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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Privacy Preserving Public Auditing in Secured Cloud Storage Using Block Authentication Code

Sajeev V[1], Gowthamani R[2]

Department of Computer Science, Nehru Institute of Technology, Coimbatore, India[1, 2]

Abstract: Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper we propose a system of auditing using BAC (Block Authentication Code)

Key words: Third Party Auditor, Block Authentication Code, Cloud computing

I. INTRODUCTION

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable, flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside exclusively on remote data centers. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. Storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc.

While these advantages of using clouds are unarguable, due to the opaqueness of the Cloud—as separate administrative entities, the internal operation details of cloud service providers (CSP)may not be known by cloud users. The correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Secondly, for the benefits of their own, there do exist various motivations for cloud service providers to behave unfaithfully towards the cloud users regarding the status of their outsourced data. Examples include cloud service providers, for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed, or even hiding data loss incidents so as to maintain a reputation. To enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantee:

- Public auditability: to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole

data or introducing additional on-line burden to the cloud users.

- Storage correctness: to ensure that there exists no cheating cloud server that can pass the audit from TPA without indeed storing

user's data intact.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

- Privacy-preserving: to ensure that there exists no way for TPA to derive user's data content from the information collected during the auditing process.

- Batch auditing: to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.

- Lightweight: to allow TPA to perform auditing with minimum communication and computation overhead.

- Considering the large size of the outsourced data and the user's constrained resource capability, the ability to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users. Therefore, to fully ensure the data security and save the cloud user's computation resources, it is of critical importance to enable public auditability for cloud data storage so that the users may route to a third party auditor (TPA), who has expertise and capabilities that the users do not, to audit the outsourced data when needed. To provide the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol, i.e., our scheme supports an external auditor to audit user's outsourced data in the cloud without learning knowledge on the data content.

- To the best of our knowledge, our scheme is the first to support scalable and efficient public auditing in the Cloud Computing. In particular, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA.

- We prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

II. ARCHITECTURE

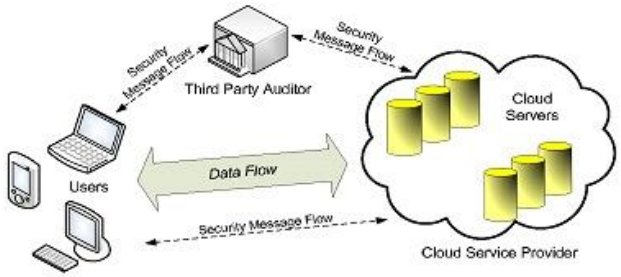

Fig 1:-Architecture of cloud data storage.

III. RELATED WORKS

- Ensuring Data Storage Security in Cloud Computing(Cong Wang, Qian Wang, and Kui Ren) Several security challenges in ensuring data storage security in large cloud systems
- Privacy Preserving Auditing and Extraction of Digital Contents(Mehul A. Shah, Ram Swaminathan, Mary Baker) Several protocols are presented that allow third party auditor to periodically verify the data stored by a service and assist in returning data intact to the customer.
- Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing(Qian Wang, Cong Wang, Jin Li, Kui Ren, and Wenjing Lou). The Merkle Hash Tree Algorithm is used for the auditing.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. PROPOSED MODEL

We propose a BAC (Block Authentication Code) for data transparent. It will overcome the existing system. That is BAC is generating the authentication code and data block is called as authentication unit. Working flow of data is: At the sender side, the authentication information BAC is generated based on a selected hash function with the packet content and a commonly agreed key as the input. Based on the value of each bit (0/1) of BAC, some packets are scheduled to be sent out with additional delays. At the receiver side, the receiver extracts the embedded BAC based on the relative packet delay and compares the extracted BAC with the BAC generated based on the received content for authentication. The following schemes are proceed in our proposed system. They are, BAC generation, BAC embedding/ BAC extraction and BAC authentication.

PROPOSED ALGORITHM

BAC GENERATION:

To present our scheme, we use the following notations:
1. The stream packets are clustered to blocks, denoted as block[i], with b packets in each block, where 0 <i< |total packet number/b|. Padding is used when necessary to generate the last block.
2. The length (in terms of bits) of the BAC for each data block is n.
3. A hash function, denoted as H(X), is a one-way hash, using an algorithm such as MD5 or SHA .
4. X,Y represent the concatenation of X with Y.
5. A secret key k is only known to the communicating parties.
6. The origin of the data stream can be identified by a flag, which is f bits, where $0 \leq f \leq n$.

ADVANTAGES OF PROPOSED MODEL

- Resource sharing is considered for data transmission.
- High security level.
- Batch Auditing can be performed.

