Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.238 – 244

RESEARCH ARTICLE

Implementation of Public Auditing for Privacy Preserving in Secure Cloud Storage

Nusrath Banu[1], Mohammed Ali Shaik[2]

[1]Pursuing M.Tech in CSE & JNTU Hyderabad, India

[2]Assistant Professor in CSE Department, ARTI, Warangal, Telangana, India

[1] nushu.banu@gmail.com, [2] niharali@gmail.com

Abstract — Cloud computing area provides solution to the problem of limited storage using which a user can remotely store his or her data and enjoy the on demand high quality applications and services from a shared pool of configurable computing resources without handling the burden of local data that is being stored and maintained but the major fact is a user no longer possess the outsourced data that makes the data integrity protection in cloud computing environment as a formidable task for the users who posses constrained computing resources which pretends to use the cloud storage as if it is local without worrying about the need to verifying the data integrity by enabling public audit ability for cloud storage as it is considered to be critical where a user can resort to a third party auditor (TPA) to check the integrity of the outsourced data and be worry free. The vulnerabilities toward user data privacy introduce no additional online burden to user and in this paper we propose a secure cloud storage system that supports privacy preserving public auditing technique which is further extended to perform audits for multiple users simultaneously and efficiently by implementing extensive security and performance analysis which is proved in the proposed scheme which is provably secure and highly efficient.

Keywords— Data storage, privacy preserving, public audit, cloud computing, batch verification

I. INTRODUCTION

In day to day life cloud computing is being utilized to its best extent and may be utilized further more in days to come in almost all areas and some of the advantages based on which we prefer using of cloud computing rather than other computing methodologies is due to on demand self-service or uninterrupted network access or due to area independent resource pooling or due to pay per use or may be due to tolerant level of risk [1].

As a developing technology with profound implications cloud computing transforms the nature of how businesses use information technology to grow itself with the utilization of all latest technologies such as cloud computing where data is centralized or outsourced over to cloud but from a user point of view when technology is being used or their related data is stored remotely to the cloud in a flexible on demand manner that brings us with

pleasing benefits such as relief of the burden for storage space management, world wide data access with location liberty and economically feasible with respect to cost of hardware or software and personnel maintenance.

Due to development and massive utilization of cloud computing brings us with new challenges in the area of security threats towards a user data that is being outsourced data to or by a cloud service provider (CSP) where data outsourcing is actually assigning user control over the fate of their own data by which the correctness of the data in the cloud is being kept at risk due to the following reasons:

- Cloud computing infrastructure is much more powerful and reliable than personal computing but it faces broad range of both internal and external threats for performing data integrity.
- When a cloud service provider acts in an unintended manner towards the cloud users regarding their outsourced data status which leads to many interpretations.
- If unfortunately the data gets corrupted user wont posses accessing or correction rights due to which user data may be lost or damaged.

Most of us will be uploading the huge amount of data on cloud and most often users will upload data that does not fit on their own computer or mobile phone and then comes the task of auditing the data correctness in a cloud environment which can be considered to be exception prone and expensive for a cloud user but we need to minimize it as much as possible such that a user does not prefer to perform too many operations as a user may not want to go through the complexity in verifying the data integrity as more than one user accesses the same cloud storage it is desirable that cloud only entertains verification request from a single user.

To fully guarantee the data integrity and to save a cloud users computation resources as well as online burden it is very important to enable public auditing service for cloud data storage such that users may be addicted to an independent third party auditor (TPA) to audit the outsourced data when as and needed where a TPA is an expert in his or her area or domain where a user needs him and auditing is carried on periodically basis where the integrity of all the data stored in the cloud on behalf of the users which provides a much more easier and affordable way for the user to ensure their storage correctness in the cloud and in addition to help users to evaluate the risk of their subscribed cloud data services the audit result given by a TPA would also be beneficial for the cloud service providers to improve their cloud based service platform.

Due to massive increase in technology and cost cutting strategies the concept of public auditing has been emerged for ensuring remotely stored data's integrity under different system and security models [2] the system of public auditing allows an external party in addition to the user himself or herself to verify the correctness of remotely stored data to implement privacy protection of users data against external auditors as they may reveal user's data to auditors which may greatly affects the security of these protocols in cloud computing when a external auditor is involved since there is scope of vulnerabilities of unauthorized information leakage toward their data security and in order to overcome this situation we need to simply provide the encrypted data before outsourcing it to an external auditor.

