www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 08, August 2023, pp : 1-5

e-ISSN : 2583-1062

Impact Factor : 5.725

ELECTRONIC VOTING SYSTEM WITH BIOMETRIC AND GSM FEATURE

Sriramsubash. G[1], Shankara Narayanan. M[2], Maha Rajan. S[3],

Dr. K. J. Prasanna Venkatesan[4]

[1,2,3]Bachelor Of Engineering, Department Of ECE, National Engineering College, Kovilpatti, (India)

[4]Professor, Department of ECE, National Engineering College, Kovilpatti, (India)

ABSTRACT

In the democratic nation of India, the voting process has had a significant impact on elections. The legitimacy that comes from having citizens choose their own representatives is the heart of any social equality. For a fair election system and to reduce the number of staff needed, electronic voting machines (EVMs) were deployed. Because of their vulnerability to hacking and electoral fraud, these computerized voting devices present significant challenges to holding a fair election. However, the two key weaknesses in the current voting mechanism are the potential for memory chip manipulation and double voting. So, in order to ensure election fairness, The traditional voting methods must be upgraded with an open authentication module, security, and dependability. This work has established fingerprint authentication for the voter based on stored data, enabling very precise identification of people and increasing election transparency.

keywords—Finger print sensor module, GSM, Arduino, Voting Machine

1. INTRODUCTION

The words “biometrics” and “metrics,” which both indicate measuring in Greek, are the origins of the phrase. Biometric technology uses a person’s unique physiological or behavioral characteristics to identify them. The face, fingerprint, hand vein, hand geometry, iris, voice, and retinal prints are the nine main biometric techniques that are regularly used. These methods rely on personal data that is constant during an individual’s lifespan. Because of their distinctiveness, stability, permanence, and simplicity of collection, fingerprints are quickly becoming the most widely used biometric technology. A fingerprint is an imprint made by the friction ridges of a finger. Ridge, valley, and minutiae make up the majority of a fingerprint. A fingerprint’s ridge is a single curved section. A valley is a void between two nearby peaks. Minute variations in ridge patterns are referred to as minutiae. An identity method based on fingerprintrecognition is employed. Fingerprinting is considered to be the most accurate and quick biometric identification method. They are safe to use, unique to each person, and they do not change throughout a lifetime. Even though fingerprint identification technology has improved, it still takes time to match a given person’s fingerprint to a database of registered fingerprints. In order to use large databases, it was our responsibility to improve fingerprint identification technology. The suggested fingerprint-based attendance system would be suitable for implementation in institutions for identification purposes as well as by enterprises to track employee attendance. Biometrics technology can solve these concerns. The proposed system was created utilizing an optical fingerprint acquisition module and an Arduino UNO.

2. LITERATURE SURVEY

A. Design of Secured E-Voting System Using Biometric

Biometrics is a method for obtaining admittance for personal identification by employing competing, non-transferable bodily traits, such as fingerprints. Since the creation of the competing technology, it has been utilized in authentication and security systems. Nowadays, there are three major types of authentications used in the security field. Anything we are aware of, such as a password, PIN, or piece of personal information, is something we possess. A person is a thing we are. The use of biometric-based computer networks and internet access is a very new and hardly used technology. This study discusses the usability of biometrics in a real-world application like electronic voting (e-voting) that uses a physical entity (voice recognition, fingerprints) and a computer network.

B. Smart Voting System Using Facial Recognition

Facial recognition verification for online voting systems is a novel authentication technology that is discussed. In order to increase the safety and usability of the election process, it plans to develop a computerized voting system.. Due to the need to travel to certain sites, such as polling cubicles, and wait in a long line to cast their ballot, the majority of individuals choose not to vote. Voters that are ineligible may also cast votes in a fraudulent manner, which can lead to a variety of issues. Because of this, we have suggested a voting mechanism in this project that is quite useful and effective. This technique can reduce the amount of money the government spends

on elections. In general, this project is being created to assist the electoral commission of India's workforce and to minimize human effort.

