Biometric Based User Authentication and Privacy Preserving In Cloud Environment

Jaichandran R[a], Muthuselvan S[b], Rajaprakash S[c], Vibin C[c] , Jeba Joel J[d], and Abhishek S Gopan[e]

A
Department of Computer Science and Engineering, Aarupadai Veedu Institute of
Technology, Vinyaka Missions Research foundation (Deemed to be University),
Paiyanoor, Tamil Nadu , India

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: Cloud technology provides advantage of storage services for individuals and organizations thus making file access easy and simple irrespective of location. The major concern is the security while the file is been outsourced. Maintaining integrity, file unchanged, gaining confidentiality during file outsourced plays an important role. In this paper, we propose identity based data outsourcing technique to provide data security during authorization and storage. For data authorization we propose finger print based authentication. The fingerprint based authentication is performed using Minutae Map algorithm (MM). For data security we convert the data owner files to hash values using SHA algorithm. Finally in the cloud storage stage, data security and data availability is addressed using multiple cloud storage system.

Keywords: Minutae Map, SHA algorithm, multiple cloud storage

1. Introduction

Cloud computing is an emerging technology making accessibility of applications globally possible. This saves much time and cost for the data owners to migrate their applications to the cloud server. The major significant part to motivate data owners to migrate to cloud server is because of SaaS, IaaS, PaaS services. The major concern in migrating to cloud server is the security aspect. The data owner integrity plays an important role and concern because the data owner loses his physical control once the file is been outsourced to a third party cloud storage. Usually the cloud storage is managed by few cloud service provider (CSP) [1].

This paper address two major concerns, 1. Data security during authorization and 2. Data security and data availability in cloud storage. Thus in the existing approaches, authorization by data owners and authorized delegates is not given much importance. Authorization plays an significant role in analyzing the request and provide response. There are many tools to execute illegal authorization which makes the authorization process difficult. Many big cloud storage providers like amazon, dropbox, Google provide initially get the permission for designated entity to upload the data files on behalf of the data owner. In this case, the system cannot able to validate whether the delegator or authorized delegated entities or not authorized persons have uploaded, modified the file [2].

We observe two critical issues not well addressed in existing proposals. First, most schemes lack a controlled way of delegatable 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 sometime the data owner has to trust the delegeatees and the cloud service provider. But to gain confidence and maintain integrity the application should be able to verify and validate authorized and unauthorized users so that the files won't be changed by unauthorized users [3] [4].

In existing approach does not ensure to support with data availability all the time. In existing approach the application is stored in a single cloud during maintenance or when the server is down, data availability is a major concern. In this case, user has to wait until the application is up again to request and get the response. To overcome this problem, multiple cloud storage system can be introduced to make the data available from server 2 if server 1 is under maintenance [5].

2. Related Works

[6] This research paper explains about the cloud storage system in which whenever the data owner get changes then the data owner again has to re-assign the designated entities in the cloud server. This is time consuming and everytime the data owner has to sign the contract with modified designated entities.

[7] This paper briefs multiple cloud storage scheme which can provide easy data migration of applications to cloud environment. In this article the authors also addressed key exposing issue as well.

[8] This paper elaborates existing auditing schemes in which it explains about the homomorphic signatures. This paper states that anyone can able to audit the data owner outsourced data without even having the knowledge of the credentials of the data owner. This is designed in the concept of data owner can easily assign the auditing task to the third party preserving the private information.

[9] This article proposed a scheme through which the delegate can perform auditing protocol to become the delegate for the outsourced data files of respective data owner's. This scheme also discuss prevention measures for collusion attacks.

[10] This paper explains multi-cloud storage system. In existing approach, storage of data in single cloud always have the risk of data availability failure due to attackers tries to perform cloud attack and compromise the server. This paper propose multiple cloud storage which reduces the risk of unavailability. This proposed scheme provides storage data in customer available budget.

[11] This paper discuss about fingerprint analysis by extraction of features like bifurcation and termination points from the finger. This paper states minutae map based feature extraction algorithm provides promising matching accuracy.

3. Methodology

The proposed architecture explains securing user data using fingerprint based authentication. For fingerprint analysis we have used standard dataset images. Also used minutiae map algorithm for fingerprint feature extraction and comparison. Along with the user fingerprint, the respective user IP and MAC address are stored. If the user satisfies the above steps then the user can able to upload and access the data from cloud. For cloud environment we have used public cloud named CloudMe. To secure the user data the user files are encrypted using SHA algorithm and stored in the cloud.

