International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

A New Mechanism for Securing Cloud Data Using Fingerprint Recognition

Mr.K.Anil & Mr.K.Dayakar
Assistant Professor, Department of Computer Science Engineering. Jayamukhi Institute of Technological Sciences.

Abstract:

Cloud computing is a technological advancement that focuses on the way we design computing systems, develop applications, and leverage existing services for building software. It is based on the concept of dynamic provisioning, which is applied not only to service but also to compute capability, storage, networking, andinformationtechnology (IT) infrastructureingeneral. Day by day we are storing heavy data, maintenance and management is going to be difficult. It raises security concerns on how to realize data deduplication in cloud while achieving integrity auditing.We propose two secure techniques, namely One Time Password and Finger Print Recognization. One Time Password and Finger Print Recognization introduces an auditing entity with maintenance of a Map Reduce cloud, which helps clients secure logins with their organs like finger,palm.It is useful for clients before uploading as well as audit the integrity of data having been stored in cloud. Compared with previous work, the computation by user in One Time Password and Finger Print Recognization is greatly reduced during the file uploading and customers always want to secure their data before uploading, and enables integrity auditing and secure deduplication on data.

Keywords:

One Time Password, Finger Print Recognization, Image capture, security, matching, biometric identification, HMAC.

I. Introduction:

Cloud storage is Model of Networked Enterprise storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Cloud storage provides customers with benefits, ranging from cost saving and simplified convenience, to mobility opportunities and scalable service. These great features attract more and more customers to utilize and storage their personal data to the cloud storage: according to the analysis report, the volume of data in cloud is expected to achieve 40 trillion gigabytes in 2020. Even though cloud storage system has been widely adopted, it fails to accommodate some important emerging needs such as the abilities of auditing integrity of cloud files by cloud clients and detecting duplicated files by cloud servers. In the process of auditing few problems are occurred while the data uploading, retrieving and security purpose.

The first problem is integrity auditing. The cloud server is able to relieve clients from the heavy burden of storage management and maintenance. The most difference of cloud storage from traditional in-house storage is that the data is transferred via Internet and stored in an uncertain domain, not under control of the clients at all, which inevitably raises clients great concerns on the integrity of their data.
The second problem is secure deduplication. The rapid adoption of cloud services is accompanied by increasing volumes of data stored at remote cloud servers. . Among these remote stored files, most of them are duplicated, according to a recent survey by EMC.75% of recent digital data is duplicated copies. This fact raises a technology namely deduplication, in which the cloud servers would like to deduplicate by keeping only a single copy for each file and make a link to the file for every client who owns or asks to store the same file. Unfortunately, this action of deduplication would lead to a number of threats potentially affecting the storage system.

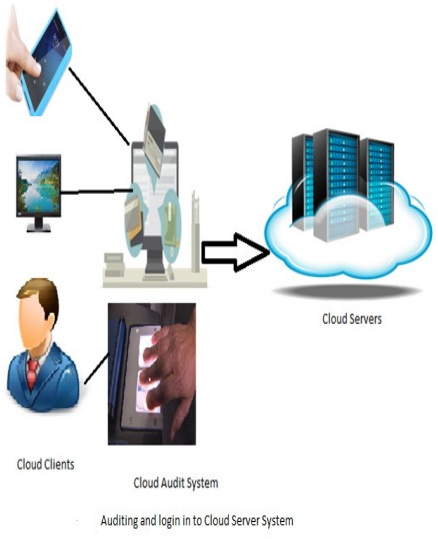
II.Related Work:

To achieving data integrity and deduplication

in cloud, There are two secure systems namely SecCloud and SecCloud+.SecCloud introduces an auditing entity with a maintenance of a Map Reduce cloud, which helps clients generate data tags before uploading as well as audit the integrity of data having been stored in cloud. This design fixes the issue of previous work that the computational load at user or auditor is too huge for tag generation. For completeness of fine-grained, the functionality of auditing designed in SecCoud is supported on both block level and sector level. In addition, SecCoud also enables secure deduplication. Notice that the "security "considered in SecCoud is the prevention of leakage of side channel information. In order to prevent the leakage of such side channel information, we follow the tradition of [3][2] and design a proof of ownership protocol between clients and cloud servers, which allows clients to prove to cloud servers that they exactly own the target data.

