A NOVEL METHOD OF DIRECTLY AUDITING INTEGRITY ON ENCRYPTED DATA

[1] K.Sumalatha, [2]M.N Sinduri, [3]C.BhanuPrakash

[1]*Asst. Prof., Dept., of CSE, AITS, Tirupati, A.P., INDIA.*

[2]*PG Scholar, Dept., of CSE, AITS, Tirupati, A.P., INDIA.*

[3]*Asst. Prof., Dept., of CSE AITS, Tirupati, A.P., INDIA.*

ABSTRACT

Now-a-days, cloud computing is providinggreater amount of storage space and massive parallel computing at effective cost. Excessive amount of data is being stored in the cloudsince the cloud computing is becoming more prevalent. However, the exponential growth of ever-increasing volume of the data has raised more number of new challenges. In this work, the problem with integrity auditing and the secure de-duplication present on cloud data is studied. Particularly, the focusis on achieving both the data integrity and de-duplication which is present in cloud, two secure systems is proposed called SecCloud and SecCloud+. The SecCloudwill offer an auditing entity with the maintenance of a Map Reduce cloud that assist clients in order to generate the data tags before they are being uploaded as well as to audit the integrity of data that is being stored in cloud.

Keywords: Seccloud , integrity auditing , seccloud+, proof of ownership convergent encryption,secure de-duplication.

INTRODUCTION

Although the cloud storage system has been mostly adopted, it still fails in accommodating some important emerging requirements such as the capability of auditing integrity of cloud files by cloud clients and also detectionof duplicated files by cloud servers. Both problems are disclosed below. The initial problem is integrity auditing. The cloud server is capable of relieving clients from the bulky burden for storage management and also maintenance. The main difference of cloud storage from the traditional in-house storage is that the data is transferred through Internet and it is stored in an uncertain domain that is notat all under control of the clients that inevitably raiseclient'sto great concerns based on the integrity of their data. These concerns are originated from the fact that the cloud storage will be affected to security threats from both the outside and inside of the cloud and in order to maintain their reputation the uncontrolled cloud servers may passively hide some data loss incidents obtained from the clients. The more serious problem is that the cloud servers might even actively and deliberately discard barely accessed data files which belong to an ordinary client in order to save money and space. With the consideration of large size of the outsourced data files and the clients' constrained resource capabilities, the initial problem is generalized as how the client can efficiently perform based on regularly integrity verifications even without the presence of local copy of data file.

LITERATURE SURVEY

Enabling Public Verifiability and Data Dynamics for the purpose of Storage Security present in Cloud Computing
Author: Qian Wang
The Cloud Computing system has been developed as the next-generation architecture of IT Enterprise. It will move the application software and also databases for the centralized along with large data centers in which the management of the data and services will not be fully trustworthy. Many of the new security challenges are brought with this ensampleand they have not been well understood. This research work will examine regarding the problem of assuring the integrity of data storage present in Cloud Computing. Particularly, the task of allowing a third party auditor (called TPA) is considered based on concern of the cloud client for verifying the integrity of the dynamic data that is stored in the cloud. The TPA introduction will dismiss the involvement of client through the auditing whether the user's data is truly stored in the cloud intact that is important during achieving economies of scale for Cloud Computing. For

data dynamics the support through the most common forms of data operation, such as block modification, insertion and deletion, is also considered as more powerful step to - ward practicality, as the services present in Cloud Computing were not limited to archive or for backup data only. The Presiding work on ensure remote data integrity will often lack the support of either public verifiability or the dynamic data operation.

Provable Data Possession during Untrusted Stores Authors: Giuseppe Ateniese

A model for provable data possession (PDP) is introduced that allows a client which has stored data present at an untrusted server for verifying that the server possesses the original data without the retrieval of it. The model will generate probabilistic proofs of possession through sampling random sets of blocks obtained from the server that drastically reducethe I/O costs. The client will maintain a constant amount of metadata in order to verify the proof. The challenge or response protocol will transmit a small and constant amount of data that minimizes the network communication. Hence, in case of widely distributed storage system the PDP model for remote data checking will support large data sets.

