International Journal of Emerging Trends in Science and Technology
8 (2) December 2022, 14-16
http://www.publishingindia.com/ijetst

Bio Metric Based Security using Cloud Centric File System

B. Padmini Devi
Associate Professor, Department of Computer Science Engineering, M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India. Email: padminidevib.cse@mkce.ac.in

ABSTRACT-The most practical paradigm for people and businesses to access low-cost, scalable, all-encompassing, and resource pooling, application, and data repository services is emerging as cloud computing. Cloud computing is becoming more and more popular, and both businesses and people are quickly converting to using it. Whereas, a sizable beneficial to crucial private data and business data—including government documents, corporation financial information, and personal health records—is transported over the Internet and kept on cloud servers. Sensitive data outsourcing, however, faces serious privacy, security, and Restriction of access issues. These are typical worries of businesses and people who use cloud services. Data owners lose some control over their data when they move sensitive data to the cloud. In light of this, this project introduces Client Centric FS, a user-side fingerprint-based secured file system. Additionally, a biometric-based cryptographic protocol called BIOCRYP was introduced, which makes use of symmetric encryption techniques to enhance the performance and security of outsourced personal and shared information.

Keywords: Cloud, Security, Bio-Metric, File System, CCFS, BIOCRYP

I. INTRODUCTION

One of the most precious resources a corporation can possess is data. The cloud is one of the greatest places to save these assets.[1] The on-demand, pay-as-you-go delivery of IT resources through the Internet is known as cloud computing. Technology services, such as processing power, repository, and databases, can be acquired on an as-needed basis from a cloud provider[2] like Amazon Web Services rather than purchasing, operating, and maintaining physical data centres and servers (AWS).

Data management is a hot topic right now because of the rise in data volumes.[3] There is a greater emphasis on making sure everything is safe and secure and that there is no chance of data hacking or breaches as businesses .[3] start to shift to the cloud. Users benefit from flexibility and data agility since the cloud allows them to work without making costly expenditures in hardware and software. Security, however.[4], becomes a top worry for Cloud owners because the Cloud is frequently shared by numerous users. There are various particular security concerns and difficulties with cloud computing. Data is kept.[5] in the cloud with a third-party supplier and accessed online. This implies that access to and management of that data are constrained.

II. EXISTING SYSTEM

Cloud service providers view risks and challenges related to cloud security as a shared responsibility. The customer is responsible for the security of the data they store in the cloud, while the cloud service provider is responsible for the security of the cloud itself. Every cloud computing user is always in charge of safeguarding.[6] their data from security risks and managing access to it, whether the service is Platform as a Service (PaaS),infrastructure-as-a-service (IaaS) like Amazon Web Services (AWS) or software-as-a-service (SaaS) like Microsoft Office 365.

- Attribute Based Encryption (ABE)
- Cipher text Policy Attribute based Encryption

A. Disadvantages of Existing System

- CP-ABE has restrictions when it comes to controlling user attributes and establishing policies.
- The requirement that each authority's attribute set be distinct arose from the complexity of the multi-authority architecture.
- Inherent key escrow: The Private Key Generator is aware of the Private Key (PKG)
- The IBE system might rely on cryptographic methods that are vulnerable to code-breaking attacks.

III. PROPOSED SYSTEM

The suggested system offers Client Centric FS, a user-side biometric-based secured file system. It was suggested to utilise a hybrid crypto system that merge biometric encryption methods and fingerprint-based user authentication to improve the efficiency and security of shared and

outsourced personal information. The contents of externalised file in the CCFS are encrypted using biometric technology. The proposed ClientCentricFS has two objectives. To begin with, create a cryptographic layer that effectively and securely encrypts any files delivered to cloud repository. Next, make use of the advised CCFS to enable protect data sharing of cloud repository at the level of specific files.

A. Modules:

- Cloud Server Web App
- Cloud Client web App
- Fingerprint Module Integration
- DCNN Fingerprint Recognition
- Fingerprint Symmetric Cryptography
- Data Owner
- Data User

B. Advantages of Proposed System

- Reduces the need for key repository space while strengthening security.
- Files with Secure Biometric Lock System
- The key is created from the user's fingerprint, so there's no need to remember it.
- This method can also be used with other biometric features like the iris, face, voice, etc.

IV. SYSTEM ARCHITECTURE

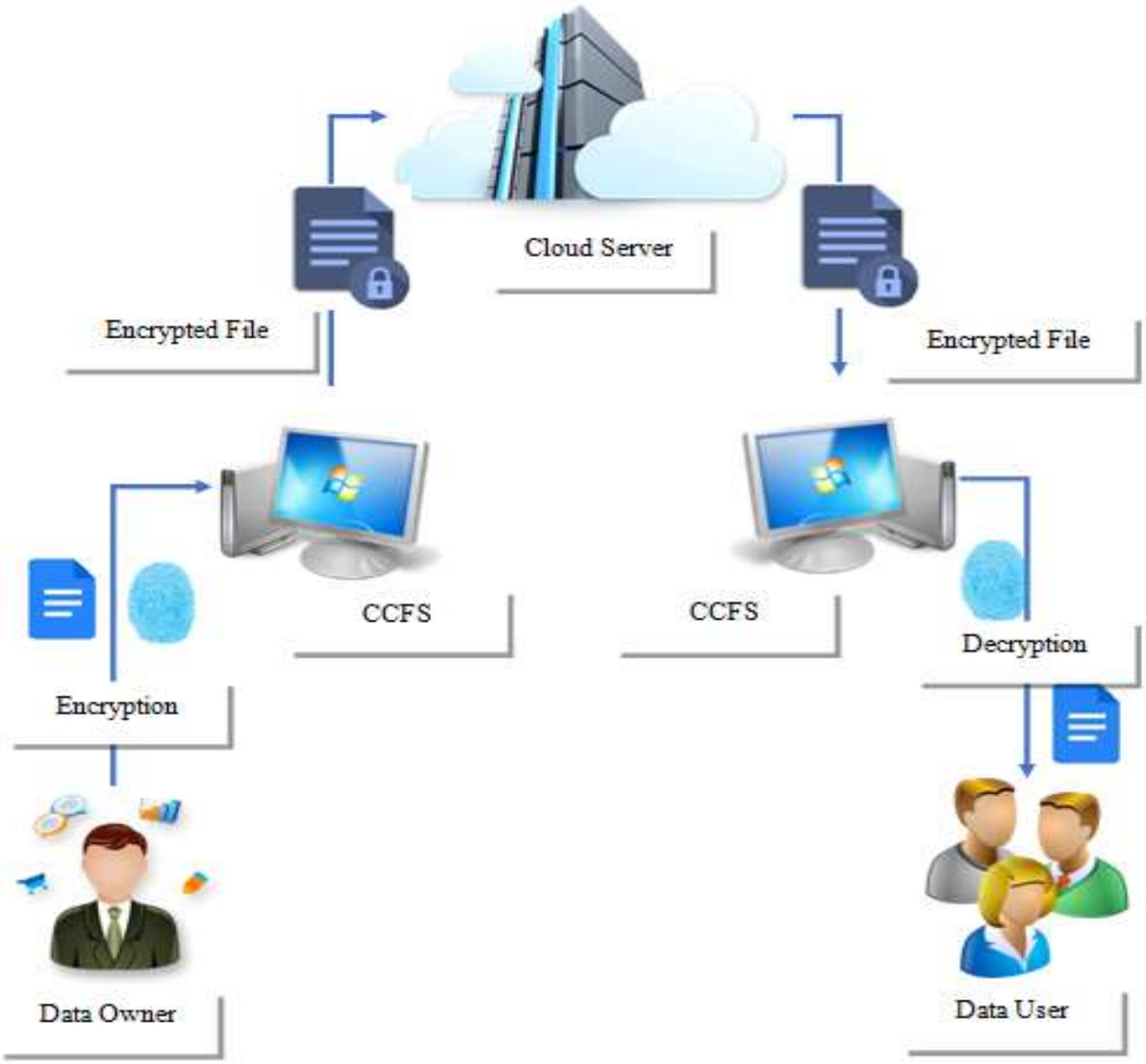

Figure 1. System Architecture Model

V. CONCLUSION

Client Centric FS is introduced in this project. To secure, the files are sent to cloud repository systems, CCFS, a user-side fingerprint-based encryption technology, is used. It has the ability to mounting a secure file system over a cloud-synchronized sector in order to carry out per-file transparent encryption using the BIOCRYP Key. CCFS proposes a Biometric Symmetric encryption strategy that combines a fingerprint and a BIOCRYP Key, which is used to encrypt data for private and shared files that are deployed, rather than adding dependencies to the asymmetric encryption cyphers. CCFS can assure the integrity of the deployed data files in order to defend the file against threats of destruction and alteration. According to a security analysis, the proposed CCFS is very secure and can successfully thwart attacks like brute-force, eavesdropping, man-in-the-middle, offline dictionary, and collusion on outsourced files.

REFERENCE

[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]. Padmini Devi B,Chitra, S, Madhusudhanan, B.: Improving Security in Portable Medical Device and Mobile Health Care System Using Trust. Journal of Medical Imaging and Health Informatics. 6(8),1955-1960(2016)

[3]. 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.

[4]. B. Padmini Devi, S.K.Aruna, andK. Sindhanaiselvan.: Performance Analysis of Deterministic Finite Automata and Turing Machine Using JFLAP Tool. Journal of Circuits, Systems, and Computers. 30(6),2150105-2150116,(2021)

[5]. 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.

[6]. 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.

[7]. Raj, P.H., Jelciana, P., Kumar, P.R.: Exploring data security issues and solutions in cloud computing. Procedia Comput. Sci. 1(125), 691–697 (2018).

[8]. Hanen, J., Kechaou, Z., Ayed, M.B.: An enhanced healthcare system in mobile cloud computing environment. Vietnam J. Comput. Sci. 3(4), 267–277 (2016)

[9]. Ramakrishnan, N., Sreerekha, B.: Enhancing security of personal health records in cloud computing by encryption. Int. J. Sci. Res.4(4), 298–302 (2015)

[10]. Akhil Behl,”Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation” 2011 World Congress on Information and Communication Technologies, 2012