iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5472

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Implementation of Aadhaar Based EVM

Kiran Chavan[1], Kashinath Raut[2], Ashish Bhingardive[3], Yogesh Kolape[4], D. M. Ujalambkar[5]
[1, 2, 3, 4, 5]*Computer Department, Savitribai Phule Pune University*

Abstract*: *The main objective of this project is safe and secure voting system using Aadhar to avoid the misunderstanding that takes place in the election. The objective of the system is to innovate an electronic voting system which will use fingerprint identification for voter identification. This system authenticates voters by matching fingerprint and eligibility is checked by verifying the age that allows only eligible candidates to vote. We get the fingerprint data from Aadhar databases and at the time of voting we scan fingerprint using fingerprint scanner and compare with Aadhar database fingerprint. If the fingerprint matches, then it allows the user to cast their vote else user will not be allowed to vote. After casting their vote or completion of the vote, the system will send a confirmation message on voter's registered mobile number. In this system counting of votes will be faster, more accurate, transparent and less manpower.

Keywords: Aadhar, Fingerprint, Voting, Biometric, Thumb.

I. INTRODUCTION

4Voting machines are the collection of mechanical and electronic equipment including hardware and software is used to define ballots to cast and count votes to report or display the election results too. In a biometric recognition system, the biometric pattern is usually stored on a central server during enrolment. The candidate's biometric template captured by the biometric device which is sent to the server where the processing and matching steps are performed. These biometric variations of human identification have used to propose the development of fingerprint scanners that are used to quickly identify users and assign access permissions. The procedure for fingerprint recognition is the electronic methods of recording and recognizing an individual fingerprint and which substantially advanced during the decade of the 21st century. which results in, the use of EVM which includes store, search, match and identification of true voters [2].

The main aim of voting is to allow voters to use their right to choose their government and political representatives. It has always been a difficult task for the election commission to conduct defect free and fair polls in our country. A lot of money power has been used on this to make sure that the elections are violent free. Almost all the voting systems include same steps such as: Voter identification and authentication, Voting and recording of votes cast, Vote counting, Publication of election results. Voter identification is required during two phases of the electoral process: first for voter registration in order to define the right to vote and afterward, at voting time, to allow a citizen to vote by verifying if the person satisfies all the requirements needed to vote (authentication).

To provide efficient solutions to the above problem, in this project we have implemented EVM with biometric functionality i.e. fingerprint scanning. This is used to verify the security to avoid fake, repeated voting etc. It also improves the accuracy and speed of the process. The system uses fingerprint features template for voter identification as we know that the fingerprint of every human being has a unique pattern [3].in this project we are using aadhar number to uniquely identify each voter and further using fingerprint verification to authenticate the voter.

II. PROPOSED SYSTEM

To overcome the problems associated with the traditional system we are proposing a voting system which is more secure, time saving and provide two level of authentication by electronic means based on individual bio-metric traits of the voters. The new system will use the bio-metric system for the voter as authentication by which at the time of election if scanned bio-metric data of the voter matches with that of saved in the system then and then only he will allow to vote otherwise he well rejected a reported as fake voter. Bio-metric properties of any individual are unique universally, which cannot be matched with anybody like fingerprint.

In the proposed method, disadvantages and drawbacks faced in the existing method can be avoided. Today we all know that the bogus or fake voting is still a major drawback in the voting system. We can switch over from ballot paper to electronic voting machine (EVM), but this problem cannot be avoided completely.

This paper will attempt to solve this problem. Today we all have AADHAAR CARD, so the government has all the database of all the users including fingerprint database. So, if we use the database effectively with the help of Micro-Controller then we can completely overcome the problem of bogus voting. Both fingerprint identification and Aadhaar number verification of the personnel

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

are compared and verified with the data stored by the microcontroller. We are also validating users based on whether he is Eighteen plus or not by checking his age or status of voting.

This paper shows how the problem of existing voting system can be solved with the help of fingerprint scanner and Microcontroller which will be convenient for every citizen to use at the polling booth. For this project Fingerprint proves to be one of the best method. As we are discussing Biometrics we need Fingerprint scanner. When coming to the implementation of project citizens have to place their finger in fingerprint sensor. When it is matched with the stored fingerprints and then we can allow the voter to go to the voting process.

