International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 4 172 - 175

Review Paper on Privacy Preservation Techniques in Cloud

Abhishek Ganorkar
Dept. of CSE,
PRPCEM, Amravati.

Prajwal Wankhade
Dept. of CSE,
PRPCEM, Amravati.

Juhi Dakhane
Dept. of CSE,
PRPCEM, Amravati.

Jeba Sheikh
Dept. of CSE,
PRPCEM, Amravati.

Amik Patel
Dept. of CSE,
PRPCEM, Amravati.

Prof. Abhishek R. Ladole
Dept. of CSE,
PRPCEM, Amravati.

Abstract: In this information world, large amounts of data are collected and analyzed every day. Cloud computing is the most known model for supporting large and complex data. Organizations are moving toward cloud computing for getting benefit of its cost reduction and elasticity features but cloud computing has potential risk and vulnerabilities. One of major problem in moving to cloud computing is its security and privacy concerns.Encryption is standalone problem for the security of data stored on the cloud. So we proposed method which combines the concept of encryption along with data deduplication methodology to enhance the privacy of data over cloud. Data deduplication is a specialized data compression technique for eliminating duplicate copies of repeating data in storage. In turns this technique saves the cost and time associated with redundant accessing and processing of data overhead involve as compared to normal operations..

*****

I. Introduction

Cloud computing derives as the collection of hardware, networks, storage, services, and interfaces that can be group together deliver aspects of computing as a service. This service mainly includes the delivery of software, infrastructure, and storage over the internet either as separate components or a complete platform based on user demand. It does not require a user to be in a specific place to gain access to Companies may find that cloud computing allows them to reduce the maintenance cost of data management, as they don't need to own their own servers and can use capacity leased from third parties. In accordance to it, the cloud-like structure allows companies to upgrade software more efficiently and quickly.

It provide users to store large volume of data and to perform application over cloud without need of any also provides greater flexibility of storing and computation of data but, Such applications can be processed, huge volume processing data sets are to be generated. For Storing some valuable intermediate datasets has been considered in order to avoid the high recomposing them.

Applications provided through the Cloud can be accessed from any device - a computer, a Smartphone, an iPad, etc. Any has access to the Internet can take the advantage of the power of the Cloud. Cloud customers can save huge capital investment of IT infrastructure and concentrate on their own core business. Hence many organizations have been migrating or building their business into cloud and privacy issues will be brought about through holding intermediate datasets. The occurrence of intermediate dataset storage increases the attack surface so that the risk of original data privacy is at being compromised. The intermediate dataset storage might be out of control of the original data owner and can be accessed and shared by other applications. These situations make the privacy protection of an original dataset an vital necessity. Nevertheless, few attentions are paid to such a typical cloud privacy issue incurred by intermediate datasets.

A traditional counter measure is to conceal ALL intermediate datasets by encryption. But these valuable datasets are usually shared by multiple users or accessed frequently, which requires repeat en/decryption. Storage and computation services in cloud are equivalent from an economical perspective because they are in proportion to their usage in cloud environment. Thus, this technique is used to improve storage utilization and can also be applied to network data transfers to reduce the number of bytes that must be sent. Instead of keeping multiple data copies with the same content, deduplication eliminates redundant data by keeping only one physical copy and referring other redundant data to that copy.

II. Literaturesurvey:

ElhadjBenkhelifa and Dayan Fernando et al. **[**5**]** proposed a novel hybrid solution for increased security to be implemented as part of a real business case project. The project is concerned with highly sensitive data; hence a more complex security approach is needed. The proposed hybrid solution, Single-Sign-On and two-factor authentication, is accepted by the project consortium and end-users to be a state-of-the-art and highly secure authentication approach.

Several deduplication schemes have been proposed by J. R. Douceur et al.[3] showing how deduplication allows very appealing reductions in the usage of storage resources. The problems of identifying and coalescing identical files in the distributed file system, for the purpose of reclaiming storage space consumed by incidentally redundant content.

Convergent encryption is a cryptographic primitive introduced by J. R. Douceur et al. attempting to combine data confidentiality with the possibility of data deduplication. Convergent encryption of a message consists of encrypting the plaintext using a deterministic (symmetric) encryption scheme with a key which is deterministically derived from the plaintext. Clearly, when two users independently attempt to encrypt the same file, they will generate the same ciphertext which can be easily deduplicated. Unfortunately, convergent encryption does not provide semantic security as it is vulnerable to content guessing attacks.

Recently Jan Stanek et al. [6] proposed an encryption scheme that guarantees semantic security for unpopular data and provides weaker security and better storage and bandwidth benefits for popular data. For popular data that are not particularly sensitive, the traditional conventional encryption is performed. Another two-layered encryption scheme with stronger security while supporting deduplication is proposed for unpopular data. In this way, they achieved better tradeoff between the efficiency and security of the outsourced data.

Later, Bellare M., Keelveedhiet. et. Al [9] formalized convergent encryption under the name message-locked encryption. As expected, the security analysis presented in highlights that message-locked encryption offers confidentiality for unpredictable messages only, clearly failing to achieve semantic security.

