International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 4 Issue 2, February 2017

ISSN: 2394-4404

Implementation Of Convergent Encryption Scheme To Minimize The Cloud Storage Requirement

Prerana Dakhane

Student, Department of CSE,
Winaganga College of Engineering, Nagpur, India

Prof. Swati Patil

Asst. Professor, Department of CSE,
Winaganga College of Engineering, Nagpur, India

Abstract: ***Data de-duplication is a compression techniques that is used to remove the repetitive which can be used in cloud computing architecture. Convergent techniques has been used to encrypt data before out sourcing for privacy and security. But it has few limitations of convergent encryption so in proposed system techniques of cryptographic tuning is applied to make the encryption more secure and flexible. Data de-de-duplication prevents the storage of repetitive blocks and implements the pointer concept which puts the pointer to the existing block. Access control is provided in this application which allows the data owner the freedom of selecting users to have access to the published file. The integrity of data outsourced into the cloud is managed by the hash calculation of any content that follows the proof-of–ownership module. Proposed system calculate the hash value of the content on source on destination side and request the hash value for the cloud side to predict the tampering of data.***

The expected analysis shows the flexible improvement in execution time and development cost.

Keyword: De-duplication, cryptographic tunning, convergent techniques.

I. INTRODUCTION

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. Cloud computing model allows on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing provide users and enterprises with various storage and processing capabilities for data in either privately owned, or third-party data centers.

Cloud computing has privacy concerns because the service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or even delete information. The information can be shared by the cloud providers with third parties if necessary for purposes of law and order even without a warrant. Solutions to privacy of data can be done by encrypting data while uploading and downloading on cloud. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access.

II. LITERATURE REVIEW

JIN LI, YAN KIT LI, XIAOFENG CHEN, PATRICK P. C. LEE, WENJING LOU; A HYBRID CLOUD APPROACH FOR SECURE AUTHORIZED DE-DUPLICATION. IEEE TRANSACTION ON PARALLEL AND DISTRIBUTED SYSTEM VOL: PP NO: 99 YEAR 2014.

Description: Data de-duplication is one of important data compression techniques for eliminating duplicate copies of repeating data, and has been widely used in cloud storage to reduce the amount of storage space. To protect the confidentiality of sensitive data while supporting de-duplication, the convergent encryption technique has been used to encrypt the data while outsourcing. To provide better data security, this paper makes the first attempt to formally address the problem of authorized data de-duplication. They also provide several new de-duplication techniques supporting authorized duplicate check in a hybrid cloud architecture. As a proof of concept, they implement a prototype of their proposed authorized duplicate check scheme and conduct test

bed experiments using their prototype. They show that there proposed authorized duplicate check scheme incurs minimal overhead compared to normal operations.

M. BELLARE, S. KEELVEEDHI, AND T. RISTENPART; MESSAGE-LOCKED ENCRYPTION AND SECURE DE-DUPLICATION. IN EUROCRYPT, PAGES 296–312, 2013.

Description: This papers formalize a new cryptographic primitive, Message-Locked Encryption (MLE), is the key under which encryption and decryption are performed is itself derived from the message. MLE provides a way to achieve secure de-duplication (space-efficient and secure outsourced storage), a goal currently targeted by numerous cloud-storage providers. This paper provide definitions both for privacy and for a form of integrity that it call tag consistency. Based on this foundation, this make both practical and theoretical contributions. On the practical side, It provide ROM security analyses of a natural family of MLE schemes that includes deployed schemes. On the theoretical note the challenge is standard model solutions, and this make connections with deterministic encryption, hash functions secure on correlated inputs, sample and then extract paradigm to deliver schemes under different assumptions and for different classes of message sources. Our work shows that MLE is a primitive of both practical and theoretical interest.

M. BELLARE, S. KEELVEEDHI, AND T. RISTENPART. DUPLESS; SERVER-AIDED ENCRYPTION DE-DUPLICATION. IN PROC OF USENIX LISA 2013

Description: Cloud storage service providers such as Dropbox, Mozy, and others perform de-duplication to save space by storing only one copy of each file uploaded. Dupless describe as secure de-duplicated storage resisting brute-force attacks, and realize it in a system. In DupLESS, clients encrypt under message-based keys obtained from a key-server via an oblivious PRF protocol. It enables client to store encrypted file with an existing, have the service provide de-duplication.

