IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

Two Level Authentication for E-Voting System Using IoT Technology

Swarnalatha M[1], Pooja Dharshini G[2], Castin Keerthana B[3], Hari Dharshini K S[4],Yazhini M[5], Sriman. S[6]
Assistant Professor[1] and Students[2,3,4,5,6]
Karpaga Vinayaga College of Engineering & Technology, Chengalpattu, India

Abstract: *Voting is a citizen's most fundamental right and one of his or her most significant obligations. The votes we cast determine the country's destiny, and we must vote honestly and without succumbing to any pressure, since, as the saying goes, "with power comes tremendous responsibility." We must guarantee that our votes are not tampered with after they have been cast. As a result, the existing voting method (EVM) is simple to manipulate, i.e., there is a lot of human interaction, which might jeo pardise election outcomes. As a result, in this project, we will attempt to address this vulnerability by implementing a two-step verification system that will help avoid the middle man attack, namely, only when the voter is physically present can the voter's fingerprint be registered, and only then will the OTP be sent to the user's mobile number.*

Keywords: Arduino UNO, Keypad, RFID Reader, RFID Tag, GSM, Finger Print Sensor

I. INTRODUCTION

Voting is the most basic right of every citizen and is one of the most important responsibilities of every citizen.The votes which we cast decide the future of our country, and we must vote honestly and not succumb to any sort of pressure as the phrase goes **"With great power comes great responsibility"**.

Now once our votes are cast, we should ensure they are not manipulated in any way. The current voting system (EVM) is easy to manipulate i.e., there is a lot of human intervention which in turn could compromise the results of the elections, hence in this project we will try to solve this problem by introducing a **two-step verification which will help avoid the middle man attack** i.e. only when the voter is physically present, the fingerprint of the voter can be registered and only then the OTP will be sent to user's mobile number this in turn prevents fake voters.

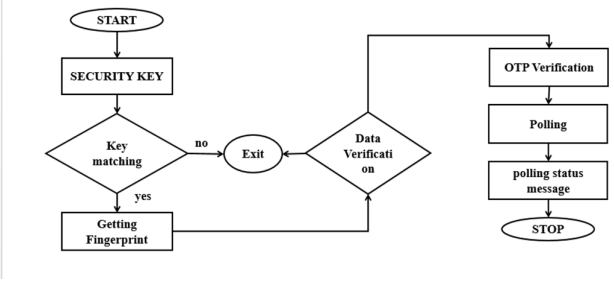


Figure 1.1: Work Flow Diagram

The administrator would have access to the system with a password. Following OTP verification, the individual can vote and receive a confirmation message from the person to whom he voted. The device will count votes for each voter in the same way that present electronic voting machines do. After the polling, the administrator would be able to examine the results as a message. Both voter identification and vote counting would be done in real time with great precision. Our system is fully offline, with just the administrator and voter having access. As a result, hacking the data would be extremely difficult.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

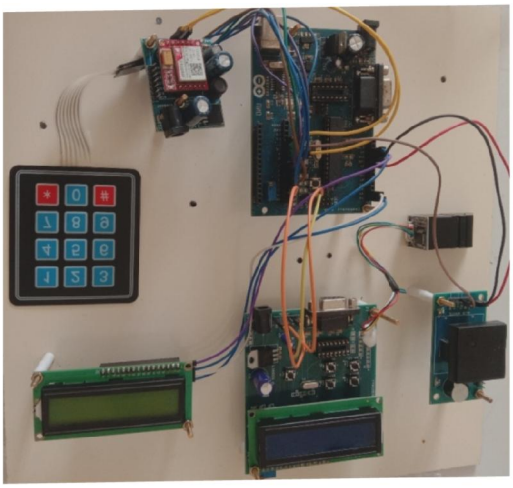


Figure 1.2: Technology setup

II. HARDWARE REQUIREMENT

The Arduino Uno is a microcontroller board grounded on the ATmega328 (datasheet). It comprises of 14 digital input/output pins (out of which 6 can be utilized as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a facilitation for USB connectivity, a power jack, an ICSP header, and a reset button. Its designs comprises of assistances that supports the microcontroller in every possible way.In order to get to work with it one has to simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery. It is accessible in two different versions namely Arduino Uno and Genuino Uno which could be The variations is observed with reference to the region.

