ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Re-Encryption and Replication for Sharing Data on Cloud with Third Party Auditor

Manoj V. Mohite[1], Yogesh S.Patil[2], Dinesh D. Patil[3]

P.G. Student, Department of Computer Engineering, SSGB Engineering College, Jalgaon, Maharashtra, India[1]

Assistant Professor, Department of Computer Engineering, BVM Engineering College, Jalgaon, Maharashtra, India[2]

Head of Dept., Department of Computer Engineering, BVM Engineering College, Jalgaon, Maharashtra, India[3]

ABSTRACT: So many security issues that are acquiring great attentions nowadays in Cloud computing, for the data protection, integrity, and identity management .Data protection is one of the most important security issues, because organizations won't transfer its data to remote machines if there is no guaranteed data protection from the cloud service providers. Many techniques are suggested for data protection in cloud computing, but there are still a lot of challenges in this subject. Three aspects of security are confidentiality, integrity and availability. Confidentiality is hiding information and resources. Integrity refers to the trustworthiness of data or resources, which usually prevents any incorrect or unauthorized changes. Availability refers to the ability to use the information or resource. Popular cryptographic protocols for encryption of data that establish a secure communication for clouds. Many protocols are there, which provides various security goals for cloud computing. it turns augmenting popular for data owners to outside supplier their information to public cloud servers while allowing data users to regain this data. To relate to seclusion safe searches over encrypted cloud data have become cause more research works under the sole owner model Cloud Computing is current buzzword in the market Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well, and give a proficient public trustworthiness auditing plan the problem of integrity auditing and secure replication on cloud data .Specifically, aiming at achieving data security, confidentiality and availability in cloud.

KEYWORDS: TPA (Third Party Audit), Replication, Re-Encryption, AES (Advanced Encryption Standard).

I. INTRODUCTION

Cloud computing is a way to convenient and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort. In other words, Cloud Computing is the blend of a technology, platform that provides hosting and storage service on the Internet. Main goal of the cloud computing is to provide scalable and cost effective on-demand computing infrastructures with good quality of service levels. Many organizations developing and availing cloud computing products and services but have not properly considered the implications of processing, storing and accessing data in a shared and virtualized environment. Actually, many developers of cloud-based applications desperate to include security. In other cases, developers simply cannot provide real security with currently affordable technological capabilities. Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be utilized by the client and deployed by the vendor such as amazon, google, IBM, salesforce, zoho, rackspace, Microsoft. It also shares required software's and on-demand tools for various IT organizations. Benefits of Cloud computing are enormous. The most important one is that the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is not only for Multinational companies but it's also being used by Small and medium enterprises.

Confidentiality [1].This service is used securely to protect the contents of the message and not allow to access information to any third person other than the person.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Authentication: It is related to the identification and authentication. Parties that communicate with each setup will be able to identify each other. Information receiver system, verifies the identity of the sender to see whether the information was sent by the authorized person or another person.

Data integrity: This service prevents unauthorized modification of data this service controls information access and only allows authorized persons to access data.

Availability: In case of software failure data mart loss the information of particular client duo to different causes like network down, file outage etc. Data mart takes the copy from backup warehouse. It increases the availability [2][3] of information. Data mart S1 loss the information P1, then it can take information S1 from backup warehouse and reconfigure it. If data mart S2 and S3 lost the information then they can also able to recover the information from backup ware house.

II. RELATED WORK

C. Wang, Q. Wang, K. Ren, and W. Lou [4] proposed Cloud computing can be visualized as the next-generation architecture of IT industry. Contrary to traditional solutions, where the IT services are under proper physical, logical and individual controls, cloud computing moves the application software and databases to the big data centers, where the administration of the data and services may not be fully reliable. This unique attribute, however, poses many new security challenges which have not been well understood. In this paper, focus is on cloud data storage security, which has always been an prime aspect of quality of service.

According to Sun Microsystems, Inc. [5] even though virtualization and cloud computing can help enterprises 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 typically true for the SaaS provider. Some security concerns are worth more discussion. For example, in the cloud, you lose control over resources in some respects, so your security model must be reassessed. Enterprise security is bit good enough (or better as) the least faithful partner, department, or vendor. Can you trust your data to your service provider? This excerpt discusses some aspects you should consider before answering that question.

