Global Journal of Engineering Science and Research Management

SECURE AND EFFICIENT DATA INTEGRITY PROOF AND RECOVERING DATA FOR IDENTITY-BASED PROXY-ORIENTED DATA UPLOADING IN CLOUD COMPUTING (IB-PODUC)

Ushamani G D*, Dr Y.C Kiran
* Computer Science BNMIT Bangalore

DOI: 10.5281/zenodo.573506

KEYWORDS: Cloud computing, identity-based cryptography, proxy public key cryptography, remote data integrity checking.

ABSTRACT

More customers might need to store their data to PCS (open cloud servers) alongside the fast change of distributed computing. New security issues must be explained with a specific end goal to help more customers process their data in people in general cloud. Right when the customers is constrained to get to PCS, he will appoint its intermediary too handle his data and exchange them. On the other hand, remote data coordinating checking is additionally an imperative security issue in broad daylight distributed storage. It makes the customers check whether their outsourced data is kept set up without downloading entire data. From the security issues, to propose a novel intermediary situated data transferring and remote data incorporating checking model in character based open key cryptography: IB-PODUC Commonly, System model and Security display. By then, a solid IB-PODUC convention is planned by utilizing the bilinear pairings. The proposed IB-PODUC convention is provably secure in view of the hardness of CDH (computational Diffie-Hellman) issue. Our IB-PODUC convention is in like manner successful and versatile. In perspective of the primary client's endorsement, the proposed IB-PODUC convention can comprehend private remote data coordinating checking, assigned remote data incorporating checking and open remote data Integrity checking.

INTRODUCTION

Cloud computing have been a newest drift in now a days. Diverse types of services are been provided from dissimilar type of cloud service providers. Vast and bulky amount of data are been stored on the cloud, present at remote locations. The users of the cloud are also escalating now a days. At most, various types of services are been extended by diverse cloud service providers are enormous storage for the different types of the data, utensils for administration and processing of different types of data. All these are doable because of cloud been made a public podium. Many users from different part of the worlds can store the data, extract, and data, process the data, manipulate data and many more. Even though cloud storages have titanic advantages, some challenges with security issues are to be encountered for cloud storages needs that need to be accepted by all the cloud attackers.

The cloud server‘s store various data‘s of different clients, who prefer attack‘s target and the data‘s are being in front of a wide range of warnings and attacks. Especially, different from usual type of data storage processes, in cloud the, owners of the data need not possess data bodily after data is out sourced into the cloud service provider who are not trust commendable. For advantages of the individuals, cloud service providers may disregard a part of less habitually accessed data, to save storage space. Also, cloud service providers may be enforced to hide the data corruption caused by cloud server hackers to maintain reputations. It has been documented that the security issues, such as data integrity checking and availability, are the core hurdles for the storage of data on the cloud to be profitably adopted. As, this rate is been increasing, the security issues and considerations, for the same are also been mounting day by day. Providing confidentiality, integrity, security and availability of data are also been ever-increasing day by day. In view of the fact that, users are storing their data on the public cloud servers and performing all sorts of processing from server side, providing confidentiality, integrity, security and availability of data at public cloud platforms are also been ever-increasing on a daily basis. Users are expecting security for their data in a variety of aspects. For the same, we provide remote data integrity checking using proxy server with Partial data method is used to address the problem. Our proposed system is competent and very bendy. Based upon the actual client‘s authorization, our proposed system, will extend private data integrity checking using partial data.

LITERATURE SURVEY

[1]. H. Wang, "Proxy provable data possession in public clouds," IEEETrans. Services Comput., vol. 6, no. 4, pp. 551–559, Oct./Dec. 2013.

Recently, cloud computing rapidly expands as an alternative to conventional computing due to it can provide a flexible,dynamic and resilient infrastructure for both academic and business environments. In public cloud environment, the client moves its data to public cloud server (PCS) and cannot control its remote data. Thus, information security is an important problem in public cloud storage, such as data confidentiality, integrity, and availability. In some cases, the client has no ability to check its remote data possession, such as the client is in prison because of committing crime, on the ocean-going vessel, in the battlefield because of the war, and so on. It has to delegate the remote data possession checking task to some proxy. In this paper, we study proxy provable datapossession (PPDP). In public clouds, PPDP is a matter of crucial importance when the client cannot perform the remote data possession checking. We study the PPDP system model, the security model, and the design method. Based on the bilinear pairing technique, we design an efficient PPDP protocol. Through security analysis and performance analysis, our protocol is provable secure and efficient.

