Centralized Access all Government Services based on Digitalization of India using Biometric Technology

Prachi Joshi
Department of Computer Engineering
JSPM's BSIOTR WAGHOLI, PUNE.

Rupali Mahale
Department of Computer Engineering
JSPM's BSIOTR WAGHOLI, PUNE.

Aishwarya Waghmare
Department of Computer Engineering
JSPM's BSIOTR WAGHOLI, PUNE.

Anamika Temkar
Department of Computer Engineering
JSPM's BSIOTR WAGHOLI, PUNE.

Prof. Monali Mohite
Department of Computer Engineering
JSPM's BSIOTR WAGHOLI, PUNE.

ABSTRACT: Now a days in the industries and companies there has been rising demand for secure system that must be dependable. One of the tool for authentication is biometric authentication. It is one of the consistence and fast means of identify the object and the another tool is available for authentication is barcode system. Also barcode is chip in cost than biometric but now a days biometric is easily available and more efficient to use. To solve the problem of carrying and showing identity card for government officer and services. We are going to develop a system which will save time and hassle for the officer waiting to check the document of the user whose information in save in the database in the server. We store the data is very safely and securely based on one way encryption algorithm.

Keywords: Biometric Device, Document Authentication, Controller, Digitalization, Security.

I. INTRODUCTION

Each system faces common problem of to identify/verify authorized person. The system may give chance to any dishonest person if he/she knows your password or Security PIN. From the above paragraph, we can make conclusion that the Password is not suitable for our authentication system. Due to this, we have to explore new authentication system i.e., biometric authentication system. Biometric uses human's physiological and behavioural characteristics. The Biometric characteristics have good extent of uniqueness, availability, collectability. If we use this characteristics in our daily authentication system, the system gives good performance and throughput. In this paper, we mentioned about finger-print authentication system based on biometric finger-print recognition. In all biometric techniques, fingerprint recognition is considered the most prominent and reliable one[7][8].

In the IoT world many devices are connected in the internet, it will be useful for develop the IoT system on large scale. There are many security issues in IoT some are: Authentication, Authorization, Privacy and Data Confidentiality. In the security system there has been many attacks on system has been happen many aatacks can happen one or more layers of system that is 1.Hardware Layer 2.Network Layer 3.Cloud Layer At the first layer there is Hardware layer attacker get access to the IOT hardware and attacker can knows key or security parameters stores inside IOT device attacker also can re-develop virtual IOT device using the security parameters because of these the duplicate virtual IOT device can save duplicate or false data to the server and get access of secure information about the user from the server in network in which IOT device are connected there are some particular attacks are available using these attack and attacker can get access to security parameter of device without any having physical access of the device researcher have executed electromagnetic based side channel attackes to steal keys of RSA and ECC based encryption using side channel attckes AES encryption key can be stolen from IOT device since the IOT device are connected to the internet such devices are vulnearable to attacks through the networks[6].

DoS attacks based on protocols like SSDP which is widely used in IoT devices, have increased significantly after 2013. There have been other cases of network attacks where the attacker attacked IoT devices from outside and used IoT devices to gather personal details of the owners1. An IoT device with a proper authentication mechanism can avoid many such situations. In this paper, we propose a secure authentication protocol to authenticate the IoT device and the server. Some of the current authentication mechanisms, which are mostly based on single password-based mechanism, are vulnerable to side channel and dictionary attacks[9][10][11]. We have designed a multi key authentication mechanism, such that, even if the secret key used for ongoing authentication is retrieved successfully by the attacker, the attacker cannot gain access to the unused authentication keys and the authentication system is secure from the side channel attack or similar attacks. The key values keep changing over the time, which prevents attacks[7][8].

II. LITERATURE SURVEY

Chopra, Ghadge, Padwal, Punjabi, & Gurjar, 2014, explained that There can be improvements made when the image is captured using a camera, as it decreases the resolution factor of the images and thus, degrade their quality. The project can be extended for recognition of handwritten characters as well as its application in various fields of recognition of diverse cards. Thus, the system has achieved the clarification for automatic reading of Aadhar Card with a good accuracy.