K. Ren, C. Wang, and Q. Wang [6] proposed that Although virtualization and cloud computing can help enterprises 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 typically true for the SaaS provider. Some security concerns are worth more discussion. For example, in the cloud, you lose control over resources in some respects, so your security model must be reassessed.

M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan [7] proposed that An increasing number of online service providers offer to store user email, photos, file system backups, and other digital assets. Currently, user cannot make informed decisions about the risk of losing data stored with any typical service provider, decreasing their incentive to rely on these services. We argue that TPA is one who is prime in creating an online service oriented economy, because it allows users to analyze risks, and it increases the efficiency of insurance based risk mitigation. We describe aspects and system hooks that support both internal and external auditing of online storage services, describe catalyst for service providers and auditors to adopt these approaches, and list challenges that is required to be resolved for such auditing to become a reality.

III. EXISTING SYSTEM

In existing system decryption key is more powerful in the sense that it allows decryption of multiple cipher texts, without increasing its size.[8] In Key-Aggregate Cryptosystem, users encrypt a message not only under a public-key, but also under an identifier of cipher text called class. That means the cipher texts are further categorized into different classes. The key owners have a master-secret called master-secret key, which can be used to achieve secret keys for different classes. More significantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys that is the decryption power for any subset of cipher text classes. The sizes of cipher text, public-key, and master-secret key and aggregate key in our KAC schemes are all of constant size. The public system parameter has size in proportion to the number of cipher text classes, but only a small part of it is needed each time and it can be fetched on demand from large (but non-confidential) cloud storage.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Last results may achieve a similar property featuring a constant-size decryption key, but the classes need to conform to some pre-defined hierarchical relationship. Our work is flexible in the sense that this constraint is eliminated, that is, no special relation is required between the classes

IV. SYSTEM ARCHITECTURE

The process is carried out as follows:-

Step1: Owner sends data to cloud provider for storing.

Step2: cloud provides receive data and perform re-encryption.(AES+ Blind Sign) Cross Encryption by using two algorithms to encrypt as well as decrypt data.

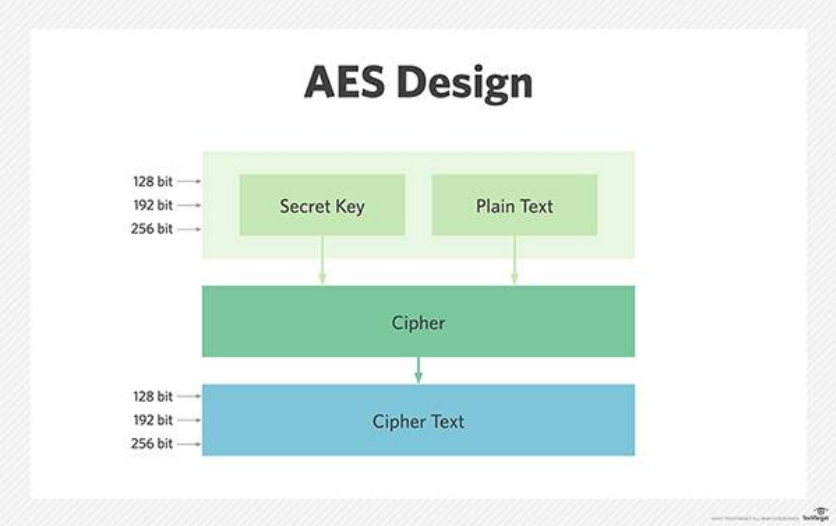

Fig:Working of AES

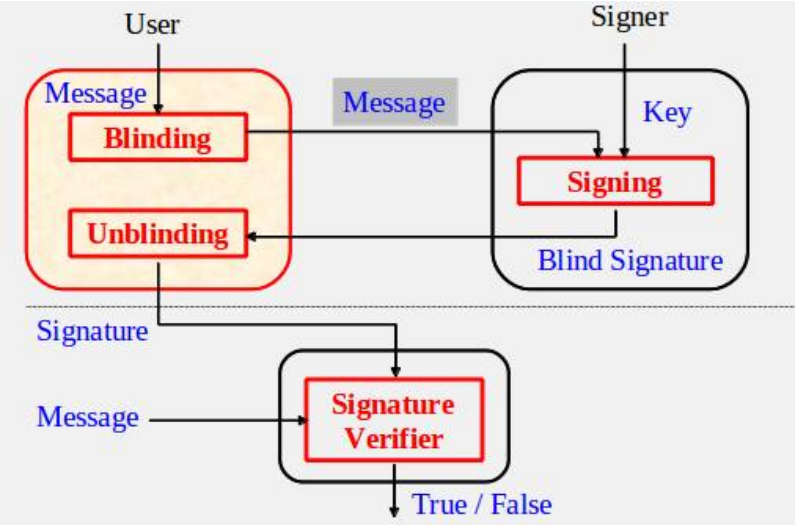

Fig: Architecture of Blind Sign Algo.

