International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

BIOMETRIC VOTING USING BLOCK CHAIN

K.Sanjai[1],,S. Sakthi [2],K. Sajith[3], Mrs.V. Hema Supervisor [4]

Department of ECE Muthayammal, Engineering College, Namakkal, Tamil Nadu, India
sanjaikumaresan.ks@gmail.com, [2]sakthisr40@gmail.com, [3]sajith6111@gmail.com

Abstract –

Usually, voting is done by casting their vote in the polling booth. As technology increases, the nowadays electronic voting machine is used for casting votes. This paper is about an IoT-based voting machine with fingerprint authentication. The main aim of this project is to make voting secure using fingerprint authentication and also to reduce malpractices. The details of the voter along with their fingerprint are stored in the database. If the fingerprint matches with the stored fingerprint, the system checks the radar number of the user and if authenticated, itchecks if multiple votes have been cast. If the fingerprint matching is not correct "Matching failed" message will be displayed and if the Aadhar number is not correct, then the "Aadhar not match" message will be displayed. A voter can enter his/her native place and vote for the corresponding candidate using thing speak and the result can be obtained using the same. The Arduino Uno is the controller used in this voting machine. A fingerprint is used to authenticate the user. There is at least a little difference between the fingerprints of each person. When malpractice occurs, an "Already voted" message will be displayed. The Arduino IDE is used for programming the board and the cloud is used to display ballot cards and to store the result. The system provides an alert on malpractice and only an authorized voter can cast the vote.

INTRODUCTION

The Virtual Circuit is a pattern-matching circuit that can be implemented on a customized memory circuit. By exploiting the massive parallel processing latent in memory circuits, the VC algorithm has a complexity. i.e. In addition, its latest version based on a novel design using NAND Flash memory structure referred to as enhanced VC is highly energy efficient. For example, it is found that for content-based search at the same search throughput, EVC has the potential to deliver 100– 1000 times in energy saving on difficult databases. In this brief, we investigate the feasibility of implementing a k-NN classifier on a VC circuit and its performance in terms of classification accuracy and complexity. Electronic voting has been an active research topic with many advantages over traditional voting but poses its unique challenges. Other voting requirements, such as verifiability and receipt- freeness, make the problem even more challenging due to their inherently contradicting nature In our proposed GSM mobile voting scheme, communication between the mobile equipment and the Global System for Mobile Communication**s**(GSM) network uses standard GSM. Hence GSM security features apply. Among these, the subscriber identity authentication feature is particularly used in the protocol.The ME computes a response SRES from RAND as well. Then the value SRES computed by the ME is signaled to the visited network, where it is compared with the value SRES computed by the Alternative Current(AC). The access of the voter will be accepted or denied depending upon the result of comparing the two values. If the two values of SRES are the same, the mobile subscriber has been protected, and the connection is allowed to proceed. As modern communications and the Internet, today are almost accessible electronically, computer technology users bring the increasing need for electronic services and their security. Usages of new technology in the voting process improve the elections naturally.

LITERATURE SURVEY

E-voting techniques and systems have not beenaccepted and deployed by society due to variousconcerns and problems. One particular issue associated with many existing electronic-voting techniques is the lack of transparency, leading to the failure to deliver voter assurance. In this work, we propose an assumable, transparent, and mutual restraining electronic-voting protocol that exploits the existing two-party political dynamics in the US. The proposed electronic-voting protocol consists of three original technical contribution universal verifiable voting vector, forward and backward mutual lock voting, and in-process check , in combination, resolves the apparent conflicts in voting such asanonymity vs. accountability and privacy vs. verifiability. Especially, the trust is split equally among tallying authorities who have conflicting interests and will technically restrain each other in process, which allow any voter to verify that individual vote is indeed counted and also allow any third party to audit the tally. A robust, assumable,transparent, and mutual restraining electronic- voting a protocol that exploits conflicts of interest in multiple tallying authorities, such as the two-party political system in the US. The new protocol consists of a few novels technique universal verifiable voting vector, forward and backward mutual lock voting, and enforcement – that, in combination, resolves the apparent conflicts such as anonymity vs.accountability and privacy vs.verifiability.

