International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 1 Issue 1 –AUGUST 2013.

Enhanced Data Storage Security and Trust Environment in Cloud Computing

Arif Sultana Shaik[#1], S. Rama Krishna[*2]

[#]*PG Scholar, Dept. of CSE, VRS & YRN College of Engg. & Technology, Chirala, AP*

[1] arifsultana.shaik@gmail.com

[*]*Associate Professor, Dept. of CSE, VRS & YRN College of Engg. & Technology, Chirala, AP*

***Abstract*— Cloud computing plays an important role in data sharing or transfer of information from one place to another. The services provides by the cloud is greatly enjoyed by the user. The storage of the user's data in the cloud provides the high standard of qualities and more enjoyable services to the users. The data of the user is automatically stored in the cloud without encumber the software and hardware tools. In cloud data storage, it provides many benefits to the users in an evidently. In this cloud storage, new type of risk arisen in the correctness of the users storage data or information. To overcome the above issue in the cloud, we propose new flexible auditing mechanisms in this paper. In order to address the new obstacle and for further perfect secure about the user's data and dependable cloud storage services is propose in this paper. Through this proposal data or information of the user utilizing the similarity token used and distributed erasure-coded information also used. Our proposed mechanism helps the data storage in the lightweight data transfer with less cost and provides the storage correctness assure in the cloud storage. The proposed design helps us to find the information or data error localization. Our proposed design supports for the full secure about the storage data of the user and effective outsource data. It also significant in updating, deletion and append of the user data. Our proposed algorithm protects the user's information from the several types of attacks as shown in our experimental analysis.**

***Keywords*— Data integrity, dependable distributed storage, error localization, data dynamics, cloud computing, attacks, user's data, software and hardware.**

I. INTRODUCTION

Cloud computing [38], is an emerging paradigm in the computer industry where the computing is moved to a cloud of computers. The cloud computing core concept is, simply, that the vast computing resources that we need will reside somewhere out there in the cloud of computers and we'll connect to them and use them as and when needed. Cloud computing is the next general step in the evolution of on demand information technology services and products. Cloud computing is a means by which highly scalable and fully technology based services can be easily consumed over the internet on an as-needed basis. To a large extent, cloud computing will be based on virtualized resources. The convenience and efficiency of this approach, however, comes with security risks and data privacy. A significant barrier to the adoption of cloud services is thus user fear of confidential data leakage and loss of privacy in the cloud. Privacy is an important and fundamental human right that encompasses the right to be left alone, many techniques are proposed under different systems and security models. In all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency, stateless verification etc. Considering the role of the verifier in the model all the schemes presented before fall into two categories: private audit ability and public audit ability.

Recent of years, cloud computing is an emerging technology for the data sharing through the internet on the needed basis. The user enjoys all the accommodation service provides by the cloud and at the same time, the user's got worrying for losing control of their own personal data's or information including financial, health and so on. Sharing of data's or information using cloud storage is recently increasing due to the user love in cloud services very much when compared to other services. While data sharing in the cloud they don't worry about the hardware and software complexities. The service provides by the cloud, through the online to the user and also provides the large amount of space for the data storage purpose and customizable resources over the computing. At same instance, it eliminates the local machines for data maintenance. The user enjoys full services of the cloud and thanks for the availability and integrity of their data or information. The cloud storage services are more powerful and scalable when compared to the other computing services. The broad ranges of the services are available in the cloud storage services. The cloud computing provides the highly valuable services to users and have the number of issues that is related to the accountability of the users. To overcome the data lose happen for the user, we need effective or perfect mechanism to monitor the user's data in the cloud services. But the cloud has got some obstacle in the data transfer service from one place to destination because it happens through unknown intermediate machine. Due to this, user or consumer avoids some services in the cloud. Although the cloud services are used for the data storage purpose, some

type of issues arisen in the long term data storage in the cloud services. Due to these issues, lacking of the integrity and availability of the cloud storage gets exploded.

In order to get the performance gains in the assurance and integrity in the cloud services, the efficient method is required. This method helps the user's data or information correctness and verify according to the users in the clouds. Hence, the verification of cloud storage correctness must be conducted without explicit knowledge of the whole data files [10], [11], [12], [13]. However the data stored in the cloud storage service is frequently updating by the user produce the effective service. The updating services include deletion, modification, appending, insertion, and so on. The frequently updating the data of the user produces the quality in the storage service of the cloud and also reduce the integrity and assurance issues.