P. ANDERSON AND L. ZHANG; SECURE AND FAST LAPTOP BACKUPS WITH ENCRYPTED DE-DUPLICATION. IN PROC. OF USENIX LISA, 2010.

Description: Many people now store large quantities of personal and corporate data on laptops and home computers. These often have poor or intermittent connectivity, and are vulnerable to theft or hardware failure. Conventional backup solutions are not well suited to this environment, and backup are frequently inadequate. This paper describes an algorithm which takes advantage of the data which is common between users to increase the backups speed, and it reduces the storage requirements. This algorithm supports per-user client-end encryption which is necessary for confidential personal data. It also supports a unique feature which allows immediate detection of common sub trees, avoiding the need to query the backup system for every file. They describe a prototype implementation of this algorithm for Apple OS X, and present an analysis of the potential effectiveness, using real data obtained from a set of users.

M. BELLARE, C. NAMPREMPRE, AND G. NEVEN; SECURITY PROOFS FOR IDENTITY BASED IDENTIFICATION AND SIGNATURE SCHEMES. J. CRYPTOLOGY, 22(1):1-61, 2009.

Description: This paper provides either security proofs or attacks for number of identity-based identification and signature schemes defined either explicitly or implicitly in existing literature. Underlying these is a framework that helps to explain how these schemes are derived and on the other hand enables modular security analyses, thereby helping to understand, simplify, and unify previous work.

III. PROBLEM STATEMENT

A. ACCESS TO AUTHORIZED USER

To develop a system only authorized users should get download access to shared files in his access domain.

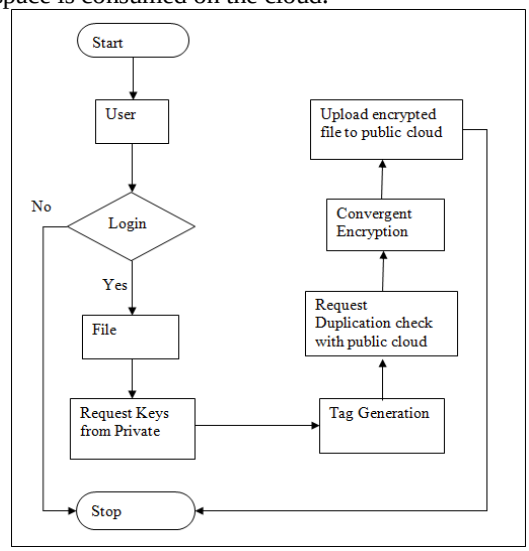
B. CONFIDENTIALITY

Cloud service providers are the third party service providers. So, it's not secure to store confidential contents as it is on cloud, to maintain confidentiality the proposed system need to implement encryption/ decryption scheme. But if it stored encrypted files on cloud then, user can't check the new file going to be uploaded on cloud is already present or not. So, in this paper convergence key is generated based on signature/ hash function on original data. So that user can achieve confidentiality as well as de-duplication.

IV. PROPOSED SYSTEM

Now-a-days, Cloud Computing allows organizations and users to store their structural data or information on a Cloud.

Through the study and research of the process of storing the encrypted data within the Cloud .We observed many problems like there are number of files with different names having the same content, which may lead to more costing of storage and more space is consumed on the cloud.