JiaXuet.al present a PoW scheme allowing client-side deduplication in a bounded leakage setting. They provide a security proof in a random oracle model for their solution, but do not address the problem of low min-entropy files. Recently, M. Bellareet.al presented DupLESS a server-aided encryption for deduplicated storage which uses a modified convergent encryption scheme with the aid of a secure component for key generation.

HongweiLiet. al.[10] presented an identity based authentication for cloud computing, based on the identity-based hierarchical model for cloud computing (IBHMCC) and corresponding encryption and signature schemes. Being certificate-free, the authentication protocol aligned well with demands of cloud computing. Performance analysis indicated that the authentication protocol is more efficient and lightweight.Recently, S. Bugielet. al provided an architecture consisting of twin clouds for secure outsourcing of data and arbitrary computations to an untrusted commodity cloud. K. Zhang et. al also presented the hybrid cloud techniques to support privacy-aware data-intensive computing. Proposed system considers addressing the authorized deduplication problem over data in public cloud.

NesrineKaanicheet. Al [15] proposed a new client-side deduplication scheme for securely storing and sharing outsourced data via the public cloud. It ensures better confidentiality towards unauthorized users. That is, every client computes a per data key to encrypt the data that he intends to store in the cloud. As such, the data access is managed by the data owner and also introduces a new cryptographic method for secure Proof of Ownership (PoW), for improving data security in cloud storage systems, providing dynamic sharing between users and ensuring efficient data deduplication.

III. Proposed system:

Data Deduplication

This technique is used to improve storage utilization and can also be applied to network data transfers to reduce the number of bytes that must be sent. In the deduplication process, unique chunks of data, or byte patterns, are identified and stored during a process of analysis.

 ISSN: 2321-8169
172 - 175

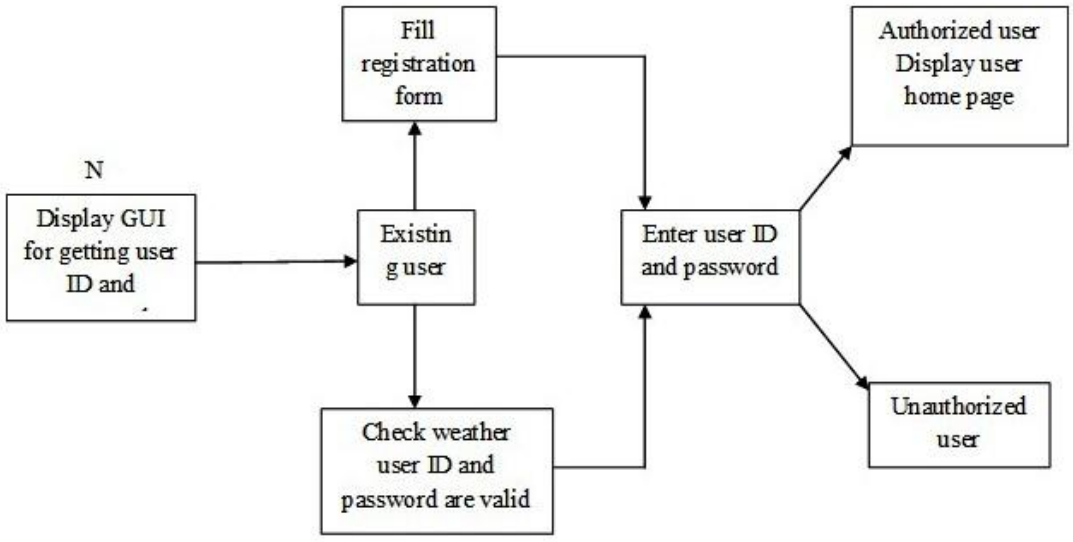
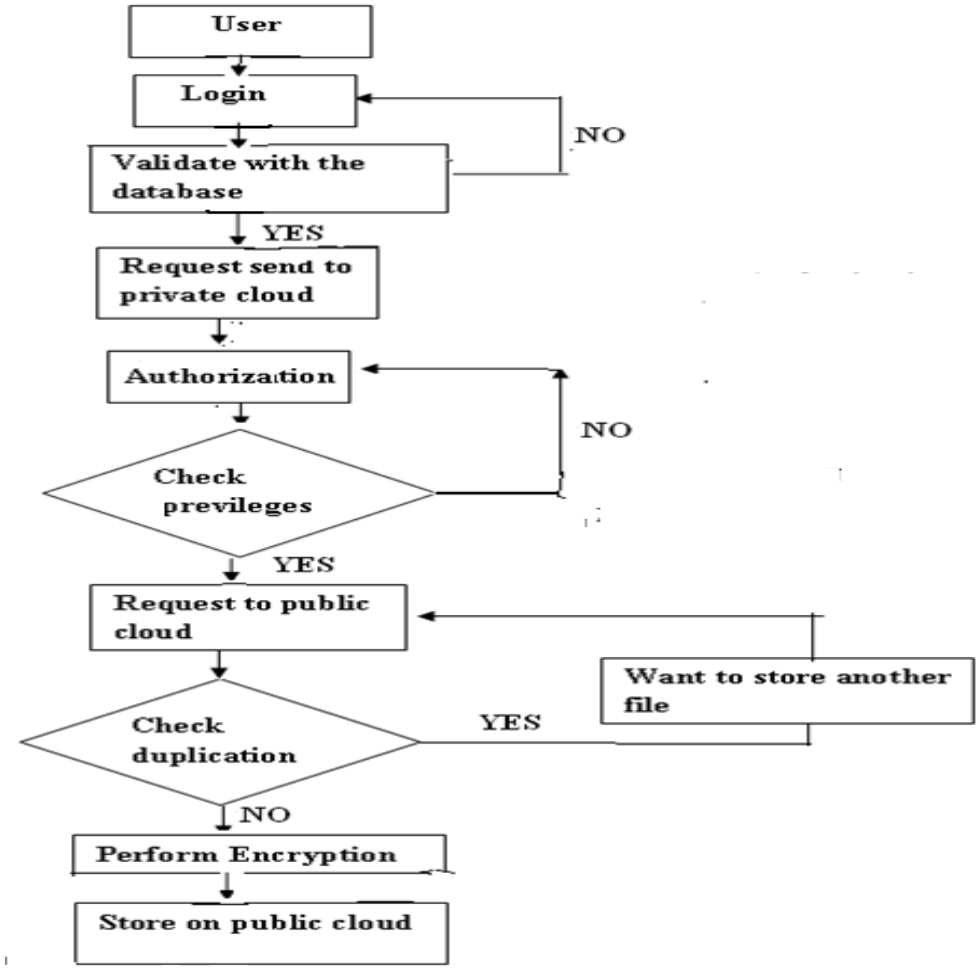