In order to achieve the perfect assurance and integrity in the cloud services we implement new idea for towards secure of user data and dependable data storage in the cloud and we made different research about this works and security models as shown in the following reference books[10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22]. By using the research works we make new idea in the correctness of storage data or information implemented but it is not guarantee in the data availability in case of the server failures and many researchers also proposed many distributed services for correctness of storage data across the multiple servers. As a result of many proposed distributed protocols, dynamic data storage in the cloud remains has some issues and limits in the integrity and assurance.

So in order to overcome the issues in the existing services in cloud, we propose effective auditing mechanisms in this paper. Our proposed scheme addresses all the problems in the old model; it supports the huge amount of data storage correctness and ensures the availability of the data users in the cloud. To overcome the above issue in the cloud, we propose new flexible auditing mechanisms in this paper. In order to address the new obstacle and for further perfect secure about the user's data and dependable cloud storage services is propose in this paper. Through this proposal the data or information utilizing the similarity token used and distributed erasure-coded information also used. Our proposed mechanism helps the data storage in the lightweight data transfer with less cost and provides the storage correctness assure in the cloud storage. The proposed design helps us to find the information or data error localization. Our proposed design supports for the full secure about the storage data of the user and effective outsource data. It also significant in updating, deletion and append of the user data. Our proposed algorithm protects the user's information from the several types of attacks as shown in our experimental analysis.

II. RELATED WORKS

In this section, we briefly discuss the works which is similar techniques as our approach but serve for different purposes.

C. Wang, Q. Wang, K. Ren, and W. Lou [1], Cloud computing has been envisioned as the next-generation architecture of IT enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server (s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

Sun Microsystems, Inc [3],Potential users of cloud services often fear that cloud providers' governance is not yet mature enough to consistently and reliably protect their data. As the trend toward cloud-based services continues to grow, it has become clear that one of the key barriers to rapid adoption of enterprise cloud services is customer concern over data security (confidentiality, integrity, and availability). This paper introduces the concept of transparent security and makes the case that the intelligent disclosure of security design, practices, and procedures can help improve customer confidence while protecting critical security features and data, thereby improving overall governance. Readers will learn how transparent security can help prospective cloud computing customers make informed decisions based on clear facts.

K. Ren, C. Wang, and Q. Wang [4],Although virtualization and cloud computing can help companies accomplish more by breaking the physical bonds between an IT infrastructure and its users, heightened security threats must be overcome in order to benefit fully from this new computing paradigm. This is particularly true for the SaaS provider. Some security concerns are worth more discussion. For example, in the cloud, you lose control over assets in some respects, so your security model must be reassessed. Enterprise security is only as good as the least reliable partner, department, or vendor. Can you trust your data to your service provider? This excerpt discusses some issues you should consider before answering that question.

With the cloud model, you lose control overphysical security. In a public cloud, you are sharing computing resources with other companies. In a shared pool outside the enterprise, you don't have any knowledge or control of where the resources run. Exposing your data in an environment shared with other companies could give the government "reasonable cause" to seize your assets because another company has violated the law. Simply because you share the environment in the cloud, may put your data at risk of seizure. Storage services provided by one cloud vendor may be incompatible with another vendor's services should you decide to move from one to the other. Vendors are known for creating what the hosting world calls "sticky services;" services that an end user may have difficulty transporting from one cloud vendor to another (e.g., Amazon's "Simple Storage Service" [S3] is incompatible with IBM's Blue Cloud, or Google, or Dell).

M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan [12],A growing number of online service providers offer to store customers ' photos, email, file system backups, and other digital assets. Currently, customers cannot make informed decisions about the risk of losing data stored with any particular service provider, reducing their incentive to rely on these services. We argue that thirdparty auditing is important in creating an online service oriented economy, because it allows customers to evaluate risks, and it increases the efficiency of insurancebased risk mitigation. We describe approaches and system hooks that support both internal and external auditing of online storage services, describe motivations for service providers and auditors to adopt these approaches, and list challenges that need to be resolved for such auditing to become a reality.

