Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 09, September-2018

An Aadhaar Based Identification Management of Attendees/Attendants in Smart Societies

Himanshu Sharma[1], Dr. Prateek Jain[2]
Faculty of Engg. & Tech., CSE[1]
Manav Rachna International Institute of Research and Studies[1]
Accendere KMS Pvt. Ltd, New Delhi[2]

Abstract: **Aadhaar Based identification is playing a vital role in our real-life scenario and is being required in every sort of transaction/loan/purchase/tax purpose etc. It has been implemented as a security mechanism for various activities too like for applying the passport/licence etc. This paper aims at introducing the presentation phase of a system that will be referred as Aadhaar Based Identification (ABI). This system ensures better security with very less hardware specification need. It is a desktop-based attendees management system for the smart cities/residential societies which can be handled by any person with the knowledge of basic technical skills. There are some unique features introduced in the system like the introduction of UIDAI based server that will be used for confirming the identity of the attendant with the UIDIA website/database by providing the valid Aadhaar card number. This feature will be the pivot point of the paper and interesting points will be discovered using this.**

Key terms: IoT, Attendance Management System, ABI, UIDAI, Aadhaar, Identification.

1. INTRODUCTION

Attendance is for regularly going or being present at a place or event. The attendance management is regarded as a very important process to keep record of the number of people present at any place. In this paper we are considering the attendance management system in residential areas like housing societies, apartments etc. Conventional way of maintaining the attendance in the residential areas include a logbook in which a security guard regularly update the record of the visitor using the credentials like name, phone, address, purpose and time (Shailendra1, 2015). There are a number of examples in our daily life where people are faking these security systems by providing fake identity as there is no verification of the details provided by the visitor. The security management system used in these sectors are still applying file organisation which make the data handling a very complex task. These systems are not reliable and not robust. Data recovery from these file based organisation is very difficult and it require a large physical space for keeping the logbooks used in the process. These logbooks weren't eco-friendly and had to be sold out as waste when they created a huge waste of space. This also led to regular loss of data which could be used for analysis later on if needed. It was good according to that timeline but now with the changing dynamics these systems need to be upgraded. Therefore, there emerged a need to evolve from this existing system of attendance management and add the IT components to upgrade the system by providing online platform for updating and recording the daily attendance in the residential areas[1][2]. This document helps us explain how we can better the system of logbook recovery through IoT based AADHAR Identification Entry System. The system introduced in this paper is called Aadhaar Based Identification. It provides a reliable attendance management system and overcome all the problems faced in maintaining attendance with current file organisation system. This process will include a little bit of Hardware as an overhead, but will prove to be much helpful in the coming years .For example it will contain detailed information of the service providers within the perimeter of the residential complex with exact time and date. This would help track activity of individuals. It can also help with the local police in tracking down the suspected/wrongdoer by having information regarding the last trace of that specific person or group of people in the complex. This will also reduce manpower consumption for data entry as just a few of equipment's would be needed for the same, along with a computer for which a trained individual would be assigned for the job with restricted access (only data entry) to the system database. The biggest advantage of this system would be that the data store is not lost at the end of the month. It would be backed up to the database for review later (if needed). This will also give us the ability to search through the database created at the local server for specific individuals for related information [3]. The resource usage for the system proposed in this paper will be kept minimum keeping in mind the ability of the operator to conveniently operate and carry out all the intended operations needed in the process of attendance management.

COMPONENTS IMPLEMENTING THE PROJECT INCLUDE:

Figure 2.1: Desktop Computer

Figure 2.2: Barcode Reader

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 09, September-2018

Figure 2.3: Finger Print Sensors

Desktop: An electronic device that is configured at the workplace and designed according to the convenience of the organisation will be the first hardware requirement of the system introduced in the system (shown in figure 2.1).

Bar Code Reader: It is an electronic device that read and output the barcode in the computer (shown in figure 2.2).

Fingerprint sensor: It is an electronic device designed for scanning the biometric information of the attendant and it will be used in case of any failure in the Bar code system (figure 2.3).

3. ADVANTAGES OF THE ABI

- ✓ Data Redundancy- The first and foremost advantage of the Aadhaar Based Biometric Identification is its ability to deal with records redundancy and in-consistency [4]. The concept of redundancy arises due to multiple occurrence of same record in single query. This problem is solved using the concept of data consistency in the database.
- ✓ The concept of Data Sharing is also an important advantage in which the data can be shared across different departments [5].
- ✓ Data Concurrency- The access to the data is provided to more than one person for accessing the same data at the same time. Inconsistencies tend to occur when changes made by one user fail to co-occur with those of the other users [6].
- ✓ Data searching – Data entries could be easily searched for in the database using simple in-built searching functions whereas such an operation cannot be performed on the traditional file system [7].
- ✓ Data integrity – Some restrictions may need to be applied on the data before inserting it in the database. The file system does not provide any such procedure as to check these constraints automatically. Whereas Database Administrator maintains data integrity by enforcing user defined constraints on data by itself[8][9].

4. FUNCTIONALITY OF THE AADHAAR BASED IDENTIFICATION

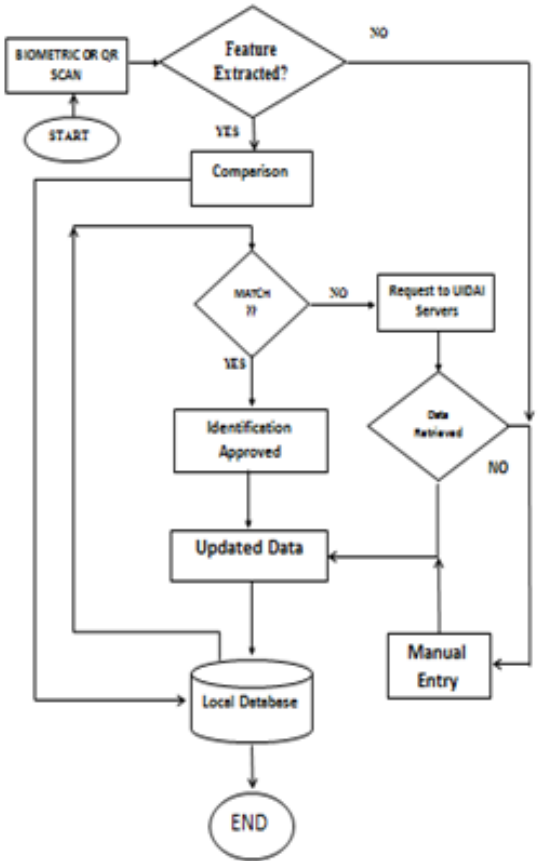

Figure 3.1: Flow chart for Functionality of Aadhaar Based Identification

3.1. Explanation of the Flow chart:

Step 1. The process begins with registering the credentials of the attendant which include Biometrics or QR code on Aadhaar card.

Step 2. The features extracted will be compared with the data in the local database maintained at the client side.

Step 3. If the features match with any of the existing records then the date and time of the entry will be updated and stored in the database. This step will reduce the overhead of requesting the UIDAI servers again and again.

Step 4. Else a request to fetch details of the attendant will be sent to the UIDAI along with the features extracted. The data returned by the servers will be updated in the database at the client side.

Step 5. Worst case scenarios:

→ Hardware Malfunctioning.

→ No data returned by the UIDAI servers.

→ The attendant doesn't have Aadhaar card.

These worst cases will be solved by the Manual Entry button which will fetch the basic details of the attendant along with any ID which will be attached as an image with the record for authenticity proof.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 09, September-2018

3.2. Maintaining local database server

The credentials that will be collected form the visitor will be matched to the records present in the local database using the database server as if the visitor's details are already in the database then there is no need to approach the Aadhaar server. Therefore, this database is maintained to balance the overhead of going to the Aadhaar server repeatedly which causes several problems like delay in data retrieval.

Figure 3.2: Everyone will fall under the UIDAI scanner

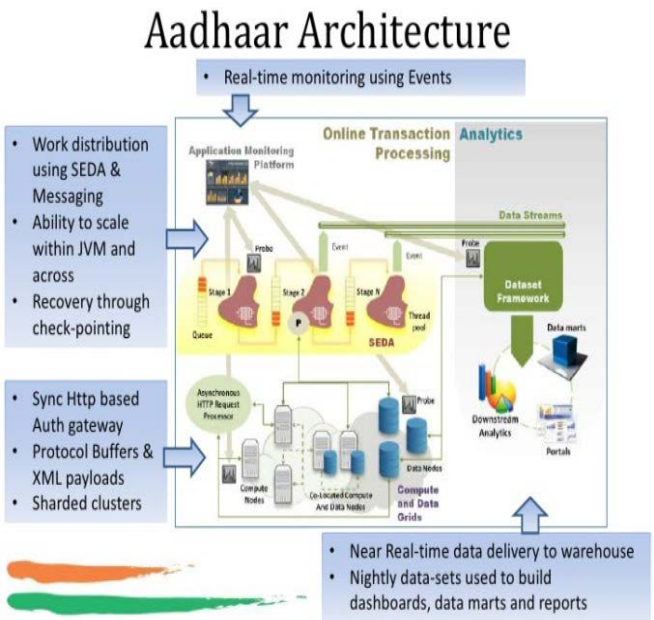

Figure 3.3: Aadhaar Architecture

5. PROPOSED MODEL

Step 1: The first page that will be encountered by the operator is the one-time authentication of that operator and after the verification of the password the operator will be eligible to handle the software. There will be a login session for the operator and it will be his own responsibility to logout.

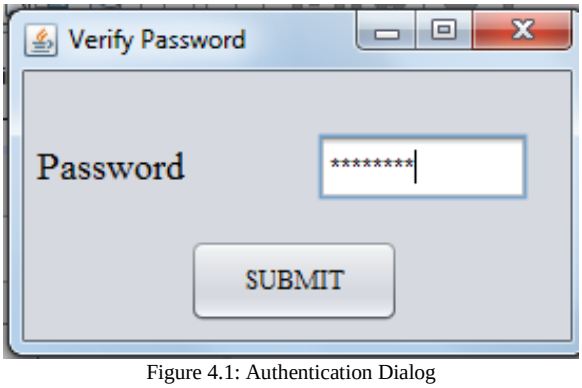

Figure 4.1: Authentication Dialog

Step 2. After the verifying the credentials, the front page of the software will be available which will look like:

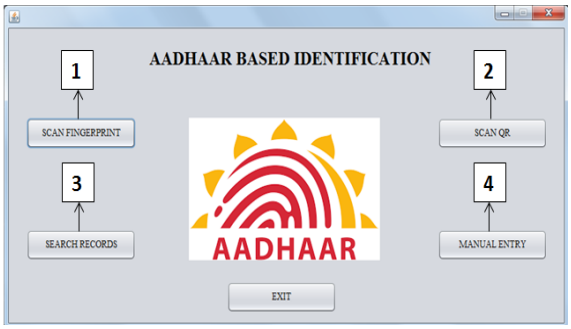

Figure 4.2: The Front page

Following is the detailed description of the functions performed by each button of the form:

1. Scan Fingerprint: This button will open another form in which the attendant's biometric credentials will be recorded and will be uploaded for the purpose of fetching data from UIDAI servers.

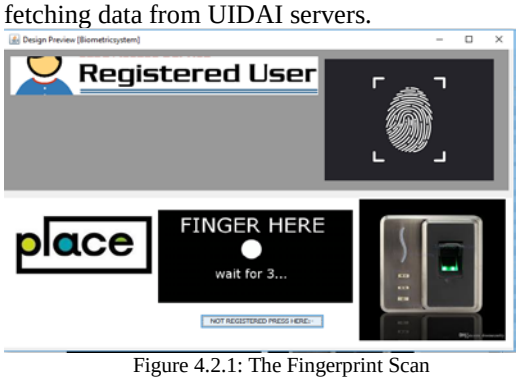

Figure 4.2.1: The Fingerprint Scan

2. Scan QR: This button will be used as an alternative to the scan fingerprint option, in case our fingerprint scanner is malfunctioning then the operator will check for the QR code of the Aadhaar card.

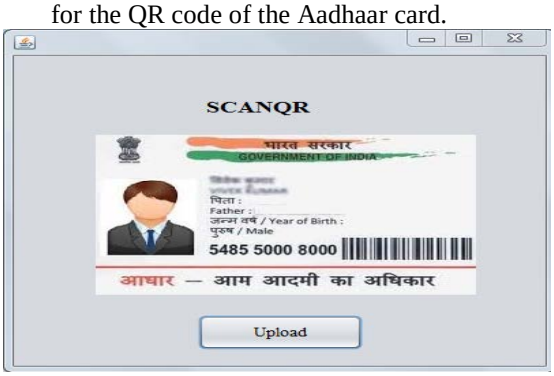

Figure 4.2.2: The QR code Scan

3. Keeping the worst-case scenario in the mind we developed a form which will allow the operator to manually update the record of the attendant in those cases where all the input methods not apply like absence of Aadhaar card, Hardware malfunction etc.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 09, September-2018

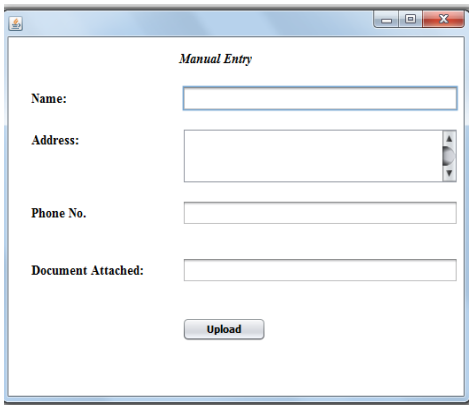

Figure 4.2.3: Manual Entry

4. The "Search Records" buttons will search the records in the database.

6. CHALLENGES OF AADHHAR BASED IDENTIFICATION

- ✓ Initial Acceptance in the society will be a major challenge for the system in laying down its roots.
- ✓ Authorization: The documentation of the project needs to be up to the level of concreteness required by the UIDAI. The acceptance of the document by the UIDAI will assure the future of the project and ease the process of getting permission for accessing the Aadhaar details of the attendants [10].
- ✓ Illiteracy: The lack of basic computing skills in the operator will cause problems in the execution phase of the project. However, this problem will be solved by the tutorial attached with the software.
- ✓ Worst case scenario: In any case if the attendant doesn't have the Aadhaar card then manual registration of the details needs to be done.
- ✓ Privacy Considerations: Respect for privacy rights and expectations is integral to ensuring tr ust in the [11] Internet, and it also impacts the ability of individuals to speak, connect, and choose in meaningful ways (Nam).

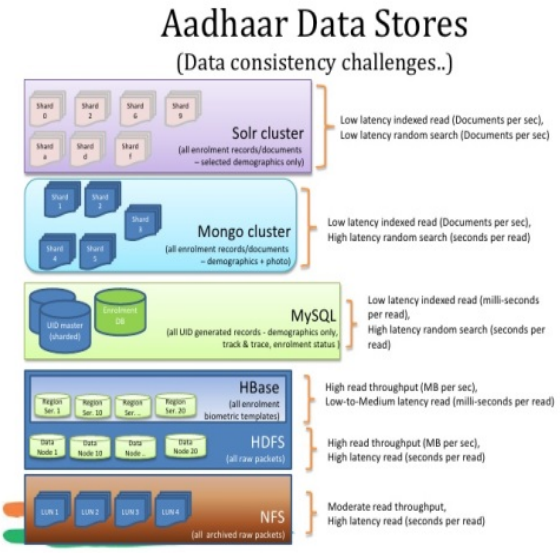

Figure 5.1: Challenges

7. CONCLUSION

This paper will introduce a good sort of thing in the market that will ensure greater safety features. It in introduce the initial structure of the Aadhaar Based Biometric Identification using which attendance management can be optimised. The software that will be used in the accomplishment of the project will be simple and can be handled with little knowledge of computer. It mainly deploys the development of attendance management system using the biometric details of the attendant which will further be used in fetching the data from the UIDAI servers for better authenticity. This technology allows us a faster and more convenient access to the world as it is design to connect other devices and system so that it continue to evolve because people may want to install and further customize home automation devices themselves. The main idea of designing system is to provide many modern security features then traditional system of using file organization. As the technology continues to evolve, the range of possibilities are going to grow as through this technology with Aadhaar connectivity more applications will develop like person rating system based on their character and occupation such that when customer needs services he/she can choose a right service provider with help of Aadhaar based rating system. Further this technology helps police or crime reporter to catch buglers, thieves, criminals.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to Ms. Sunita Virmani, FET, MRIIRS for their valuable comments that led to substantial improvements on an earlier version of this manuscript.

REFERENCES

[1] Liew Ken Nam, University Tunku Abdul Rahman, "Fingerprint Recognition Student Attendance Management System"

[2] Sagar Shukla, GeeksforGeeks, "Advantages of DBMS over File system"

[3] Rishabh Mishra, Prashant Trivedi, Prof. B. Majhi, Department of Computer Science and Engineering National Institute of Technology Rourkela, "Student Attendance System Based on Fingerprint Recognition and One-to-Many Matching".

[4] Joo, D.Y and Kim, J.K.: Creative & active convergence model of IoT, Korea Institute for Industrial Economics & Trade, Korea (2014).

[5] Gauer, A.: Smart city Architecture and its applications based on IoT, Procedia computer science, (2015), Vol.52, pp.1089-1094.

[6] Bagula, A., Castelli, L and Zennaro, M.: On the design of smart parking networks in the smart cities: An optimal sensor placement model, Sensors, (2015), Vol.15, No.7, pp.15443-15467.

[7] Wentao Shang UCLA Los Angeles, CA wentao@cs.ucla.edu Yingdi Yu UCLA Los Angeles, CA yingdi@cs.ucla.edu Ralph Droms Cisco Systems Cambridge, MA rdroms@cisco.com Lixia Zhang UCLA Los Angeles, CA lixia@cs.ucla.edu, "Challenges in IoT Networking via TCP/IP Architecture".

[8] Jaswanth Renganathan, SRM UNIVERSITY, Chennai," I O T , W H ER E I T B E GA N T O W H E RE I T I S N O W !".

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 09, September-2018

[9] Anupama Kaushik Assistant Professor, Department of IT, Maharaja Surajmal Institute of Technology, Delhi, India," IOT-An Overview".

[10] Ms. Yogita Pundir1 , Ms. Nancy Sharma2 , Dr. Yaduvir Singh3 Research Scholar , M.tech (CS), Ideal Institute of Technology, Ghaziabad, India 1 Research Scholar, Ph.D (CS), Mewar University, Chittorgarh, India 2 Associate Professor, Ideal Institute of Technology, Ghaziabad, "Internet of Things (IoT) : Challenges and Future Directions".

[11] Shailendra, M. Singh, M. A. Khan, V. Singh, A. Patil and S. Wadar, "Attendance management system," 2015 2nd International Conference on Electronics and Communication Systems (ICECS), Coimbatore, 2015, pp. 418-422.