II. PROBLEM STATEMENT

In this paper we consider three types of people involved and they are 1) cloud user or a data owner is a person who will be deploying large amounts of data onto a cloud and will be bearing all the expenses related to storage and services of a cloud server system. 2) is the cloud service provider who installs and maintains the cloud with required application program interface and some significant storage capabilities and 3) is the third party auditor which may be a single person or a organization who is hired to audit the data by a cloud user for consistency and maintenance of data which is backed up periodically and maintain all the specifications being provide by cloud service provider.

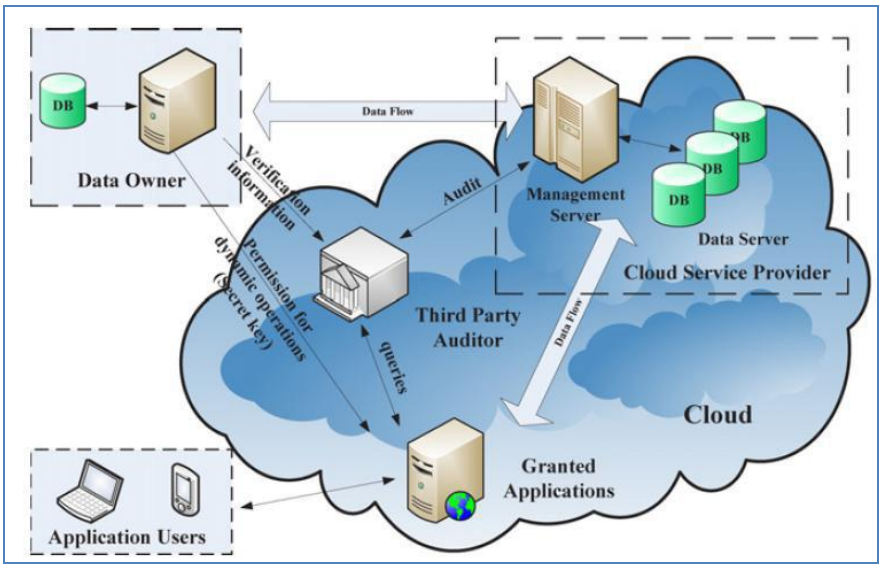

Fig. 1 Architecture of cloud data storage service.

The above figure Fig1 specifies the architecture of proposed system which is based on the cloud data storage service where a cloud service provider maintains multiple databases and many management servers will be installed which may be arranged in a parallel or distributed architecture depending on its specifications a granted applications server will be delivering data to the end users or application servers.

There are many types of attackers in today's world but broadly speaking there are two types of attackers such as internal attacker and external attacker where a internal attacker is a unsatisfied employee of same organization and the external attacker is a external intentional who wants to access the data or files in any case an attack may be software bugs, hardware failures or bugs in the network path or economically motivated hackers, or any other case such as a cloud service provider for creation reputation may add or modify some part of our files or data and the proposed solution in using third party auditor we can check the files on demand towards the above mentioned discrepancies or file corruption or data corruption and the only risk in this approach is when an auditor outsources the task to sub auditors since we can't rely on everyone.

III. PROPOSED SYSTEM & IMPLEMENTATION

This section we propose a solution space for the above specified problem space which comprises of complete outsourcing solution of the data along with the integrity checking by providing two schemes which delegate notifications to users who expect data dynamics.

We provide a algorithm which performs four tasks such as 1) KeyGenerator() the task is to generate a random key with the life time of the key for a certain extent or time span using 128 bit SHA1 algorithm using MD5 message digest. 2) SignatureGenerator() a digital signature is generated based on the user where every user will be having different signature or unique signature or private key based on 64 bit DES algorithm 3) GenProof() is the result generated by a cloud server to generate a proof of data storage 4) VerifyProof() is a part of program which is run by the auditor and results will be generated based on the implementation of tasks.

The whole process will go like this firstly user initializes the public and secret parameters of the system by executing KeyGenerator() function and preprocess a specific data file by using SignatureGenerator() to generate the verification metadata and the user then stores the data file and the verification metadata at the cloud server and deletes its local copy as part of preprocessing the user may alter the data file by expanding it or including additional metadata to be stored at server then the auditor may issues an audit message to the cloud server to make sure that the cloud server has retained the data file properly without any discrepancies at the time of the audit which results into a response message by a cloud server on executing GenProof() by giving file and its verification metadata as inputs and then the auditor and user will verifies the response towards consistency of cloud data using VerifyProof() method.