M.A. Shah, R. Swaminathan, and M. Baker [13], a growing number of online services, such as Google, Yahoo!, and Amazon, are starting to charge users for their storage. Customers often use these services to store valuable data such as email, family photos and videos, and disk backups. Today, a customer must entirely trust such external services to maintain the integrity of hosted data and return it intact. Unfortunately, no service is infallible. To make storage services accountable for data loss, we present protocols that allow a third-party auditor to periodically verify the data stored by a service and assist in returning the data intact to the customer. Most importantly, our protocols are privacy-preserving, in that they never reveal the data contents to the auditor. Our solution removes the burden of verification from the customer, alleviates both the customer's and storage services' fear of data leakage, and provides a method for independent arbitration of data retention contracts.

Juels and Kaliski Jr. [10] described a formal "proof of retrievability" (POR) model for ensuring the remote data integrity. Their scheme combines spot-checking and errorcorrecting code to ensure both possession and retrievability of files on archive service systems. Shacham and Waters [17] built on this model and constructed a random linear function-based homomorphic authenticator which enables unlimited number of challenges and requires less communication overhead due to its usage of relatively small size of BLS signature. Bowers et al. [18] proposed an improved framework for POR protocols that generalizes both Juels and Shacham's work. Later in their subsequent work, Bowers et al. [23] extended POR model to distributed systems. However, all these schemes are focusing on static data. The effectiveness of their schemes rests primarily on the preprocessing steps that the user conducts before outsourcing the data file F. Any change to the contents of F, even few bits, must propagate through the error correcting code and the corresponding random shuffling process, thus introducing significant computation and communication complexity. Recently, Dodis et al. [20] gave theoretical studies on generalized framework for different variants of existing POR work. Ateniese et al. [11] defined the "provable data possession" (PDP) model for ensuring possession of file on untrusted storages. Their scheme utilized public key-based homomorphic tags for auditing the data file. However, the precomputation of the tags imposes heavy computation overhead that can be expensive for an entire file. In their subsequent work, Ateniese et al. [14] described a PDP scheme that uses only symmetric key-based cryptography. This method has lower overhead than their previous scheme and allows for block updates, deletions, and appends to the stored file, which has also been supported in our work. However, their scheme focuses on single server scenario and does not provide data availability guarantee against server failures, leaving both the distributed scenario and data error recovery issue unexplored. The explicit support of data dynamics has further been studied in the two recent work [15] and [16]. Wang et al. [15] proposed to combine BLS-based homomorphic authenticator with Merkle Hash Tree to support fully data dynamics, while Erway et al. [16] developed a skip list-based scheme to enable provable data possession with fully dynamics support. The incremental cryptography work done by Bellare et al. [36] also provides a set of cryptographic building blocks such as hash, MAC, and signature functions that may be employed for storage integrity verification while supporting dynamic operations on data. However, this branch of work falls into the traditional data integrity protection mechanism, where local copy of data has to be maintained for the verification. It is not yet clear how the work can be adapted to cloud storage scenario where users no longer have the data at local sites but still need to ensure the storage correctness efficiently in the cloud.

III. PROPOSED WORK

In order to overcome the issues in the existing services in cloud, we propose effective auditing mechanisms in this paper. Our proposed scheme addresses all the problems in the old model; it supports the huge amount of data storage correctness and ensures the availability of the data users in the cloud.

Through this proposal the data or information utilizing the similarity token used and distributed erasure-coded information also used. Our proposed mechanism helps the data storage in the lightweight data transfer with less cost and provides the storage correctness assure in the cloud storage. The proposed design helps us to find the information or data error localization i.e. it is used to find the misbehaving server in the services. Our proposed design supports for the full secure about the storage data of the user and effective outsource data. It also significant in updating, deletion and append of the user data.

Our main contributions in this paper, is summarized below: our proposed scheme achieves the strong the integration over the storage data correctness and to find the misbehaving server, when it is compared to the other schemes. Our proposed algorithm supports the perfect secure over the user's data or information and effective dynamic operations on updating the user data periodically. Our experimental analysis and results show that our proposed scheme is highly efficient when compared to the other schemes. And also show that our proposed design prevents the user data from the various attacks.