III.Proposed Work:

OTP and Biometric Identification: In our Secure Auditing and Deduplicating Data in Cloud by using OTP and Palm vein Technology. we are using OTP and palm vein technology techniques because this technique is better than other techniques .how it should going to be perform while we are enter data in to the cloud and retrieve data from cloud we maintain the secure and don't repeat file which means Deduplicating Data.



Whenever we store data in the cloud in this technique we can get one time password from the Cloud server. The process of storing data or auditing data was at first time the clients are registered with mobile number and also given the client palm lines. In the process of storing and retrieving that we can get password to our registered mobile number by using this hacker should not do hacking, because there is no chances for hacking, for every step of transactions need the otp only so that the hacker doesn't know about that password. Only the candidates or clients know the password through that only we can login.

Next deduplicating Data in cloud. In this process sever side maintain different areas different memory Segmentation for different users. but same area clients are the enter the same information then, we can get information about that already existing or new exist all are know about that. If the client new to cloud to store data then the cloud servers sends the information to those who are existed clients in the cloud.If we lose the mobile we can login based on the Finger Print Recognization for three times, at that time you can authenticate and set your new details, given permission to the only Finger Print Recognization for login in to cloud.

The One Time Password Generator: This OTP is based on the very popular algorithm HMAC SHA. The HMAC SHA is an algorithm generally used to perform authentication by challenge response. It is not an encryption algorithm but a hashing algorithm that transforms a set of bytes to another set of bytes. This algorithm is not reversible which means that you cannot use the result to go back to the source.

A HMAC SHA uses a key to transform an input array of bytes. The key is the secret that must never be accessible to a hacker and the input is the challenge. This means that OTP is a challenge response authentication. The secret key must be 20 bytes at least; the challenge is usually a counter of 8 bytes which leaves quite some time before the value is exhausted. The algorithm takes the 20 bytes key and the 8 bytes counter to create a 8 digits number. This means that there will obviously be duplicates during the life time of the OTP generator but this

doesn't matter as no duplicate can occur consecutively and an OTP is only valid for a couple of minutes.

There are few reasons why this is a very strong method.

- The key is 20 digits
- A password is a couple counter/password, only valid once and a very short time
- The algorithm that generates each password is not reversible
- With an OTP token, the key is hardware protected
- If the OTP is received on your phone, the key always stays at the server

Those few characteristics make the OTP a strong authentication protocol. The weakness in an authentication is usually the human factor. It is difficult to remember many complex passwords, so users often use the same one all across the internet and not really a strong one. With an OTP, you don't have to remember a password, the most you would have to remember would be PIN code (4 to 8 digits) if the OTP token is PIN protected. In the case of an OTP sent by a mobile phone, it is protected by your phone security. A PIN is short but you can't generally try it more than 3 times before the token is locked. The weakness of an OTP if there is one, is the media used to generate or receive the OTP. If the user loses it, then the authentication could be compromised. A possible solution would be to protect this device with a biometric credential, making it virtually totally safe.

Using an OTP sent to a phone: This is usually the authentication method used when a transaction is verified with an OTP. The bank system sends you an OTP and you then have few minutes to enter this OTP. This mechanism doesn't need any synchronization process as the OTP is originally generated by the server and send to a third party device. The server expects that you type the correct OTP within generally 2 minutes. If you fail to do it, you just ask a new OTP and then enter it within the given time. When a system supports both authentication methods, it means that the back-end has 2 different keys and counters; one pair for the OTP token and one pair for the OTP transmitted by SMS.

Biometric Identification System:

The steps in processing a finger image include capture of the image, image processing, feature detection, and matching. The procedures used by different vendors vary in detail, but have a general similarity. This discussion is based primarily on a technical report by Hopkins
(1997), but it includes information from several other vendors, as well.

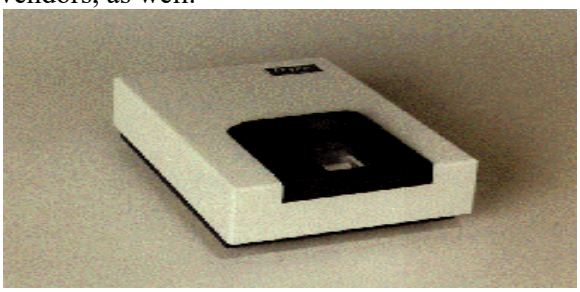
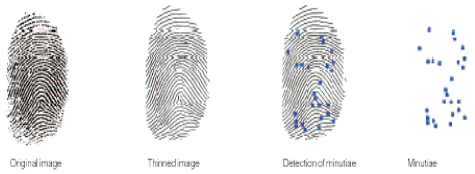


Image capture:

An example of a device for capturing a finger image. This device consists of a light source, a prism on which the finger is placed, one or more lenses, and a digital video camera. The user of the sensor places his or her finger on the dark area of the sensor, where the prism is located. The output of the sensor is a digital image, as illustrated in the first pane. Although this technology is typical of the state of the art, other technologies can also be used, including holographic and thermal imaging technology.

Image processing:

The image produced by the sensor must then be converted to an internal representation that can be analyzed to find identifying characteristics. Levels of gray in the original image are transformed to solid black lines representing fingerprint ridges on a white background. The algorithms that conduct this processing simplify the image, clarify smudged areas, and produce an unambiguous, skeletal image. This simplification process is called thinning and produces a result that is illustrated in the second pane.



Simulated image processing and minutiae extraction

Matching:

Matching algorithms are proprietary products of their respective vendors, and consequently cannot be described in detail. However, all matching algorithms must be able to match images that may be different in quality, coverage, and orientation. Scanned images may be blurred, may contain smudges and discontinuities, and may vary in contrast. The matching algorithm must be able to ignore these quality differences between images taken at different times. In addition, individuals may present different parts of their finger to be imaged, and the orientation of their finger may vary between sessions. The matching algorithm must be able to identify the corresponding areas of the images under these conditions. The result of this step of the process is an index that indicates how similar the images are. If the index is over a threshold level, usually set by the user, then the two images being compared are judged to be made by the same person.

The matching algorithm will then be applied only to images in the same bin or filter category. Binning and filtering can substantially decrease the time required to complete the matching algorithm. It also decreases the likelihood that the algorithm will incorrectly match two images from different fingers (termed a false match). However, because there may be errors in the assignment of images to bins or filter categories, use of binning or filtering increases the likelihood that the algorithm will miss a match between two images from the same finger

.

Biometric Identification System Be Used:

Initial applications of biometric identification technology were in police and military applications. More recently, biometric identification technology has been applied to a wider variety of civilian applications. Some of these applications are briefly described below:

- The Immigration and Naturalization Service (INS) has developed a method that frequent international travelers can use to speed the entry process at selected airports (Wing, 1997).The traveler who has enrolled in the system goes to a kiosk, presents a card, and places the right hand in a hand geometry reader. After verifying the identity of the traveler, the system issues a receipt, and the traveler can bypass normal inspection lanes.

- INS has also used voice recognition as part of an automated point of entry at the U.S.-Canada border. It is also developing, along with other agencies, voice recognition capability for a similar system at the Mexican border..

IV.Conclusion:

The cloud computing technology develops during the last decade, outsourcing data to cloud service for storage becomes an attractive trend, which benefits in sparing efforts on heavy data maintenance and management. Nevertheless, since the outsourced cloud storage is not fully trustworthy, it raises security concerns on how to realize data deduplication in cloud while achieving integrity auditing. So that we are include the finger identification and OTP register mobile, through that we can access our account. If we don't have or loss the mobile, provide three transactions for registered biometric. In case of we have both mobile and biometric we can directly access our account. Through this technology hackers couldn't hake our accounts and we are in safe side.

REFERENCES

[1] Bahuguna, R. D., & Caroline, T. (1996). Prism fingerprint sensor that uses a holographic Optical element. *Applied Optics*, *35*, 5242-5245.
[2] Beale, A. (February 20, 1997). *Facial thermo gram system*. Paoli, PA: Unisys Corporation. Beckwith, B. (November 1997). Illinois biometric identification demonstrations. *Biometrics in Human Services User Group, 1(6).*

[3] Broderick, J., Morrey, B., & Fischer, C. (1997). Network authentication solution. *Info World Electric* [On-line]. Available: http://www.infoworld.com/cgi-bin/displayTC.pl?/970616comp.html

[4] Chandrasekaran, R. (March 30, 1997). Brave new whorl: ID systems using the human body are here, but privacy issues persist. *Washington Post*, p. H1.

[5]BuyyaR,PandeyS,VecchiolaC.Cloudbustoolkitormarketorientedcloudcomputing.Proceedingofthefirstinternationalconferenceoncloudcomputing(CloudCom2009,Springer,Germany).Beijing, China: December1_4, 2009.