Step3: full copy of encrypted data stores on data warehouse audit by TPA.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

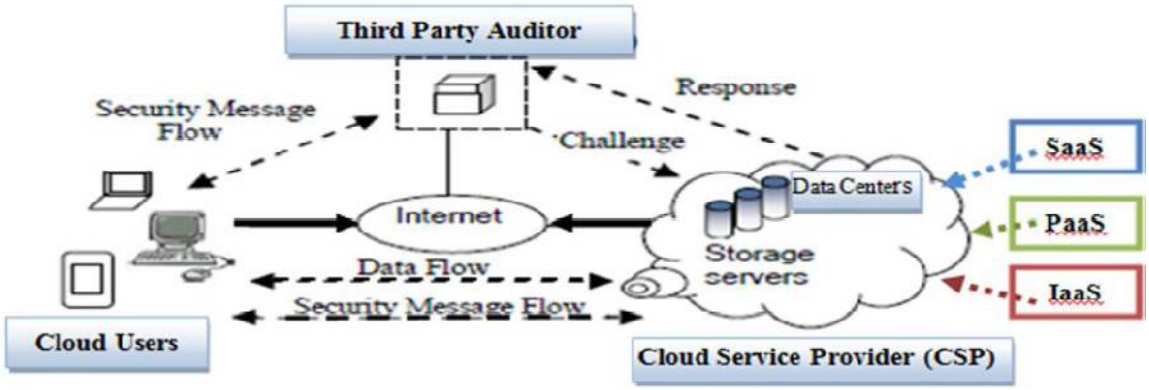

Fig: Architecture of TPA

Step4: After backup, performing replication and divide the data in parts according to the availability of data marts (in our system use three data marts S1, S2, S3). Privacy-preserving To ensure that there exists no way for verify to derive users' data from the information collected during the auditing process [9][10][11].

Step5: Storing the different part of information on different data mart.

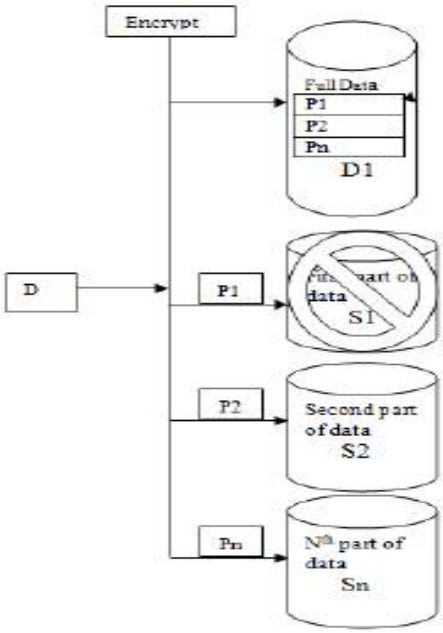

Fig: System Architecture for Replication

Step6: Repeat Steps as per storing request

If the data mart crashes or down lead to the unavailability of information. The proposed system also removes that drawback. Whenever data mart is crashes or down then client's request also able to extract the data from backup warehouse. In Proposed scenario data mart S1 is fail and not responding the user request. In this case the part of information P1 is lost. The proposed system allow user to extract the information from backup ware house. The

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

availability of data mart also effect on security of information. In case of large no of data marts the data divide in more parts and store different parts in different data marts. Each data marts have very small part of information. Whenever data mart is hacked by attacker then it can take only small part of information

1. Compared with that of its ancestor, providing binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.
2. Unlike most privileged works for assuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.
3. Not only high security [12] but also performance analysis shows that the proposed scheme is highly effective and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

In circumstances in which software fail to work data mart loss the information of particular client due to various reasons like network down, file outage etc. Data mart takes the copy from backup warehouse. It increases the availability of information. Data mart S1 lost the information P1, then it can take information S1 from backup warehouse and reconfigure it. If data mart S2 and S3 lost the information then they can also able to recover the information from backup ware house.

The data mart if crashed or down also impact on the availability of information. The proposed system also removes that drawback. Whenever data mart is crashes or down then client's request also able to extract the data from backup warehouse. In Proposed scenario data mart S1 is fail and not responding the user request. In this case the part of information P1 is lost. The proposed system allow user to extract the information from backup ware house. The availability of data mart also effect on security of information. In case of large no of data marts the data divide in more parts and store different parts in different data marts. Each data marts have very small part of information. Whenever data mart is accessed by unauthorized user then it can take only small part of information

V. FLOW OF SYSTEM

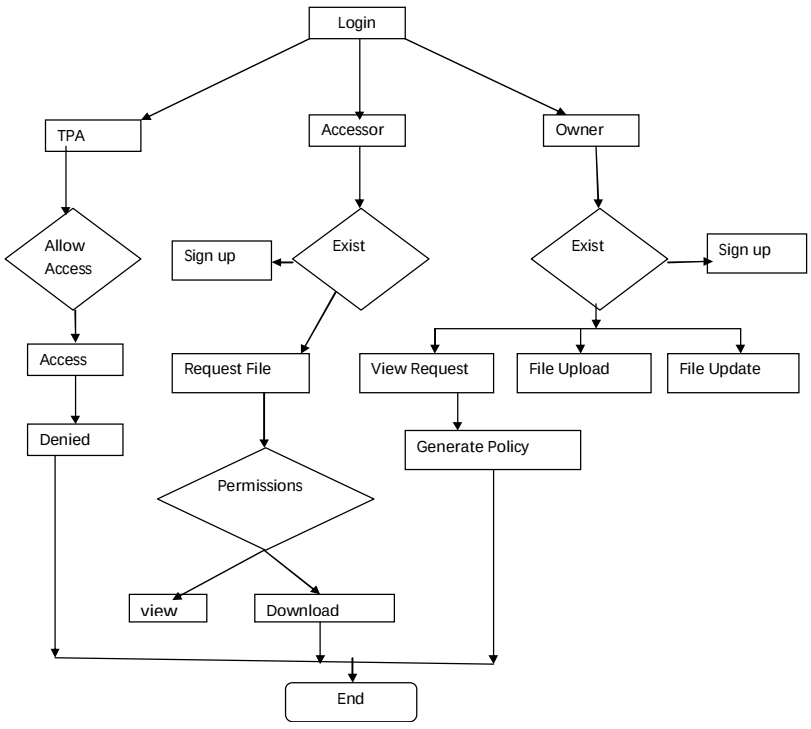

Fig: Flow Chart

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

VI. IMPLEMENTATION

User needs first register and login into system. After that he uploads his file onto the system. Then user provides the secret key for re-encryption of original data. As well as this system support dual encryption methodology like data is encrypted using secret key and secret key is also encrypted which provide better security mechanism. using two algorithm AES and Blind Sign. Similarly these algo. Used to by the requester to decrypt the file. The file is verified by the TPA before it can be accessed by requester. If the requester try to download the without verification (not possible) also file alert message is generate at the TPA login.

Fig: File uploads by owner.