IMPLEMENTATION DETAILS

EXISTING SYSTEM

Voting is a important part of the democratic process. As such, the efficiency, reliability, and security The Technologies involved are critical. Traditional voting technologies include hand-counted paper ballots. These paper-based systems can result in several problems,including stolen, or miscounted ballots,unacceptable percentages of lost Vote lostthrough invalid ballot marks, limited accommodations for people with disabilities. As the modern communication and Internet technology, today are almost accessible electronic technology, the computer technology users, brings the increasing need for electronic services and their security. Usage of current technology in the voting process improve the elections.

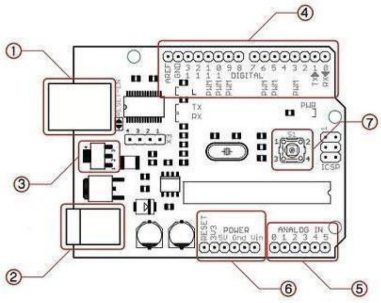
PROPOSED SYSTEM

In this system, we are using fingerprint as the biometric method of authentication and its online version. The voter's fingerprint and aadhar number are enrolled and stored in a database. During the process of voting the voting machine ask for the aadhar number if it matches with the saved aadhar number, it checks whether the fingerprint matches with the aadhar. If the fingerprint matches, then the system checks whether that person has already voted, for the same election. If the voter has not voted then "Fingerprint and aadhar number matches. Cast vote" message be displayed. After voting, the register will be incremented. If that person has voted before, then the "already voted" message is displayed along with abuzzer sound.

I. Hardware components:

1. Arduino

Arduino is an open source tool for creating programs that are far superior to desktop computers. The physical world can be sensed and controlled by sensors programmed using Arduino programming. It can be powered by a USB cable or an external 9 volt battery, but accepts a voltage of 7 to 20 volts. This open-source computing platform is based on a simple micro-controller board, and a development environment for implementing software on the board

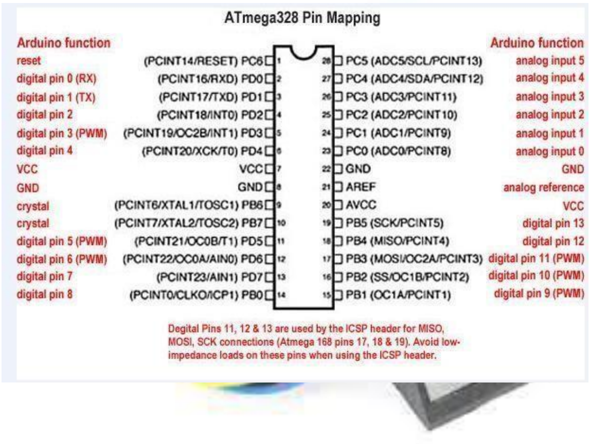


The most important parts on the Arduino board high lighted in red:

1: USB connector
2: Power connector
3: Automatic power switch
4: Digital pins
5: Analog pins
6: Power pins
7: Reset switch

