

Implementation of biometric based individual Identity in health care centres

Varun Kumar M

TIFAC-CORE, VIT University, Vellore, India-632 014.

*Corresponding author: E-Mail: varunkarnambut@gmail.com

ABSTRACT

In the day today scenario, each and every individual's biometric patterns (Iris Scan, Finger Prints Impression) were feed into Aadhar database and biometric characteristics were considered to be unique for every, and every individuals. Suppose if a person met with an accident somewhere and he was seemed to be death or he/she is in unconscious state, So It is highly difficult to trace the individual identity of the person who had met with the accident and it is highly time consuming. In order to eradicate this problem I am coming up with a best possible solution, that is each and every government and private hospitals whom were licensed by State & central government and the Government & Private Emergency free ambulance services as to provide with a Biometric Authentication Device (BMAD), which in turn connected with Centralized Aadhar database server by means of common website through web services. Through BMAD individuals biometric patterns were feed into the common website, which is connected with Centralized Aadhar database server. The main objective of the idea proposed here is to provide automated identity in health care centres for each and every individuals dwelling in the globe by matching the individual's biometric patterns with the biometric patterns stored in the existing Centralized Aadhar database server by means of Internet services and to provide emergency alerts (SMS services or Phone call) to the family of the concerned individual.

KEY WORDS: Biometric Authentication Device (BMAD), Unique Identification (UID), Know your customer (KYC), Unique Identification Authority of India (UIDAI), Biometrics, Database, Aadhar.

1. INTRODUCTION

The main objective of the idea proposed here is to provide automated identity in health care centres for each and every individuals dwelling in the globe by matching the individual's biometric patterns with the biometric patterns stored in the existing Centralized Aadhar database server by means of Internet services and to provide emergency alerts (SMS services or Phone call) to the family of the concerned individual.

Biometrics Authentication Technology: Biometrics were automated methods of identifying a individual or verifying the identity of a individual based on a physiological or behavioral characteristics. Biometrics is real-time mechanism that can be combined with other mechanism to make more securitized, easy usage of verification solutions and identifying individuals. Presently the various existing biometric characteristics were fingerprint scan, facial scan, retinal scan, iris Scan, vein pattern scan, digital signatures, keystroke dynamics, voice scan, hand and finger geometry and so on.

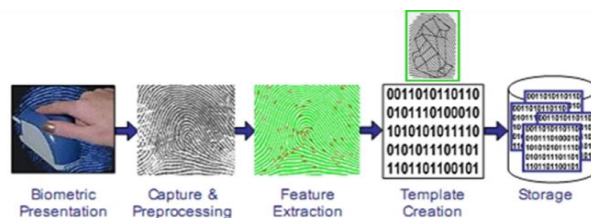


Figure.1. Storing of Biometric Characteristics into database

Biometric technology is used in wider area in various applications like organizations and E-Governance services, National Security, Airports, Banks, offices. Latently implemented in ATM machines, voting Machines, net banking and in Attendance monitoring Systems.

Benefits of Biometric technology: Biometric technology has various benefits like uniqueness, global acceptance, universality, static, measurable, user friendly, accurate and comfortable to use.

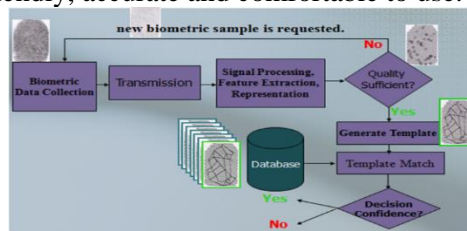


Figure.2. Pattern matching of biometric characteristics from the storage database

Unique Identification (UID): The unique identification (UID) is a mission mode project initiative that provides identification for citizens residing in the country and it is used primarily for delivering welfare services to the citizens effectively. It also act as a effective mechanism to monitor enormous schemes and programs of the government. Authentication framework contains UIDAI and its supporting organizations such as AUAs (Aadhaar User Agencies) & KUAs (e-KYC User Agencies), whom were the service providers or government elements who provides Aadhaar authentication as part of their delivery of service and ASAs (Aadhaar Service Agencies) & KSAs (e-KYC Service Agencies) those who provides AUAs & KUAs securitized connectivity of network to UIDAI's CIDR. The concept of a unique identification (UID) was established by the Department of Electronics & Information Technology (Deity), Ministry of Communications and Information Technology, Government of India. The Unique Identification Authority of India (UIDAI) is responsible to lay plans and policies to real time existence of UID scheme, to govern and maintaining the UID database and to make updates and to maintain the database.

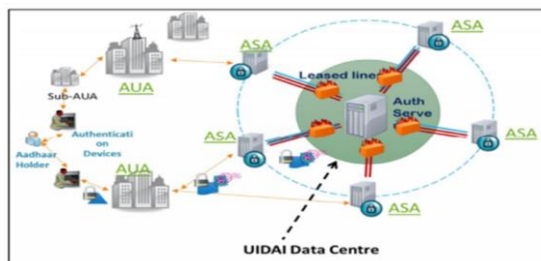


Figure.3. UIDAI Architecture framework

Aadhaar: Aadhaar is one-time standardized enrolment of resident resides in the nation by means of their biometric characteristics such as iris scan, fingerprints scan, facial scan and a single Aadhaar number is provided for an individual. Aadhaar contain Demographic Details like Name, Address, DOB, Gender, mobile number, email and Biometric information like Fingerprints, Iris, Face.

Advantages of Aadhaar:

- Fool-verification and Robust distinguishing proof of inhabitants
- Lower exchange costs.
- Change of conveyance of social welfare programs by making them more comprehensive of groups, now minimized, from such advantages because of absence of identity.
- Permit the administration bodies to move from indirect to direct advantages exchange through electronic channels.

Various features of Aadhaar:

- It is just a 12 digit number
- Random number with no insight
- Less amount of information
- Numbers once issued might never be reissued
- Aadhaar is for all occupants
- Uniqueness guaranteed through biometrics
- Aadhaar does not present Citizenship, Rights and Entitlements
- Security and Privacy of Resident information
- Universal Online Authentication Platform

In India, failure to demonstrate individual identity is the greatest obstruction that keeps the financially weaker and the minimized areas of society from getting to advantages, loan subsidies, and business services from service supplier offices in both government and private parts the nation over in light of the fact that they require verification of personality and location before provisioning an administration or advantage for people, be that as it may, till date there remains no broadly acknowledged, and verifiable and portable identification number, which addresses the issue expressed previously. Accordingly, every time people looking for benefits or services, they experience a full cycle of individual identity. Distinctive service providers have different necessity and procedure of confirmation of personal identity, which prompts burden to people, drags out check process and ends up being costly for service providers. This leads to the need of a individual identification which is overall accepted throughout the globe and evident to guarantee viability of KYC (Know your Customer) at negligible expense to the service providers.

2. METHODS & MATERIALS

Biometrics and Aadhaar card can be characterized as a quantifiable physiological and behavioral characteristic that can be thusly compared & captured with another case at the time of individual confirmation. These innovations are a protected method for authentication since information of both advances are one of a kind, can't be shared, can't be replicated and can't be disregarded. GSM is utilized for making an impression on higher powers when unique mark and Aadhaar card acknowledgment false likewise sort wrong secret key. Our project idea secures the individual data with least hazard factor. Proceed with it, it gives a solid secret pass word to the usage of it by the system administrator. We can utilize one this system framework in large scale in all medical and health care institutes with more security.

Proposed System: The Biometric characteristics of each and every individuals dwelling in the globe along with their personal details like name, address, contact number and parents details would be feed into centralized database server. In case of any accidents the health care centres make use of BMAD, obtains the biometric patterns and feed the obtained patterns into common proposed Website, which in turn connected with centralized Aadhar database server.



Figure.4. Functioning of the Proposed System

The obtained biometric pattern would be matched with the existing biometric pattern of Aadhar database, If the Biometric patterns matches ,the centralized server displays the details about the individual (with his/her family members contact numbers) to the health care centres through which the request for individual identity were been made. The Health care centres as to take of the responsibility for alerting the family members of the individual, whom had met with an accident through SMS services or through a phone call.

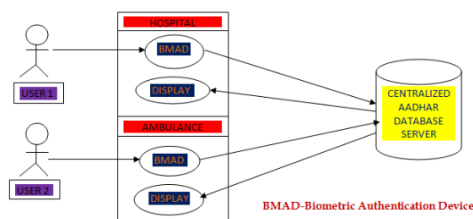


Figure.4. Architecture of the Proposed System

Hospital Module: In this module the doctor or the medicinal consultant in a hospital has to login the UIDAI portal and as provide the patient biometric characteristics to the UIDAI portal by means of Biometric Authentication device (BMAD) provided with them. BMAD captures biometric characteristics and it is passed to the AADHAR database and the proposed system pattern matches the biometric characteristics with already existing biometric characteristics feed to the database and after pattern matching the information, the results(Demographic details) obtained is passed to the display unit connected with the proposed system in an hospital.

Ambulance Module: In this module the doctor or the medicinal consultant in 108 ambulance service has to login the UIDAI portal and as provide the patient biometric characteristics to the UIDAI portal by means of Biometric Authentication device (BMAD) provided with them. BMAD captures biometric characteristics and it is passed to the AADHAR database and the proposed system pattern matches the biometric characteristics with already existing biometric characteristics feed to the database and after pattern matching the information, the results (Demographic details) obtained is passed to the display unit connected with the proposed system in an ambulance.

BMAD module: Biometric Authentication device (BMAD) captures biometric characteristics of an individual and the obtained data's were passed to the AADHAR database.

Database module: Database has various demographic (like Name, Address, DOB, Gender, mobile number, email) and biometric information (fingerprint scan, facial scan, retinal scan, iris Scan) of all citizens resides in the nation.

Benefits of the Proposed System:

- Speedy Information gathering.
- Time Consuming.
- Highly Accurate.

www.jchps.com

- Easy to understand.
- Highly advanced & easy to handle.
- Portable.
- Reliable.
- Multi users can access at a same time.

3. RESULTS

From review of previous research studies, we may come to a conclusion 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 individual identity in health care systems is proposed in this paper. Along with AADHAAR CARD authentication for more security; also included in this paper. Finally, positive and accurate results can be drawn out after observing the AADHAR CARD & Fingerprint Biometric Authentication scheme results.

4. CONCLUSION

In upcoming future, if the system proposed comes to real time existence, it saves time in medicinal centre and it highly reduces complexity of identifying individuals during critical emergencies like accidents, death and so on. This system provides accurate information about an individual, whenever in need and it is universally accepted.

5. ACKNOWLEDGEMENT

I sincerely thank m2m IOT forum-2016 held in New Delhi, India. Supported by the Department of Electronics & Information Technology (Deity), Ministry of Communications and Information Technology, Government of India for selecting this idea has one of the best idea for implementing in Indian nation.

REFERENCES

- Abhijeet S. Kale, Sunpreet Kaur Nanda, Design of Highly Secured Automatic Teller Machine System by using Aadhaar card and Fingerprint, International Journal of Advance Research in Computer Science and Management Studies, 2 (1), 2014, 320-322.
- Nazneen Shaikh, M.H. Kadakia, Riddhi Bhavsar, Aadhaar India- The Most Prominent E Governance Scheme, Research Paper Management, 3 (4), 2014.
- Nimesh P. Bhojak, Assess the awareness level of people on Aadhaar Card as public wellbeing, International Journal of Interdisciplinary and Multidisciplinary Studies (IJIMS), 2 (5), 2015, 88-95.