All in one using Smart Card and Biometric Technology for digitalization of India based IoT.

Kunal S. Wagh, Vishnudas K. Talware, Harish R. Patil, Priyanka U. Gaikwad
Prof. Sarla A. Chimegawe
Department of Information Technology

JSPM's BHIVRABAI SAWANT INSTITUTE OF TECHNOLGY AND RESEARCH

WAGHOLI, PUNE.

ABSTRACT: There has been rising demand for secure system that must be dependable and quick respond for the industries and company. Biometric authentication is one of the consistent and fast means of identify the material object. In this system we use the smart card and biometric because of smart access to the any application. To overcome problem of showing any card for particular government officer and services. We are going to develop a system which will save time and hassle for the officer wanting to check the document of the particular user whose information is stored in the data base. We stored the data is very securely based on encryption algorithm.

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

1. INTRODUCTION

The most of the authentication systems use User-name – Password, Security Pin, One Time Password, Photo ID etc., and 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.

2. PROBLEM STATEMENT

To overcome problem of showing any card for particular government officer. we are going to develop a system which will save time and hassle for the officer wanting to check the document of the particular user whose information is stored in the data base.

3. LITERATUREREVIEW

(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.

(Deepu& 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, AnishBhart, SanjoySahoo, 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.

4. PROPOSED FLOW

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

Step 1: Start.

Step 2: Centralized server running.

Step 3: Fingerprint scanner or Smart card access wait for finger press and card read.

Step 4: Data simultaneously send to the controller.

Step 5: Authentication process identification

Step 6: All documents check from the database server

Step 7: Display the customer ID on Screen

Step 8: The authentication will be automatically success from the user card.

If (thumb isvalid&&card is valid)

Authentication successful;

Else

Authentication is failure;

Step 9: After success of the authentication documents will be displayed.

Step 10: End.

5. PROPOSED SYSTEM

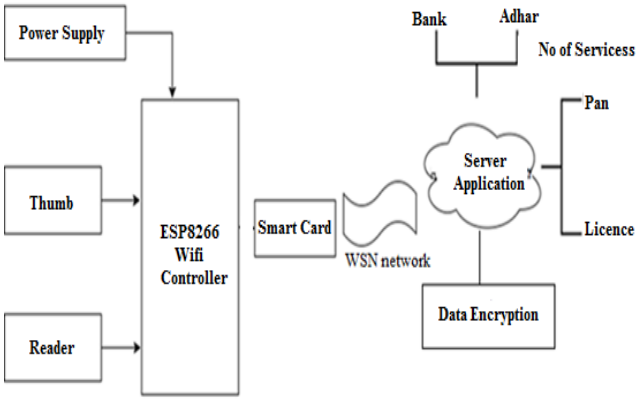

Fig 1.System diagram

Fingerprint Module:
We are going to use GT511c3 fingerprint module contains the optical scanner for fingerprint reading and can store the unique values by using identification number.

Smart Card:
Smart Card is an ID system that uses small radio frequency identification devices for identification and tracking purposes. An RFID tagging system includes the tag itself, a read/write device, and a host system application for data collection, processing, and transmission.

Wi-Fi 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.

Data Secure Encryption:
Encryption Process:

KeyGenCE(M) → K is the key generation algorithm that maps a data copy M to a convergent key K;

EncCE(K,M) → C is the encryption algorithm that takes both the convergent key K and the data copy M as inputs and then outputs cipher text C;

DecCE(K,C) → M is the decryption algorithm that takes both the cipher text C and the convergent key K as inputs and then outputs the original data copy M;

TagGen (M) → T(M) is the tag generation algorithm that maps the original data copy M and outputs a tag T(M)

APPLICATIONS:
The entire project idea is to develop safe and secure system 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.

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.

6. FUTURESCOPE

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.

7. CONCLUSION

This system allows for the availability of all the important documents that a user will require when he's applying for a bank loan 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.

8. ACKNOWLEDGMENTS

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 friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide Prof. Sarla A. Chimegawe Madam 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.

9. REFERENCES

[1] AamirNizamAnsari , Mohamed Sedkyl, Neelam Sharma and AnuragTyagil 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-VerlagVol 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] AndreyLarchikov, Sergey Panasenko, Alexander V. Pimenov, PetrTimofeev 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. IoannisDeliyannis (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.