D. Sumithra *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 1, January- 2014, pg. 1-8 **ISSN: 2321-8363**

Public Auditing & Automatic Protocol Blocking with 3-D Password Authentication for Secure Cloud Storage

P. Selvigrija, Assistant Professor, Department of Computer Science & Engineering, Christ College of Engineering &Tech., Pondicherry

D. Sumithra, M.Tech, II Year, Department of Computer Science & Engineering, Christ College of Engineering &Tech., Pondicherry

E-Mail Id: sumithra.deva@gmail.com

Abstract

Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. User level security is provided using the 3-D Password by combining textual, graphical and Biometric Finger print. For data level security symmetric key based encryption/decryption using Galois Counter Mode (GCM).

Keywords: 3-D password; Automatic protocol blocker; third party auditing; Audit

I. INTRODUCTION

Cloud computing is a general term for anything that involves delivering hosted services over the internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour it is elastic - a user can have as much or as little of a service as they want at any given time and the service is fully managed by the cloud service provider (the consumer needs nothing but a personal computer and Internet access).The ad- vantage of cloud is cost saving. The prime disadvantage is security. Cloud

computing is used by many software industries now a days. Since the security is not provided in cloud, many companies adopt their unique security structure. Introducing a new and uniform security structure for all types of cloud is the problem we are going to tackle in this paper. Since the data placed in the cloud is accessible to everyone, security is not guaranteed.

To ensure security, cryptographic techniques cannot be directly adopted. Sometimes the cloud service provider may hide the data corruptions to maintain the reputation. To avoid this problem, we introduce an effective third party auditor (TPA) to audit the user's outsourced data when needed.

Infrastructure Models There are many considerations for cloud computing architects to make when moving from a standard enterprise application deployment model to one based on cloud computing.

- Software as a Service (SaaS) Software as a service features a complete application offered as a service on demand. A single instance of the software runs on the cloud and services multiple end users or client organizations.

- Platform as a Service (PaaS) Platform as a service encapsulates a layer of software and provides it as a service that can be used to build higher-level services.

- Infrastructure as a Service (IaaS) Infrastructure as a service delivers basic storage and compute capabilities as standardized services over the network. Servers, storage systems, switches, routers, and other systems are pooled and made available to handle workloads that range from application components to high-performance computing applications.

II. PUBLIC AUDITING

Cloud computing is a model which provides a wide range of applications under different topologies and every topology derives some new specialized protocols. TPA is the third party auditor who will audit the data of data owner or client so that it will let off the burden of management of data of data owner. TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would not only help owners to evaluate the risk of their subscribed cloud data services, but also be beneficial for the cloud service provider to improve their cloud based service platform. This public auditor will help the data owner that his data are safe in cloud.

With the use of TPA, management of data will be easy and less burdening to data owner but without encryption of data, how data owner will ensure that his data are in a safe hand. When n numbers of user are using the data than consistency of data is quite important because anyone can use the data, modify the data or delete the data. So to resolve the data dynamics is become an important task of the data owner. So in my scheme we added the information of insertion, updating and deletion in the message.

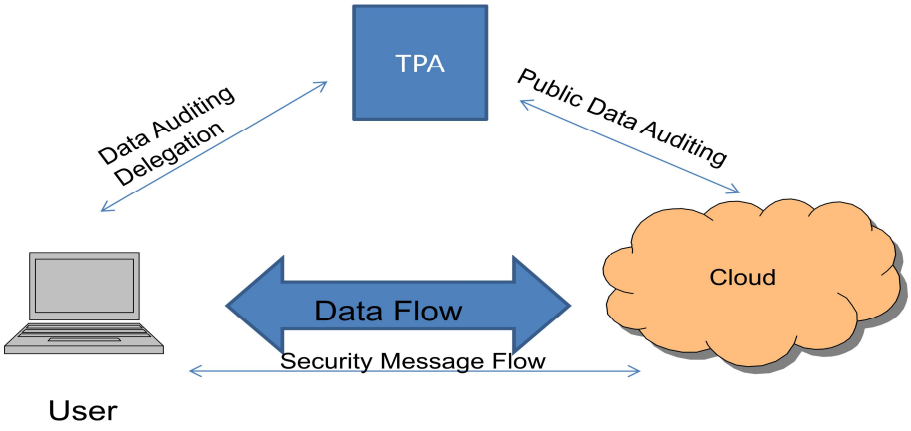

Figure 1: Cloud Storage Architecture

The system and Threat Model: We consider a cloud data storage service involving three different entities, the cloud user (U), who has large amount of data files to be stored in the cloud, the cloud Server (CS), which is managed by the cloud service provider (CSP) to provide data storage and has significant storage space and computation resources., the third party Auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user request.

Third Party Auditor Third Party Auditor is kind of inspector. There are two categories: private auditability and public auditability. Although private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would help owners to evaluate the risk of their subscribed cloud data services, and it will also be beneficial to the cloud service provider to improve their cloud based service platform [6]. Hence TPA will help data owner to make sure that his data are safe in the cloud and management of data will be easy and less burdening to data owner.