V. SYSTEM DESIGN

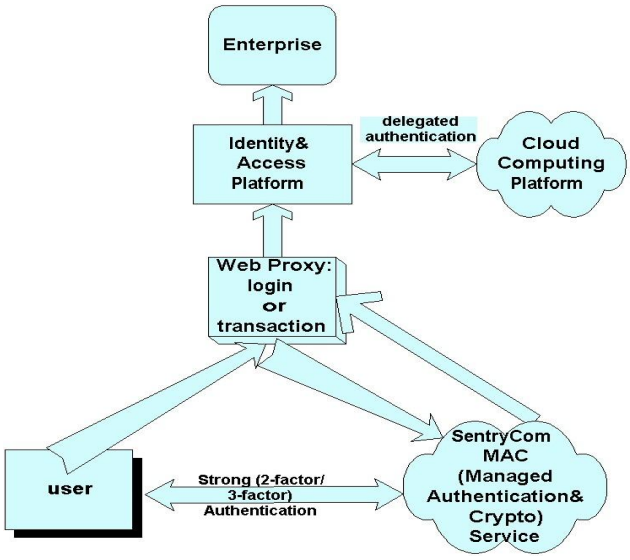

Fig2: System Design

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

VI. PERFORMANCE ANALYSIS

We now access the performance of the proposed privacy preserving public auditing schemes to show that they are indeed light weight.

Cost of privacy preserving protocol

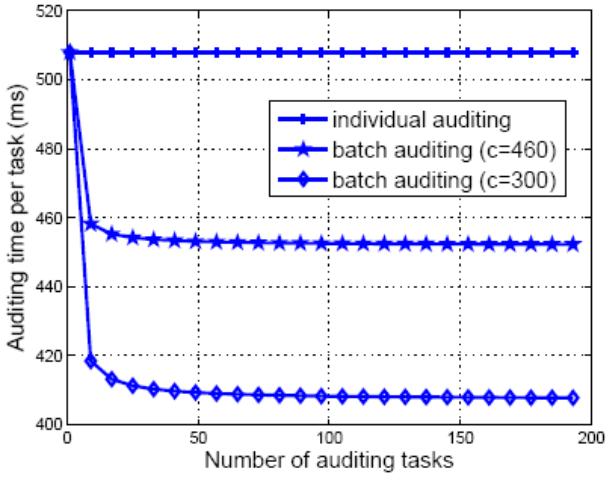

Fig 3 shows the comparison of auditing time between individual and batch auditing.

Comparison between auditing using different schemes.

The auditing using BAC is highly efficient as compared to the other schemes of auditing like Merkle Hash Tree algorithm

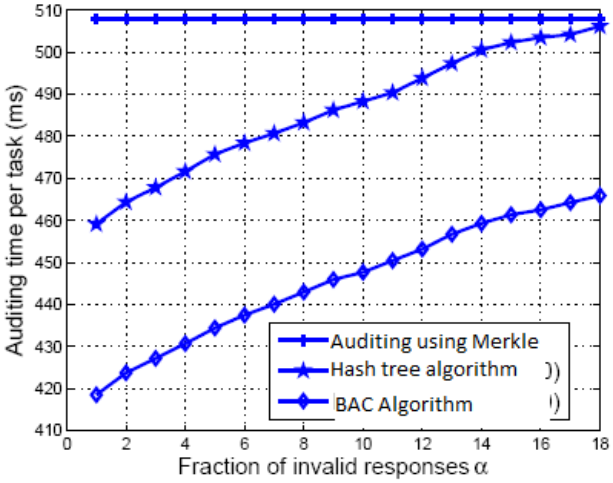

Fig4: Comparison between various schemes

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The above fig compares the auditing of Merkle Hash tree algorithm with the Block Authentication code. The auditing using BAC is done using MD5 or SHA.

VII. CONCLUSION

In this Project, we propose a privacy-preserving public auditing system for data storage security in Cloud Computing, where TPA can perform the storage auditing without demanding the local copy of data. We utilize the BAC authentication code generator. Using data blocks, authentication procedure is done and reduces the time delay. We further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner, i.e., simultaneously. Extensive security and performance analysis shows that the proposed schemes are provably secure and highly efficient. We believe all these advantages of the proposed schemes will shed light on economies of scale for Cloud Computing.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.
[2] Amazon Web Services (AWS), Online at http://aws. amazon.com.
[3] Google App Engine, Online at http://code.google.com/appengine/. Microsoft Azure, http://www.microsoft.com/azure/.
[4] 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/admnsimp/pl104191.htm,1996.
[5] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. of NDSS'01, 2001.
[6] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. of SP'02, 2002
[7] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. of SP'03, 2003.
[8] J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in Proc. of CCS'05, 2005
[9] J. Anderson, "Computer Security Technology Planning Study," Air Force Electronic Systems Division, Report ESD-TR-73-51, 1972, http: //seclab.cs.ucdavis.edu/projects/history/.
[10] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Scalable secure file sharing on untrusted storage," in Proc. of FAST'03, 2003.
[11] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. of NDSS'03, 2003.
[12] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. of NDSS'05, 2005.2006.