Figure1: System architecture

In this system new user has to fill registration form by sign up they if they are already registered then they can directly sign in up to system. Admin checks thevalid credential over user's inputs. After the sign in user does not get access to particular file unless admin does not gives authorization over it.



Implementation of Authorized Duplicate check

In this system once user logged in admin will validates all the user inputs. Based on it, system permits for further operation on the private cloud. Here admin will checks the authorization and privileges given to users, such as upload, download and update the content of those particular files. While uploading any multimedia file on to the cloud it will create a token using random number generator in to the database. In the future whenever user wants to download it needs to enter token generated. To avoid duplication system will check the same contents in those file and avoid the repeated uploading or downloading of such a file to the cloud..

IV. Conclusions

With the duties of this paper, westudied a variety of techniques for data deduplication. This shows the survey of various deduplication techniques in cloud computing.In this encryption is come with data deduplication method for providing security to data in cloud. It also shows its pros, cons and challenges for further works. It gives improve results over the existing approach.

V. References

[1] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou, "A Hybrid cloud approach for secure authoriseddeduplication," IEEE Transactions on Parallel and Distributed Systems, 2014.

[2] 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,"In3rd International Workshop on Security in CloudComputing, 2011.

[3] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer, "Reclaiming space from duplicate files in a serverless distributed file system,"InICDCS, 2002.

[4] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg," Proofs of ownership in remote storage systems,"ACM, 2011.

[5] ElhadjBenkhelifa, Dayan Fernando,"A Novel cloud hybrid access mechanism for highly sensitive data exchange," The Fourth International Conference on Cloud Computing,2013.

[6] J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl, "A secure data deduplication scheme for cloud storage,"InTechnical Report, 2013.

[7] Bellare, M., Keelveedhi, S., Ristenpart, "T.: Message-locked encryption and secure deduplication," In: Advances in Cryptology, 2013.

[8] Xu, J., Chang, E.C., Zhou, J,"Weak leakage-resilient client-side deduplication of encrypted data in cloud storage," In: 8th ACM SIGSAC symposium.

[9] Bellare, M., Keelveedhi, S., Ristenpart, T, "DupLESS: server-aided encryption for deduplicated storage," In: 22nd USENIX conference on Security, 2013.

[10] Hongwei Li, Yuanshun Dai1, Ling Tian, and HaomiaoYang,"Identity-Based Authentication for Cloud Computing,"In Cloud Com ,2009.

[11] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider,"Twin clouds: An architecture for secure cloud computing,"InWorkshop on Cryptography and Security in Clouds , 2011.

[12] K. Zhang, X. Zhou, Y. Chen, X.Wang, and Y. Ruan. "Sedic: privacyaware data intensive computing on hybrid clouds,"InProceedingsof the 18th ACM conference on Computer and communications security,USA, 2011.

[13] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes, "2009.

[14] R. D. Pietro and A. Sorniotti," Boosting efficiency and security in proof of ownership for deduplication,"ACM, 2012.

[15] NesrineKaaniche, Maryline Laurent, "A Secure Client Side Deduplication Scheme in Cloud Storage Environments," 6th international conference on new technologies,mobility and security , 2014.