ARDUINO UNO R3 MICROCONTROLLER

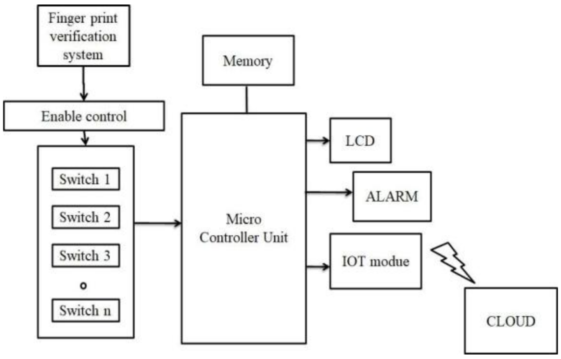
2. Finger print



ATmega328 Pin Mapping

Arduino function		Pin	Pin		Arduino function
reset	(PCINT14/RESET) PC6	1	28	PC5 (ADC5/SCL/PCINT13)	analog input 5
digital pin 0 (RX)	(PCINT16/RXD) PD0	2	27	PC4 (ADC4/SDA/PCINT12)	analog input 4
digital pin 1 (TX)	(PCINT17/TXD) PD1	3	26	PC3 (ADC3/PCINT11)	analog input 3
digital pin 2	(PCINT18/INT0) PD2	4	25	PC2 (ADC2/PCINT10)	analog input 2
digital pin 3 (PWM)	(PCINT19/OC2B/INT1) PD3	5	24	PC1 (ADC1/PCINT9)	analog input 1
digital pin 4	(PCINT20/XCK/T0) PD4	6	23	PC0 (ADC0/PCINT8)	analog input 0
VCC	VCC	7	22	GND	GND
GND	GND	8	21	AREF	analog reference
crystal	(PCINT6/XTAL1/TOSC1) PB6	9	20	AVCC	VCC
crystal	(PCINT7/XTAL2/TOSC2) PB7	10	19	PB5 (SCK/PCINT5)	digital pin 13
digital pin 5 (PWM)	(PCINT21/OC0B/T1) PD5	11	18	PB4 (MISO/PCINT4)	digital pin 12
digital pin 6 (PWM)	(PCINT22/OC0A/AIN0) PD6	12	17	PB3 (MOSI/OC2A/PCINT3)	digital pin 11 (PWM)
digital pin 7	(PCINT23/AIN1) PD7	13	16	PB2 (SS/OC1B/PCINT2)	digital pin 10 (PWM)
digital pin 8	(PCINT0/CLKO/ICP1) PB0	14	15	PB1 (OC1A/PCINT1)	digital pin 9 (PWM)

Degital Pins 11, 12 & 13 are used by the ICSP header for MISO, MOSI, SCK connections (Atmega 168 pins 17, 18 & 19). Avoid low-impedance loads on these pins when using the ICSP header.



the impressions from the pad on the last joint of fingers and thumbs and also fingerprint cards record portions of lower joint of the fingers.

II. Software Components

1. Proteus

The Proteus Design Suite is a proprietary software tool suite primarily used for electronic design automation. This software is primarily used by electrical device designers and engineers to create schematics and electronic prints for PCB manufacturing. The micro- controller simulation in Proteus works via way of means of making use of both a hex record or a debug record to the microcontroller component at the schematic. It is then co-simulated at the side of any analog and virtual electronics related to it.

CONCLUSION

E-voting systems have many advantages over the traditional way of voting. Some of these advantages are lower cost, faster calculation of results, improved accessibility, greater accuracy, and lower risk of human and mechanical problems. We tried our level best to introduce a new voting system that will be transparent, faster, and accurate and will ensure a single vote for a single person. Our proposed system has successfully covered all these problems. Moreover, this system will provide boundary-less biometric voting.finger. In forensic science, they mostly used the recovery of fingerprints from a crime scene is an important method. Deliberate impressions of whole fingerprints can be obtained by ink or any other substances transferred from the ridges on the skin to asmooth surface such as paper, etc. Fingerprint records

REFERENCE

[1].Tai-Pang , , Sai-Kit, Yeung,Jiaya, Chi-KeungTang, Closed-Form Solution To Tensor BiometricVoting:Theory And Transactions On Pattern Analysis And Machine Intelligence, Vol. 34,No. 8, August 2012

[2].Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman Attackingthe Washington, D.C. Internet Voting System In Proc. 16th Conference on Financial Cryptography & Data Security, Feb. 2012

[3]. P. George Saleem S Tevaramani Comparison Of Face Recognition Using Transform Domain Techniques World Of CS And Information Technology Journal ISSN: 2221-0741 Vol. 2, No. 3, 82-89, 2012

[4].D. Ashok Kumar, T. UmmalSariba Begum A Novel design of Biometric Voting System Using Fingerprint Journal Of Innovative Technology & Creative Engineering (Issn: 2045-8711) Vol.1 No.1 January2011

[6].KashifHussainMemon, Dileep Kumar and Syed Muhammad Usman,Next Generation A Secure E-Voting System Based On Fingerprint Method 2011 (2011)

[7].ShivendraKatiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi SteganographyInternational Conference On EmergingApplications Of Information Technology 2011

[8]. KalaichelviVisvalingam, R. M. ChandrasekaranSecured Electronic Voting Protocol Using Authentication Advances In InternetOf Things, 2011

[9].Feras A. Haziemeh, mutazKh. Khazaaleh, Khairall M. Al-Talafha New Applied E Voting System Journal Of Theoretical And Applied Information 31st March 201148

[10].Hari K. Prasad_ J. Alex HaldermanyRopGonggrijp Scott Wolchoky Eric WustrowyArunKankipati_ Sai Krishna Sakhamuri_VasavyaYagati_ _Netindia,