Deepz & Dr. Vijay Singh, 2012, Knowlton & Whittemore, 2008, suggested that the government will use the information to issue identity cards the word which is generally known as AADHAR CARD. (Tiwari, 2013)described that the user logins to the account using his aadhar card number and the password provided him at the time of registration and giving vote.

Shah & Shah, 2014, Goel & Singh, 2014, described that National Bureau of Investigation in Philippines, India's most recent Aadhaar card includes QR code implementation. Based on the all information we should consider the government consider only one card for the identity card of the person as Aadhaar card which is also helpful to provide the different government activities like to take subsidy and also take advantages of the different governments' scheme.

Kale & E, 2014, told that the growth in the electronic transaction scheme has resulted in a greater demand for accurate & fast user identification and authentication. An embedded fingerprint biometric authentication scheme for ATM banking systems is proposed in this paper. Along with AADHAARCARD authentication for more security.

Akhil Mittal, Anish Bhart, Sanjoy Sahoo, Tapan K Giri, 2011, suggested that Aadhar Card is unique for person which have person's finger print and retina scan. It can used to identify person anywhere in the country. (Velapure et al., 2015)(Velapure et al., 2015) found that the distinctiveness with registration through aadhar number and face recognition will offer very strong security for the secret information about vote.

Gupta & Dhyani, 2013)found that e- Voting model has been integrated with AADHAR CARD or Unique Identification (UID) card data base using cloud. By integrating e-Voting model with cloud infrastructure and ADHAAR CARD record, percentage of polling would raise and can supply authentic electoral voting mechanism to satisfy the need of the voters.

III. PROPOSED WORK

The granular details and specifications will be explained. And we also explain the flow of the system using algorithm.

(1) Start.
(2) Centralized server running.
(3) Fingerprint scanner wait for finger press.
(4) Data simultaneously send to the controller.
(5) Authentication process identification
(6) All documents check from the database server
(7) Display the customer ID on Screen
(8)The authentication will be automatically success the user card.
If (thumb is not valid)
Authentication failure;
Else
thumb is valid;
(10) After success of the authentication documents will be displayed..
(11) End.

A. PROPOSED SYSTEM

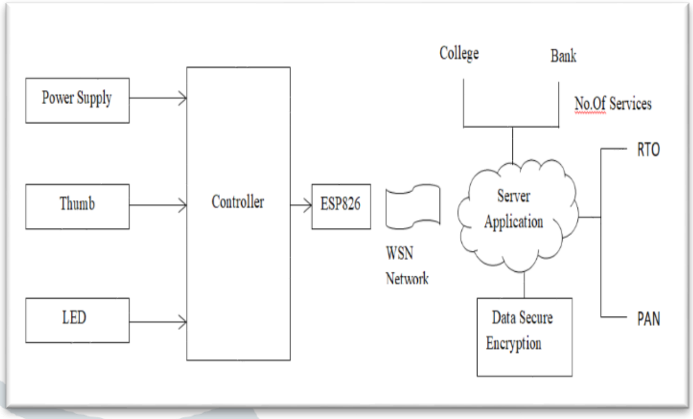


Fig 1.System diagram

Fingerprint Module:
We going to use GT511c3 fingerprint module contains the optical scanner for fingerprint reading and can store the images by using identification number[14].

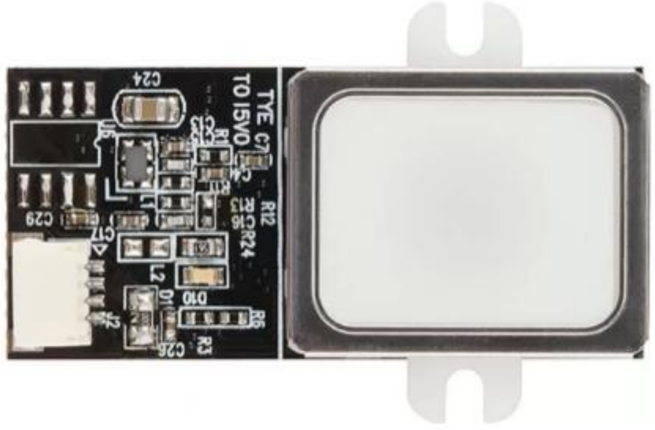


Fig 2. Thumb hardware module

Wifi module:
We are going to use ESP8266 wifi module is a name of the microcontroller designed by Espress if systems. The ESP8266 itself is a self-contained WiFi networking and the microcontroller to transfer the data[15].