III. PROPOSED ARCHITECTURE

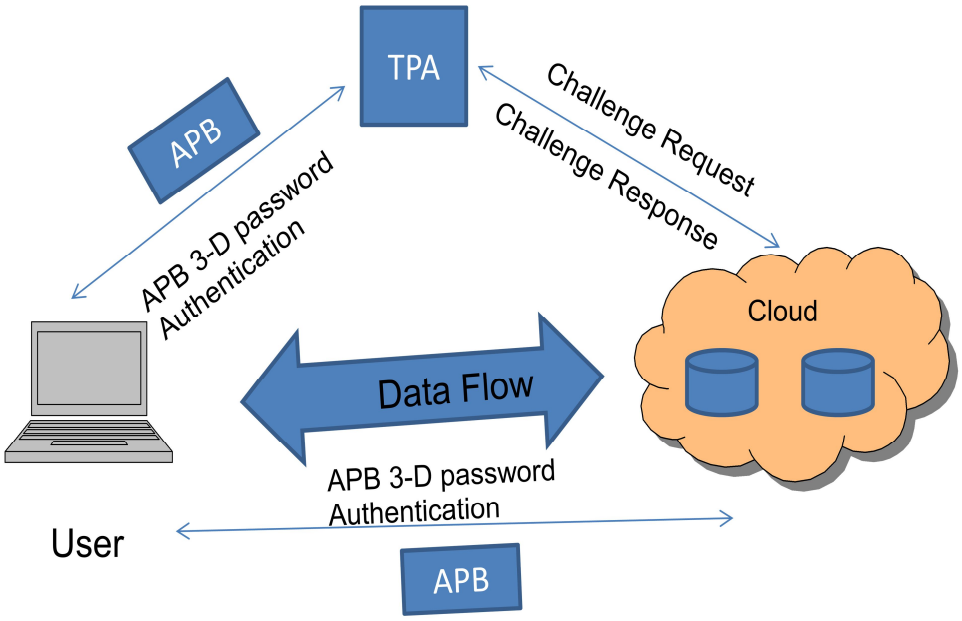

Figure2: Security using APB

AUTOMATIC PROTOCOL BLOCKER

The proposed system is designed to prevent the unauthorized data access for preserving data integrity. The system monitors the user requests according the user specified parameters and it checks the parameters for the new and the existing users. The system accepts existing validated user, and prompts for the new users for the parameter to match requirement specified during user creation for new users. If the new user prompt parameter matches with cloud server, it gives privileges to access the Automatic Protocol authorized the system automatically blocks the Audit protocol for specific user. Based on the 3-D password authentication the blocking of unauthorized user accessing the cloud storage is carried out.

3-D PASSWORD AUTHENTICATION

The dramatic increase of computer usage has given rise to many security concerns. One major security concern is authentication, which is the process of validating who you are to whom you claimed to be. In general, human authentication techniques can be classified as knowledge based (what you know), token based (what you have), and biometrics (what you are). Knowledge-based authentication can be further divided into two.

- Recall based and
- Recognition based.

Recall-based techniques require the user to repeat or reproduce a secret that the user created before. Recognition based techniques require the user to identify and recognize the secret, or part of it, that the user selected before. One of the most common recall-based authentication schemes used in the computer world is textual passwords. One major drawback of the textual password is its two conflicting requirements: the selection of passwords that are easy to remember and, at the same time, are hard to guess.

Graphical password - Many authentication systems, particularly in banking, require not only what the user knows but also what the user possesses (token-based systems). However, many reports have shown that tokens are vulnerable to fraud, loss, or theft by using simple techniques. Various graphical password schemes have been proposed. Graphical passwords are based on the idea that users can recall and recognize pictures better than words. However, some of the graphical password schemes require a long time to be performed. Moreover, most of the graphical passwords can be easily observed or recorded while the legitimate user is performing the graphical password; thus, it is vulnerable to shoulder surfing attacks.

Biometric Password- Biometrics (or biometric authentication) refers to the identification of humans by their characteristics or traits. Biometrics is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. For secure authentication to any medium the biometric authentication will be highly secure.

1. 3-D PASSWORD

3-D password – The 3-D password authentication is used to avoid the unauthorized accessing the cloud storage. The 3-D password authentication scheme is multi factor authentication method to provide more security to the cloud accessing.

1. Textual password – In textual password a secret question will be asked by the cloud server for authentication for the proper user login.
2. Graphical password – the user will be given the image as the password, the mouse clicked by the user on the image is taken as the password.
3. Biometric password - Biometric password based fingerprint image.

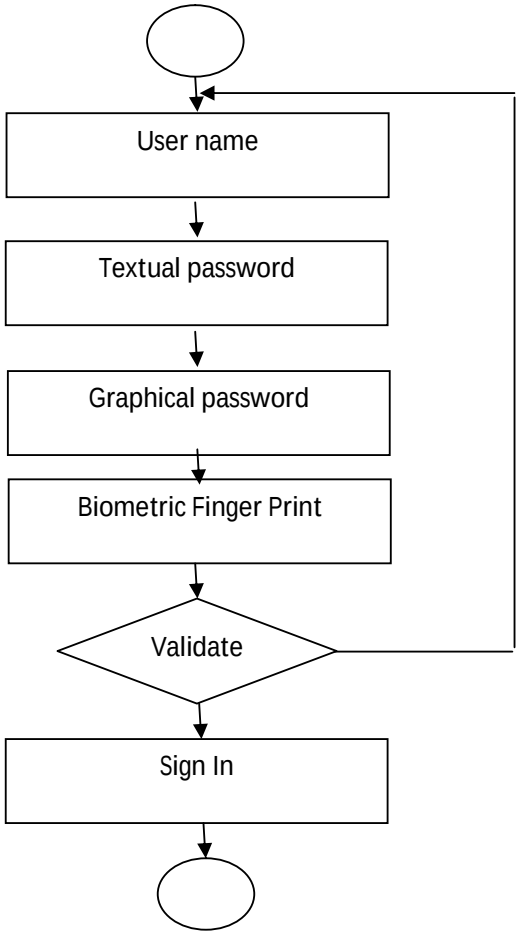

Figure 3: 3-D password

2. AUDIT

Upon user request the Third Party Auditor (TPA) verifies the user data on the cloud server, using the GCM encryption and decryption algorithm.

A) GALOIS/COUNTER MODE (GCM)

Galois/Counter Mode is a mode of operation for symmetric key cryptographic block ciphers that has been widely adopted because of its efficiency and performance. GCM throughput rates for state of the art, high speed communication channels can be achieved with reasonable hardware resources. It is an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality. GCM is defined for block ciphers with block sizes of 128, 192, and 256 bits.

GCM Encryption – Whenever the user stores the data into the cloud server the data is encrypted using GCM encryption algorithm.

GCM Decryption -The GCM decryption algorithm is used to retrieve the original stored data from the cloud server.

IV. CONCLUSION

Public auditing can be achieved using the Automatic Protocol Blocking for the secure cloud storage, which improves the efficiency of the user storage. Thus the 3-d password will improve the user level security in Cloud Server and the data level security will be effectively provided using the GCM based encryption and decryption algorithms. Thus the public auditing ensures that the data leakage and data loss will be reduced and more number of users will be improved.

REFERENCE

[1] G. Divya Zion, D.Kavitha "Remote Sensing Data as a Service in Hybrid Clouds: Security Challenges and Trusted Third-party Auditing Mechanisms"Vol. 1, Issue 7, September 2012.-pg: 1

[2] Sichuan Province Email: wangshaohui@njupt.edu.cn1. -pg:2

[3] RagibHasan" Security and Privacy in Cloud Computing" Johns Hopkins Universityen.600.412 Spring 2010.-pg: 2,5

[4] Balakrishnan.S, Saranya.G, Shobana.S, Karthikeyan.S" Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud" IJCST Vol. 2, Issue 2, June 2011.-pg: 31,34, 61.

[5] Everaldo Aguiar "An Overview of Issues and Recent Developments in Cloud Computing and Storage Security "University of Notre Dame, Notre Dame, IN, e-mail: eaguiar@nd.edu.-pg: 1, 4,5

[6] Cong Wang, Qian Wang, and KuiRen "Ensuring Data Storage Security in Cloud Computing" Email: {cwang, qwang, kren}@ece.iit.edu.-pg:2,3

[7] K.S.Sathiyapriya" Integrity And Security Check Through Data Coloring And Water Marking Using Third Party Auditor In Cloud Computing Atmosphere"Vol. 2 Issue 1, 2012,95-99.-pg: 1, 2,6.

[8] Wang Shao-huiP 1, 2 *P , Chang Su-qinP1P, Chen Dan-weiP1P, Wang Zhi-weiP "Public Auditing for Ensuring Cloud Data Storage Security With Zero Knowledge Privacy" 1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing210046, China; pg:1 to 19.

[9] Operations in cloud computing environment "vol. 2 no. 10 October 2012.-pg: 2

[10] Katukam Ganesh" Ensuring and Reliable Storage in Cloud Computing" Vol. 3 (5) , 2012,5157 – 5163.pg: 3, 4

[11] D. Kishore Kumar, G.VenkatewaraRao, G.SrinivasaRao" Cloud Computing: An Analysis of Its Challenges & Security Issues" Issue 5, October 2012.-pg: 1, 2

[12] Balakrishnan.S, Saranya.G, Shobana.S, Karthikeyan.S" Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud" IJCST Vol. 2, Issue 2, June 2011.-pg: 34, 61 and -pg: 31,61

