] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in *Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*. Springer- Verlag, 2001, pp. 552–565.

[5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in *Proc. In- ternational Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. Springer-Verlag, 2003, pp. 416–432.

[6] H. Shacham and B. Waters, "Compact Proofs of Retrievability," in *Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*. Springer- Verlag, 2008, pp. 90–107.

[7] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S.Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in *Proc. ACM Symposium on Applied Computing (SAC)*, 2011, pp. 1550–1557.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, 2010, pp. 534–542.

[9] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," in *Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*. Springer-Verlag, 2001, pp. 514–532.

[10] D. Boneh and D. M. Freeman, "Homomorphic Signatures for Polynomial Functions," in *Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. Springer-Verlag, 2011, pp. 149–168.

[11] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen, "Practical Short Signature Batch Verification," in *Proc. RSA Con- ference, the Cryptographers' Track (CT-RSA)*. Springer-Verlag, 2009, pp. 309–324.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2006, pp. 89–98.