C. Electronic voting machine (EVM) using fingerprint sensor

We employ fingerprint scanners in the electronic voting system to verify votes. Electronic voting systems based on fingerprints have several benefits, including the fact that voters don't need to carry ID cards or go through a laborious registration process. Data is sent to the controlling unit of verification when a finger is put on the fingerprint sensor. The controller retrieves data from the storage device, compares it to recent user data, and returns the results. If the fingerprint matched with one already saved, the user was allowed to cast a vote. The voting process is made as simple as following the instructions that are given on the LCD; this approach helps to reduce voting system corruption.

3. HARDWARE DESCRIPTION

A. ARDUINO MICROCONTROLLER:

The core elements of a computer's central processing unit (CPU) are found on an integrated circuit (IC) called a microprocessor. It is a clock-driven, register-based, multipurpose silicon device that can be programmed. It accepts binary data as input and processes it in line with memory-stored instructions. Microcontrollers are silicon chips with an integrated CPU, memory, and I/O. Microprocessors are silicon chips that feature ALU, register circuits, and control circuits. . Due to advances in integrated circuit technology, low-cost microprocessors are readily available. It will make computer systems less expensive. High- Speed The technology used in microprocessor chips allows them to operate at very fast rates. Millions of commands can be carried out by it every second. Little Size extremely large scale and ultra-large scale integration technology allows for the production of microprocessors with an extremely small physical footprint. This will reduce the overall size of the computer system. Power Usage is Low Typically, metal oxide semiconductor technology is used to create microcontrollers, and MOSFETs (Metal Oxide Semiconductor Field Effect Transistors) operate in the saturation and cut-offmodes. Hence, in comparison to others, power usage is relatively low. Reduced Heat Production Semiconductor devices won't produce as much heat as vacuum tube devices.

B. Matrix Keypad

Microcontrollers process user input from a matrix keypad, a small, portable input device. This is present in many everyday items, including calculators, digital locks, gas pumps, and do-it-yourself projects. Membrane keypads are one of the varieties; they are smaller and can be pasted on top of your creative ideas. For microcontroller applications, this compact 16-button keypad serves as a valuable human interface component. The keypad's useful adhesive backing makes it simple to place the keypad in a variety of situations. BlocklyProp projects and blocks, a C library, and a tutorial are all well- supported for usage with the Propeller microprocessor. The advantage of using a matrix keypad is that it enables the programmer to utilize fewer pins overall. In a 44-matrix keypad, 16 push button switches are connected to four rows and four columns.

C. GSM MODEM SIM900

The GSM modem is a specific sort of device that utilises the subscriber's mobile number to operate as a cell phone over a network and accepts a SIM card. The modem Sim300 utilises the EGSM900MHz, DCS1800MHz, and PCS1900MHz frequencies and is a tri- band GSM/GPRS device. The GSM modem may function at voltages ranging from -3 to -15 volts for logic high and +3 to +15 volts for logic low as it is an RS232-logic level compliant device. In order to convert TTL into RS232, a MAX232 logic level converter is used between the microcontroller and the GSM board. The microcontroller signal is sent to the GSM modem via pin 11 of the max232. On pin 2 of the GSM modem, the microcontroller's signal was picked up. The microcontroller receives the signals from pin 3 of the GSM modem via MAX232.

D. FINGERPRINT MODULE (R305)

It has a fingerprint sensor and a TTL UART interface. The user can set up the module in 1:1 or 1: N mode while recognising a person and keep the fingerprint data there. A 3V3 or 5V microcontroller can directly connect with the fingerprint module. The PC interface requires a level converter (like MAX232). This fingerprint sensor module makes it simple to add fingerprint detection and verification. These modules, which are typically found in safes, use a potent DSP chip to generate images, carry out calculations, find features, and carry out searches. To capture images, find prints, hash data, and do searches, send data packets using TTL serial to any microcontroller or system. You can also enlist new fingers right away. The on-board flash memory has a maximum capacity of 162 fingerprints. When taking a picture, a red LED in the lens illuminates, letting you know it is functioning.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 08, August 2023, pp : 1-5

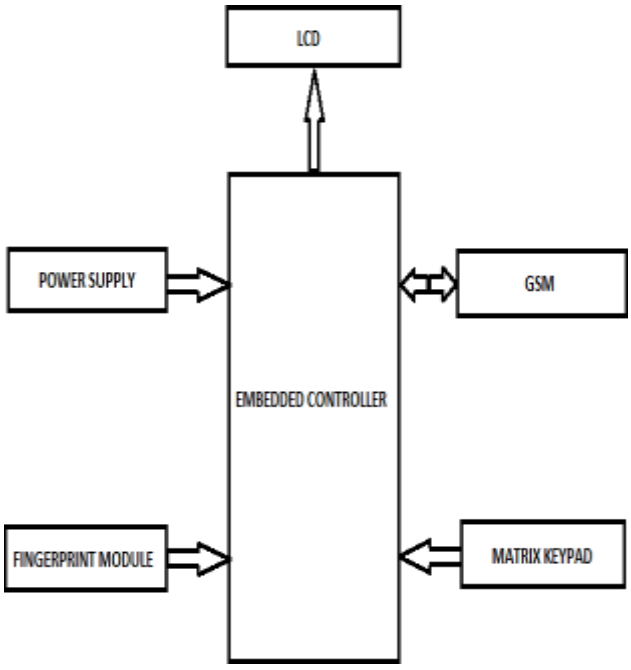
E. Arduino Nano

An ATmega328P or ATmega628 microprocessor serves as the basis of the Nano, a small Arduino board. The connection is identical on the Arduino UNO board. A nano board is a microcontroller board that is sustainable, small, trustworthy, and versatile. It is small compared to the UNO board. The Arduino Mini is set up using the Arduino (IDE), which is accessible across a number of platforms. This phrase alludes to an integrated development environment. The operating voltage for the Nano board spans from 5V to 12V. Nano has 22 input/output pins in all. There are 8 analogue pins and 14 digital pins. The 14 digital pins include 6 PWM (Pulse Width Modulation) pins. The Arduino Nano's 6 PWM pins are used to translate digital signals into analogue impulses. The conversion is carried out by adjusting the pulse's width. The Arduino Nano's crystaloscillator operates at a 16MHz frequency. Many applications, including robotics, control systems, instrumentation, automation, and embedded systems, employ the Arduino Mini.

F. LCD – Liquid Crystal Display

Liquid crystal displays (LCDs) use materials that combine the properties of liquids and crystals. These materials don't have melting points; instead, they have a temperature range where the molecules are almost as mobile as they would be in a liquid yet are structured in a crystal-like pattern. An LCD consists of a liquid crystal material placed between two glass panels. On the inside surface of the glass plates are transparent electrodes that specify the characters, symbols, or patterns that will be displayed. Because of the presence of polymeric layers between the electrodes and the liquid crystal, the orientation angle of the liquid crystal molecules is preserved. One polarizer is adhered to each of the two glass panels' exteriors. The light rays travelling through them would be rotated to a specific angle and in a specific direction by this polarizer. When the LCD is turned off, the two polarizers and the liquid crystal rotate the light rays so that they exit the LCD with no orientation, giving the LCD its translucent appearance. If the electrodes received enough voltage, the liquid crystal molecules would align in a specific orientation. The required characters would be activated or highlighted as a result of the polarizer rotating the light beams as they moved through the LCD.

4. BLOCK DIAGRAM



5. DESIGN AND IMPLEMENTATION

The biometric voting system that uses fingerprints is separated into two sections: the first section is for registration, and the second section is for casting votes for the candidates of your choice. Every voter or user must register in the system using a push button or key. During this procedure, the user must press the ENROLL key. After that, the LCD will prompt them to enter the location ID of the Arduino memory region where their finger will be stored. Use the UP/DOWN keys to enter your ID. The OK key is offered for ID choosing. The finger must be placed over the fingerprint module, it will ask. For correct identification, the LCD will request that you remove your fingerprint from the fingerprint module and then place it there once more. The fingerprint module takes an image during this process, formats it appropriately, and stores it with the designated ID in the memory. Once that a voter has registered with the system, he or she may vote for their preferred candidate. In a similar vein, every user must register. All of these

specifics pertain to a single system, and the data for that system will only be stored there; there is no interconnection between the two systems. To prevent hacking, all the systems are segregated from one another. The voting procedure is broken down into a few easy steps. After pressing the match key, the Display will prompt the user to place their finger over the fingerprint sensor in order to cast their vote. At that point, Arduino will store the user ID. The user can now vote, but to do so, they must once more place their finger over the fingerprint scanner while the scanner captures their finger's image and looks up their unique ID in the system. The authorised voter will be shown on the LCD if finger ID is recognised. It indicates that the user is a valid voter and that the voting process will proceed to the next stage. Voters can now select a key to vote for their preferred candidate. Every time a voter casts a ballot, their registered mobile number receives an alert message for the

candidate and an OTP on their phone. The suggested voting system based on Arduino is trustworthy in terms of security, dependability, fairness, and election transparency.

6. HARDWARE SETUP

OUTPUT

Fig. 1 Found Match (vote will be accepted)

Fig. 2 Not Found (Vote will not be accepted)

7. CONCLUSION

This project explored EVM (Electronic Voting Machine) introduction and variations, EVM issues, taxonomy, and biometric based EVM. Our efforts to comprehend electronic voting methods have left us hopeful but anxious. This project proposes that the EVM system be further researched and invented in order to reach all levels of the community, so that voter confidence increases and election authorities get more involved in acquiring the innovated EVM's for conducting seamless, secure, tamper-resistant elections.

8. RFERENCES

[1] W. Lu, A. L. Varna, and M. Wu, "Confidentiality-preserving image search: Acomparative study between homomorphic encryption and distance-preservingrandomization," IEEE Access, vol. 2, pp. 125–141, 2014.

[2] A. Ara, M. Al-Rodhaan, Y. Tian, and A. Al-Dhelaan, "A secure privacy preserving data aggregation scheme based on bilinear elgamal cryptosystem for remote health monitoring systems," IEEE Access, vol. 5, pp. 12 601–12 617, 2017.

[3] L. Chen, M. Lim, and Z. Fan, "A public key compression scheme for fully homomorphic encryption based on quadratic parameters with correction," IEEE Access, vol. 5, pp. 17 692–17 700, 2017.

[4] Z. Li, C. Ma, and D. Wang, "Towards multi-hop homomorphic identity-based proxy re-encryption via branching program," IEEE Access, vol. 5, pp. 16 214–16228, 2017.

[5] X. Yi, R. Paulet, and E. Bertino, Homomorphic Encryption and Applications. New York: Springer, 2014.

[6] C. Esposito, A. Castiglione, B. Martini, and K.-K. R. Choo, "Cloud manufacturing: Security, privacy, and forensic concerns," IEEE Cloud Computing, vol. 3, pp. 16–22, 2016.

[7] O. Hasan, L. Brunie, and E. Bertino, "Preserving privacy of feedback providers in decentralized reputation systems," Computers & Security, vol. 31, pp. 816– 826, 2012.

[8] V. Kiruthika Priya, V. Vimaladevi, B. Pandimeenal, T. Dhivya, "Arduino based smart electronic voting machine", 2017 International Conference on Trends in Electronics and Informatics (ICEI) Year: 2017, conference Paper, Publisher: IEEE.

[9] Rahil Rezwan, Huzaifa Ahmed, M. R. N. Biplo, S. M. Shuvo, Md. Abdur Rahman, "Biometrically secured electronic voting machine", 2017 IEEE Region 10 Humanitarian Technology Conference (R10- HTC).

[10] Prof. Sunita Patil, Amish Bansal, Utkarsha Raina, Vaibhavi Pujari, Raushan Kumar, "E-Smart Voting Machine with Secure Data Identification Using Cryptography", 2018 Publisher: IEEE.

[11] Annalisa Franco, "Fingerprint: Technologies and Algorithms for Biometrics Applications", Year: 2011, Course Publisher: IEEE.

[12] Soumyajit Chakraborty, Siddhartha Mukherjee, Bhaswati Sadhukhan, KaziTanviYasmin, "Biometric Voting System using Adhar Card in India" 2016.