Efficient and Secure Data Preserving in Cloud Using Fog Security

M. Shalima Sulthana* and V. Sandeep Kumar Reddy

 # Student of M.Tech, SSITS, Rayachoti, Kadapa, Andhra Pradesh, India

 # Department of CSE, SSITS, Rayachoti, Kadapa, Andhra Pradesh, India

Abstract*— The computing is centralized computing also called as Cloud computing which provides centralized access of data storage, processing and use of other applications and systems. The cloud computing provides on demand high quality applications and services in wired and wireless environment. It provides various applications and services to used a shared pool of configurable computing resources. As the data of the cloud users is outsourced and there is log burden to the server due to high storage and processing. As the cloud usage is increased in large size sector there I s a challenging issue to provide security and auditing to the stored data in the cloud server. The aim of the project is to provide enhanced privacy security and auditing features to the cloud usage. The project provides public auditing with third party, who can make auditing without making a copy of data and gives protection from hackers by fog or bluff data. Through external auditing and fog computing there provides data integrity and security for outsourced data. To provide high security and introduce an trust and effective external party auditing, the following two fundamental requirements are provided, Third party can make auditing without any copy of data and gives protection to the third party auditing. Secondly gives fog security from third party and other malicious attackers.

Index Terms—**Backup; Privacy; Central Repository; Remote Repository, Parity cloud, Parity Cloud Service.**

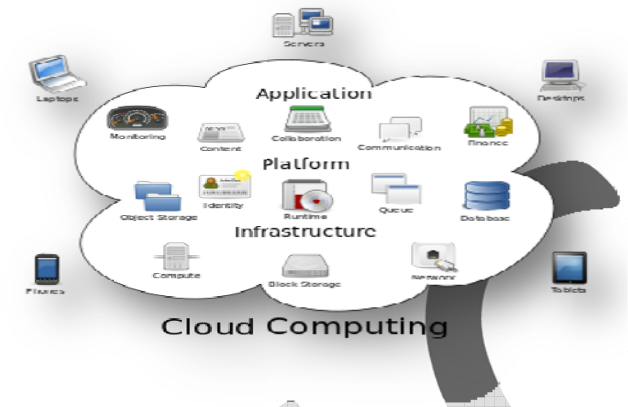
Manuscript received July, 2014. ***M. Shalima Sulthana***, *Student of M.Tech, Department of CSE, SSITS, Rayachoti, Kadapa, Andhra Pradesh, India. Email:m.s.sulthana2012@gmail.com*

V. Sandeep Kumar Reddy, *Associate Professor Department of IT, SSITS, Rayachoti, Kadapa y, Andhra Pradesh, India. Email:sandeepreddy.1223 @gmail.com*

I. INTRODUCTION

The next generation computing is Cloud computing, where we have centralized computing resources (both hardware and software) and the centralized resources are delivered as service over a network i.e. Internet, Intranet or Extranet. Cloud Computing provides huge storage, processing, applications, Operating systems, Network and various other infrastructures, all the specified features are centralized in big server called cloud server. These features can be accessed in various shapes required by the surfer, they can access in Systems, Mobiles, Tabs and other media required. Briefly discussing the common use of cloud is a symbol of abstraction in a complex infrastructure in centralized location. Cloud computing provides trust to remote services with a user's data, software, applications, security and computations accessed in any media. Central Cloud computing consists of hardware, Software and Application resources made available on the Internet and Mobile wireless technology as managed by third party services, all the cloud servers are accessed to third party and from third party users or surfers take access to use the resources in their required form. These services typically provide access to advanced software applications and high-end networks of server computers.

The next generation of computing in Internet will be cloud computing, through cloud computing we can reduce the infrastructure, maintenance of huge systems and provide green computing with one centralized system providing resources services to a wide range of users. To overcome the drawbacks of investment, maintenance and over rid of attackers the proposed architecture is cloud architecture. The following figure shows the structure of cloud computing.



