ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 10, Issue 8, August 2023

Biometrics Based Smart Electronic Voting System Using Internet of Things

Jonnala Madhukar Reddy[1], M.Udhayakumar[2]
[1]PG Scholar, Electrical & Electronics, Ponnaiyah Ramajayam Institute of Science and Technology, Thanjavur-613 403, Tamilnadu, India.
[2]Assistant Professor, Electrical & Electronics, Ponnaiyah Ramajayam Institute of Science and Technology, Thanjavur-613 403, Tamilnadu, India.

Abstract: In every election, he election commission is facing a lot of troubles and different type of problems throughout the election. The most familiar issue faced by the election commission is inappropriate confirmation with respect to the arrangement of casting the votes, duplication or illegal casting of votes. In this project, a secure and new voting system is developed to improve the existing voting system using iris recognition. Iris one of the most secure biometric of person identification. The main goal of this article is to avoid duplication of casting votes. This project focuses on sophisticated voting system using finger print and iris. This project focuses on sophisticated voting system using iris and Finger print technologies. The voting process is carried out only if the finger print matches with the stored value and We are scanning individual's iris and storing it in a voter's database by giving appropriate AADHAR card no. If a person comes for voting, then his or her iris is detected and this detected image is compared to image in voter's database. When the iris is detected we get the information about the voter in our PC, then that information is compared to the voter's finger print. If both the details get matched, then the person is allowed to vote. The current voting system is not secure, there are some individuals who give dummy votes or they are registered at more than one place. In this paper the Security of the voter is discussed and in general and the focus is on making the voting system more robust and reliable by eliminating dummy voters. After successful completion of voting the details of voting is stored in cloud using IoT. The data are collected and calculated automatically. The total voting and data are calculated automatically and the result is shown in IoT at the End of the Day itself. It will reduce the storage of voting machine for certain no of days and also reduce change of voting machine by illegal person.

I. INTRODUCTION

Voting is the right of each citizen to cast the vote and select their leader. India is a democratic country and each citizen has the right to vote and show their option. People also have the right to change the ruling party in upcoming election by voting for the candidate. Voting is not done to elect the government leaders, but also conducted to elect the leaders in schools, colleges, banks, society, etc. Biometrics is a way used to recognize a person based on his physical nature. The fingerprint, iris, face, voice, etc. are the mainly used biometrics to recognize a person. There are two key functions for biometrics, first is one to one matching and other is one too many matchings. In one to many matching the biometric sample is compared with the already stored samples. In one to one matching, it compares with the previously stored sample. Biometric method results in a faster security, and more convenient method for user verification. Biometric method is better than password security. Fingerprint is unique for each individual so it can be used as a mark of signature, verification and authentication.

II. IOT (INTERNET OF THINGS)

The Internet of things (stylized Internet of Things or IoT) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. In 2013 the Global Standards Initiative on Internet of Things defined the IoT as "the infrastructure of the information society. "The IoT allows objects to be sensed and/or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine (M2M) communications and covers a variety of protocols, domains, and applications, the vision of the Internet of things has evolved due to a convergence of multiple technologies, including

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 10, Issue 8, August 2023

ubiquitous wireless communication, real-time analytics, machine learning, commodity sensors, and embedded systems.

III. EXISTING SYSTEM

Electronic voting (also known as E-voting) is voting using electronic systems to aid casting and counting votes. Voting machines use a two-piece system with a balloting unit presenting the voter with a button for each choice connected by a cable to an electronic ballot box. An EVM consists of two units:

1. Control Unit
2. Balloting Unit

The two units are joined by a five-meter cable. The Control Unit is with the Presiding Officer or a Polling Officer and the Balloting Unit is placed inside the voting compartment. Instead of issuing a ballot paper, the Polling Officer in-charge of the Control Unit will press the Ballot Button. This will enable the voter to cast his vote by pressing the blue button on the Balloting Unit against the candidate and symbol of his choice. The controller used in EVMs has its operating program etched permanently in silicon at the time of manufacturing by the manufacturer. No one can change the program once the controller is manufactured.

DISADVANTAGES

The main drawback of this system is that, voter's id checking process is manual hence possibilities of illegal voting by a wrong candidate. And also, possibility of multiple votes by same person. To avoid this problem, Author going to use E- voting system.

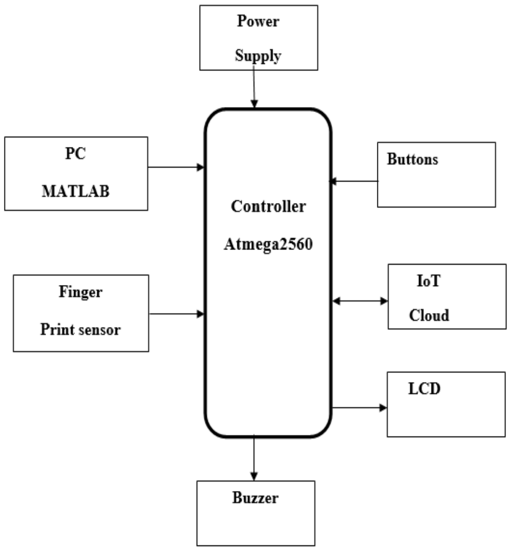
IV. PROPOSED SYSTEM

- This project is very used to improve the security performance in the voting machine. In this project finger print with iris we used for voting purpose
- Now day's some person makes the duplicate vote ID card. But in this project human iris is used for caste the vote.
- So this project improves the security performance and avoid forgery vote because naturally one human iris is different from other human.
- After matching of human finger print and iris the system will allow the voting otherwise alert system will turn on
- Vote counting directly update through cloud using Node Mcu

ADVANATGES

- Iris recognition accuracy
- Iris act like digital passwords that cannot be lost, forgotten or stolen.
- The processing speed is high so it's has less computational time.

