iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** XII **Month of publication:** December 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XII, Dec 2018- Available at www.ijraset.com

Secured Digital Document Sharing using Biometric and TNP Record Updating

Kaustubh Sant[1], Vaishali Rahinj[2], Fareen Shaikh[3], Aishwarya Salunkhe[4], Pavan Sharma[5]
[1, 2, 3, 4]*BE Students, Computer Department, NMIET, Pune*
[5]*Assistant Professor, Computer Department, NMIET, Pune*

Abstract: ***There has been rising demand for secure system that must be dependable and quick respond for the industries and company. Biometric is one of the consistent and fast means of identify the user. Research has made some drastic changes which make its programming a lot shorter and easier. It rarely happens that we require to carry important documents along with us which may get damaged, lost etc. To overcome problem of carrying the documents everywhere and updating TNP documents every time. A proposed work helps students to share digital documents using Biometrics & saves the time for TNP document verification.***

Keywords: Digital Document System, Encryption, Decryption, Cloud, TNP Records, Biometric.

I. INTRODUCTION

The paper that will be designed will be very helpful for storing the important documents at one place securely. This paper's design is through the inspiration and motivation of real life scene of manually updating the data and carrying the huge documents every time to avoid this problem and preventing the useful documents from getting lost this system was thereby decided to be designed. The idea was taken from various IEEE papers and with the reference of the internet and other sources.

To overcome problem of carrying the documents everywhere and updating TNP documents every time. The paper help students to share digital documents using Biometrics & saves the time for TNP document verification.

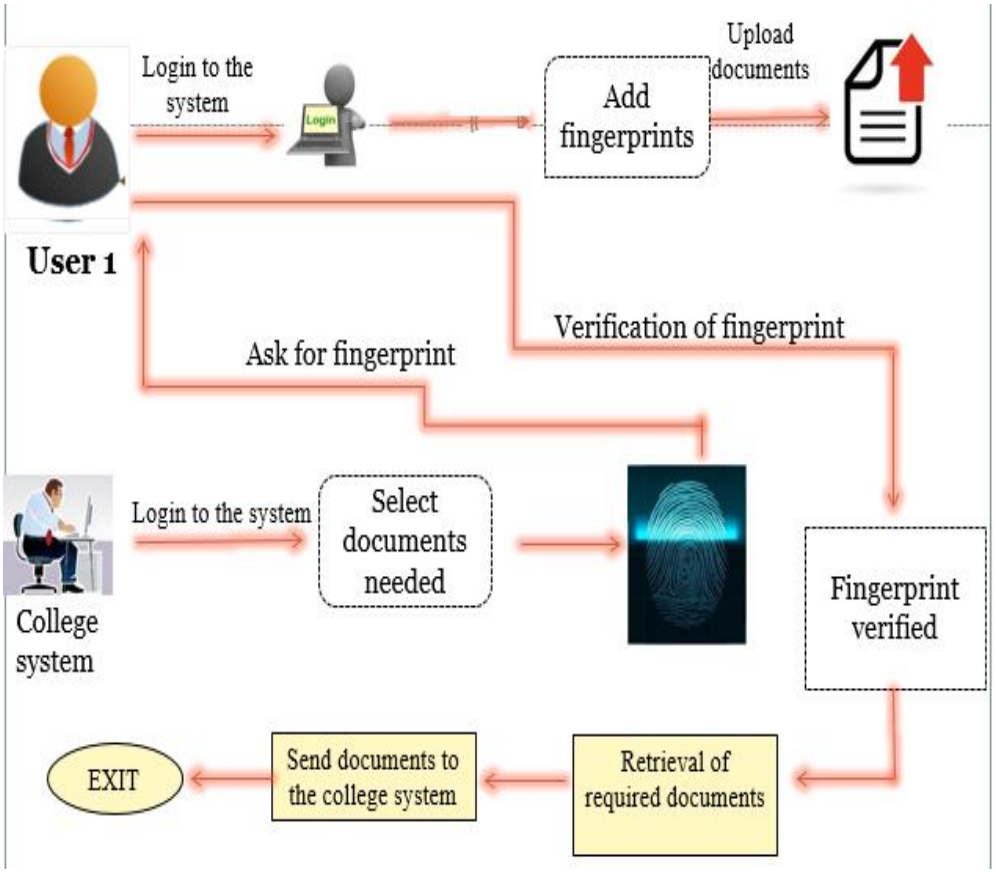


Figure 1. System Architecture

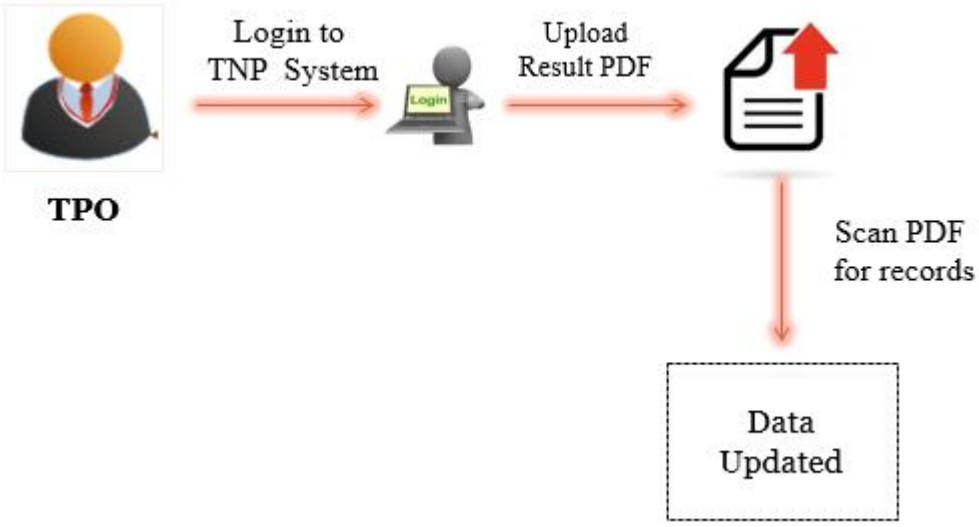


Figure 2. System architecture

II. LITERATURE SURVEY

A Survey on A Digital Envelope Scheme for Document Sharing in a Private Cloud Storage by Jedidiah Yanez-Sierra, Arturo Diaz-Perez, Victor Sosa-Sosa, J. L. Gonzalez, this paper presents a Digital Envelope scheme for secure document sharing in private cloud storage scenarios. This paper addresses the file sharing and key distribution in a private cloud storage using three main ideas i) The Encryption of documents before being stored in the cloud storage by combining cryptographic systems, ii) the construction of a document-sharing envelope to encapsulate all necessary information to perform sharing workflows, and iii) the development of well-defined assurance workflows by using a configurable workflow architecture that allows us to perform all the assurance operations on user-side. [1]

A review on Fingerprint Recognition paper by Gualberto Aguilar, Gabriel Sánchez, Karina To scano, Moisés Salinas, Mariko Nakano, Hector Perez. There are two major methods for fingerprint matching: Minutiae matching and global pattern matching. The first approach analyses the ridge bifurcations and endings, while the second method represents a more macroscopic approach. The last approach considers the flow of ridges in terms of, for example, arches, loops and whorls. As the equal-error-rate is low, the fingerprint recognition is very accurate. Furthermore, the cost of such systems compareed to other biometric systems is quite low and the user acceptance is very high. The strength of fingerprint identification is that it can be deployed in a wide range of environments, besides that it is a proven core technology and; their ability of enrolling multiple fingers can increase the system accuracy and the flexibility dramatically. [2]

Ako Muhamad Abdullah present a paper on Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data: The Advanced Encryption Standard (AES) algorithm is one of the block cipher encryption algorithms that was published by National Institute of Standards and technology (NIST) in 2000. The main aims of this algorithm were to replace DES algorithm after appearing some vulnerable aspects of it. NIST invited experts who work on encryption and data security all over the world to introduce an innovative block cipher algorithm to encrypt and decrypt data with powerful and complex structure. One of the most crucial aspects that NIST was considered to choose algorithm it is security. The main reasons behind this was obvious because of the main aims of AES was to improve the security issue of DES algorithm. AES has the best ability to protect sensitive data from attackers and is not allowed them to break the encrypt data as compared to another proposed algorithm. This was achieved by doing a lot of testing on AES against theoretical and practical attack. [3]