A. Block Diagram

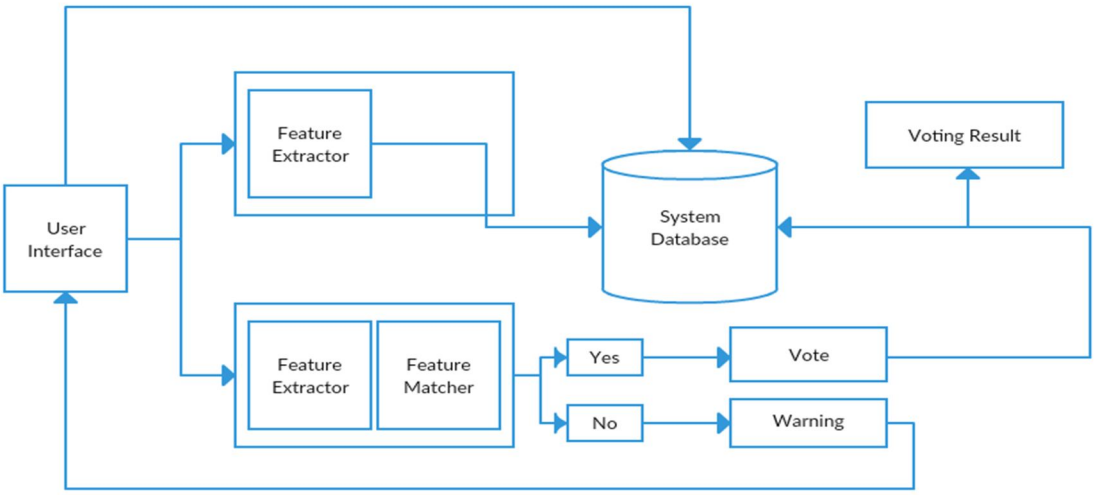


Fig. 1 Block Diagram of AADHAR Based EVM

B. Fingerprint Scanner

This is a fingerprint sensor module having the TTL UART interface for direct connection to the micro controller to PC through MAX232 / USB-Serial adapter for communication. The fingerprint data store in the module and it can configure it in 1:1 or 1: N matching for identifying the individual's identity. The Fingerprint module can directly interface with 3v3 or 5v Micro controller. A level converter (like MAX232) is necessary for interfacing with PC serial port. The optical bio metric fingerprint reader having great features and can be embedded into a varieties of end products, such as access controls, attendance system, safety deposit boxes, car door locks [5].

Fig. 2 Fingerprint Module

III.PRINCIPLE OF WORKING

The microcontroller which we are using in our project will take only 3.3v of a power supply as it is low power consumption. After switching the power supply, to press the reset button. The first mode is to register the fingerprints, so voter should have to keep the finger on the optical scanner where it scans the image and saves it with a unique id number. From microcontroller, we have to give connections to the LCD display in order to show the process of voting. Switches are also connected to the microcontroller where we have 16 keys in which four keys (A, B, C, D) are used for different parties and Numeric keys are used for Entering Aadhar Number and # key is used to indicate the end of input.

Fig. 3 Aadhaar Based EVM

The personal details of the voters in an area are already registered in the database. During the election, the voter keeps their fingerprint in the biometric sensor. At the same time, a camera captures the image of the voter and compares the image and the details, stored in the database. If the same person was found to be voted already, the voting would be canceled.

During the voting, each person will place the finger on the module and it will scan the fingerprint. If the fingerprint is matched with the stored data then the voter will be allowed to cast the vote. After that, he/she can put his valuable vote to his favorite candidate and a message will be received that the vote is cast. In case the fingerprint is not matched then the respective voter is said to be not an Authorised voter and he is not allowed to vote. After this, we will receive a message that user identification failed. If the candidate tries to vote again then a message will be sent that voter already voted. After completion of voting, the results will be seen by the supervisor.

A. Voting Results

We are showing the voting result using Pie chart which will display the party name having the highest number of votes