[2]. H. Wang, "Identity-based distributed provable data possession in multicloudstorage," IEEE Trans. Services Comput., vol. 8, no. 2, pp. 328–340,Mar./Apr. 2015.

Remote data integrity checking is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multicloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, we propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multicloud storage. The formal system model and security model are given. Based on the bilinear pairings, a concrete ID-DPDP protocol is designed. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH(Computational Diffie-Hellman) problem. In addition to the structural advantage of elimination of certificate management,our ID-DPDP protocol is also efficient and flexible. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification, and public verification.

[3].Privacy-Preserving Public Auditing for Secure Cloud Storage Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, KuiRen, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE.

Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a Third-Party Auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user.A secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design. The homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, further extend our privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

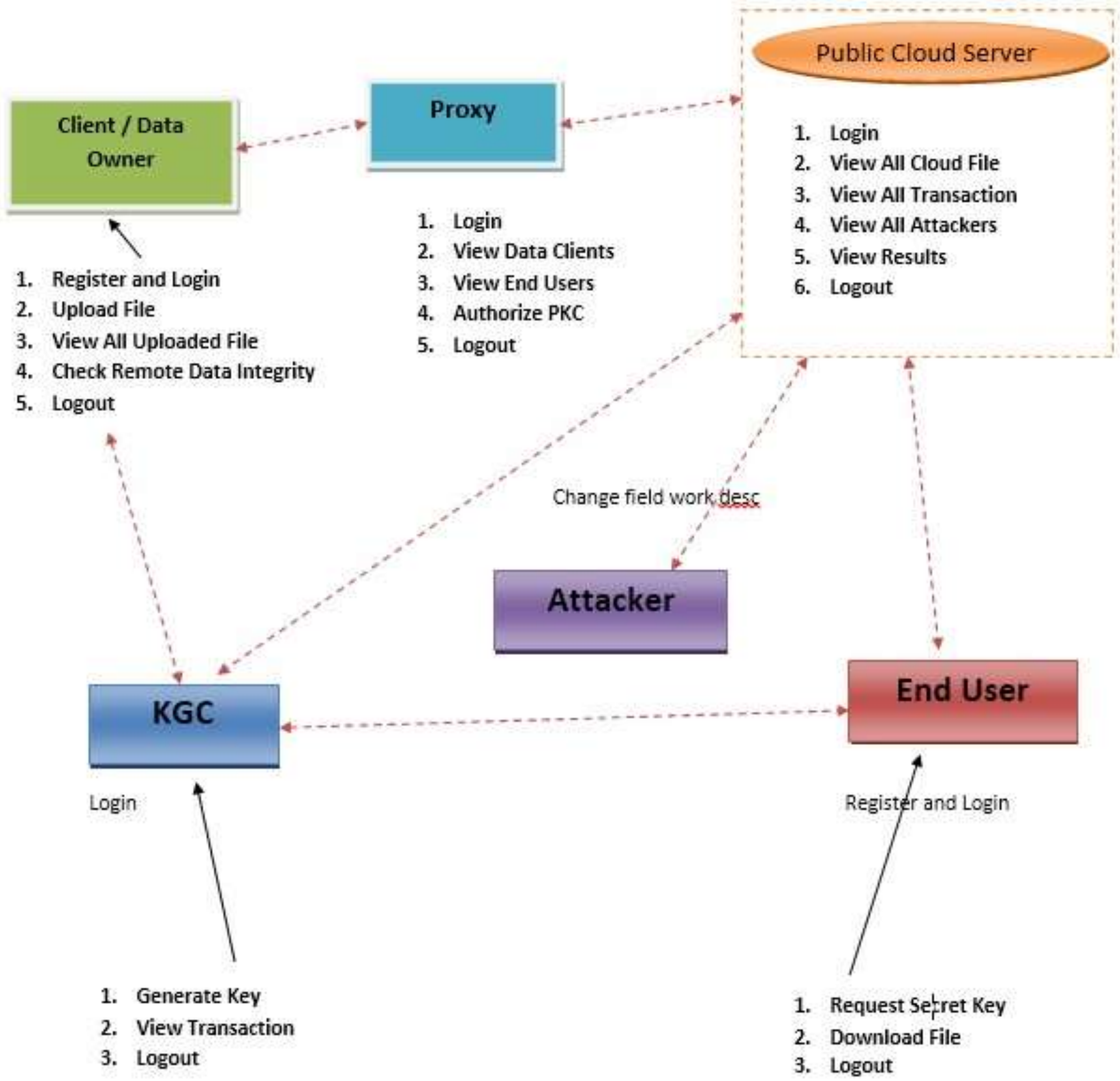
[4].DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage SystemsKan Yang, Associate Member, IEEE, XiaohuaJia, Fellow, IEEE, KuiRen, Senior Member, IEEE, Bo Zhang, Member, IEEE, and RuitaoXie, Student Member, IEEE