Figure 2.1: Ardunio Uno

Radio frequency identification (RFID) has been used in a number of practical applications, such as improving supply chain management, tracking household pets, accessing office buildings, and speeding up toll collection on roadways. RFID is used to automatically identify people, objects, and animals using short range radio technology to communicate digital information between a stationary location (reader) and a movable object (tag). RFID technology can be used to track products in a manner similar to using bar codes for product identification, but RFID also carries additional benefits. RFID does not require line of sight to read the tag, has a longer read range than bar code reader, and tags can store more data than bar codes. Readers can simultaneously communicate with multiple tags. Like other information systems, RFID systems are vulnerable to attack and can be compromised at various stages of their use. Attacks against an RFID system can be categorized generally into four major groups: attacks on authenticity, attacks on integrity, RFID Technology, Security Vulnerabilities, and Countermeasures 365 attacks on confidentiality, and attacks on availability. Besides being vulnerable to common attacks such as eavesdropping, man-in-the-middle, and denial of service, RFID technology is, in particular, susceptible to spoofing and power attacks. This section illustrates different kinds of attacks and provides countermeasures against these attacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

Figure 2.2: RFID Reader EM-18

This is a finger print sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person. The FP module can directly interface with 3v3 or 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC serial port. Optical biometric fingerprint reader with great features and can be embedded into a variety of end products, such as: access control, attendance, safety deposit box, car door locks.

Fig 2.3: Fingerprint Sensor

The GSM shield by Arduino is used to send/ receive messages and make/receive calls just like a mobile phone by using a SIM card by a network provider. We can do this by plugging the GSM shield into the Arduino board and then plugging in a SIM card from an operator that offers GPRS coverage. The shield employs the use of a radio modem by SIMComm. We can communicate easily with the shield using the **AT** commands. The **GSM library** contains many methods of communication with the shield. This GSM Modem can work with any GSM network operator SIM card just like a mobile phone with its own unique phone number.

Figure 2.4: GSM

This DC 12V 4×3 Matrix 12 keys Membrane Switch Keypad is high-quality soft touch feeling button keypad with 100 million life-stroke lifespans and good resistance to environmental conditions.This DC 12V 4×3 Key Matrix Membrane Switch Keypad is a high-quality product at very low cost for your application needs.This 12-button keypad provides a useful human interface component for microcontroller projects. Convenient adhesive backing provides a simple way to mount the keypad in a variety of applications. The Keypad 4×3 features a total of 12 buttons in Matrix form. This is a membrane keypad with no moving parts. A female 7-pin berg connector is require for interfacing it with your microcontroller circuits.Ultra-thin design & adhesive backing provides easy integration to any project.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

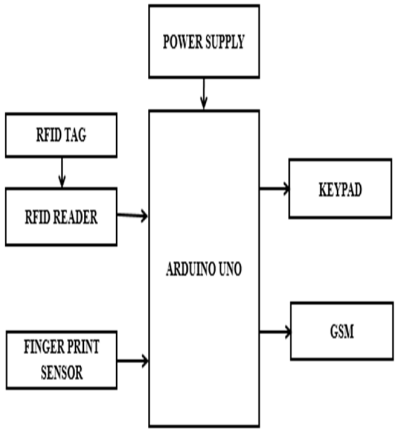
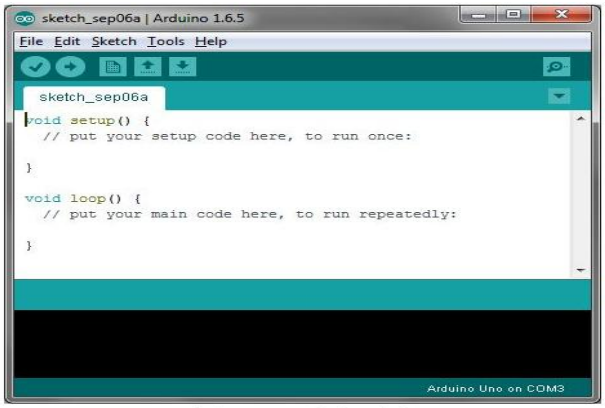


Figure 2.5: Block Diagram

III. SOFTWARE REQUIERMENTS

1. **Arduino IDE**
2. **Embedded C**

This is the Arduino IDE once it's been opened. It opens into a blank sketch where you can start programming immediately. First, we should configure the board and port settings to allow us to upload code. Connect your Arduino board to the PC via the USB cable.ARDUINO IDE: Board Setup.You have to tell the Arduino IDE what board you are uploading to. Select the Tools pulldown menu and go to Board. This list is populated by default with the currently available Arduino Boards that are developed by Arduino. If you are using an Uno or an Uno-Compatible Clone (ex. Funduino, Sain Smart, IEIK, etc.), select Arduino Uno. If you are using another board/clone, select that board.