II. LITERATURE SURVEY

A literature survey or literature review means study of references papers and old algorithms that we have read for designing the proposed methods. It also helps in reporting summarization of all the old references papers, their drawbacks. The detailed literature survey for the project helps in comparing and contrasting various methods, algorithms in various ways that have implemented in the research.

The literature study prescribed in this research of the project, supports high availability of data, Various algorithms, Various old references papers, comparison of the methods. This design supports various types of jamming attacks preventions like combined cryptography methods, strong commitment methods, elliptic method and all or nothing methods.

RELATED WORK OR LITERATAURE STUDY

Privacy MAC Based Solution and Study

Privacy Based Mac authentication provides user data to be authenticated using random data blocks. This operation provides the surfer or user to upload data blocks and to cloud server and provide its secret key to Third party auditor. The External auditor is having chance of making blocks and retrieve data blocks with user secret key to check correctness of stored data on the cloud. Problems with this system are listed below as

- No Security for key, as third party gets the key to making auditing of user transactions.
- The server online burden is increased due to download and upload operations in a single system.
- Data Communication & computation are huge complexity due to multi keys maintains in the server.
- Third party requires knowledge of user keys and the data blocks for verification
- It supports only for static data not for dynamic data processing in online cloud server processing.

Third Party Based Solution

It supports efficient public auditing without retrieving data block. It is aggregated and required constant bandwidth. It is possible to compute an aggregate Third party based solution which authenticates a linear combination of the individual data blocks.

Privacy Preserving Public Auditing Proposed by Cong Wang

The privacy public auditing allows the third processing auditing, along with user to check the integrity of the outsourced data stored on a cloud & Privacy Preserving allows third party auditing to do auditing without requesting for local copy of the data. Through this scheme, TPA can audit the data and cloud data privacy is maintained.

III. EXISTING AND PROPOSED SYSTEM

EXISTING SYSTEM:

In the Existing systems, the notion of public audit ability has been proposed in the context of ensuring remotely stored data integrity under different system and security models. Public audit ability allows an external party, in addition to the user himself, to verify the correctness of remotely stored data. However, most of these schemes do not consider the privacy protection of users' data against external auditors. Indeed, they may potentially reveal user's data to auditors. This severe drawback greatly affects the security of these protocols in cloud computing. From the perspective of protecting data privacy, the users, who own the data and rely on TPA just for the storage security of their data, do not want this auditing process introducing new vulnerabilities of unauthorized information leakage toward their data security.

Disadvantages

- 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.
- Does not provides external security from hackers.
- No batch auditing reports provided by the cloud servers.
- Second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status.
- In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those un accessed data and might be too late to recover the data loss or damage.
- Encryption does not completely solve the problem of protecting data privacy against third-party auditing but just reduces it to the complex key management domain. Unauthorized data leakage still remains possible due to the potential exposure of decryption keys.

PROPOSED SYSTEM:

In this project, it provides homomorphic authenticator, Batch auditing and Fog Mitigating security technique to achieve a privacy-preserving public auditing system with enhanced fog security from malicious attackers. In Cloud servers for cloud data storage by the data owners we require a high security keeping all above requirements of the customer in mind. To support efficient handling of multiple auditing tasks, Enhanced security and Fog Mitigating we further explore the technique of fog security, homomorphic encryption and to extend our main result into a multi-user setting. In the multi user concept a user can perform multiple tasks simultaneously. Extensive fog security and performance analysis shows the proposed schemes are provably secure and highly efficient. Fog security restricts the attackers from theft of data. We also show how to extent our main scheme to support batch auditing for user activities upon delegations from users.

Advantages

Public auditability: Cloud servers provides to allow the external party to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.

Fog Security: provides fog data in the cloud, when a malicious attacker attacks the server the server provides fog data instead of restricting the user.

Storage correctness: The project provides to ensure that there exists no cheating cloud server that can pass the external processing by the audit without indeed storing users' data intact.

Privacy preserving: Provides a high security with external security to ensure that the external party cannot derive users' data content from the information collected during the auditing process.