Fig 3. ESP8266 wifi module

B. ALGORITHM

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes.

AES Algorithm:

```
For encryption of data:-
START
Step 1- U=Upload (image file)
Step 2- R= Read (input file)
Step 3- K=Key generation (file)
             e.g= key=123456;
Step 4- E=Encrypt(file, key)
Step 5- C=Convert (file)
      If(encrypt),
        Else,
Step 6- D=Decrypt (file)
        if (decode)
        Else
Step 7- Download file
         END
```

C. SYSTEM FLOW

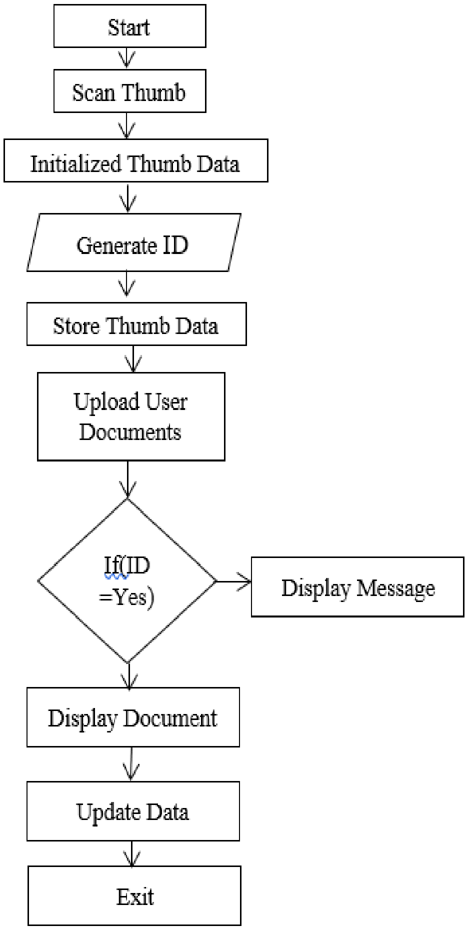


Fig 4. System flow

D. APPLICATIONS

The entire project idea is to develop safe and secure ystem to access the documents using Fingerprint:

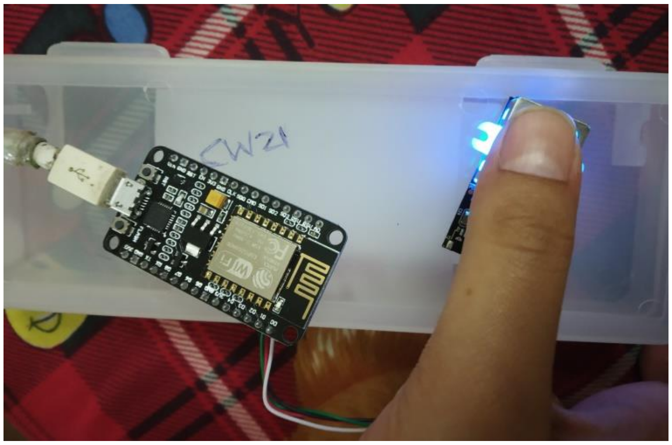
- Banks: To open an account and to apply for loans
- RTO : To apply for license and RC
- College : For admission
- Passport office: For verification purpose.

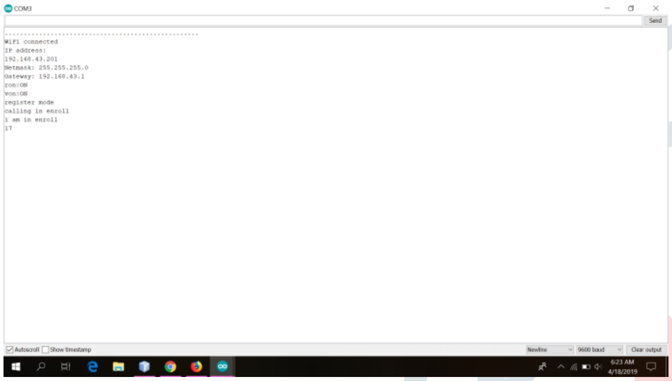
E. ADVANTAGES

- The Digitalization provides more reliable backup of documents.
- No need of carrying documents all the time
- The Digitalization will provide less time consuming in government processes.
- The system is eco friendly
- The system provides more security due to biometric access for authentication.

IV. RESULT

Hardware Setup:





```
.................................................
WiFi connected
IP address:
192.168.43.201
Netmask: 255.255.255.0
Gateway: 192.168.43.1
ron:ON
von:ON
register mode
calling in enroll
i am in enroll
17
```

V. FUTURE SCOPE

The system can be expanded to provide the authentication by using the face recognition by interfacing camera with raspberrypi**.** The system can be expanded to include various other options to secure the documents of a person and storing it.

VI. CONCLUSION

This system is used for all types of user for the availability of all respective important document of particular user. Also all document are saved securely in the server. User can get there particular document easily by using thumb scanner. This allows for the secure and protected way of viewing individual document without the hassle of the traditional methods of carrying all the documents wherever we go.

REFERENCES

[1] Aamir Nizam Ansari , Mohamed Sedkyl, Neelam Sharma and Anurag Tyagil Faculty of Computing, Engineering " RFID-Based Students Attendance Management System" Vol 2, Issue 7, July 2015.

[2] G.Lakshmi Priya1, M.Pandimadevi, G.Ramu Priya1, and P.Ramya., " Face Recognition Based Attendance International Journal of Engineering and Techniques - Volume 2 Issue 3, May – June 2016 ISSN: 2395-1303 http://www.ijetjournal.org Page 32 Marking System", in Architecting the Internet of Things, Berlin, Germany: Springer-Verlag Vol 4, Issue 5, pp 38-43,jan 2011.

[3] ehun-wei Tseng et.al Department of Infonnation Management Cheng Shiu University Kaohsiung County, Taiwan Design and Implementation of a RFID-based Authentication System by Using Keystroke Dynamics.

[4] Andrey Larchikov, Sergey Panasenko, Alexander V. Pimenov, Petr Timofeev ANCUD Ltd. Moscow, Russia Combining RFID-Based Physical Access Control Systems with Digital Signature Systems to Increase Their Security.

[5] M. Vazquez-Briseno, F. I. Hirata, J. de Dios Sanchez-Lopes, E. Jimenez-Garcia, C. Navarro-Cota and J. I. Nieto-Hipolito. Using RFID/NFC and QR-Code in Mobile Phones to Link the Physical and the Digital World, Interactive Multimedia, Dr. Ioannis Deliyannis (Ed.), ISBN: 978-953-51-0224-3, InTech, 2012.

[6] P. Solic, J. Radić, N. Rozic. Software defined radio based implementation of RFID tag in next generation mobiles, IEEE Transactions on Consumer Electronics, vol. 58, no. 3, pp. 1051-1055, August 2012.

[7] 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.

[8] 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.

[9] Corporate Information and Personal Data Leakage in 2012. InfoWatch Analytic Report (In Russian). Information Security, #3, 2013.

[10] https://ieeexplore.ieee.org/document/6567741

[11]https://www.semanticscholar.org/paper/RFID-Authentication-Protocols-using-Symmetric-Song/4ebb35d84a4c857784f73a1c24532ea4ad4c54a4

[12] https://digitalguardian.com/dskb/data-encryption

[13]https://www.intechopen.com/books/interactive- multimedia /using-rfid-nfc-and-qr-code-in-mobile-phones-to-link-the-physical-and-the-digital-world.

[14] https://www.sunrom.com/p/finger-print-sensor-r305

[15] https://www.sparkfun.com/products/13678