Arduino IDE Default Window

Figure 3.1: Ardunio IDE Default Window

Embedded C Programming is the soul of the processor functioning inside each and every embedded system we come across in our daily life, such as mobile phone, washing machine, and digital camera.Each processor is associated with an embedded software. The first and foremost thing is the embedded software that decides functioning of the embedded system. Embedded C language is most frequently used to program the microcontroller.Earlier, many embedded applications were developed using assembly level programming. However, they did not provide portability. This disadvantage was overcome by the advent of various high level languages like C, Pascal, and COBOL. However, it was the C language that got extensive acceptance for embedded systems, and it continues to do so. The C code written is more reliable, scalable, and portable; and in fact, much easier to understand.C language was developed by Dennis Ritchie in 1969. It is a collection of one or more functions, and every function is a collection of statements performing a specific

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

task.C language is a middle-level language as it supports high-level applications and low-level applications. Before going into the details of embedded C programming, we should know about RAM memory organization

IV. Conclusion and Future Works

It is a dream of every country to hold a fair election where a common person can register his or her vote to decide the future of the country. This system enables us to secure the voting system in a very fair and unbiased manner, it brings us one more step closer to a fair and secure election, it also would enable real time access and hassle-free election experience for the voters. Due to the merits this system provides the state and central elections can be held on the same day without any hassle. The system can also be installed in any KYC centers where people can access the easily. Future works are:

- We can use a 1mb flash memory finger print module for increasing the capacity.
- External memory can be provided for storing the finger print image, which can be later accessed for comparison.
- Smart Card reader module is supposed to be introduced with theexisting module for further security, and to reduce the database storage.
- Audio output can be introduced to make it user friendly for illiterate voters.
- Retina scanning can also be developed.

References

[1]. 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.

[2]. 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).

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

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

[5]. A. Piratheepan, S. Sasikaran, P. Thanushkanth, S. Tharsika, M. Nathiya, C. Sivakaran, N. Thiruchchelvan and K. Thiruthanigesan, "Fingerprint Voting System Using Arduino", College of Technology Jaffna, Sri Lanka University College.

[6]. R. Murali Prasad, Polaiah Bojja, Madhu Nakirekanti [Murali Prasad 2016] discuss about the user login with the aadhar number and a password. It checks whether that person is eligible for casting vote.

[7]. Ashok Kumar D., Ummal Sariba Begum T., A Novel design of Electronic Voting System Using Fingerprint,International Journal ofInnovative Technology & Creative Engineering (ISSN:2045-8711),Vol.1,No.1. pp: 12 19, January 2011.

[8]. 8.Benjamin B., Bederson, Bongshin Lee., Robert M. Sherman., Paul S., Herrnson, Richard G. Niemi., Electronic Voting System Usability Issues, In Proceedings of the SIGCHI conference on Human factors in computing systems, 2003.

[9]. California Internet Voting Task Force. A Report on the Feasibility of Internet Voting, Jan.2000.

[10]. Chaum D., Secret-ballot receipts: True voter-verifiable elections, IEEE Security and Privacy38-47, 2004.

[11]. Darcy, R., & McAllister, I., Ballot Position Effects, Electoral Studies, 9(1), pp.5-17, 1990.

[12]. Gritzalis D., [Editor]., Secure Electronic Voting, Springer- Verlag, Berlin Germany, 2003.

[13]. D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, R. A Kemmerer, W. Robertson, F. Valeur, and G. Vigna, An Experience in Testing the Security of Real-World Electronic Voting Systems, IEEE Transactions on Software Engineering, vol. 36, no. 4, 2010.

[14]. Mazidi Md.Ali, Mazidi J.G., McKinlay R. D., the 8051 microcontroller & embedded systems, (Pearson Prentice Hall, Delhi, 2006).

[15]. Alam, M.R. ; Univ. Kebangsaan Malaysia ; Masum, M. ; Rahman, M. ;Rahman, A.,Design and implementation of microprocessor based electronic voting system, Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference, 24-27 Dec. 2008.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

[16]. D. Molnar, T. Kohno, N. Sastry, and D. Wagner, Tamper- Evident, History Independent, Subliminal-Free Data Structures on PROM Storage-or-How to Store Ballots on a Voting Machine (Extended Abstract), in Proc. of IEEESymp. Security and Privacy, pp. 365-370, 2006.

[17]. R. Hite, All Levels of Government are needed to Address Electronic Voting System Challenges, Technical report, GAO, 2007.