Batch auditing: The project is extended with multiple auditing and secure efficient auditing capability to cope with multiple auditing operations from possibly large number of different users activities simultaneously

IV. MODULES OF THE PROJECT

SYSTEM MODEL MODULE

In this module, first we develop four users to show the operations of the project: User, Cloud Service Provider , **Hacker and Third Party Auditor:**

User: users, who makes registration and pays amount to the cloud server and cloud server provides data to be stored in the cloud and rely on the cloud for data and other computation, Generally user consist of both single or individual consumers and big organizations.

Cloud Service Provider (CSP): a CSP is also called administrator, who has significant resources and expertise in building and managing distributed cloud resources and storage servers, owns and operates live Cloud Computing systems.

Hacker: Hacker is shown in the project, to extend the fog security from malicious hacking activities from hacker.

Third Party Auditor (TPA): The external third party, who has expertise and capabilities and access to the cloud to make auditing of user assess without getting the copy of the data of the user. The auditing is done as trusted process on behalf of the user interest.

TPA MODULE

In this module, we develop external TPA, External Third Party Auditor, independent third party auditor, making the cloud storage publicly verifiable. However, as pointed out by the recent work, to securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy. Namely, TPA should not learn user's data content through the delegated data auditing.

PRIVACY PRESERVING MODULE

In this module, we develop a privacy preserving security as a secure cloud system where, we ensure that the external third party cannot derive users' data content from the information collected during the third party auditing process. We motivate the public auditing system for users, on user behalf the data storage security in cloud computing and provide a privacy-preserving auditing protocol for external auditing without copying the data. Our providing protocol or scheme enables an external TPA auditor to audit user's cloud data without learning or copying the data content. To the best of our knowledge, we have designed a new protocol scheme is the first to support scalable and efficient privacy-preserving public storage auditing in cloud.

BATCH AUDITING

In this module, we develop 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. Specifically, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner

V. DISCUSSION AND CONCLUSION

In this project, we propose a privacy-preserving public auditing system with enhanced fog data storage security

in cloud computing. We have utilize the homomorphic and fog security linear authenticator and random masking to guarantee that the external third party would not learn or have copy of data content stored on the cloud server during the efficient auditing process, The proposed system not only eliminates the burden of cloud user activities from the tedious and possibly expensive auditing task, Malicious attackers and other users' fear of their outsourced data leakage. Considering the extensibility the project is provided with concurrently handle multiple audit sessions, Fog security to the data stored in the cloud and Third party auditing without copying the data which is outsourced, we further extend our privacy-preserving public auditing protocol into a multiuser and batch auditing 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.

FUTURE ENHANCEMENTS

Our preliminary experiment conducted on some external servers like Amazon instance further demonstrates the fast performance of our design on both the cloud and the auditor side. We leave the full-fledged implementation of the mechanism on commercial public cloud as an important future extension, which is expected to robustly cope with very large scale data and thus encourage users to adopt cloud storage services more confidently

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST working definition of cloud computing," Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2009.

[2] 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.

[3] M. Arrington, "Gmail disaster: Reports of mass email deletions," Online at http://www.techcrunch.com/2006/ 12/28/gmail-disasterreports-of-mass-email deletions / , December 2006.

[4] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors," Online at http://www.techcrunch. com/2008/07/10/ mediamaxthelinkup-closes-its-doors/, July 2008.

[5] Amazon.com, "Amazon s3 availability event: July 20, 2008," Online at http://status.aws.amazon.com/s3-20080720.html, 2008.

[6] S. Wilson, "Appengine outage," Online at http://www. cio-weblog.com/50226711/appengine outage.php, June 2008. [7] B. Krebs, "Payment Processor Breach May Be Largest Ever," Online at http://voices.washingtonpost.com/securityfix/ 2009/01/payment processor breach may b.html, Jan. 2009.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.

[9] M. A. Shah, R. Swaminathan, and M. Baker, "Privacypreserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[10] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370.

[11] A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.