Data access control is an effective way to ensure data security in the cloud. However, due to data outsourcing and un trusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Ciphertext- policy Attribute-BasedEncryption(CP-ABE)is a promising technique for access control of encrypted data. However, due to the inefficiency of decryption and revocation, existing CP-ABE schemes cannot be directly applied to construct a data access control scheme for multiauthority cloud storage systems where users may hold attributes from multiple authorities. Data access control for multi authority cloud storage (DAC-MACS), an effective and secure data access control scheme with efficient decryption and revocation.

[5].Toward Secure and Dependable Storage Services in Cloud ComputingCong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, KuiRen, Senior Member, IEEE, Ning Cao, and Wenjing Lou, Senior Member, IEEE.

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks toward the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. The proposed design 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. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, propose an effective and flexible distributed scheme with explicit dynamic 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. By utilizing the homo- morphic token with distributed verification of erasure- coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers.

ARCHITECTURE DIAGRAM



SYSTEM ANALYSIS

EXISTING SYSTEM

In this system, the system implemented an efficient IB-PODUC protocol for secure data uploading and storage service in public clouds. Bilinear pairings technique makes identity-based cryptography practical. The protocol is built on the bilinear pairings. The system first reviews the bilinear pairings. Then, the concrete IB-PODUC protocol is designed from the bilinear pairings. At last, based on the computation cost and communication cost, the system gives the performance analysis from two aspects: theoretical analysis and prototype implementation and data integrity but there is no data recovery techniques.

PROPOSED SYSTEM

Cloud computing provides various kinds of services to its users. Storage-as-a-service is one of the services provided by cloud infrastructure in which large amount of electronic data is stored in cloud. As valuable and important data of enterprises are stored at a remote location on cloud we must be assured that our data is safe and be available at any time. In situations like Flood, Fire, earthquakes or any hardware malfunction or any accidental deletion our data may no longer remain available. To maintain the data safety there must be some data backup technique for cloud platform to recover valuable and important data efficiently in such situations mentioned above. This paper provides a review on various backup techniques used for Cloud Computing platform regarding this concern and also, the system gives the formal definition, system model and security model. Then, a concrete IB-PODUC protocol is designed by using the bilinear pairings. The proposed IB-PODUC protocol is provably secure based on the hardness of CDH (computational Diffie-Hellman) problem. Our IB-PODUC protocol is also efficient and flexible. Based on the original client's authorization, the proposed IB-PODUC protocol can realize private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking.

SYSTEM REQUIREMENT

This Chapter describes about the requirements. It specifies the hardware and software requirements that are required in order to run the application properly. The Software Requirement Specification (SRS) is explained in detail, which includes overview of this dissertation as well as the functional and non-functional requirement of this dissertation.

SRS for A Hybrid Cloud Approach for Secure Authorized Deduplication

Table: 3.1 Summaries of SRS

Functional	Register and Login, Upload File, View All Uploaded File ,Check Remote Data Integrity, View Data Clients ,View End Users, Authorize PKC, View All Cloud File ,View All Transaction ,View All Attackers ,View Results, Generate Key ,View Transaction, Request Secret Key,Download File
Non- Functional	Data Owner never monitors the Cloud activities
External interface	LAN , Routers, WAN
Performance	Finding File Hacker Information, File Sharing efficiency fairness between Cloud Server and Remote User, Finding Private Key,Checking Data Integrity with Original Data User.
Attributes	File name, owner name, public key, secret key, user details, reg details, attackers, File name, cloud name, ip address, secret key, reg details, priv key