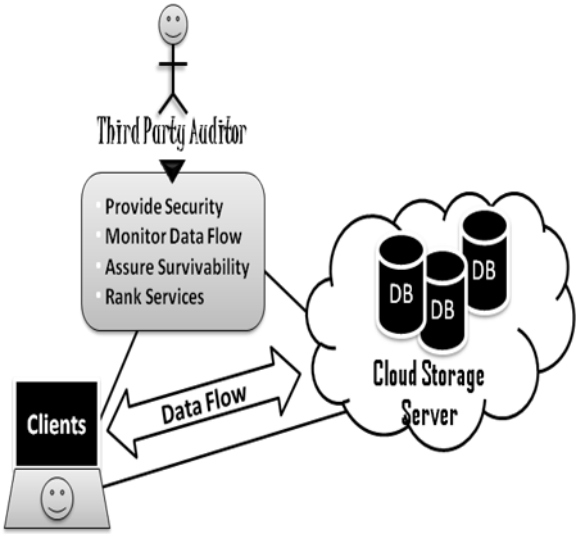

Fig 1: Proposed Cloud Architecture

IV. Simulation Works/Results

The secured and trust environment architecture for cloud data storage is illustrated above in Fig. 1. Three different network entities to e considered during design:

Client: An entity, which has large data files to be stored in the cloud and relies on the auditor for data maintenance and security, can be either individual consumers or organizations.

Cloud Storage Server: An entity, which is managed by Cloud Service Provider, has significant storage space and computation resource to maintain the clients' data. Acknowledge the stored data with security code.

Third Party Auditor: An entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request. Responsible to assure security and survivability of data stored in cloud.

Security Key: Our key distribution mechanism ensures that clients can acquire the keys they need to access the blocks they are authorized to access. To offload as much work as possible to the cloud, the cloud performs this key distribution verifiably.

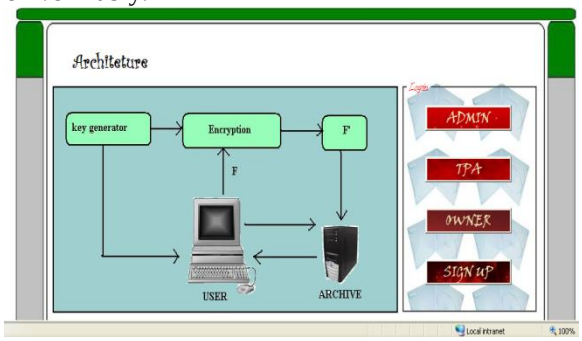

Fig 2: Implementation of the proposed system

Fig 3: File details of the cloud server

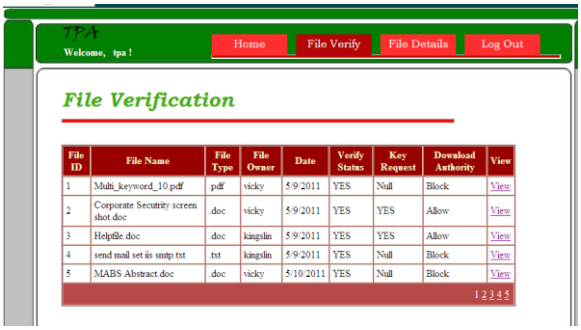

Fig 4: Trust creation module

V. Conclusion

In this paper, we mainly address the problems in the security of the user's data storage in the cloud. Our target of this paper is to achieve the perfect integrity and availability of cloud data storage service and to ensure that quality of cloud storage services for the users at effective manner. In order to achieve this perfection in the service of the cloud, we proposed an efficient and distributed scheme for dynamic data storage in the cloud services. This scheme requires the user to update the information frequently. The updated information of the user in the cloud is fully secured by our proposed schemes. Through this proposal data or information of the user utilizing the similarity token used and distributed erasure-coded information also used. Our proposed mechanism helps the data storage in the lightweight data transfer with less cost and provides the storage correctness assure in the cloud storage. The proposed design helps us to find the information or data error localization. Our proposed design supports for the full secure about the storage data of the user and effective outsourced data. Through detailed security and extensive experiment results, we show that our scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks.

VI. REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing,"Proc. 17th Int'l Workshop Quality of Service (IWQoS '09),pp. 1-9, July 2009.