ISSN: 2394-4404

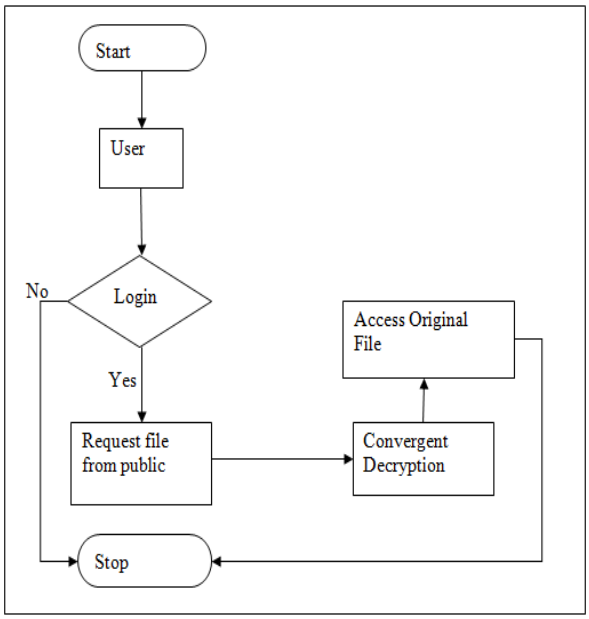


Figure 1: Block diagram of system architecture

Solution to this is to provide the de-duplication with convergent encryption schemes. Data de-duplication is one of important data compression techniques used for removing duplicate copies of data, and it has been widely used in cloud storage to save bandwidth and to reduce the amount of storage space. To protect the confidentiality of sensitive data supporting de-duplication, a new convergent encryption technique has been proposed to encrypt the data before outsourcing.

V. CONCLUSIONS

The authorized data de-duplication was proposed to protect the data security by including differential privileges of users in the duplicate check. We also presented new de-duplication techniques supporting authorized duplicate check in hybrid cloud architecture, in which the duplicate-check tokens of files are generated by the private cloud server with private keys. We used convergent encryption with modification version to deal with brute force attack using Domain Separation and Cryptographic tuning to make better authorized de-duplication technique.

REFERENCES

[1] Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou. A Hybrid Cloud Approach for Secure Authorized De-duplication IEEE transaction VOL:PP NO:99 2014.
[2] M. Bellare, S. Keelveedhi, and T. Ristenpart. Message-locked encryption and secure de-duplication. In EUROCRYPT, pages 296–312, 2013.
[3] M. Bellare, S. Keelveedhi, and T. Ristenpart. Dupless: Serveraided encryption for de-duplicated storage. In USENIX Security Symposium, 2013.
[4] P. Anderson and L. Zhang. Fast and secure laptop backups with encrypted de-duplication. In Proc. of USENIX LISA, 2010.
[5] M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. J. Cryptology, 22(1):1–61, 2009.
[6] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg. Proofs of ownership in remote storage systems. In Y. Chen, G. Danezis, and V. Shmatikov, editors, ACM Conference on Computer and Communications Security, pages 491–500. ACM, 2011.
[7] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou. Secure de-duplication with efficient and reliable convergent key management. In IEEE Transactions on Parallel and Distributed Systems, 2013.
[8] Ng and P. Lee. Revdedup: A reverse de-duplication storage system optimized for reads to latest backups. In Proc. of APSYS, Apr 2013.
[9] W. K. Ng, Y. Wen, and H. Zhu. Private data de-duplication protocols in cloud storage. In S. Ossowski and P. Lecca, editors, Proceedings of the 27th Annual ACM Symposium on Applied Computing, pages 441–446. ACM, 2012.
[10] R. D. Pietro and A. Sorniotti. Boosting efficiency and security in proof of ownership for de-duplication. In H. Y. Youm and Y. Won, editors, ACM Symposium on Information, Computer and Communications Security, pages 81–82. ACM, 2012.
[11] J. Xu, E.-C. Chang, and J. Zhou. Weak leakage-resilient client-side de-duplication of encrypted data in cloud storage. In ASIACCS, pages 195–206, 2013.
[12] J. Yuan and S. Yu. Secure and constant cost public cloud storage auditing with de-duplication. IACR Cryptology ePrint Archive, 2013:149, 2013.
[13] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider. Twin clouds: An architecture for secure cloud computing. In Workshop on Cryptography and Security in Clouds (WCSC 2011), 2011.
[14] A.Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, and J. C. S. Lui. A secure cloud backup system with assured deletion and version control. In 3rd International Workshop on Security in Cloud Computing, 2011.
[15] K. Zhang, X. Zhou, Y. Chen, X.Wang, and Y. Ruan. Sedic: privacyawaredata intensive computing on hybrid clouds. In Proceedings of the 18th ACM conference on Computer and communications security, CCS'11, pages 515–526, New York, NY, USA, 2011.