FUNCTIONAL REQUIREMENTS

Functional Requirement defines a function of a software system and how the system must behave when presented with specific inputs or conditions. These may include calculations, data manipulation and processing and other specific functionality. In this system following are the functional requirements:-

- The owner should login by using authorized user name and password.
- The Owner has to browse the files, generate the MAC address and encrypt data, upload to cloud server.
- Then the proxy server will authorize the data to cloud server and public key is requesting by the data owner.
- After generating key in the kgc,it will be given to end user and data owner.
- The user should register under data owner, after registration success. User should login by authorized user name and password.
- The Cloud server has to authorize the valid remote users. if the Remote user is hacker then he has to Automatic block in the cloud server. The data should be integrated by the cloud server.
- The Remote user has to use correct Secret key and file name. If anyone is wrong then he is detected as attacker.
- The Attributes are File name, owner name, public key, secret key, user details, reg details, attackers, File name, cloud name, ip address, secret key, reg details, priv key

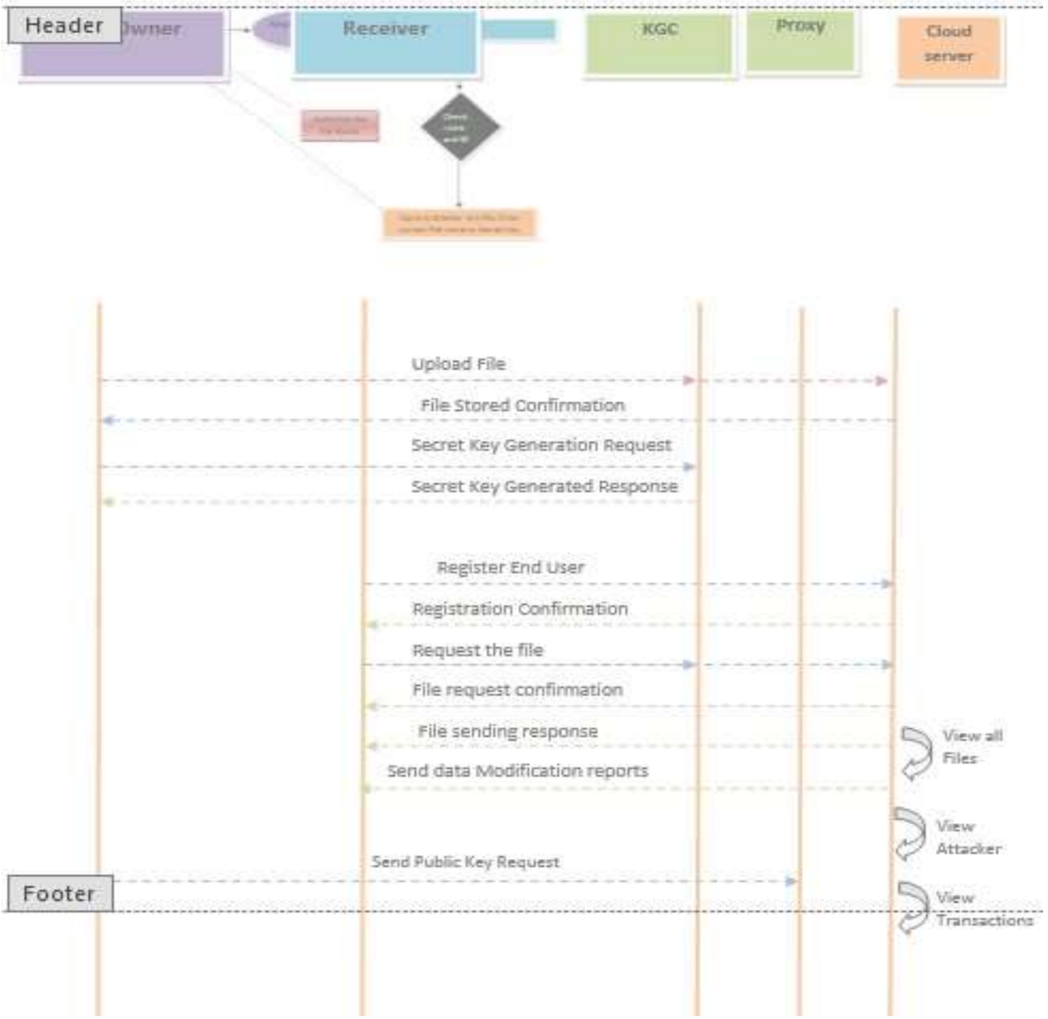
NON – FUNCTIONAL REQUIREMENTS

Non – Functional requirements, as the name suggests, are those requirements that are not directly concerned with the specific functions delivered by the system. They may relate to emergent system properties such as reliability response time and store occupancy. Alternatively, they may define constraints on the system such as the capability of the Input Output devices and the data representations used in system interfaces. Many non-functional requirements relate to the system as whole rather than to individual system features. This means they are often critical than the individual functional requirements. The following non-functional requirements are worthy of attention.

