

# Paperless India-Smart Digitization using Cloud

<sup>#1</sup>Dr. Vilas. V. Deotare, <sup>#2</sup>Vicky Kumar Singh, <sup>#3</sup>Vasu Singh, <sup>#4</sup>Hrishikesh Bhagat



<sup>1</sup>vilasdeotare@gmail.com  
<sup>2</sup>kumar.vicky756@gmail.com  
<sup>3</sup>vasusingh52@gmail.com  
<sup>4</sup>hrishibhagat08@gmail.com

<sup>#1234</sup>Department of Electronics and Telecommunications,  
 Sinhgad Institute of Technology, Lonavala  
 Savitribai Phule Pune University, Pune-41, India.

## ABSTRACT

For Public Sector and Government Agencies, with tens or hundreds of thousands of documents, a document management system is becoming a mandate to organize, index and control their documents in a hassle-free manner. Public Sector and Government Agencies deal with Documents which range from Public View documents, Tenders, to the most Confidential and Secret Documents which are intended only for view of certain designated personnel and documents need in collage verification purpose. Storing all these documents as physical records not just consumes a lot of space but also is a tedious affair to file these documents and manage them safely with restricted access. So we are providing one digital solution to this problem with RFID card and fingerprint scanner. User will get authenticated by unique id of RFID associated with each document. It also contain ESP8266 wifi module for sending a data to server and then data will store in cloud at some random position. It is a system proposed by us that is firstly implemented on small scale and if get successful then going to implement it on a large scale.

**KEYWORDS-:** DIGITAL, AUTHENTICATION, WEB APLICATION, WIFI MODULE, FINFERPRINT SENSOR, RFID

## ARTICLE INFO

### Article History

Received: 31<sup>st</sup> May 2019

Received in revised form :  
 31<sup>st</sup> May 2019

Accepted: 3<sup>rd</sup> June 2019

**Published online :**

**4<sup>th</sup> June 2019**

## I. INTRODUCTION

The ubiquitous nature of the Internet allows most of today's information technology systems to provide services that are of a global scope. A traveller in India may use Airbnb to book a hotel in Japan and may use Google maps to find its location. A student in the United States may use Face book to chat with her family in Brazil and to send them a gift via Amazon. As online users enjoy the convenience of global services, data transmission across borders and information privacy becomes an important consideration. Therefore, providing services and systems that are privacy-preserving to users across the regions is a challenging mission. So, what we are experiencing nowadays is digital life, in every day to day life we are dependent on digital way of doing that work. But there is still one case where we are using papers for doing that work which is government documents or any documents educational, medical etc. We have to carry file of documents while we are going for any government work such as for issuing driving license or any educational work. So we are proposing digital solution on this problem by replacing bunch of documents with just single RFID card. This system combines hardware part

consist of fingerprint and RFID with software part contain main website and for storage purpose cloud.

## II. RELATED WORK

(M. Hattingh, 2001), Explains that Major changes are taking place in the global workplace. The European Foundation reveals that work is becoming more intensive, more than 50% of workers are working at high speed or tight deadlines most of the time, the nature of the work is driven by customer demands and the number of people working with computers has increased to 41% in 2000. The strain on the employee is ultimately reflected in the work-related health issue of muscular pains in the neck and shoulders reported by a quarter of the workforce (European Foundation, 2000). Closer to home, statistics support this trend by indicating that the number of Internet users in Africa has increased by nearly 100%, from 2.5 million in 2000 to nearly 5 million in 2001, with South Africa having two-thirds of Africa's internet population.

(Government of India, 2015), **DigiLocker** is an online service provided by Ministry of Electronics and IT

(MeitY), Government of India under its Digital India initiative. DigiLocker provides an account in cloud to every Indian citizen to access authentic documents/certificates such as driving license, vehicle registration, and academic mark list in digital format from the original issuers of these certificates. It also provides 1GB storage space to each account to upload scanned copies of legacy documents.

(Andrey Larchikov, Sergey Panasenkov, Alexander V. Pimenov, Petr Timofeev, 2012), Digital signature systems are adopted worldwide. Using the legally valid digital signatures for payment orders demands involving the strong security mechanisms to prevent secret keys leakage or unauthorized use and other possible risks. Typically digital signature calculation is performed by cryptographic smart cards or USB tokens containing secrets keys. Personal computers with digital signature systems are usually equipped with access control and management systems that allow to provide restricted access to the computers and to supervise processes running on them. However, it keeps some possibilities of attacks on digital signature systems, mainly resulting from incorrect or erroneous user behaviour. We propose to use RFID technology to combine functions of physical access control, computer's access control and management, and digital signature systems. This combination allows to drastically increasing systems' security. Even low-end RFID tags can add one security level into the system, but high-end RFID tags with cryptographic possibilities and slight modification of digital signature calculation procedure make it possible to prevent obtaining digital signatures for fraudulent documents. The further evolution of the proposed scheme is permanent monitoring by means of periodical controlling user's RFID tag, whether authenticated user is present at the computer with restricted access.