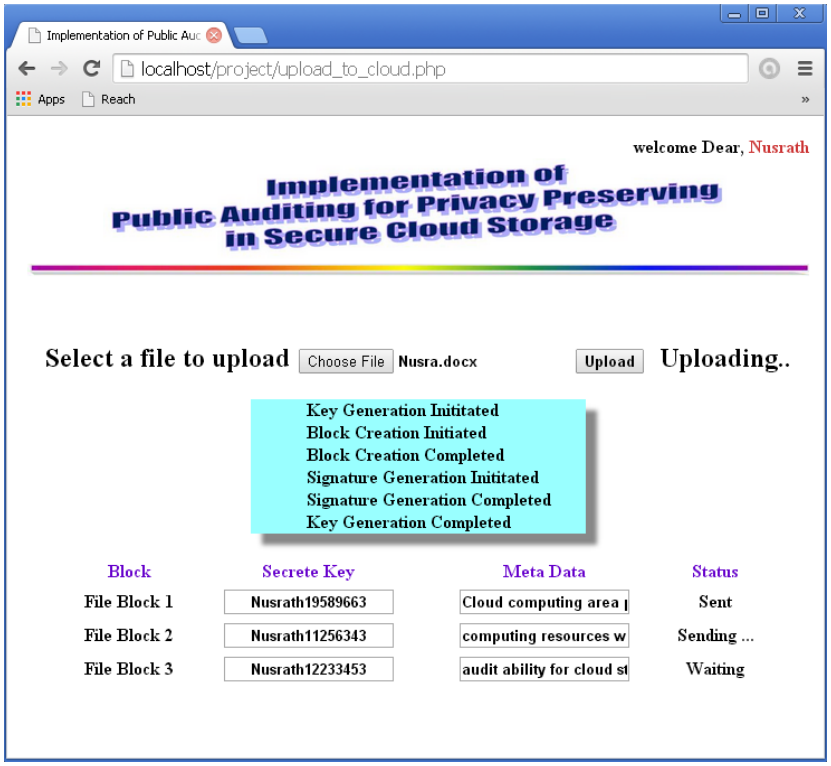

Fig. 2 Uploading a file to cloud by a data owner.

In the above figure Fig2 we are uploading a file to cloud after performing login operation as we have registered with only once cloud and performing this application so we are not selecting which cloud and the implemented cloud is a PHPCloud, once the file is uploaded then the file will be splitted into equal length blocks here in this application we have divided block size to be 15kb due to which only three blocks have been created because the file size we have selected is of 40.8kb so it is splitted into three blocks as shown in the figure and secrete key is randomly generated and metadata is shown.

The Below figure Fig3 represents generation of GenProof() methods implementation where all the list of files being deployed to the cloud will be generated with the proofs using the 128 bit key which will be given to the auditor to verification or auditing purpose or sometimes user himself or herself will be performing this auditing task. In the below screen once we hit the Generate button the process begins by first initiating proof generation process and once the task is completed then the proof generation completed status will be displayed and in the below section all the list of files uploaded to PHP cloud will be displayed along with the generated proof key which a user can view or download as a separate file or by hitting the Download All button all the proof keys can be generated in a single file, depending on the requirement of a user we can give a single file to an auditor or complete list of files in the cloud can be given.