The key non-functional requirements are:

- Security: The system should allow a secured communication between Cs and Data Owner, User and File Owner
- Energy Efficiency: The Energy consumed by the Users to receive the File information from the cloud server
- Reliability: The system should be reliable and must not degrade the performance of the existing system and should not lead to the hanging of the system.

SEQUENCE DIAGRAM



Header
Public Key Response Confirmation
Verify File
File verification report
Delete File
Delete Response
Authorize Users and Data

CONCLUSION

This paper proposes the novel security considered IB-PODUC publically cloud. The paper formalizes IB-PODUC's framework model and security display. At that point, the essential solid IB-PODUC convention is implied by exploitation the straight pairings system. The solid IB-PODUC convention is indisputably secure and temperate by exploitation the formal security verification and power investigation. On the inverse hand, the anticipated IB-PODUC convention additionally can comprehend nonpublic remote learning honesty checking, designated remote information trustworthiness checking and open remote learning respectability checking bolstered the main customer's approval.

REFERENCES

1. Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, “Mutual verifiable provable data auditing in public cloud storage,” J.Internet Technol., vol. 16, no. 2, pp. 317–323, 2015.
2. Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, “Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing,” IEICE Trans. Commun., vol. E98-B, no. 1, pp. 190–200, 2015.
3. E.-J. Yoon, Y. Choi, and C. Kim, “New ID-based proxy signature scheme with message recovery,” in Grid and Pervasive Computing (Lecture Notes in Computer Science), vol. 7861. Berlin, Germany: Springer-Verlag, 2013, pp. 945–951.
4. M. Mambo, K. Usuda, and E. Okamoto, “Proxy signatures for delegating signing operation,” in Proc. CCS, 1996, pp. 48–57.
5. X. Liu, J. Ma, J. Xiong, T. Zhang, and Q. Li, “Personal health records integrity verification using attribute based proxy signature in cloud computing,” in Internet and Distributed Computing Systems (Lecture Notes in Computer Science), vol. 8223. Berlin, Germany: Springer- Verlag, 2013, pp. 238–251.
6. B.-C. Chen and H.-T. Yeh, “Secure proxy signature schemes from the weil pairing,” J. Supercomput., vol. 65, no. 2, pp. 496–506, 2013.
7. E. Kirshanova, “Proxy re-encryption from lattices,” in Public-Key Cryptography (Lecture Notes in Computer Science), vol. 8383. Berlin, Germany: Springer-Verlag, 2014, pp. 77–94.
8. H. Guo, Z. Zhang, and J. Zhang, “Proxy re-encryption with unforgeable re-encryption keys,” in Cryptology and Network Security (Lecture Notes in Computer Science),vol. 8813. Berlin, Germany: Springer-Verlag, 2014, pp. 2033.
9. P. Xu, H. Chen, D. Zou, and H. Jin, “Fine-grained and heterogeneous proxy re-encryption for secure cloud storage,” Chin. Sci. Bull., vol. 59, no. 32, pp. 4201–4209, 2014.
10. S. Ohata, Y. Kawai, T. Matsuda, G. Hanaoka, and K. Matsuura, “Re-encryption verifiability: How to detect malicious activities of a proxy in proxy re-encryption,” in Proc. CT-RSA Conf., vol. 9048. 2015, pp. 410–428.
11. G. Ateniese et al., “Provable data possession at untrusted stores,” in Proc. CCS, 2007, pp. 598–609.
12. H. Shacham and B. Waters, “Compact proofs of retrievability,” in Proc ASIACRYPT, vol. 5350. 2008, pp. 90–107.
13. Q. Zheng and S. Xu, “Fair and dynamic proofs of retrievability,” in Proc. CODASPY, 2011, pp. 237–248.