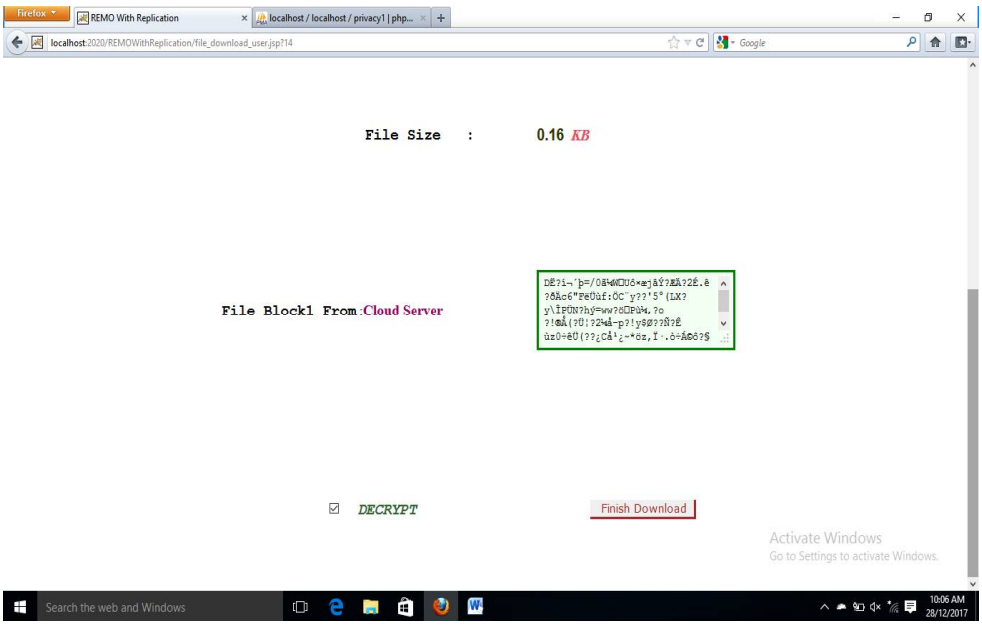

Fig: File Downloads by owner

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

VII. PERFORMANCE EVALUATION

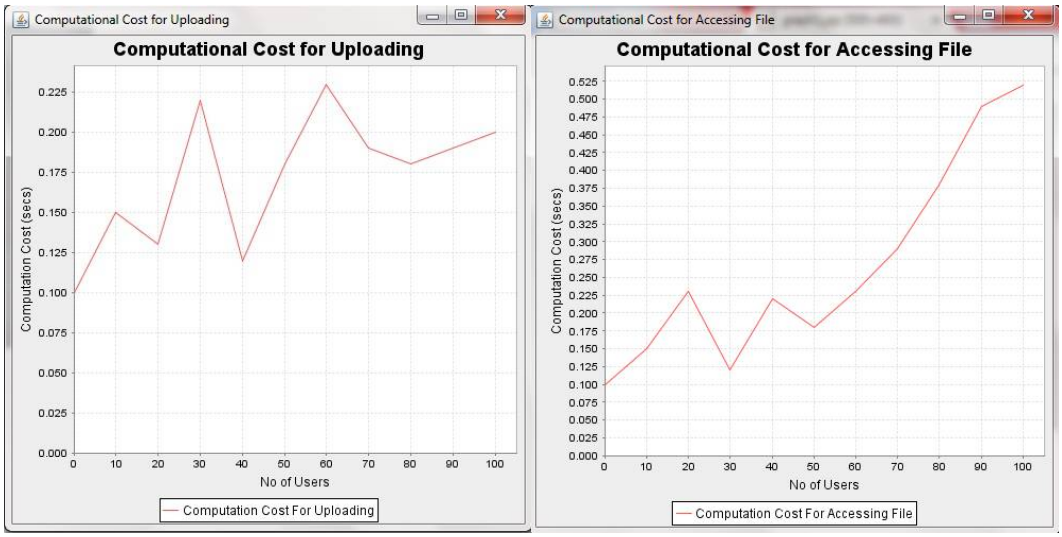

Fig:i) Computational cost achieved at uploading ii) Computational cost accessing file

VIII. CONCLUSION AND FUTURE WORK

Thus, the problem of data security in cloud storage resolved up to greater extent by Re-encryption and audit is efficiently done rights to access the data issued by owner and TPA checks valid uploads and availability increased by replication and the recovery as the replica is maintained. Thus even though database crashes the recovery is possible using any of the replicas. Future challenge is to keep consistency among replicas with minimum amount delays i.e. Response time.

REFERENCES

1. 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.
2. A. 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.
3. Amazon.com, "Amazon S3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, July 2008.
4. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Centralized Server," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), pp. 1-9, July 2009
5. Sun Microsystems, Inc., "Building Customer Trust in Centralized Server with Transparent Security," https://www.sun.com/offers/details/sun_transparency.xml, Nov. 2009.
6. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Centralized Server ," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012
7. 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.
8. Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng,‖Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage‖, IEEE Transactions On Parallel And Distributed System, Vol 25, No. 2 February 2014.
9. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Centralized Server ," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.
10. C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Centralized Storage," IEEE Trans. Computers, preprint, 2012, doi:10.1109/TC.2011.245.
11. R.C. Merkle, "Protocols for Public Key Cryptosystems," Proc. IEEE Symp. Security and Privacy, 1980.
12. 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.