[2] Amazon.com, "Amazon Web Services (AWS)," http://aws.amazon.com, 2009.

[3] Sun Microsystems, Inc., "Building Customer Trust in Cloud Computing with Transparent Security," https://www.sun.com/offers/details/sun_transparency.xml, Nov. 2009.

[4] K. Ren, C. Wang, and Q. Wang, "Security Challenges for thePublic Cloud,"IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012.

[5] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof-mass-email-deletions, Dec. 2006.

[6] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors," http://www.techcrunch.com/2008/07/10/mediamaxthelinkup-closesits-doors, July 2008.

[7] Amazon.com, "Amazon S3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, July 2008.

[8] S. Wilson, "Appengine Outage," http://www.cio-weblog.com/ 50226711/appengine_outage.php, June 2008.

[9] B. Krebs, "Payment Processor Breach May Be Largest Ever," http://voices.washingtonpost.com/securityfix/2009/01/ payment_processor_breach_may_b.html, Jan. 2009.

[10] Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files,"Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07),pp. 584-597, Oct. 2007.

[11] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores,"Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, Oct. 2007.

[12] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07),pp. 1-6, 2007.

[13] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, http://eprint.iacr.org, 2008.

[14] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession,"Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm '08),pp. 1-10, 2008.

[15] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing,"Proc. 14th European Conf. Research in Computer Security (ESORICS '09),pp. 355-370, 2009.

[16] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09),pp. 213-222, 2009.

[17] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt '08),pp. 90-107, 2008.

[18] K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation,"Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 43-54, 2009.

[19] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession,"Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS '08),pp. 411-420, 2008.

[20] Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of Retrievability via Hardness Amplification,"Proc. Sixth Theory of Cryptography Conf. (TCC '09), Mar. 2009.

[21] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,"IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[22] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "PrivacyPreserving Public Auditing for Secure Cloud Storage,"IEEE Trans. Computers,preprint, 2012, doi:10.1109/TC.2011.245.

[23] K.D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage,"Proc. ACM Conf. Computer and Comm. Security (CCS '09),pp. 187-198, 2009.

[24] T. Schwarz and E.L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS '06), pp. 12-12, 2006

[25] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A Cooperative Internet Backup Scheme," Proc. USENIX Ann. Technical Conf. (General Track),pp. 29-41, 2003.

[26] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery,"ACM Trans. Computer Systems,vol. 20, no. 4, pp. 398-461, 2002.

[27] L. Carter and M. Wegman, "Universal Hash Functions," J. Computer and System Sciences,vol. 18, no. 2, pp. 143-154, 1979.

[28] J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasure-Coded Data," Proc. 26th ACM Symp. Principles of Distributed Computing,pp. 139-146, 2007.

[29] J.S. Plank and Y. Ding, "Note: Correction to the 1997 Tutorial on Reed-Solomon Coding," Technical Report CS-03-504, Univ. of Tennessee, Apr. 2003.

[30] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing,"Proc. IEEE INFOCOM,Mar. 2010.

[31] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[32] R.C. Merkle, "Protocols for Public Key Cryptosystems,"Proc. IEEE Symp. Security and Privacy,1980.

[33] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance,"Proc. IEEE INFOCOM,Apr. 2009.

[34] J.S. Plank, S. Simmerman, and C.D. Schuman, "Jerasure: A Library in C/C++ Facilitating Erasure Coding for Storage Applications -Version 1.2," Technical Report CS-08-627, Univ. of Tennessee,Aug. 2008.

[35] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication,"Proc. 16th Ann. Int'l Cryptology Conf. Advances in Cryptology (Crypto '96),pp. 1-15, 1996.

[36] M. Bellare, O. Goldreich, and S. Goldwasser, "Incremental Cryptography: The Case of Hashing and Signing,"Proc. 14th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '94), pp. 216-233, 1994.

[37] D.L.G. Filho and P.S.L.M. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer," Cryptology ePrint Archive,

[38] Dinh Tien Tuan Anh, Wang Wenqiang, and Anwitaman Datta," City on the Sky: Flexible, Secure Data Sharing on the Cloud" arXiv:1108.3915v3 [cs.DB] 21 Sep 2011