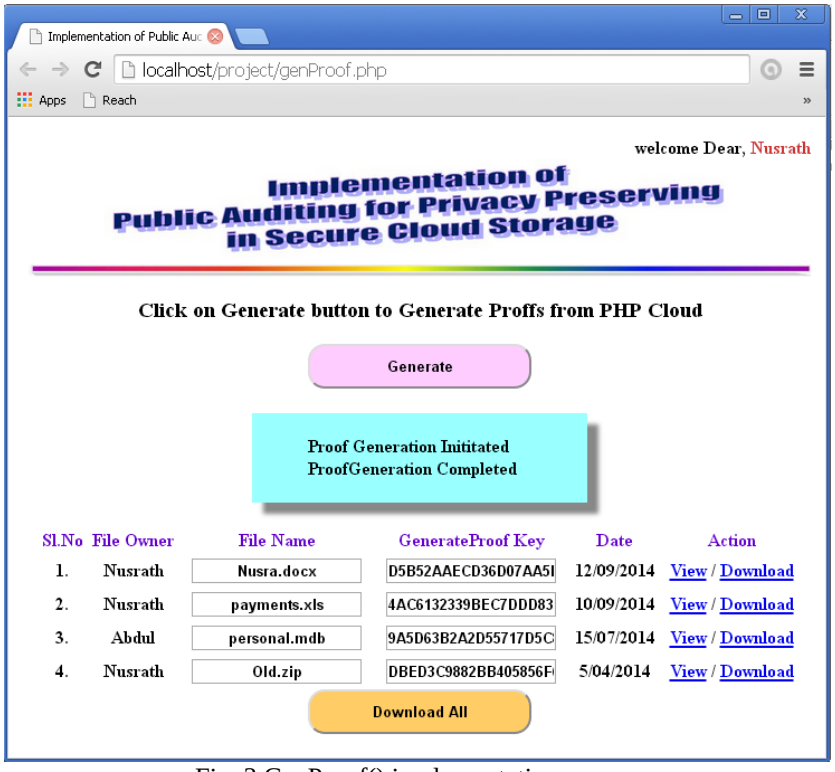

Fig. 3 GenProof() implementation screen.

In our proposed system to achieve the privacy preserving public auditing we integrate the homomorphic linear authenticator with random masking technique where the linear combination of sampled blocks in the server response is masked with random number generated by the server by which auditor will not be able to build up a correct group of linear equations and therefore cannot view the user data which is in encrypted form even though when a auditor or attacker tries to attack or decrypt a file it is possible to only some extent may be to a single block since we are applying block level separate key by which block level security is achieved.

And there is no scope for anyone to identify that into how many blocks a file is being divided since every block is of same size and each file is divided into fixed size of blocks so it is almost impossible to find each block and try to compromise it either by an auditor or an attacker.

The below figure fig4 represents the status being received by the auditor which comprises of list of files on which auditing is being performed with date and time of auditing performed, when the result of audit is accurate then auditor will take no action but when the file is corrupted then the file need to be re deployed and but when status is found malicious then auditor finds the IP address from which the attack had being initiated and if the cloud is compromised then auditor will take security actions by implementing some stealth tools and re deploys the attacked files.

Fig. 4 status report by an auditor

For reporting the performance results of our proposed solution space for the above mentioned problem space we used Weka 6.0 to generate working results when the user data is outsourced with an Intel Dual Core processor running at 2.56 GHz and with 3 GB of RAM on PHP cloud with space of 10TB is shown in below figure fig.5:

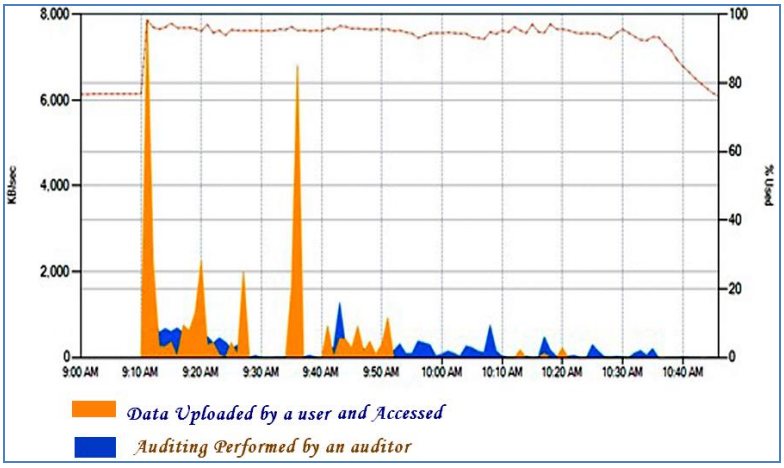

Fig. 5 Performance chart of the proposed system.

IV. CONCLUSION

In this paper we have proposed a scheme for handling privacy preserving public auditing system for data storage security in cloud computing environment that uses homomorphic linear authentication technique using random masking technique to guarantee that the third party auditor will not extract any knowledge stored or about the data available on the on the cloud server while performing batch auditing process and also we proposed that system which will not allow a hacker to attack data on the cloud by which data leakage on cloud is efficiently handled from both internal and external attackers.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html, June 2009.
[2] 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, 2007.
[3] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.
[4] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.
[5] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," http://www.cloudsecurityalliance.org, 2009.