### III. PROPOSED FLOW

In the Proposed System, we used hardware component i.e. microcontroller ATmega328P, RFID, Fingerprint sensor (GT-511C3) and Buzzer to notify user while registration. The proposed system also has software part contain website and cloud as a storage purpose. Whenever user registered on hardware through fingerprint and RFID a unique fingerprint number and RFID number is generated and it will reflect to the main website for that particular user. The actual flow of system is explained by using algorithm:

#### USER REGISTRATION (HARDWARE)

- 1) Registration on hardware (for authentication purpose)
- 2) Input (RFID, Fingerprint sensor)
- 3) Output (if fingerprint capture then User registered Else not registered)
- 4) End

#### USER REGISTRATION (SOFTWARE)

- 1) Registration window (RFID & Fingerprint nos. automatically transferred to registration page through ESP8266)
- 2) Registration success
- 3) End

#### ADMIN PART

- 1) Admin login
- 2) Document Upload of registered user
- 3) User Login (User can see their documents)
- 4) If user want to use this system in different application
- 5) User authentication (RFID& Fingerprint)
- 6) If RFID& Fingerprint matches then authentication success Else not success
- 7) OTP option available to access the document for the user (extra authentication)
- 8) System successfully access document from the server
- 9) End

### IV. PROPOSED SYSTEM

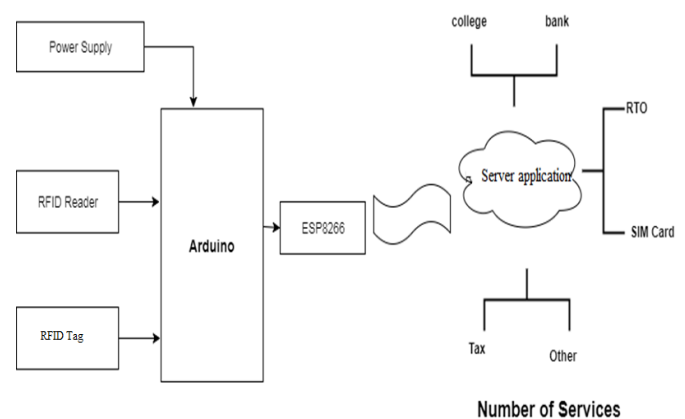


Figure 1: System diagram

In proposed system, when user comes for the first time to give his essential document, first registration has been done in hardware using RFID module and fingerprint sensor that data will send to ESP8266 through microcontroller ATmega328P for uploading it to the server. ESP8266 is a wifi module that is used to send the data to the server. Now the software part comes into the picture where separate registration of that particular user will do. Now the admin will upload all the documents of user using his ID and password and a unique card to that user for any future access of his document. User need to carry a unique identification card (RFID card) every time whenever user want to access his document for different application like college admission, RTO offices, Passport offices, Banks etc For verification of documents. If somehow user misplaced his RFID card then OTP (one time password) section is provided in which a 5 digit random number will send to the user's registered mobile number for verification of that user and hence admin can access that user documents. User can see his uploaded documents with the help of user login section and in case user want to update his personal data then he can do it through update section. Major component of the system:

**User:**

In this module user register into the system. All information (Name, Mobile No., RFID No., Email-ID, and Password) of user stored into data based. Every time user needs to carry a unique identification card (RFID card). To provide batter security OTP section also provided for the user.

**Admin:**

When user comes for the first time, its admin responsibility to take the documents from the user and upload to the cloud and provide a unique identification card to the user for future references. For deletion purpose only admin has authority to delete that document.

**Security:**

To provide security in the system (Hardware) biometrics (fingerprint) will be taken from the user. Now for software OTP and cryptography technique is used.

**Data Storage:**

All the data from the system is stored on a cloud at different locations for particular user.

## V. RESULT

Fingerprint sensor (GT-511C3) capable of taking 200 fingers and have inbuilt ROM. User can register anyone of his finger at a particular time for authentication purpose. This can enhances the security in the system. RFID is also used which is a low frequency module and has a range within 10cm. Due to this system user need not to carry documents everywhere so there will be a less chance that documents gets stolen or misplaced. It also reduces the paper workload from various services.

