ISSN: 0976-3104
SPECIAL ISSUE : Emerging Technologies in Networking and Security (ETNS)
Rajasaranya kumariet al.

ARTICLE OPEN ACCESS

PRIVACY AUGMENTATION BY ACCOMPLISHING TRACEABILITY OVER ORUTA

R. Rajasaranya Kumari[1*], R. Vinod[2], U. Velmurugan[3], N. Rupavathy[4]
[1,2]Department of Computer Science and Engineering, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai, INDIA
[3]Department of Computer Science and Engineering, Vel Tech (Owned by RS Trust), Avadi, Chennai, INDIA
[4]Department of Computer Science and Engineering, Vel Tech Dr.RR & Dr SR Technical university, Avadi, Chennai, INDIA

ABSTRACT

Aims: *Cloud Computing is a set of IT Services that are provided to a customer over a network and these services are delivered by third party provider who owns the infrastructure. It is used not only for storing data, but also the outsourced data can be shared by multiple users. Due to this there exists a problem in integrity.****Materials and methods:****The objective is to provide security to the data stored in the public cloud. Several mechanisms have been designed to support public auditing on shared data stored in the cloud.****Results:****With the privacy preserving mechanism, the public auditor audits and verify the integrity of the shared data in the cloud without seeing the data called as public auditing. Along with public auditing security is improved to the data in the public cloud.* ***Conclusion:****Normally the data is stored only in a single server. But, Here multiple servers are used for storing data for security purpose.*

Published on: 08th– August-2016

KEY WORDS

traceability, data security, public auditing, shared data

***Corresponding author: Email:** rajasaranya@velhightech.com

INTRODUCTION

Mobile app markets are creating a fundamental model shift in the way software is delivered to the end users. The Cloud computing is a new concept of computing technique, by which computer resources are provided dynamically via Internet. It attracts considerable attention and interest from both academia and industry. However, it also has at least three challenges that must be handled before applied to our real life. First of all, data confidentiality should be guaranteed. When sensitive information is stored in cloud servers, which is out of users' control in most cases, risks would rise dramatically. The servers might illegally inspect users' data and access sensitive information. On the other hand, unauthorized users may also be able to intercept someone's data. Secondly, personal information is at risk because one's identity is authenticated according to his information. As people are becoming more concerned about their privacy these days, the privacy-preserving is very important. Preferably, any authority or server alone should not know any client's personal information.

Recently, many mechanisms [2], [3] have been proposed to allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing. In these mechanisms, data is divided into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking [3]. A public verifier could be a data user who would like to utilize the owner's data via the cloud or a third-party auditor (TPA). Moving a step forward, Wang et al. designed an advanced auditing mechanism [2] (named as WWRL in this paper),so that during public auditing on cloud data, the content of private data belonging to a personal user is not disclosed to any public verifiers. That is, there is a leakage of identity privacy.

Recently proposed access control models, such as attribute-based access control, define access control policies based on different attributes of the requester, environment, or the data object. ABE features a mechanism that

THE IIOAB JOURNAL
ISSN: 0976-3104

enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. Especially, ciphertext-policy provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access. Various types of clouds are present such as private cloud, public cloud, hybrid cloud and community cloud. Our aim is to improve security and audit the data in the public cloud.

Oruta is a novel privacy preserving public auditing mechanism. Here Oruta uses ring-signature for public auditing. By using ring signature, public verifier is able to verify the integrity or correctness of shared data without retrieving the original data fully. With the privacy preserving mechanism, the public auditor audits the shared data in the cloud without seeing the data called as public auditing. In this paper, along with public auditing we have improved data security in public cloud. Here we have achieved traceability (tracking the fake users). Data privacy is also improved by blocking the fake user fromaccessing the data from the public cloud.

This paper proposes a erasure correction code algorithm to protect the users' data stored in the cloud storage from the unauthorized access. The paper is organized as follows. Section II gives the detail on the various issues in cloud data storage ie problem statement. Section III describes about the architecture diagram. Section IV talks about the related work. Section V, gives the conclusion for the paper.

	PDP[9]	WWRL[5]		Proposed system
Public Auditing	✓	✓		✓
Data Privacy	×	✓		✓
Identity Privacy	×	×		✓
Traceability	×	×		✓

Fig: 1. Comparison among Different Mechanisms

PROBLEM STATEMENT

The system model in this paper involves four parties: the cloud server, original user, a group of users and a public verifier. Cloud storage consists of several servers. The original user outsouce the data to the cloud. He will register the authorized user who can share that data from the cloud. Only that authorized user can share the data from the cloud. The problem exists when any other unknown person or user knows the authorized users' password ie the security problem arise. The shared data can be easily downloaded by the fake user. There is no traceability(ie the fake user cannot be tracked). Due to this Data Privacy in cloud is not preserved. Normally the outsourced data is kept only in private cloud.

Our mechanism should be designed to achieve the following properties: (1) **Public Auditing**: A public verifier is able to check the integrity of shared data without viewing the data from the cloud. (2) **Correctness**: A public verifier is able to correctly verify shared data integrity. (3) **Traceability:** Trackingthe fake user from accessing the data from the cloud. (4) **Data Privacy**: Data shared in cloud should not be should not be downloaded by the fake user. **(5) Data security**: Only the data Owner and the authorized user are allowed to access or download the data. The user will be given some priviledges.

THE IIOAB JOURNAL
ISSN: 0976-3104

ARCHITECTURE DESIGN

In this paper, we are going to achieve traceability (tracking the fake user). The Original user first register his account for login. The original user registers the users accounts whom he wants to share his data. Those users will be given some priviledges. Data will be stored in three different servers for security purpose. Now when the original user uploads the data to the public cloud, the data will get split up into three sub blogs. Then the splitted files will get encrypted and stored in three different servers. The data is splitted and then encrypted using erasure correction code technique. If the user enters and try to download the file, OTP will be generated and send to the mail. If the OTP is valid, it allows the user to download the file. When the OTP is valid, the data is decrypted and then merged using erasure correction code technique and the downloaded as a original file. If the OTP is invalid, the user will be considered as fake user and he is not allowed to download the data or accessing the data from the cloud.

ERASURE CORRECTION CODE:

The technique used here is erasure correction code. Erasure correction code is a method of data protection in which data is broken into fragments, expanded and encrypted into redundant data pieces and stored across a set of different locations or different servers. This algorithm is also used for decrypting the data and merging the data from different locations or different servers. This technique is described clearly in reference[4].