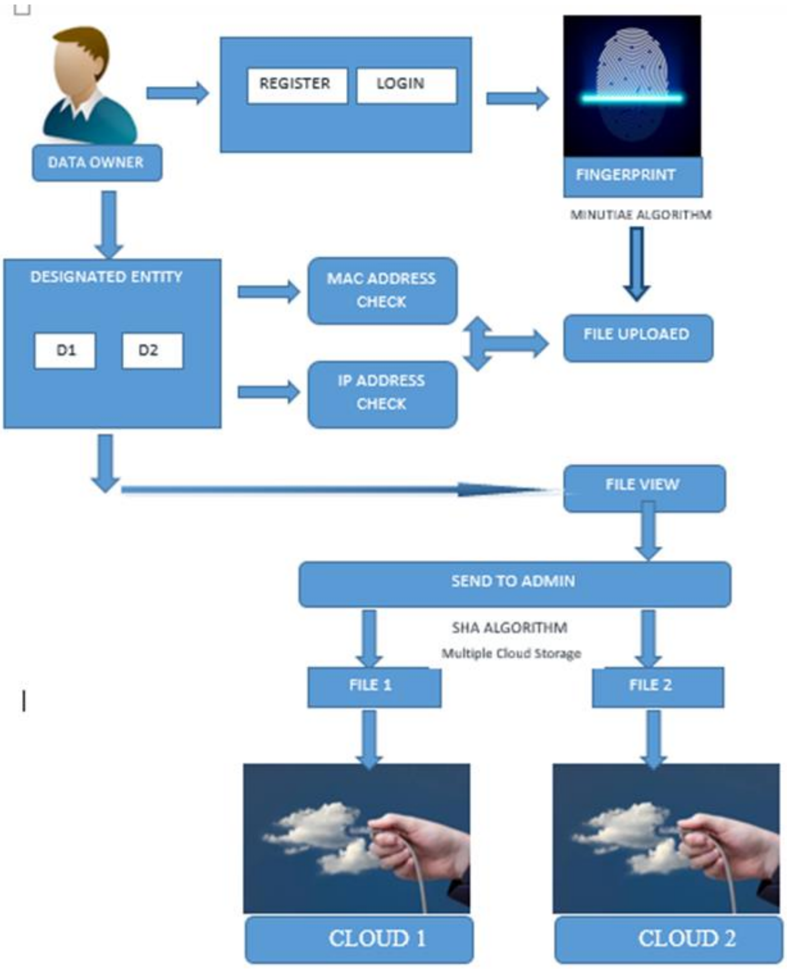


Fig 1. Proposed Architecture

We propose identity-based data outsourcing technique in which the data owner and designated entities are audited before accessing the files and getting into the application. The IBDO technique mainly provides two advantages during data authorization and data storage. The data authorization phase involves mainly authorizing the data owner and designated entities. Designated entities are nothing but can able to upload, modify, delete the file on behalf of data owner, when the data owner is unavailable. The application find it difficult to validate authorized and unauthorized users during authorization. To resolve this problem, we proposed fingerprint based analysis along with MAC address validation, file type analysis makes the unauthorized access of files difficult making collusion attack also difficult for the intruders. For fingerprint analysis, we have used minutiae maps algorithm for fingerprint feature extraction and matching. Minutiae Map algorithm identifies the bifurcation and termination values from the fingerprint image. Ridge termination is the point at which ridge ends. Bifurcation is the point at which ridge splits into two halves. This is been explained in the below figure 2. Our module extracts user fingerprint total bifurcation, termination values along with its location (X, Y coordinates) and stores in the database during user registration.

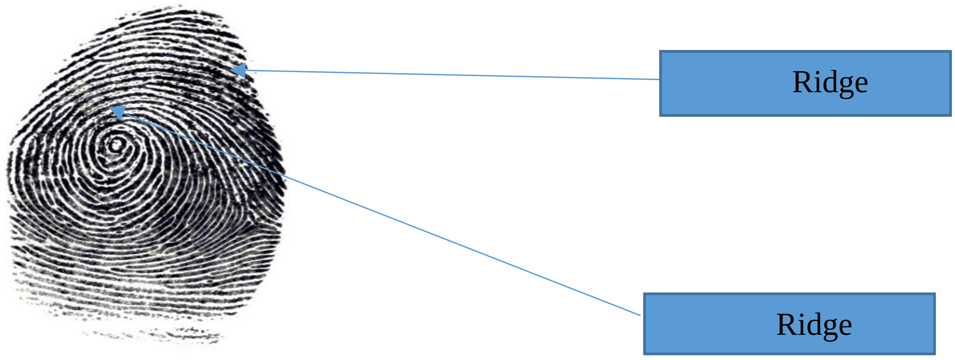


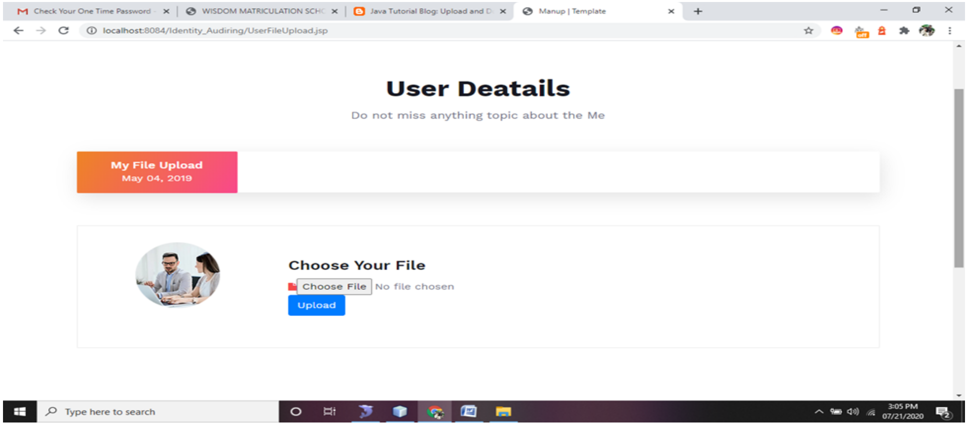
Fig 2. Fingerprint analysis using minutae map algorithm

Figure 2 explains the fingerprint analysis using minutae map algorithm extracting the bifurcation and termination features from the input fingerprint image.

To add more security protocols along with fingerprint analysis, we integrated MAC address validation and previous file type access pattern analysis.

The data security during data transmission and storage system is provided using SHA algorithm and multiple cloud storage system. The SHA algorithm eliminates the complex cryptographic process by usage of hash values. Finally data security and data availability is performed using multiple cloud storage. In this the data owner file is duplicated and stored in multiple cloud servers to make the data available whenever the server is down due to maintenance. For cloud storage, we are using public clouds, namely 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.

4. Experimental Results


Check Your One Time Password
WISDOM MATRICULATION SCHC
Java Tutorial Blog: Upload and D
Manup | Template

localhost:8084/Identity_Audiring/UserFileUpload.jsp

User Deatails

Do not miss anything topic about the Me

My File Upload
May 04, 2019

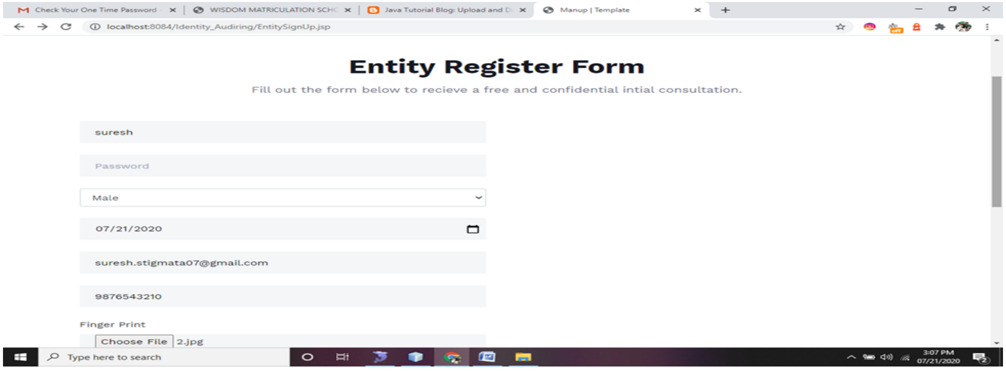
Choose Your File

Choose File No file chosen

Upload
Type here to search
3:05 PM
07/21/2020

Fig 3. Dataowner file upload

After successful biometric based authentication, the data owner can able to access the application and can able to upload the file.


Check Your One Time Password
WISDOM MATRICULATION SCHC
Java Tutorial Blog: Upload and D
Manup | Template

localhost:8084/Identity_Audiring/EntitySignUp.jsp

Entity Register Form

Fill out the form below to recieve a free and confidential intial consultation.

suresh

Password

Male

07/21/2020

suresh.stigmata07@gmail.com

9876543210

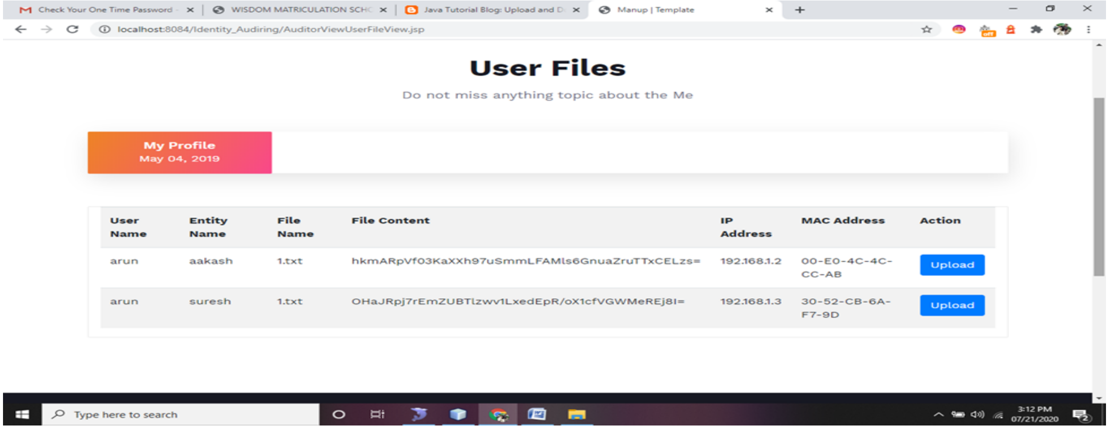
Finger Print

Choose File 2.jpg

Type here to search
3:07 PM
07/21/2020

Fig 4. Designated Entity enrollment

The data owner can assign designated entities to perform the operational activities on behalf of his absence. While registering the designated entities, the data owner has to submit the designated entities fingerprint image as well.


Check Your One Time Password
WISDOM MATRICULATION SCHC
Java Tutorial Blog: Upload and D
Manup | Template
localhost:8084/Identity_Audiring/AuditorViewUserFileView.jsp
Type here to search
3:12 PM
07/21/2020

User Files

Do not miss anything topic about the Me

My Profile
May 04, 2019

User Name	Entity Name	File Name	File Content	IP Address	MAC Address	Action
arun	aakash	1.txt	hkmARpVf03KaXXh97uSmmLFAMls6GnuaZruTTxCELzs=	192.168.1.2	00-E0-4C-4C-CC-AB	Upload
arun	suresh	1.txt	OHaJRpj7rEmZUBTlzwv1LxedEpR/oX1cfVGWMeREj8I=	192.168.1.3	30-52-CB-6A-F7-9D	Upload

Fig 5. MAC, IP address and file type pattern

Figure 5 shows the view page of the users in our application. The view page managed by the super admin consists of data owner name, designated entities, file types, ip address and mac address. If there is any discrepancy the respective entity would be blocked and allowed for further inspection.

5. Conclusion

Motivated by the application needs, this paper addresses the problem of secure authorization and data security. For secure authorization, we used fingerprint analysis using minuate map algorithm. File security is performed using SHA algorithm. Thus the proposed system is provably secure and efficient by making the data available using multiple cloud storage system.

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. 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. Kiruthika, U., Somasundaram, T.S. & Raja, S.K.S. Lifecycle Model of a Negotiation Agent: A Survey of Automated Negotiation Techniques. Group Decis Negot (2020). https://doi.org/10.1007/s10726-020-09704-z
10. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy Preserving Public Auditing for Secure Cloud Storage,” Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–275, 2013.
11. Y. Wang, Q. Wu, B. Qin, X. Chen, X. Huang, and J. Lou, “Ownership-hidden group-oriented proofs of storage from prehomomorphic signatures,” Peer-to-Peer Networking and Applications, pp. 1–17, 2016.
12. Sampathkumar, A., Murugan, S., Rastogi, R., Mishra, M.K., Malathy, S. and Manikandan, R., 2020. Energy Efficient ACPI and JEHDO Mechanism for IoT Device Energy Management in Healthcare. In Internet of Things in Smart Technologies for Sustainable Urban Development (pp. 131-140). Springer, Cham.