Secured Cloud Based Document Management System. In this paper the transition towards paperless offices and increasing adoption of electronic transfer of information through emails and other web-based content has prompted organizations to have a system which would manage their documents effectively. A cloud-based document management system provides a hassle-free classification and identity system that tags documents with information. Electronic documents are considered to be the most valuable information assets in enterprises. As the cloud security era is coming, the existing systems need to be upgraded with most cost-effective

measures, so a document security management system suitable for cloud security is also designed. With more documents being integrated electronically and transferred as knowledge points, organizations see document management system as an integral tool to handle growing surge of data and respond to audits without heavy burdens to the business. [4]

Attribute-Based Data Sharing Scheme Revisited in Cloud Computing paper by Shulan Wang, Kaitai Liang, Joseph K. Liu, Member, IEEE, Jianyong Chen, Jianping Yu, Weixin Xie. In this paper, the weighted attribute is introduced to not only extend attribute expression from binary to arbitrary state, but also to simplify access policy. Thus, the storage cost and encryption cost for a ciphertext can be relieved. The paper proposes an improved key issuing protocol to resolve the key escrow problem of CP-ABE in cloud computing. The protocol can prevent KA and CSP from knowing each other's master secret key so that none of them can create the whole secret keys of users individually. Thus, the fully trusted KA can be semi-trusted. Data confidentiality and privacy can be ensured. The paper also presents weighted attribute to improve the expression of attribute. The weighted attribute can not only express arbitrary-state attribute (instead of the traditional binary state), but also reduce the complexity of access policy. Thus, the storage cost of ciphertext and computation complexity in encryption can be reduced. Besides, it can express larger attribute space than ever under the same condition. [5]

Online Training and Placement System presented by Suraj Trimukhe, Anil Todmal, Kanchan Pote, Monali Gite, Asstt. Prof. S.S. Pophale presented System can guarantee to keep the records are safe and privacy which is stored in database. It converts unstructured data into Structured data and sorted format. It is very helpful, reliable and performs well functional to get an alert message and emails on cell phone. Also, this system helps us to take the record of alumni. The overall performance of The paper is shown by graphs. All the record stored in excel format. According to company criteria TPO Just enter the requirement of company and according to that the list of eligible students get display and TPO notify them. [6]

Paper by Bhavani Thuraisingham, Vaibhav Khadilkar, Anuj Gupta, Murat Kantarcioglu, Latifur Khan named Secure Data Storage and Retrieval in the Cloud aims to combine cloud computing technologies with security mechanisms so that cooperating organizations can share vast amounts of data securely. This paper presents a system that allows cooperating organizations to securely share large amounts of data. We have ensured that the organizations have a large common storage area by using Hadoop.[7]

Enhancing Security and Privacy in Biometrics Based Authentication System Using Multiple Secret Sharing paper by Sonali Patil, Kapil Tajane, Janhavi Sirdeshpande This paper proposes a merging of biometrics with secret sharing to reduce the computational complexity and space complexity of an authentication system. This merging also enhances security and privacy in a biometric authentication system.[8]

Panchami G. Rudrakshi, Sanjeevkumar M. Hatture present a paper A Model for Secure Information Storage and Retrieval on Cloud using Multimodal Biometric Cryptosystem in which a novel model for secure information storage and retrieval from cloud using multimodal biometric cryptosystems is proposed. The paper efficiently authenticates the user and protects the information through multimodal biometric cryptosystems and reduces the storage infrastructure requirement of the electronic applications by using securely the cloud storage. Enrollment is the first stage for biometric authentication to generate a template that can be used for all subsequent matching. These templates are averaged and updated each time the user attempts authentication. The device uses a proprietary algorithm to extract features from the object under test and stores them in database. In the proposed model the user has to enroll himself by providing his voice as an answer to text prompted questions and entering with keyboard for keystroke dynamics, iris and finger print samples. Using the features of behavioural biometric modalities i.e. voice and keystroke dynamics the feature vector is generated. [9]

There are three types of cloud computing deployment models: 1) Private Cloud: A private cloud is extensively used in single organizations for offering services to internal users.

A private cloud could be used to maintain the security of a city or to provide privacy to organizational data. 2) Public Cloud: Public cloud infrastructure allows all services to be publicly accessible. Sometimes these services are free to the public. External enterprises can use resources offered by the cloud at free of cost. 3) Hybrid Cloud: A hybrid cloud offers best of both a private and public cloud structures. This delivers an infrastructure for a public cloud while continuing control over vital data using the private cloud. These models differ on features like control, flexibility, and management. This model is also termed as a cloud-computing stack. [10]

In the current system all training and placement activities are done manually, there are more chances of error. It is very time-consuming activity for collecting, managing, updating student data as number of student increases. The notice board is old method of informing student about the placement activities. The training and placement officer have to short list according to company requirement. It is required to design of a computerized student automation module to speed up capabilities. [6]

III.PROPOSED WORK

It is very important to keep personal information or confidential information from hackers. So, authentication is most important at this stage. Traditionally password and other authentication methods to protect their confidential information. But these techniques provide low security mechanism. Because sometimes user cannot remember password, which can result in user error or password can be stolen by hacker or unauthorized persons. Today Biometric recognition and cryptography techniques are used together. Some of the biometric techniques commonly use are image recognition, fingerprint, iris recognitions and commonly used cryptographic techniques are symmetric key cryptography and asymmetric key cryptography.[10] The paper is of digital document sharing using biometric system that can share user's documents with their fingerprints and OTP.

Initially the user will add his fingerprints and upload the documents so that by using biometrics retrieval required documents in collage or institute become easy.

TPO co-ordinator will first upload the mark list PDF then the marks will be updated according to the Permanent Registration Number (PRN).

A. Advantages Of Proposed Work

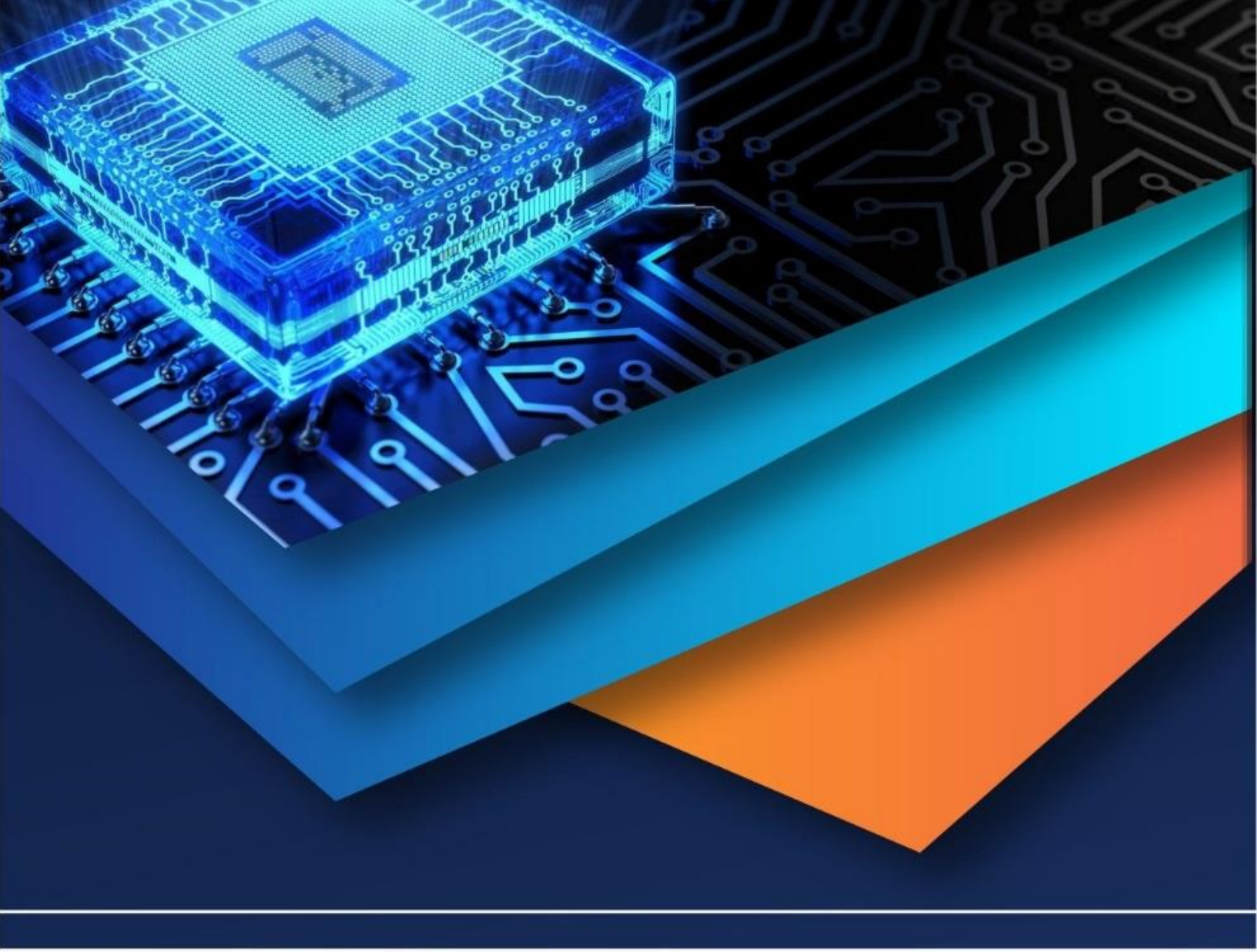
1) No need to carry all document files everywhere.
2) avoid damage and loss of documents.
3) All training and placement activities are done automatically, there are no chances of error.