Remote Data Checking by Using Provable Data Possession Authors: Giuseppe Ateniese

A model for provable data possession (PDP) is suggested that can be used for the purpose of remote data checking: A client who has stored data present at an untrusted server may verify whether that the server possesses the original data without the retrieval of it. The model will generate probabilistic proofs of possession through the sampling of random sets of blocks obtained from the server that drastically reduces I/O costs. The client will maintain a constant amount of metadata for verifying the proof. The challenge or response protocol will transmit a small and constant amount of data that will minimize the network communication. Hence, the PDP model for remote data checking is of lightweight and supports large data sets in case of distributed storage systems. The model is also robust in which it incorporates mechanisms to mitigate the arbitrary amounts of data corruption.

A Survey on Secure Authorized De-duplication present in Hybrid Cloud Now-a-days, cloud computing is providinggreater amount of storage space and massive parallel computing at effective cost. Excessive amount of data is being stored in the cloud as the cloud computing becomes more prevalent. However, the exponential growth of ever-increasing volume of data has raised many of the new challenges. The De-duplication technique is regarded as specialized data compression technique that eliminates redundant data as well as it will improve storage and bandwidth utilization. The Convergent encryption technique is proposed in order to enforce confidentiality in case of de-duplication that will encrypt the data before outsourcing. For better protection of data security, various privileges of user to address problem of authorized data de-duplication are introduced. Several new de-duplication constructions that support authorized duplicate check present in hybrid cloud architecture are presented which will incur minimal overhead than to the normal operation.

PROPOSED SYSTEM

It is determined that the proposed SecCloudsystem has achieved both integrity auditing and also files de-duplication. However, this cannot avoid the cloud servers from knowing the content of file s that have been stored. In the other words it is said that the functionalities of integrity auditing and secure de-duplication were only imposed on plain files. In this section, SecCloud+is proposed which will grant for integrity auditing and de-duplication present on encrypted files. The System Model when compared with SecCloud, the recommended SecCloud+ will involve further trusted entity called key server, that is responsible in assigning clients with the secret key (based on the file content) for the purpose of encrypting files. This architecture is present in line with the recent work. But our work is distinguished with the past one by allowing for integrity auditing present on encrypted data. SecCloud+ will follow the same three protocols (i.e., the file uploading protocol, the integrity auditing protocol and the proof of ownership protocol) as with the SecCloud. The only anomaly is that the file uploading protocol present in SecCloud+ will involveadditional stages for the communication among cloud client and also key server. The client requires during communicating with the key server in order to get the convergent key to encrypt the uploading file before the phase in Sec Cloud.

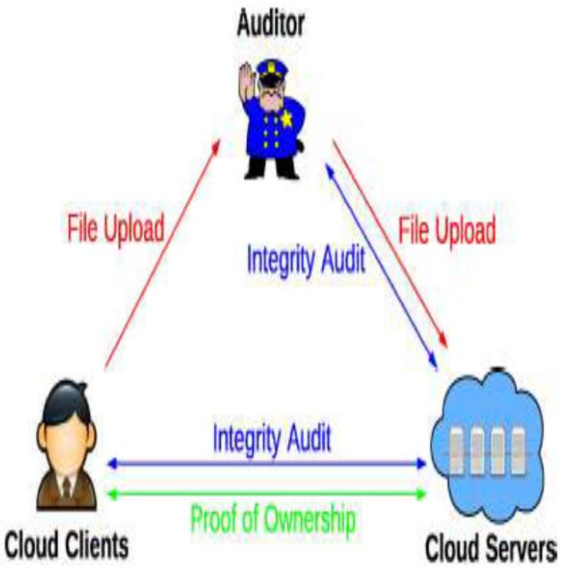

Fig: proposed system

CONCLUSION

We mainly focus on achieving both data integrity and data de-duplication present in cloud, SecCloud and SecCloud+ are proposed. The SecCloud will introduce an auditing entity with the maintenance of a Map Reduce cloud that helps the clients in generating data tags before uploading and audit the integrity of data that have been stored in cloud. In addition, SecCoud will enable secure de-duplication with the introduction of Proof of Ownership protocol (called POP) and prevents the leakage of side channel information present in de-duplication. Compared with the existing work, the computation by user in case of SecCloud is greatly reduced during the file uploading and auditing phases. The Sec - Cloud+ is an advanced construction that is motivated by the fact that customers will always require their data to be encrypted before uploading, and

it allow for integrity auditing as well as the secure de-duplication directly on to the encrypted data.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I.Stoica, and M. Zaharia , ―A view of cloud computing,‖ Communication of the ACM, vol. 53, no. 4, pp.50–58, 2010.