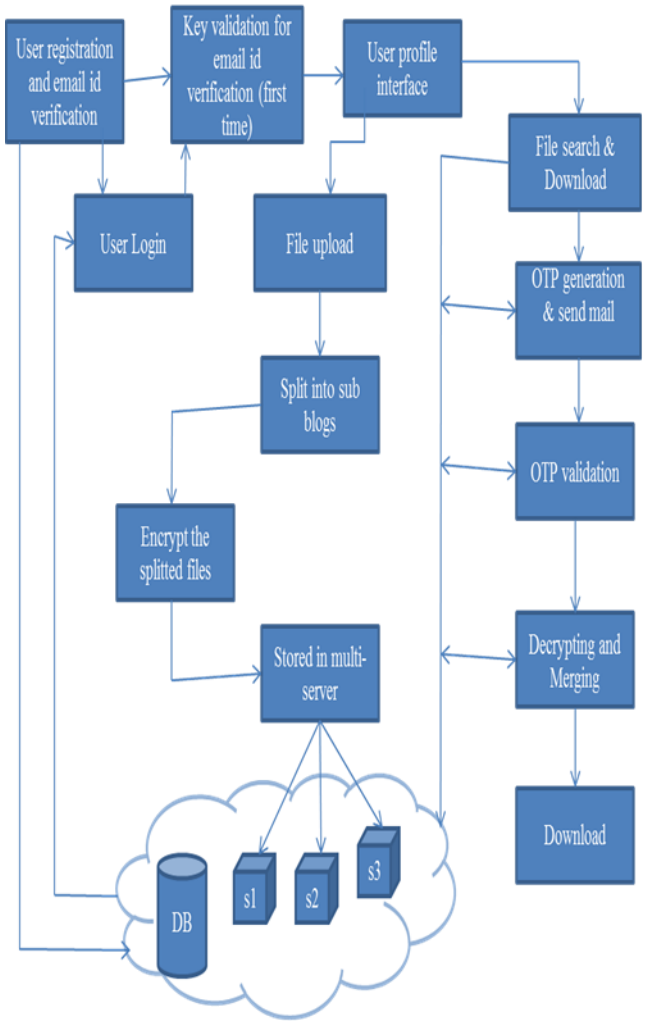

Fig: 3. Tracking the fake user

THE IIOAB JOURNAL
ISSN: 0976-3104

RELATED WORK

The paper "Privacy Preserving Public Auditing for Secure Cloud Storage" [5] is used to enable the TPA to perform audits for multiple users simultaneously and efficiently. Combination of HLA and random masking is used, which enables TPA to perform auditing without viewing the content.The paper"PORs: Proofs of Retrievability for Large Files" [10] providesPOR's scheme which is also able to check the correctness of data on an untrusted server. The original file is added with a set of randomly-valued check blocks called sentinels. The Drawbackis itfocus only on personal data in the cloud. In [4] RDC is a technique by which user can check the integrity of data outsourced in servers, Audit the correctness of data under the multi-server scenario.The methods used here is replication, erasure coding, network coding. Erasure coding is a method of data protection in which data is broken into fragments, encoded and stored in multiple servers. Erasure coding is used in Privacy augmentation. In [3] the verifier is able to publicly audit the integrity of data without retrieving the entire data, which is referred to as public auditing. But, this mechanism is only suitable for auditing the integrity of personal data.

CONCLUSION

In this paper, we propose a Privacy augmentation by accomplishing traceability over oruta. A technique is used to improve data security called erasure correction code. Data Privacy in cloud is improved by tracking the fake user and blocking them from downloading the data from cloud. We utilize ring signatures, so that a public verifier is able to audit shared data integrity without viewing the entire data. Along with public auditing, data security and data privacy is improved.

.

REFERENCES

[1] C Wang, Q Wang, K.Ren, and W Lou.[2010] Privacy- Preserving Public Auditing for Data Storage Security in Cloud Computing, Proc. *IEEE NFOCOM*, pp. 525-533,.

[2] G Ateniese, R Burns, R Curtmola, J Herring, L Kissner, Z Peterson, and D Song.[2007]Provable Data Possession at Untrusted Stores, *Proc. 14th ACM Conf. Computer and Comm. Security* (CCS '07), 598-610,

[3] B Chen, R Curtmola, G Ateniese, and R Burns.["Remote Data Checking for Network Coding-Based Distributed Storage Systems," Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.

[4] C Wang, SS Chow, Q Wang, K Ren, and W Lou.[. 2013] Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, 62(2): 362-375

[5] C Wang, Q Wang, K Ren, and W Lou.[2009] Ensuring Data Storage Security in Cloud Comp puting, Proc. 17th Int'l Workshop Quality Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9,.

[6] G Ateniese , RD Pietro, LV Mancini, and G Tsudik.[2008]Scalable and Efficient Provable Data Possession, Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm'08),.

[7] B Wang, B Li, and H Li.[2012] Knox: Privacy- Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l *Conf. Applied Cryptography and Network Security* (ACNS'12),pp. 507-525, June

[8] RL Rivest, A Shamir, and Y Tauman.[2001]How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 552-565.

[9] A Juels and BS Kaliski.[2007]PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 584-597,

[10] B Wang, B Li, and H Li.[2012]Oruta: Privacy- Preserving Public Auditing for Shared Data in *The Proc. IEEE Fifth Int'l Conf. Cloud Computing*, 295- 302.