BLOCK DIAGRAM



HARDWARE REQUIREMENTS

- Atmega2560
- Finger Print
- IoT(ESP8266)
- Buzzer
- LCD
- Buttons
- 12V Power Supply

SOFTWARE REQUIREMENTS

- Arduino IDE
- Proteus
- Language: Embedded C
- Cloud Server

V. MODULES

Iris Recognition

Iris recognition is done by following modules,

1. Image Acquisition
2. Iris Segmentation
3. Feature Extraction
4. Recognition

Image Acquisition:

- Image acquisition in image processing can be broadly defined as the action of retrieving an image from some source, usually a hardware-based source, so it can

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 10, Issue 8, August 2023

be passed through whatever processes need to occur afterward.

- Performing image acquisition in image processing is always the first step in the workflow sequence because, without an image, no processing is possible. The image that is acquired is completely unprocessed and is the result of whatever hardware was used to generate it, which can be very important in some fields to have a consistent baseline from which to work.
- Test iris images are acquired from gallery.

Iris Segmentation*:*

- Next, a segmentation algorithm is used, which would localise the iris region from an eye image and isolate eyelid, eyelash and reflection areas.
- Automatic segmentation is achieved using the circular Hough transform for localising the iris and pupil regions, and the linear Hough transform for localising occluding eyelids. Thresholding is also employed for isolating eyelashes and reflections.
- Third, the segmented iris region is normalised to eliminate dimensional inconsistencies between iris regions.
- This is achieved by implementing a version of Daugman's rubber sheet model, where the iris is modelled as a flexible rubber sheet, which is unwrapped into a rectangular block with constant polar dimensions.

Feature Extraction:

- Third, detection of interest points in iris and find strongest features in iris via Harris Spatio temporal corner detector and SURF feature descriptor.
- Finally mean feature calculated from HSTCP and SURF.

4Recognition:

- This is the last stage for iris recognition.
- In that, machine learning models such as SVM and KNN classifiers are used for iris recognition.

Node MCU

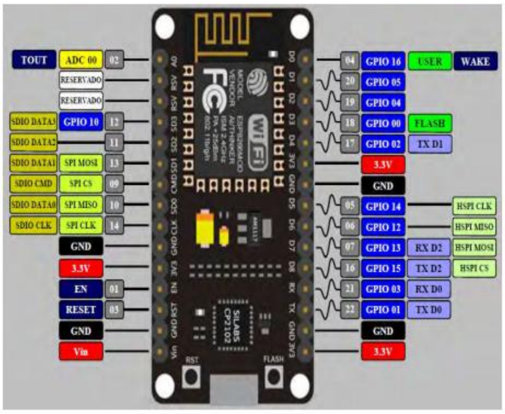


Fig: Node MCU Pin diagram

VI. CONCLUSION

This project suggest that the EVM system has to be further studied and innovated to reach all the levels of community, so that the voter's trust on the election process will increase and election officials will make more involvement in purchasing the innovated EVM's for conduct efficient, secure, corruption free Elections . Further innovations can be made so that the voter can vote wherever they are during the election, getting to choose the candidate competing in their home constituency without the necessity of travel. The described model consisting of fingerprint sensor can also be modified to be used with Retina scanner which provides even more secure and technologically advanced solution to fake voting and impersonation. This concludes that the Aadhar based EVM will useful to avoid rigging in election by impersonation, to avoid time consumption and all the while keep the voter's information more secured. The conventional paper ballot method also consumes lot of man power and security issues to the Electoral Commission which can by reduced by this system.

REFERENCE

1. M. A. Khan and K. Salah, "IoT security: Review, Blockchain Solutions, and Open Challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.

2. U. D. Gandhi, P. M. Kumar, R. Varatharajan, G. Manogaran, R. Sundarasekar, and S. Kadu, "HIoTPOT: Surveillance on IoT Devices Against Recent Threats," Wireless personal communications, vol. 103, no. 2, pp. 1179–1194, 2018.

3. G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 10, Issue 8, August 2023

framework for securing connected and autonomous vehicles," Sensors, vol. 19, no. 14, pp. 1–15, 2019.

4. M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study," International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, p. 383, 2017.

5. F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtysson, ` "Blockchain-based E-Voting System," in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018, pp. 983–986.

6. R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust management in social internet of vehicles: Factors, challenges, blockchain, and fog solutions," International Journal of Distributed Sensor Networks, vol. 15, no. 1, pp. 1–22, 2019.

7. X. Lin, J. Wu, A. K. Bashir, J. Li, W. Yang, and J. Piran, "Blockchainbased incentive energy-knowledge trading in iot: Joint power transfer and ai design," IEEE Internet of Things Journal, 2020.

8. J. Chen, J. Wu, H. Liang, S. Mumtaz, J. Li, K. Konstantin, A. K. Bashir, and R. Nawaz, "Collaborative trust blockchain based unbiased control transfer mechanism for industrial automation," IEEE Transactions on Industry Applications, vol. 56, no. 4, pp. 4478–4488, 2019.

9. X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, "A Secure Verifiable Ranked Choice Online Voting System based on Homomorphic Encryption," IEEE Access, vol. 6, pp. 20 506–20 519, 2018.