[2] J. Yuan and S. Yu, ―Secure and constant cost public cloud storage auditing with deduplication,‖ in IEEE Conference on Communications and Network Security (CNS) , 2013, pp. 145–153.

[3] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, ―Proofs of ownership in remote storage systems,‖ inProceedings of the 18th ACM Conference on Computer and Communications Security . ACM, 2011, pp. 491–500.

[4] S. Keelveedhi, M. Bellare, and T. Ristenpart, ―Dupless: Serveraided encryption for deduplicated storage,‖ in
Proceedings of the 22Nd USENIX Conference on Security, ser. SEC'13. Washington, D.C.: USENIX Association, 2013, pp. 179–194. [Online]. Available:https://www.usenix.org/conference/usenixsecurity13/technicalsessions/presentation/bellare

[5] G. Ateniese, R. Burns, R. Curt mo la, J. Herring, L. Kissner, Z. Peterson, and D. Song, ―Provable data possession at untrusted stores,‖ in Proceedings of the 14th ACM Conference on Computer and CommunicationsSecurity, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 598–609.

[6] G. Ateniese, R. Burns, R. Curt mo la, J. He rring, O. Khan, L. Kissner, Z. Peterson, and D. Song, ―Remote data checking using provable data possession,‖ ACM Trans. Inf. Syst. Secur., vol. 14, no. 1, pp. 12:1–12:34, 2011.

[7] G. Ateniese, R. Di Piet ro, L. V. Mancini, and G. Tsudik, ―Scalable and efficient provable data possession,‖ in
Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, ser. Secure Comm '08. New York, NY, USA: ACM, 2008, pp. 9:1–9:10.

[8] C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, ― Dynamic provable data possession,‖ in
Proceedings of the 16th ACM Conference on Computer and Communications Security , ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 213–222.

[9] F. Seb´e, J. Domingo-Ferrer, A. Mart inez-Balleste, Y. Deswarte, and J. -J. Quisquater, ―Efficient remote data possession checking in critical information infrastructures,‖ IEEE Trans. on Knowl. and Data Eng.,vol. 20, no. 8, pp. 1034–1038, 2008.

[10] H. Wang, ―Pro xy provable data possession in public clouds,‖IEEE Transactions on services Computing, vol.
6, no. 4, pp. 551–559, 2013.

[11] E. H. Miller, ―A note on reflector arrays (Periodical style—Accepted for publication),‖IEEE Trans. Antennas Propagat., to be published.

[12] J. Wang, ―Fundamentals of erbiu m-doped fiber amplifiers arrays (Periodical style—Sub mitted for publication),‖IEEE J. Quantum Electron., submitted for publication.

Author Details

Mrs.K.Sumalatha received her M.tech Degree in Computer Science from JNTUA, Anantapuram in 2010 and B.Tech Degree in Computer Science and Engineering from JNTUH, Hyderabad in 2007. Currently she is working as an Assistant Professor in Annamacharya Institute of Technology and Sciences, Her areas of interest include software Engineering, Computer Architecture and Cloud Computing

Mrs.Sindhuri.MN pursuing M.tech in Annamacharya Institute of Technology and Sciences

Mr.C.BhanuPrakash received his M.tech Degree in Computer Networks from JNTUA, Anantapuram in 2012 and B.Tech Degree in Information Technology from JNTUH,Hyderabad in 2006. Currently he is working as an Assistant Professor in Annamacharya Institute of Technology and Sciences, His areas of interest include Data Structures, Networks and Grid Computing