IV.CONCLUSION

The Proposed paper can guarantee to secure document sharing digitally and update the TNP record automatically. Approach start with the storing documents on cloud with security of biometric (Fingerprint) followed by sharing with the fingerprint and OTP and upload result pdf files and fill the TNP records. Hence, System might be secure to shared online documents and avoid the TNP record updating manually.

REFERENCES

[1] Jedidiah Yanez-Sierra, Arturo Diaz-Perez, Victor Sosa-Sosa, J. L. Gonzalez. A Digital Envelope Scheme for Document Sharing in a Private Cloud Storage, 2015.
[2] Varsha Jawale, vedashri Jundre, Reshma Bathe : Secure Cloud based Document management System, 2013.
[3] Ako Muhamad Abdullah. Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data, 2017.
[4] Gualberto Aguilar, Gabriel Sánchez, Karina To scano, Moisés Salinas, Mariko Nakano, Hector Perez Fingerprint Recognition,2007.
[5] Shulan Wang, Kaitai Liang, Joseph K. Liu, Member, IEEE, Jianyong Chen, Jianping Yu, Weixin Xie Attribute-Based Data Sharing Scheme Revisited in Cloud Computing, 2016.
[6] Suraj Trimukhe, Anil Todmal, Kanchan Pote, Monali Gite, Asstt. Prof. S.S. Pophale Online Training and Placement System, 2017.
[7] Bhavani Thuraisingham, Vaibhav Khadilkar, Anuj Gupta, Murat Kantarcioglu, Latifur Khan Secure Data Storage and Retrieval in the Cloud, 2011.
[8] Sonali Patil, Kapil Tajane, Janhavi Sirdeshpande Enhancing Security and Privacy in Biometrics Based Authentication System Using Multiple Secret Sharing, 2015
[9] Panchami G. Rudrakshi, Sanjeevkumar M. Hatture paper A Model for Secure Information Storage and Retrieval on Cloud using Multimodal Biometric Cryptosystem, 2014
[10] Anupam Baruah, Prof. (Dr.) Lakshmi Prasad Saikia, Biometric System Using Cryptography: A Survey, ISSN 2320–088X, 2015



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY