Secured Fingerprint Based Voting System using IoT

Er.Mausmi Dagwar *1, Chaitali Kawadkar *2, Saurabh Nidhan *3, Niraj A. Kurhade *4 Krunal G. Padole *5

1 Assistant Professor, 2, 3, 4, 5 Student
Computer Science and Engineering Department,
Priyadarshini J.L College of Engineering - Nagpur, Maharashtra 440009, India

Abstract

Within the current situation, most of the countries of the globe hold their elections victimization electronic choice Machines, wherever your vote gets registered electronically fifteen with the assistance of associate Electronic Machine while not victimization and wasting ballot paper to vote for elections. As security could be a major concern today, guaranteeing that no one exercises the correct to vote doubly is that the main facet. sixteen we are able to resolve this issue by introducing Finger Print based mostly choice, wherever an individual is approved supported his Finger Print. this may place associate finish to pretend choice. The domain of the project is that the net of Things wherever we tend to square measure building Fingerprint based mostly Biometric mechanical device victimization Arduino. twelve we all know that IoT is that the system of reticulated computing devices, mechanical and digital machines, objects, and also the ability to transfer knowledge over a network while not requiring human-to-human or human-to-computer interaction. Thus, our Fingerprint on-line module is associate application wherever the user is recognized by his finger pattern.

I. INTRODUCTION

Voting is associate integral a part of a democratic society of selecting leaders and contributes towards the betterment of the country. It's a decision-making mechanism wherever twenty-four security plays a vital role in choice. so as to confirm high security, mechanical device ought to be designed and developed with charge. Therefore, half dozen this project is intended for associate electronic mechanical device by victimization the fingerprint identification methodology.

Here a voter's fingerprint is employed for distinctive the voters. The system can check whether or not it matches pre-stored impressions within the info. If it matches, then the system can enable the citizen to poll his vote and otherwise stop the citizen from polling.

For a legal system to be ideal, 5 attributes should be satisfied: fidelity, robustness, coherence, consistency, safety and security. {the on-line the web the net} legal system could be a web-based system that facilitates the running of election online firmly. This technique has been developed to modify the method of organizing elections and create it convenient for voters to exercise their votes by providing the specified hardware and computer code capabilities.

The main objective of our on-line legal system is to develop a secure and reliable on-line application for the choice of elections by additionally considering the new generation of voters WHO square measure higher than eighteen years archaic. twenty-one A centralized info is maintained wherever the knowledge of all the voters is maintained. Whenever a national is victimization a web legal system, his/her data and fingerprint is verified and documented with the information gift within the info. If the information gift within the info doesn’t match with the voter’s details, then he/she is fourteen not allowed to vote. If the small print match, the system checks for double choice. If the citizen has already voted once, he/she isn't allowed to vote once more else the citizen is allowed to exercise his/her right to vote.

Location pursuit technology is presently being developed victimization varied technologies like RFID (Radio Frequency Identification), GPS (Global Positioning System), GSM (Global System for Cellular Communications), Wi-Fi, Mobile, Bluetooth, Infrared and then on [1]. GPS systems square measure additional economical than alternative navigation systems, and knowledge message reception is unaffected by climate or weather changes. The weakness of GPS is that GPS technology isn't economical if applied inside as GPS satellites have a proof that can't labour under the walls of the building.

II.METHODOLOGY

A form is created for registration purpose of the elector and candidates. Through this registration kind information vi of all the voters and candidates are collected as well as their fingerprints. On the server aspect, a worldwide info is maintained for all registered voters and candidates. Also, the server runs in time period and provides backend statistics for fourteen the whole election method. On the consumer aspect, a significant performance demand is critical. twenty-six so as to scale back the congestion rate on the network links, native|an area|a neighborhood} info at the consumer aspect is needed to host the info that prevails to 1 or a lot of local choice centres. eight This dB could be a rather dynamic and dynamical one, within the sense that the info hold on in its tables could vary over the election fundamental quantity. Here the scale of the native dB at any choice centre is simply atiny low fraction of the world dB at the server aspect. twenty three the utilization of an area dB is significant because it enhances the performance of the choice method. However, this approach creates a synchronization drawback, which can be self-addressed later during this section.

The two most vital challenges baby-faced one by associate e-Voting system is to confirm that no elector will impersonate or duplicate another elector and no elector will vote quite only once. within the projected system, we have a tendency to use associate identification followed by associate authentication method. thirteen The identification is completed via a manual credibility check by the admin WHO verifies the official Aadhar card of a elector and pulls the elector record from the native dB or hundreds the record from the central dB if it's not found within the native one.

The elector record includes a biometric description of the elector given throughout the initial registration. twenty five one in every of the foremost necessary components of technique} is fingerprint authentication method. seven The elector are rejected if his/her fingerprints don't match the hold on ones. generally the system could throw in the towel to false rejections too. so as to scale back these, we have a tendency to store many copies of the fingerprints of every elector taken at totally different time intervals. This twin method guarantees one that nobody will incorrectly impersonate a elector. seven so as to forestall 2 or a lot of votes per elector, we have a tendency to use a “Voting standing flag” which might guarantee that no elector votes for quite only once in associate election. The flag initial worth is taken as FALSE at the start of the election method.

Case A: Whenever the voter’s identity is verified via the identification step (before the authentication step) twenty two the choice standing flag is about to TRUE. however if the authentication fails, the flag is reset too FALSE.

Case B: five If the elector leaves the station while not choice, the flag is additionally reset to FALSE, so permitting the elector another likelihood to undertake once more to solid his/her vote however if the elector completes the choice method, the flag remains set to TRUE.

Case C: just in case the results of the vote isn't committed to the central dB in due time, the flag within the voter’s central record is about to TRUE, so eliminating the likelihood of another tried choice by constant elector, or by somebody WHO carries a counterfeit or a replica ID card.

Thus, whenever one the record of the elector is checked before the choice method, the choice standing flag of the elector is checked at central dB. If the flag is about to TRUE, then the elector is denied his vote. seven it's attainable that a record gets loaded at 2 totally different choice centres. once a elector makes an attempt to access the record at any of the stations, the consumer can verify the central dB choice standing flag. If it's been set to TRUE, access is denied; otherwise, it sets the flag to TRUE and access is granted.

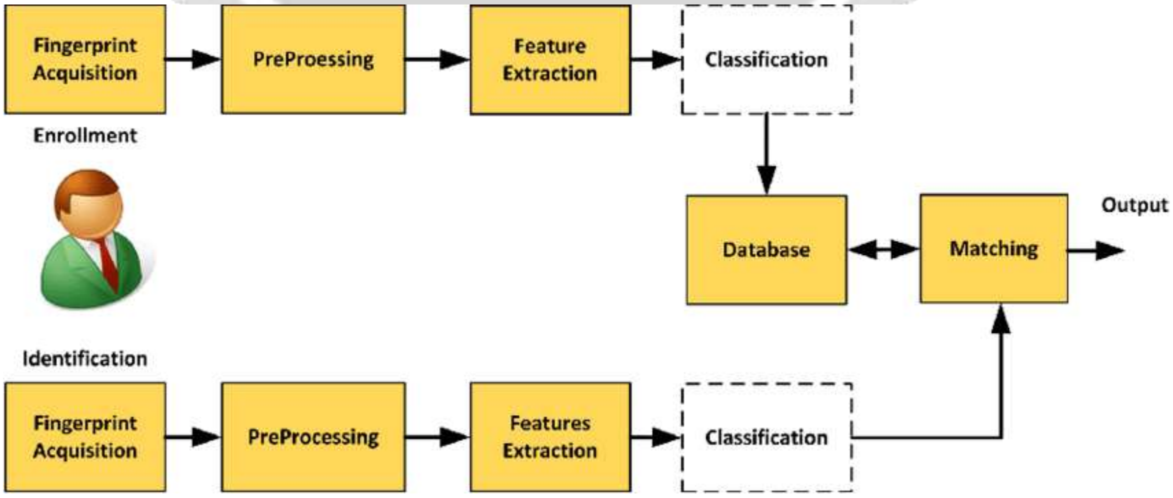
one to create the electoral system of Asian nation quicker and safer, an endeavor has been taken in order that the electoral system may be acceptable to any or all reasonably national of the state. the safety was the most concern of the entire project. a lot of security has been another compared to usual vi electronic mechanical device by adding the fingerprint feature in order that there can not be any reasonably cheating. By victimization this method, the national electoral system are safer, faster, one straightforward to use and a lot of economical. The system additionally consumes terribly low power and therefore the device is simple to hold. the full price of 1 machine would be but BDT 5500.

twenty five In one word, the system can build electoral system a lot of reliable and safer. it's higher than ancient ballot-paper system. one in a very country like Asian nation wherever government is attempting to bring technologies in each case to create the country a lot of developed, electoral system could be a superb place to use new technology like this, by that the folk can elect their right representative in smarter and secured method.

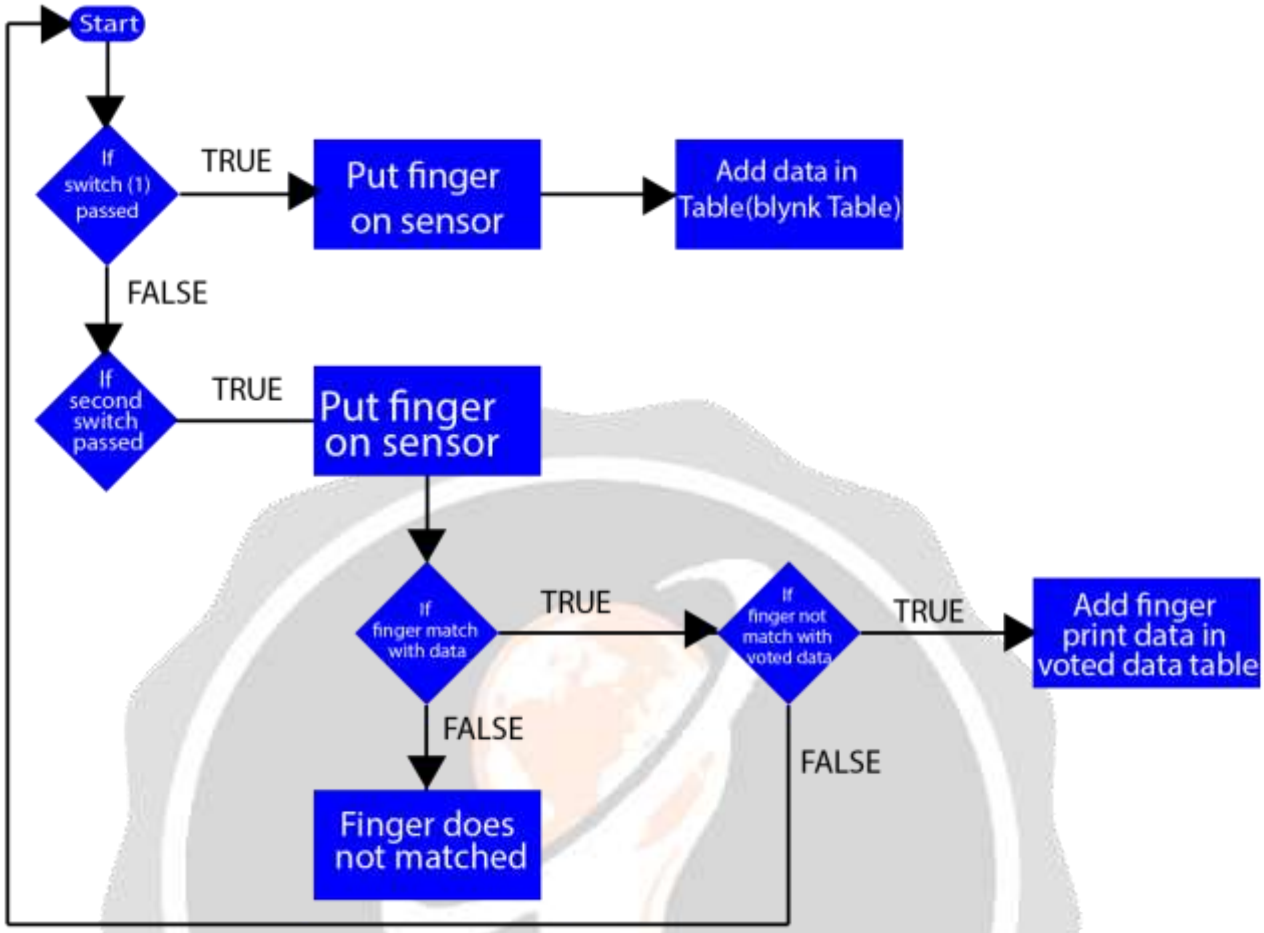
The next challenge for watching the attending system is recording usage information from its fingerprint and reportage method to the users themselves and therefore the authorities. The reportage system created should be easy, period of time and accessible in real time from anyplace. This analysis are going to be designed a system which will one discover the presence of an individual throughout operating hours. The system is intended as a result of this quality of employees is extremely high and not simply works within the workplace solely. this method will discover workers WHO perform their duties outside the workplace or out of city to abroad. Users should install APK files on their smartphones and found out workplace coordinates and their fingerprint input to the system. once users log in victimization fingerprints, the information can mechanically be sent to a information which will be accessed from anyplace via the humanoid application, through the web site and mechanically sent via MMS (Multimedia electronic messaging Service) to a connected party as a part of the personnel within the workplace.

The initial stage in style is to analyse the instrumentality needed twenty four for the detection of fingerprint GPS-based with Arduino, that is making ready the hardware and software package. the necessities analyse during this analysis are: • Controller victimization Node MCU• Communication victimization A6 SMS Module • show indicator with TFT digital display • Voice indicator victimization MP3 DF Player Module • NeoBlox 7M GPS module because the location coordinate receiver • Fingerprint Module ZFM-20 for attending input • RTC module as period of time input • 4x4 keyboard module as input generally, one {the style|the planning|the look} of the system embrace the planning of hardware and software package design, as bestowed at Fig. 1. Node MCU Mega 2560 Finger print module GPS module Power supply RTC Module MP3 Module Speaker digital display SMS Module laptop as a server web good Phone keyboard.

Node MCU mega microcontroller has USB facility because the communication line between PC/Notebook device with a microcontroller and ADC pin. Node MCU Mega microcontroller uses C artificial language as its artificial language. Programming software package victimization Node MCU software package v1.0.6. Hardware associate degreed software package Node MCU that use during this analysis is an ASCII text file sort. The fingerprint module is that the most vital part during this analysis, because it is employed because the system's main input in addition as a security tool as associate degree entrance to access the full system. The GPS operate is to discover the placement so the information is shipped to Node MCU. GPS uses UART communication lines victimization Texas and Rx pins. Since the Texas Rx Node MCU pin is already used on GSM module system, GPS uses serial software package that's on pin D10 (Rx) and D11 (Tx) then for voltage taken from 5V Node MCUand for GPS ground pin connected with Node MCU ground pin.



III WORKING



At the primary once system starts it'll connect with the Wi-Fi and therefore the credentials for that's per the program then it'll connect with the blynk server then check for the fingerprint device if any case failing then it'll stops execution at several block once all goes well it'll run the void loop the code is fourteen in such the simplest way that the default fingerprint device is organized to visualize whether or not the putted finger will vote or not it'll check information permit|and permit} user to vote if the fingerprint knowledge is on the market in option list if not then it won't allow user to vote. we've got additional 3 buttons for adding new fingerprint, for going back and clearing knowledge from information and device. the information are hold on in encrypted kind and deleting can delete all the saved fingers in device in addition as in information.

Node MCU: - NodeMCU is AN ASCII text file LUA primarily based computer code developed for ESP8266 Wi-Fi chip. four By exploring practicality with ESP8266 chip, NodeMCU computer code comes with ESP8266 Development board/kit i.e., NodeMCU Development board. Since NodeMCU is ASCII text file platform, their hardware style is open for edit/modify/build. NodeMCU Dev Kit/board contains ESP8266 Wi-Fi enabled chip. The ESP8266 may be a affordable Wi-Fi chip developed by Espressif Systems with TCP/IP protocol. For a lot of info regarding ESP8266, you'll be able to refer ESP8266 Wi-Fi Module.There is Version2 (V2) on the market for NodeMCU Dev Kit i.e., NodeMCU Development Board v1.0 (Version2), that sometimes comes in black coloured PCB.

Fingerprint/Bio Metric Sensor: - twenty Secure your project with bioscience - this all-in-one optical fingerprint device can create adding fingerprint detection and verification super easy. nineteen These modules area unit usually employed in safes - there is a high-powered DSP chip that will the image rendering, calculation, feature-finding and looking out. nine connect with any microcontroller or system with TTL serial, and send packets of information to require photos, observe prints, hash and search. you'll be able to additionally recruit new fingers directly - up to 162 finger prints are often hold on within the aboard non-volatile storage.

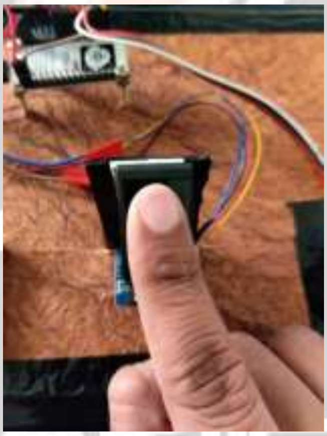
Blynk 3th party server: - Blynk is seventeen a full suite of package needed to image, deploy, and remotely manage connected electronic devices at any scale: from personal IoT comes to a lot of business connected product.

Push Buttons (3): - Biometric sensors area unit wont to collect measurable biological characteristics (biometric signals) from a person's being, one which might then be employed in conjunction with biometric recognition algorithms to perform machine-controlled person identification. three to live any form of biometric signal, a biometric device is needed. This device could either output the raw signal or in addition convert the raw signal into a group of options that's higher suited to tell apart between signals from separate people. the sort of device used depends on the biometric signal being measured. Some biometric modalities like face and voice solely need easy sensors. for example, to capture a person's voice, a good-quality mike is decent (given that the sound capture happens in a very moderately quiet environment).

OLED show Screen: - a pair of this is often a fast tutorial for our 128x64 and 128x32 component monochrome OLED displays. These displays area unit tiny, solely concerning 1" diagonal, however terribly legible thanks to the high distinction of Associate in Nursing OLED show. every OLED show is formed of 128x64 or 128x32 individual white OLEDs, all is turned on or off by the controller chip. as a result of the show makes its own light-weight, no backlight is needed. This reduces the facility needed to run the OLED and is why the show has such high contrast; we actually like this miniature show for its crispness.

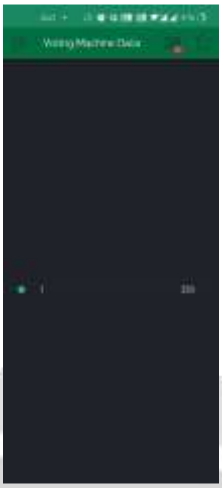
IV. RESULT

Test results of the proposed system are discussed in following figures. When system is started, it tries to look the sample of fingerprint.



When matched sample is identified, it'll validate the message on LCD.

According to the voter's selectivity, the validate message for individual parties is shown in Fig. If user wants to ascertain the statistics of individual party votes, then he/she has got to press upload button. Statistics of individual party's vote on webpage server are shown in Figs. The same voting statistics also are captured on Blynk app as shown in Fig.



V. CONCLUSION

So, when learning our fingerprint-based secured selection mechanism, it safe to mention that, this method has managed to beat most of the issues baby-faced throughout the selection amount by EVM system. ten The potency of the system depends on the programme style and therefore the flexibility that it provides also because the usability for it. This ensures a safer selection methodology that is completely needed for the healthy growth of a developing nation. eleven the projected on-line legal system victimization biometry that's the fingerprint scanner is best and quicker than the previous system. the net legal system employing a fingerprint scanner can offer an opportunity to avoid invalid votes. during this system, solely Associate in Nursing documented and registered person one is going to be ready to vote.

IV. REFERENCES

[1]A. K.Agarwala, D. T. Shahani, and P. V. Indiresan. Report of the expert committee for evaluation of the upgraded electronic voting machine (EVM). Sept. 2006.

[2] Khasawneh, M., Malkawi, M., & Al-Jarrah, O. (2008). A Biometric-Secure e-Voting System for Election Process. Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08). Amman, Jordan.

[3] Prasad, H. K., Halderman, A. J., & Gonggrijp, R. (Oct. 2010). Security Analysis of India’s Electronic Voting Machines. Proc. 17th ACM Conference on Computer and Communications Security (CCS’10).

[4] UIDAI. (2012). Role of Biometric Technology in Aadhaar Authentication.

[5] Yinyeh, M. O., & Gbolagade, K. A. (2013). Overview of Biometric Electronic Voting System in Ghana. International Journal of Advanced Research in Computer Science and Software Engineering

[6] TahaKh. Ahmed and Mohamed Aborizka (2011), ―Secure Biometric E-Voting Scheme‖, ICICIS 2011, Part I, CCIS 134, pp. 380–388, 2011. © Springer-Verlag Berlin Heidelberg 2011

[7] Raja Lakshmi, Meenakshi Nivya and KS Selvanayaki, “Student online voting system” International Journal of trend in research and development Volume 2(5),[ISSN2394-9333], Page no[438-440]

[8] Neha Gandhi, “Study on security of online voting system using biometric and stenography” International journal of computer science and communication, Volume 5, [ISSN-0973-7391] Page No. [29-32]

[9] Rahul V. Awathankar, Monika A Wadhai, Suraj Sawant, “I- Voting: A System For Every Citizen of India” International Journal of Control Theory and Application, Volume 10, [ISSN-0974-5572] Pageno.[125-130]

[10] Annisara Nadaph, Rakhi Bondre, Asmita Katiyar, Durgesh Goswami, “An Implementation Secure Online Voting System” International Journal of Engineering Research and General Science, Volume 3, Issue 2, [ISSN-2091-2730] Page no. [1110-1118].