ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

Two Factor Authentication for Cloud Service Provider Invoking Biometric Authentication and Multiple Cloud Storage System

Priyanka[1], Narmadha[2] , Gnanasekar [3]

UG Student, Department of CSE, T.J.S Engineering College, Chennai, India[1.2]

Assistant Professor, Department of CSE, T.J.S Engineering College, Chennai, India [3].

ABSTRACT: Cloud storage system provides facilitative file storage and sharing services for distributed clients.. However, some security concerns may impede users to use cloud storage. Among them, the integrity of outsourced files is considered as a main obstacle, since the users will lose physical control of their files after outsourced to a cloud storage server maintained by some cloud service provider (CSP).Thus, the file-owners may worry about whether their files have been tampered with, especially for those of importance. Hence to address integrity, controllable outsourcing and origin auditing concerns on outsourced files, we propose an Two Factor Authentication for Cloud Service Provider Invoking Biometric Authentication and Multiple Cloud storage System. Thus provides desirable features advantageous over existing proposals in securing outsourced data. Allows a user to authorize dedicated proxies to upload data to the cloud storage server on her behalf, e.g., a company may authorize some employees to upload files to the company's cloud account in a controlled way. To make the machine identify the data owner and dedicated proxies, we use an auditor to audit the incoming packets, efficient fingerprint analysis, MAC address, file type, consistence of outsourced and Eliminates complex cryptographic certificates.

I. INTRODUCTION

CLOUD platform provides powerful storage services to individuals and organizations [1]. It brings great benefits of allowing on-the-move access to the outsourced files, simultaneously relieves file-owners from complicated local storage management and maintenance [2]. However, some security concerns may impede users to use cloud storage. Among them, the integrity of outsourced files is considered as a main obstacle [3], since the users will lose physical control of their files after outsourced to a cloud storage server maintained by some cloud service provider (CSP). Thus, the file-owners may worry about whether their files have been tampered with, especially for those of importance. Considerable efforts have been made to address this issue. Among existing proposals, provable data possession (PDP) [4] is a promising approach in proof of storage (PoS). With PDP, the file-owner only needs to retain a small amount of parameters of outsourced files and a secret key. To check whether or not the outsourced files are kept intact, the file owner or an auditor can challenge the cloud server with low communication overheads and computation costs. If some part of the file has been altered or deleted, for example ,due to random hardware failures, the cloud storage server would not be able to prove the data integrity to convince the clients.

II. EXISTING SYSTEM

We observe two critical issues not well addressed in existing proposals.
[1] First, most scheme slack a controlled way of delegable outsourcing. One may note that many cloud storage systems (e.g. Amazon, Dropbox, Google Cloud storage)allow the account owner to generate signed URLs using which any other designated entity can upload, and modify content on behalf of the user. However, in this scenario, the delegate or cannot validate whether or not the authorized one has uploaded the file as specified or verify whether or not the uploaded file has been kept intact. Hence, the delegator has to fully trust the delegates and the cloud server.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

[2]Second, existing PoS-like schemes, including PDP and Proofs of Retrievability (PoR), do not support data log related auditing in the process of data possession proof.Second, existing PoS-like schemes, including PDP and Proofs of Retrievability (PoR), do not support data log related auditing in the process of data possession proof.
[3]Third, no biometric based authentication is been integrated for secure authentication of the users.
[4]Fourth, Multiple cloud storage invoking split and merge concept is not in existence, thus leading to many security threats.

III. PROPOSED SYSTEM

Hence to address integrity, controllable outsourcing and origin auditing concerns on outsourced files, we propose an **identity-based data outsourcing (IBDO) scheme**. In the proposed system, the data owner and designated entities are been audited before accessing the cloud environment.
Thus IBDO provides desirable features advantageous over existing proposals in securing outsourced data. Our IBDO scheme provides following advantages,

1. Allows a user to authorize dedicated proxies to upload data to the cloud storage server on her behalf, e.g., a company may authorize some employees to upload files to the company's cloud account in a controlled way. To make the machine identify the data owner and dedicated proxies, we use effective **fingerprint analysis, MAC address, file type, consistence of outsourced.**
2. For fingerprint analysis, we have used **minutiae maps algorithm** for fingerprint feature extraction and matching.
3. Eliminates complex cryptographic certificates, thus using **hash function algorithm (SHA).**

Once the user, dedicated proxies, data file is been audited, the file is stored in cloud server. Thus to overcome the security threats, this paper proposes **multiple cloud storage**. Thus the common forms of data storage such as files and databases of a specific user is split and stored in the various cloud storages (e.g. Cloud A and Cloud B). Databases consists of tables, rows and columns. Databases are easy to store in multiple cloud storages. Our application will act as a combiner and store different parts of the table such as rows and columns in multiple clouds using **Vertical fragmentation** and **horizontal fragmentation**. These rows and columns will be converted into hash value using **hash function** algorithm and stored in each clouds. Thus once the authorized token for the specific file is requested, searchable encryption allows keyword search on encrypted data and combines the fragments and provides the requested file to the user. For cloud storage, we are using public clouds, namely Dropbox, CloudMe. Thus multiple cloud schema provides high information security against cloud service provider trying to access the data owner files. The whole proposed system provides confidentiality, security, integrity for the data owner information.

MODULES:

1. **IDENTITY MANAGEMENT – DATA OWNERS / DEDICATED PROXIES:**

Fingerprint feature extraction:
Fingerprint based biometric authentication is an important and widely used biometric type authentication because of its cost, accuracy and feasibility. In our proposed system, the user fingerprint feature are extracted and verified using Minutiae Map algorithm (MM) [1]. Minutiae Map algorithm identifies the fingerprint ridges and extracts the bifurcation and termination values from the input fingerprint image. Ridge termination is the point at which ridge ends. Bifurcation is the point at which ridge splits into two halves which is shown in the below figure. Our proposed system provides the respective user fingerprint total bifurcation, termination values along with its location (X, Y coordinates) and stores in the database during user registration.

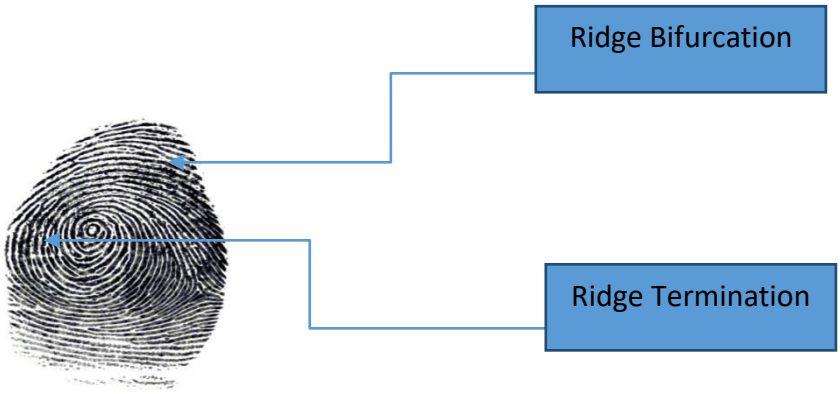
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018



In our proposed system, ideal thinned ridge is considered. We assume usually a thinned ridge will have a value 1 or 0. The algorithm uses 3*3 windows to scan the image and the bifurcation and termination in the final output image shall be represented by a dot. Let's consider (x,y) denote the pixel on the thinned ridge and N_0, n_1, ……N_7 denote its neighbours.

A pixel (x,y) is a ridge ending if,

$$\sum_{i=0}^{7} Ni = 1$$

A pixel (x,y) is a ridge bifurcation if,

$$\sum_{i=0}^{7} Ni > 2$$

2. DATA OWNER / DEDICATED PROXIES BEHAVIOUR ANALYSIS:

In this module the data owner / dedicated proxies behavior is been analyzed. For this we keep a log of origin, file types, consistence of outsourced. We use techniques to detect the MAC address whenever the data owner / dedicated proxies access. If they access from different machines or upload / access different file types an alert e-mail would be sent to the data owner. On approvalby the data owner the dedicated proxies would be allowed to access inside the application.

3. ELIMINATES COMPLEX CRYPTOGRAPHIC CERTIFICATES

To eliminate complex cryptographic certificates we used SHA algorithm for converting the plain text to cipher text.

- Step 1: Append Padding Bits….

  Message is "padded" with a 1 and as many 0's as necessary to bring the message length to 64 bits less than an even multiple of 512.

- Step 2: Append Length....

  64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.

- Step 3: Prepare Processing Functions….

  SHA1 requires 80 processing functions defined as:

  f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 <= t <= 19)
  f(t;B,C,D) = B XOR C XOR D (20 <= t <= 39)
  f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)
  f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)

- Step 4: Prepare Processing Constants....

  SHA1 requires 80 processing constant words defined as:

  K(t) = 0x5A827999 (0 <= t <= 19)
  K(t) = 0x6ED9EBA1 (20 <= t <= 39)
  K(t) = 0x8F1BBCDC (40 <= t <= 59)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

K(t) = 0xCA62C1D6 (60 <= t <= 79)

- Step 5: Initialize Buffers….

SHA1 requires 160 bits or 5 buffers of words (32 bits):

H0 = 0x67452301
H1 = 0xEFCDAB89
H2 = 0x98BADCFE
H3 = 0x10325476
H4 = 0xC3D2E1F0

- Step 6: Processing Message in 512-bit blocks (L blocks in total message)….

This is the main task of SHA1 algorithm which loops through the padded and appended message in 512-bit blocks.

Input and predefined functions:

M[1, 2, ..., L]: Blocks of the padded and appended message f(0;B,C,D), f(1,B,C,D), ..., f(79,B,C,D): 80 Processing Functions K(0), K(1), ..., K(79): 80 Processing Constant Words H0, H1, H2, H3, H4, H5: 5 Word buffers with initial values

- Step 7: Pseudo Code….

For loop on k = 1 to L
(W(0),W(1),...,W(15)) = M[k] */* Divide M[k] into 16 words */*
For t = 16 to 79 do:
W(t) = (W(t-3) XOR W(t-8) XOR W(t-14) XOR W(t-16)) <<< 1
A = H0, B = H1, C = H2, D = H3, E = H4
For t = 0 to 79 do:
TEMP = A<<<5 + f(t;B,C,D) + E + W(t) + K(t) E = D, D = C,
C = B<<<30, B = A, A = TEMP
End of for loop
H0 = H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E
End of for loop

4. SPLIT AND MERGE TECHNIQUE:

Cloud Storage usually contains business-critical data and processes, hence high security is the only solution to retain strong trust relationship between the cloud users and cloud service providers. Thus to overcome the security threats, this paper proposes **multiple cloud storage**. Thus the common forms of data storage such as files and databases of a specific user is split and stored in the various cloud storages (e.g. Cloud A and Cloud B).

Databases consists of tables, rows and columns. Databases are easy to store in multiple cloud storages. Our application will act as a combiner and store different parts of the table such as rows and columns in multiple clouds using **Vertical fragmentation** and **horizontal fragmentation**. These rows and columns will be converted into hash value using **hash function** algorithm and stored in each clouds. During response our application combines the data and sends to the verifier.

Files are stored in multiple clouds using cryptographic data splitting. The file is split into fragments and stored in distinct cloud servers with encrypted key. Thus once the authorized token for the specific file is requested, searchable encryption allows keyword search on encrypted data and combines the fragments. This is sent to the verifier.

5. DATA STORAGE:

A cloud server is defined as an entity which contains huge data storage managed by cloud service provider. This paper focuses on providing high security for user data in public cloud storages because there is a huge demand of security prospects in public cloud storages. Security threats may include some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud and cloud based attacks.

For Cloud storage we have configured public clouds. Public clouds is a personal cloud storage service (sometimes referred to as an online backup service) that is frequently used for file sharing and collaboration. The service provides 2

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

gigabytes (GB) of storage for free and up to 100 GB on various for-fee plans. Public cloudsis cloud storage service that enables users to store files on remote cloud servers and the ability to share files within a synchronized format.

SYSTEM REQUIREMENT:

SOFTWARE REQUIREMENTS

- Operating system : Windows 7 Professional.
- Coding Language : Java, Swing.
- Front End Tool : Net beans 7.0
- Front End : HTML, CSS, JavaScript
- Database : MS Sql.
- Back End Tool : SQL Yog.

IV. FUTURE WORK

In future, combination of all biometric based authentication can be implemented like Face, IRIS, Finger vein. Also implementing in real time data center would provide many challenges which can be addressed as a future work of this project.

REFERENCES

[1] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud data protection for the masses," Computer, IEEE, vol. 45, no. 1, pp. 39–45, Jan 2012.
[2] C.-K. Chu, W.-T. Zhu, J. Han, J. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," Pervasive Computing, IEEE, vol. 12, no. 4, pp. 50–57, Oct 2013.
[3] K. Yang and X. Jia, "Data storage auditing service in cloud computing: challenges, methods and opportunities," World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.
[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security. New York, NY, USA: ACM, 2007, pp. 598–609.
[5] J. Sun and Y. Fang, "Cross-Domain Data Sharing in Distributed Electronic Health Record Systems," Parallel and Distributed Systems, IEEE Transactions on, vol. 21, no. 6, pp. 754–764, 2010.
[6] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography based Secure EHR System for Patient Privacy and Emergency Healthcare," in Distributed Computing Systems (ICDCS), 2011 IEEE 31st International Conference on. IEEE, 2011, pp. 373–382.
[7] L. Guo, C. Zhang, J. Sun, and Y. Fang, "PAAS: A Privacy SPreserving Attribute-Based Authentication System for eHealth Networks," in Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on. IEEE, 2012, pp. 224–233.
[8] A. Juels and B. S. Kaliski, Jr., "PoRs: Proofs of Retrievability for Large Files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, New York, NY, USA, 2007, pp. 584– 597.
[9] H. Shacham and B. Waters, "Compact proofs of retrievability," Journal of Cryptology, vol. 26, no. 3, pp. 442–483, 2013.
[10] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "PrivacyPreserving Public Auditing for Secure Cloud Storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–275, 2013.