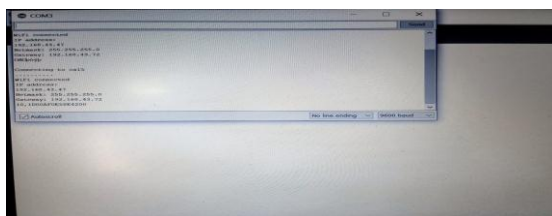
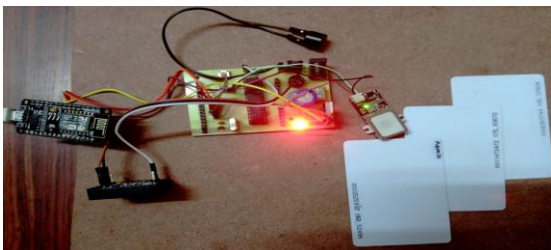


Figure 2: Hardware Implementation

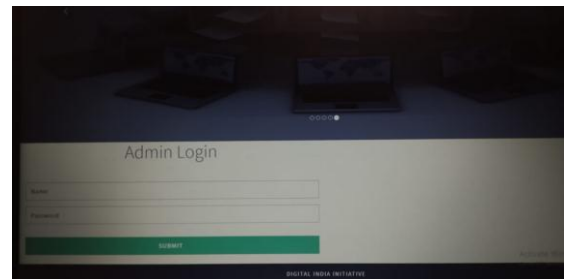
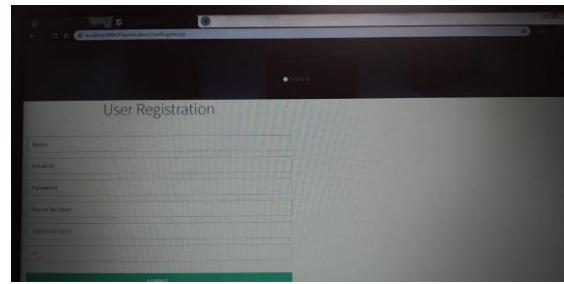
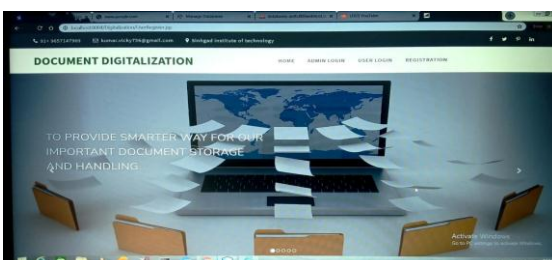


Figure 3: Software Implementation

## VI. CONCLUSION

This system allows for the availability of all the important documents that a user will require when he's applying for a RTO or for many other reasons. This allows for the secure and a protected way of viewing individual documents without the hassle of the traditional methods of carrying all the documents wherever we go.

## VII. ACKNOWLEDGEMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally, I wish to thank to all our group members and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide **Dr.V. V. Deotare** for time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

## REFERENCES

1. H. Krasnova, and N. F. Veltri, "Privacy calculus on social networkingsites: Explorative evidence from Germany and USA". In System sciences (HICSS), 2010 43rd Hawaii international conference on (pp. 1-10), IEEE, 2010, January.
2. A. Acquisti, L. Brandimarte, L., and G. Loewenstein, "Privacy and human behavior in the age of information," Science, 347(6221), 509-14, Jan 2015.

3. B. P. Knijnenburg, A. Kobsa, and H. Jin, "Dimensionality of information disclosure behavior," *International Journal of Human-Computer Studies*, 71(12), 1144-1162, 2013
4. F. Kehr, T. Kowatsch, D. Wentzel, and E. Fleisch, "Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus," *Information Systems Journal*, 25(6), 607-635, 2015.
5. A. Juels, R. Pappu, B. Parno. Unidirectional Key Distribution Across Time and Space with Applications to RFID Security, *Cryptology ePrint Archive: Report 2008/044*. Available at <http://eprint.iacr.org/2008/044>, 2008.
6. T. Hollstein, M. Glesner, U. Waldmann, H. Birkholz, K. Sohr. Security challenges for RFID key applications, *RFID SysTech 2007, 3rd European Workshop on RFID Systems and Technologies*. June, 12-13, 2007, Duisburg, Germany. Proceedings (CD-ROM), 12 pp.
7. Corporate Information and Personal Data Leakage in 2012. *Info Watch Analytic Report (In Russian)*. Information Security, #3, 2013.