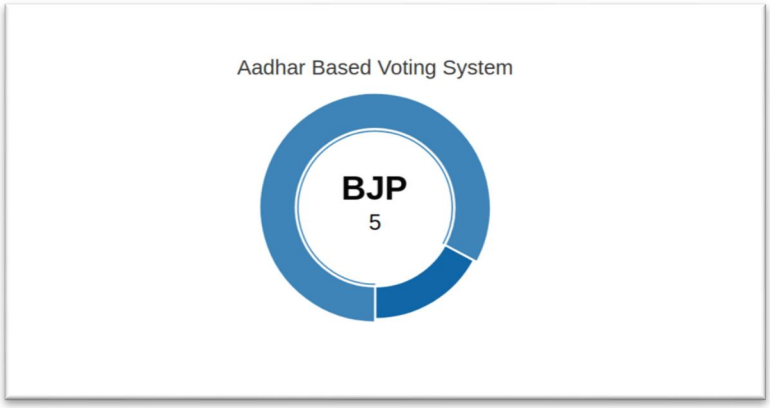


Fig. 4 Result of Voting

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

IV. FINGERPRINT IDENTIFICATION

Fingerprint verification is the method of identification based on the various patterns of fingers, which is actually unique to each person. It is the most popular way of acquiring details of any person and is the easiest and convenient way of identifying a person
Fingerprint matching has become an appropriate and suitable way for accurate personal identification. A fingerprint is composed of valleys and ridges on the surface of the fingers.
Fingerprint processing involves two parts one is fingerprint enrollment and another one is fingerprint matching. The user needs to place the finger two times on fingerprint sensor at the enrolling process. The system will extract the features from single finger image twice and generate a template of the finger based on two results and it stores the template in the database. At matching, the user enters the finger through fingerprint sensor and the system will generate a template of the finger. And it compared with templates of the finger library. For matching, the system will search the whole finger database library for matching the finger. In this case, the system returns the matching result as, success or failure. [7] [8]
When communicating, the transferring of command or data or results are all in a specific data package format. The format for data package communication is shown below:

Table I Data Package Format

2 bytes	4 bytes	1 bytes	2 bytes	-	2 bytes
Header	Address code	Package identifier	Package length	Package content (data)	Checksum

A data package transferred to the module includes the Header, Address, Package Identifier, Package Length, Package Content and Checksum as shown in above table.

Name	Symbol	Length	Description
Header	Start	2 Bytes	Fixed Value of EF01H;High byte transferred first.
Adder	ADDER	4 Bytes	Default value is 0xFFFFFFFF,which can be modified by command.High byte transferred first and at wrong adder value,module will reject to transfer.
Package Identifier	PID	1 Byte	01H : command packet
			02H : Data packet,data packet shall not appear alonr in executing processes,must follow command packet or acknowledge package.
			07H : Acknowledge Packet
			08H : End of data packet
Package Length	LENGTH	2 Byte	Refers to the length of package contents(command packets and data packets)plus the length of checksum(2 bytes).Unit is byte.Max length is 256 bytes.And high byte is transferred first.
Package Content	DATA	-	It can be commands,data,command parameters,acknowledgement results,etc.(Fingerprint character value,template are all deemed as data.)
Checksum	SUM	2 Bytes	The arithmatic sum of package identifier,package length and all package contents.Overflowing bits are omitted.High byte is transferred first.

Fig. 5 Definition of Data Package

When enrolling the new users it will process the user's image of the fingerprint into the packet as shown in above table and then write this structured packet into the fingerprint module i. e. saved as a template into the database, so that it can be used later to verify the users.

In the same way, while verifying the users, users fingerprint image is first converted into the packet (template) and then this template is compared with the already stored templates, if any template is matching then the user will be successfully verified and allowed to do next task. [8]

V. CONCLUSION

Through this article we have proposed the Secured Aadhar based electronic voting machine, which Prohibits illegal voting, User friendly and reduces the usage of papers and simple to operate. In future by extending this concept, the system can also be applied for Pass Port Verifications and validation in all countries in addition with eye retina scanning, face detection identity which may prohibit the illegal entry globally and also each country can keep track of the each foreigners, in which the global database management and privacy of each citizens is a considerable factor.

REFERENCES

[1] G.Valarmathy , V. Saranya, Riya Rose Cherian, K.Poovizhi , Smart Voting System using Aadhar , IJRE International Journal of Research in Electronics, Vol. 04 Issue Jan. 2017.

[2] J. Chenguttuvan , M.Kumaran , R. Shrinivas, Voting through Power Line Communication with Biometric Verification , International Journal of Research in Applied Science & Engineering Technology(IJRASET), Vol. 5 Issue September 2017.

[3] V. Shyan Babu, A L Shridhara, R. Kartik , Koppula Shrinivasa Rao, K. H. Murali, User Friendly Aadhar Based Electronic Voting Machine Using ARM7, International Journal of Civil Engineering ans Technology(IJCIET), Vol. 8, Issue 7, July 2017.

[4] Kavita Shinagare, Priyanka Mahimkar, Pallavi Karbhari, Biometric System Based Electronic Voting Machine, International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 5 Issue: 1.

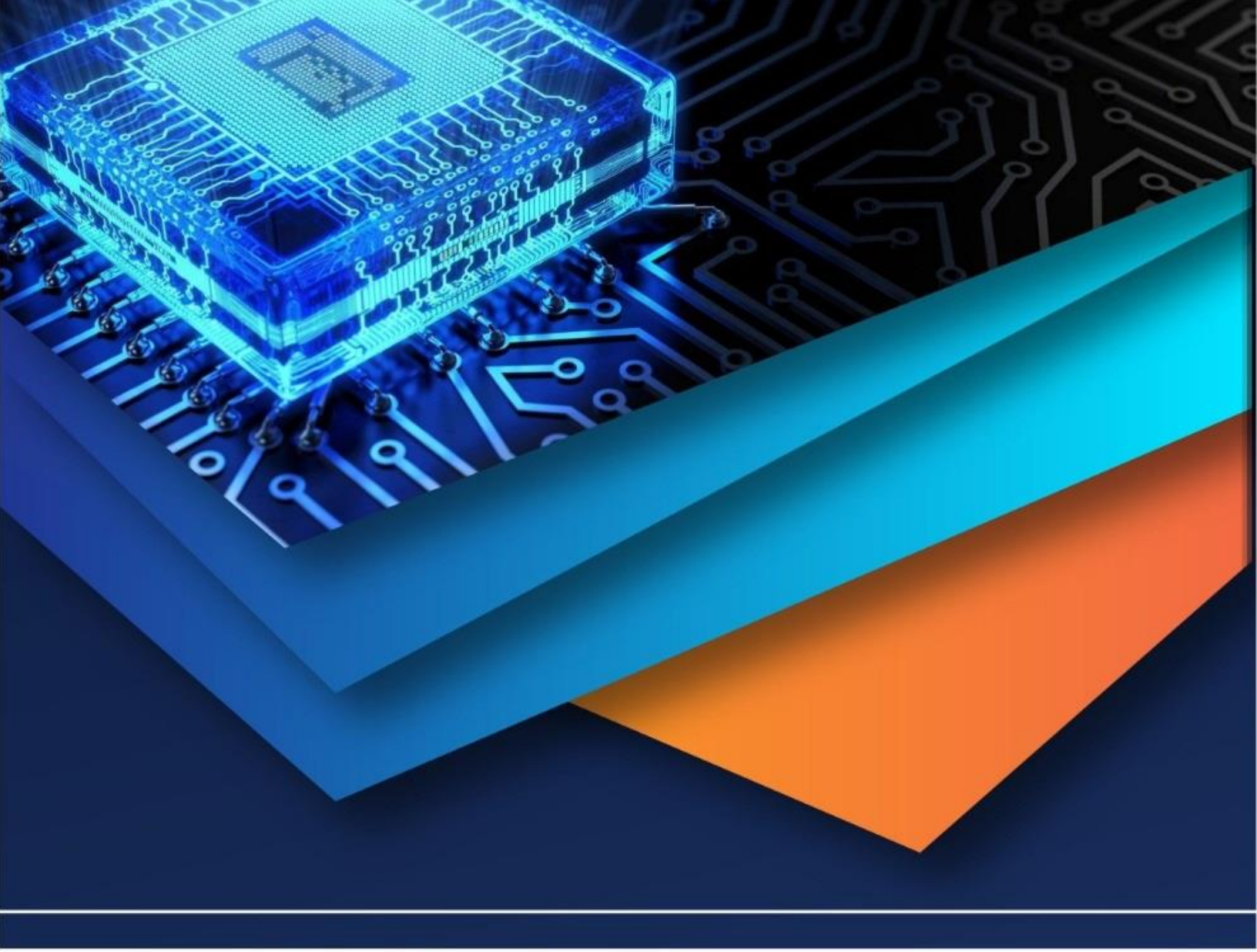
[5] https://www.sunrom.com/p/finger-print-sensor-r305.

[6] https://www.google.co.in/searchq=fingerprint+module&rlz=1C1CHBF_enIN755IN755&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjOwa3Gx9faAhUITN8KHc5zCV8Q_AUICigB&biw=1366&bih=662#imgrc=5ZjBi2daTwYNTM.

[7] https://cdn-shop.adafruit.com/datasheets/ZFM+user+manualV15.pdf

[8] A. lain, L. Hang, S. Pankaiti, and R. Bok, "An identity authentication system using fingerprint, Proceedings of IEEE, vol. 85, no. 9, pp. 1365-1388, 1997

[9] Ashraf Darwish, Aliaa Youssif, Magid Algendy,and Eman Mohamed, A Secure And Robust Prototype For Electronic Voting System, 3(3), October - December (2012), pp. 510-519, International Journal of Computer Engineering and Technology.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY