SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

CLIENTCENTRICFS AND BIOCRYP FOR SECURE ACCESS OVER OUTSOURCED DATA IN CLOUD SERVER

Oviya.E[1], Prakash.P[2], Shanlee.R[3], Vinothini.K[4], Kalaiarasi.A[5]

[1,2,3,4,5] *UG Student, Department Of Computer Science And Engineering,*
Assistant Professor, Computer Science and Engineering,
N.S.N. College of Engineering and Technology, Karur , Tamil Nadu, India

ABSTRACT

Cloud computing is emerging as the most suitable paradigm for individuals and organizations to access inexpensive, scalable, ubiquitous, and on-demand computing resources, application and data storage services. With the growing popularity of cloud computing, the number of enterprises and individuals shifting towards the use of cloud has increased rapidly. As a result, a vast amount of important personal information and critical organization data, such as personal health records, government documents, and company finance data, etc., are transmitted across the Internet and stored in cloud servers. However, outsourcing sensitive data suffers from critical security threats, privacy, and access control problems. These are common concerns of organizations and individuals using cloud services. When data owners migrate their sensitive data to the cloud, they lose an element of control over their data. With this in mind, this project presents a user-side fingerprint based encrypted file system named Client Centric FS. Moreover, a Biometric based cryptographic protocol BIOCRYP was proposed which uses symmetric encryption algorithms in order to improve the security and performance of the personal and shared files that are outsourced.

KEYWORDS- *Cloud computing, Biometric, Data privacy, Encryption, Sensors.*

INTRODUCTION

Data is one of the most valuable assets that any company can hold. One of the best ways to store these assets is within the cloud. Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-go pricing. Instead of buying, owning, and maintaining physical data centres and servers, technology services, such as computing power, storage, and databases can be accessed on an as-needed basis from a cloud provider like Amazon Web Services (AWS).

Types of Cloud Services

Cloud computing is not a single piece of technology like a microchip or a cellphone. Rather, it's a system primarily comprised of three services: software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS).

Software-as-a-service (SaaS)

It involves the licensure of a software application to customers. Licenses are typically provided through a pay-as-you-go model or on-demand. This type of system can be found in Microsoft Office's.

Infrastructure-as-a-service (IaaS)

It involves a method for delivering everything from operating systems to servers and storage through IP-based connectivity as part of an on-demand service. Clients can avoid the need to purchase software or servers, and instead procure these resources in an outsourced, on-demand service. Popular examples of the IaaS system include IBM Cloud and Microsoft Azure.

Platform-as-a-service (PaaS)

It is considered the most complex of the three layers of cloud-based computing. PaaS shares some similarities with SaaS, the primary difference being that instead of delivering software online; it is actually a platform for creating software that is delivered via the Internet. This model includes platforms like Sales force.com and Hero.

PROBLEMS IDENTIFIED

With the increase in data volumes, data handling has become the talk of the town. As companies begin to move to the cloud, there is a higher emphasis ensuring everything is safe and secure, and that there is no risk of data hacking or breaches.

SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

Since the cloud allows people to work without hardware and software investments, users can gain flexibility and data agility. However, since the Cloud is often shared between a lot of users, security becomes an immediate concern for Cloud owners. Cloud computing presents many unique security issues and challenges. In the cloud, data is stored with a third-party provider and accessed over the internet. This means visibility and control over that data is limited. It also raises the question of how it can be properly secured.

Cloud service providers treat cloud security issues and risks as a shared responsibility. In this model, the cloud service provider covers security of the cloud itself, and the customer covers security of what they put in it. In every cloud service—from software-as-a-service (SaaS) like Microsoft Office 365 to infrastructure-as-a-service (IaaS) like Amazon Web Services (AWS)—the cloud computing customer is always responsible for protecting their data from security threats and controlling access to it.

Biometrics are physical or behavioural human characteristics that can be used to digitally identify a person to grant access to systems, devices or data.

Types of Biometrics

DNA

DNA (Deoxyribonucleic Acid) is a chemical substance found in each of the approximately 100 trillion cells within the human body.

Ear

The shape and features of the human ear reveal specific characteristics that allow for the identification of an individual.

Eyes – Iris

The iris is the coloured circular segment at the front of the eye that contains the pupil at its centre.

Eyes – Retina

The retina lies at the back of the eye and detects light which is transmitted as electrical impulses to the optic nerve.

Eyes - Sclera vein

The sclera is the white part of the eye and when the eyeball turns either to the left or the right a network of veins is displayed.

Face

Face biometrics use aspects of the facial area to verify or identify an individual.

Finger Geometry

Finger geometry is a biometric process that captures features such as the shape and surface area of each finger, its length, width, thickness and the distance between the fingers.

Finger print(including palm print)

Fingerprints are formed by the raised papillary ridges that run across the skin's surface.

Gait

Every human has a specific way of walking and running and factors such as the subject's overall physique, stride and speed of movement can be captured for analysis.

Hand Geometry

Hand geometry biometric systems incorporate the salient features of finger geometry but also include the surfaces of the hand itself and its side profile.

Keystrokes (Typing)

The actions involved in typing on a keyboard can be used to identify the typist once a reference session of their typing has been recorded for comparison.

Odour

The primary body odour of individuals has been studied to determine the extent that it is distinctive is stable over time and potentially can be separated from other odours conveyed by the human body.

Signatures

The use of handwritten signatures to authenticate paper documents has a long history but in more recent times the application of modern electronic biometric techniques has automated the process.

Vascular (Vein)

The arrangement of veins in fingers and hands form a unique pattern that can be used to identify an individual.

Voice

A person's voice – i.e., the way they sound when they speak – is the result of a combination of distinctive physical attributes and distinctive behavioural attributes.

Fingerprint Biometric Authentication

Fingerprint Authentication is the act of verifying an individual's identity based on one or more of their fingerprints. The concept has been leveraged for decades across various efforts including digital identity, criminal justice, financial services, and border protections.

Fingerprint Scanners

There are three types of fingerprint scanners: optical, capacitive, and ultrasound.

SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

- **Optical scanner** takes a photo of the finger, identifies the print pattern, and then compiles it into an identification code.

- **Capacitive scanner** works by measuring electrical signals sent from the finger to the scanner. Print ridges directly touch the scanner, sending electrical current, while the valleys between print ridges create air gaps. A capacitive scanner basically maps out these contact points and air gaps, resulting in an absolutely unique pattern. These are the ones used in smart phones and laptops.

- **Ultrasonic scanners** will make their appearance in the newest generation of smartphones. Basically, these will emit ultrasounds that will reflect back into the scanner. Similar to a capacitive one, it forms a map of the finger unique to the individual.

Fingerprint Biometric Cryptosystem

Biometric Cryptography, also called Biometric Tokenization, refers to an authentication that combines inherence factors with public-key infrastructure (PKI). Biometric cryptosystems combine cryptography and biometrics to benefit from the strengths of both fields. Biometrics and cryptography are tightly coupled: the secret key is bound to the biometric information and the biometric template is not stored in plain form. It is convenient to use biometric traits for encryption, for instance someone using his fingerprint or handwritten signature to encrypt a document and securely send it over public network.

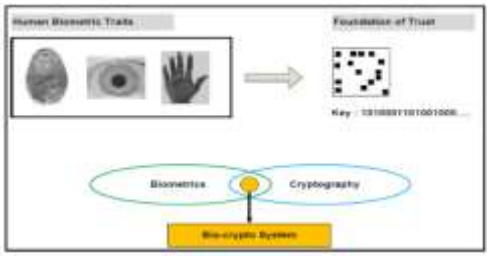

Fig. 1 BIOCRYPT

Biometric Encryption or BIOCRYPTs, is defined as process in which the owner is protected against the misuse of template data by a hacker with the help of cryptography approaches and algorithms. This process is alternatively called as 'Private Verification' falls under 'Private Biometrics'. Merging cryptography with biometrics is a new research area.

The cryptography technology needs cryptography key. This key should be as large and as random as possible. Generating such a key is however a non-trivial task. On the other hand, biometric data of a person is the richest source of randomness. This fact can be exploited to generate a random pattern and hence cryptographic key. For example, combining 10 fingerprint images of a person gives 1010 random pattern.

PROPOSED SYSTEM

The proposed system presents a user-side biometric based encrypted file system named ClientCentricFS. A hybrid cryptographic scheme was proposed that combines Fingerprint based user authentication and biometric encryption algorithms in order to improve the security and performance of the personal and shared files that are outsourced. Biometric encryption is used to encrypt the contents of outsourced files in the CCFS. The goals of the proposed ClientCentricFS are twofold. First, design a cryptographic layer that effectively encrypts all files that are outsourced to the cloud storage in a highly secure and transparent manner. Second, enable a secure data sharing of cloud storage at the granularity of individual files with the proposed CCFS.

Client Centric File System

It's a client-centric solution, which means that it contains the master copies of all the data files which are stored inside the cloud. Files are directly synchronized to storage gateways in every location in real-time for allocation. File locking and file sharing are also frequently managed in the client centric file system, allowing multiple users to access similar files from the cache without requiring to download the content from the cloud every time.

User-centric security management enables data owner to apply different security application settings to different data user roles. Data owner can create several user roles, assign an appropriate user role to each user, and define different application settings to the devices owned by users with different roles. Depending on the role of this employee in the company, Data owner can expand or limit the rights of this person to change application settings.

Client Centric Fingerprint Recognition

Fingerprint biometric is one of the most popular and widely used for authentication. The proposed system uses fingerprint at the matching score level for biometric identification. Convolutional neural networks (CNN) based fingerprint methodology is presented in this system. Input image is enhanced during preprocessing phase. Matching the enhanced fingerprint is done in recognition phase. The overall system performance is enhanced by realizing preprocessing and recognition phases. Performance of the system is evaluated and measured by FAR (False Acceptance Rate) and FRR (False Rejection Rate).

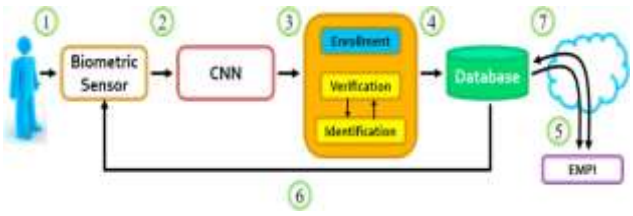

Fig.2 CNN Fingerprint Authentication

SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

Client Centric Fingerprint Enrollment

Enrollment mode is a phase of learning to gather biometric data about whom to recognize. The images are collected from a single biometric trait in the enrolment phase and are processed to obtain a clear image as well as to correct distortions and to obtain the region of interest for extracting features. The feature extraction module extracts the details from the pre-processed image. The feature vector is created by extracting specific features from the image function and storing them in a database.

Client Centric Fingerprint Authentication

In the query stage, a fingerprint is captured using sensor B, it is pre-processed using the same method and the features are extracted using the same descriptor used in the enrollment stage. Then the similarity between features S1 of the query fingerprint captured from sensor B and the features S2 retrieved from the template database by the user ID is calculated to decide whether there is a “match” or “non-match”;

Symmetric Key Encryption

Symmetric encryption uses a common secret key for both encryption and decryption. Private key encryption is best suited to be used in trusted work groups. It is fast and efficient, and properly secures large files. The leading private key encryption is DES (Data Encryption Standard). It has been extensively used and is considered to be strong encryption. Other types of private key encryption include: Triple-DES, IDEA, RC4, MD5, Blowfish and Triple Blowfish. Secret-key, single-key, shared-key, one-key, and private-key encryption are other words for symmetric-key cryptography.

Key Gen

The proposed Model takes as input the given JPEG/JPG image and gives as output a 64-bit key. The key generated is input to the parity drop table DES key generator.

Client Centric DES Symmetric Key Encryption and Decryption

Client-side biometric encryption is the cryptographic technique of encrypting data on the sender's side, before it is transmitted to a server such as a cloud storage service. Client-side encryption features an encryption key that is not available to the service provider, making it difficult or impossible for service providers to decrypt hosted data. Client-side encryption allows for the creation of applications whose providers cannot access the data its users have stored, thus offering a high level of privacy.

ADVANTAGES

- Enhances the security strength and reduces space for key storage.
- Secure Biometric Lock System for Files
- There is no need to remember the key as it is generated from user's fingerprint.

This approach also can be implemented using different biometric traits like iris, face, voice etc.

CONCLUSION

In this project, Client Centric FS is introduced. CCFS is a user-side fingerprint based encrypted file system that is implemented to secure outsourced files to cloud storage systems. It can enforce a secure file system mount over the cloud synchronized directory to perform a transparent encryption on per-file basis using BIOCRYP Key. CCFS does not introduce dependencies to the asymmetric encryption ciphers, but rather proposes a Biometric Symmetric encryption scheme that combines Fingerprint and BIOCRYP Key which is used to encrypt files for the outsourced personal and shared files. In addition, CCFS uses the IBE scheme to facilitate the outsourced file sharing accessible only by authorized users with appropriate secret keys. CCFS can guarantee the integrity of the outsourced data files and the file system data structure against tampering and deletion attacks. The performance of the proposed CCFS on different file sizes has been quantitatively evaluated on representative hardware and file sizes. Security analysis show that the proposed CCFS is highly secure and it can effectively resist attacks, such as brute-force, eavesdropping, man-in-the-middle, offline dictionary, and collusion attacks on outsourced files.

REFERENCES

1. *O. A. Khashan and M. AlShaikh, ``Edge-based lightweight selective encryption scheme for digital medical images,'' Multimedia Tools Appl., vol. 79, pp. 26369-26388, Jul. 2020*
2. *C. Yuan, X. Sun, and Q. M. J. Wu, “Difference co-occurrence matrix using BP neural network for fingerprint live detection,” Soft Computing, vol. 23, no. 13, pp. 5157–5169 2019.*
3. *E. Erdem and M. T. Sandıkkaya, “OT PaaS–One Time Password as a Service,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 743–756, 2019.*
4. *Sanchez-Gomez, J. Diaz, L. Hernandez-Encinas, and D. Arroyo, ``Review of the main security threats and challenges in free-access public cloud storage servers,'' in Computer and Network Security Essentials. Cham, Switzerland: Springer, 2018, pp. 263-281.*
5. *O. A. Khashan and N. M. Khafajah, ``Secure stored images using transparent crypto filter driver,'' IJ New Secure., vol. 20, no. 6, pp. 1053-1060, 2018.*
6. *G. Panchal and D. Samanta, “A novel approach to fingerprint biometric based cryptographic key generation and its applications to storage security,” Computers & Electrical Engineering, vol. 69, pp. 461–478, 2018.*
7. *S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, “Chaotic Map-Based Anonymous User Authentication Scheme with User Biometrics and Fuzzy Extractor for Cloud sourcing Internet of Things,” IEEE*

SJIF Impact Factor 2022: 8.197| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 7 | Issue: 6 | June 2022 - Peer Reviewed Journal

Internet of Things Journal, vol. 5, no. 4, pp. 2884–2895, Aug 2018.

8. *A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment," IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4900–4913, 2018.*
9. *Q. Wei, H. Zhu, R. Lu, and H. Li, "Achieve efficient and privacy preserving online fingerprint authentication over encrypted outsourced data," in 2017 IEEE International Conference on Communications. IEEE, 2017, pp. 1–6.*
10. *C. Zhang, L. Zhu, and C. Xu, "An efficient privacy-preserving biometric identification based on perturbed term in the cloud," Information Sciences, vol. 409, pp. 56–67, 2017.*
11. *D. Leibenger, J. Fortmann, and C. Sorge, ``Encryption FS goes multi-user: Adding access control to an encrypted file system,'' in Proc. IEEE Conf. Common Net Secure (CNS), Oct. 2016, pp. 525-533.*
12. *A. A. Nasiri and M. Fathy, "Alignment-free fingerprint cryptosystem based on multiple fuzzy vaults," in Artificial Intelligence and Signal Processing (AISP), 2015 International Symposium on. IEEE, 2015, pp. 251–255.*
13. *G. P. Blanton M, "Secure and efficient iris and fingerprint identification," Biometric Security, 2015.*
14. *O. A. Khashan, A. M. Zin, and E. A. Sundararajan, ``Image FS: A transparent cryptography for stored images using a file system in user space,'' Frontiers Inf. Technol. Electron. Eng., vol. 16, no. 1, pp. 2842, Jan. 2015.*
15. *Z. J. F. Q. HE Kang, LI Mengxing, "Finger code based remote fingerprint authentication scheme using*
16. *homomorphic encryption," Computer Engineering and Applications, km.vol. 49, no. 24, pp. 78–82, 2013.*