International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 9, Issue 5, May-2024, http://ijmec.com/, ISSN: 2456-4265

RFID BASED SMART ELECTRONIC VOTING SYSTEM FOR REDUCING ELECTROL FRAUDS

Ms. E. Rajitha [*1], Mr. Mohammed Rahman [*2], Mr. Pathan Altaf Dastagir [*3], Mr. Saad Afzal [*4],
[*1, 2, 3] B. Tech. Student Dept. of ECE, Shadan College of Engineering and Technology
[*4] Assistant Professor, Dept. of ECE, Shadan College of Engineering and Technology
rajithaece2003@gmail.com[*1], mdrahman04042002@gmail.com [*2], altafpathan7887@gmail.com *[3], mohdsaad005@gmail.com[*4]

Abstract : This project describes the design, operation of smart EVM using microcontroller, RFID, GSM technology to improve the election process by avoiding the electoral fraud and to ensure safety, security, reliability, guarantee and transparency and smooth conduct of elections in the country as the voting is of crucial importance in the society where people determine its government. This paper talks about an innovative approach for voting process where the device communicates with the RFID tag which is embed in the voter ID card. When the voter scans his card, the controller checks the ID and if it matches, the vote can be accessed. The voter inserts the password through keypad and if the password is confirmed then the person is allowed to vote and this process is repeated for every person.

Voting is a method for a group, such as a meeting or an electorate, in order to make a collective decision or express an opinion, usually following discussions, debates or election campaigns. Democracies elect holders of high office by voting. Residents of a place represented by an elected official are called "constituents", and those constituents who cast a ballot for their chosen candidate are called "voters". There are different systems for collecting votes.

Key Words: Arduino UNO, RFID Reader, EVM, GSM.

INTRODUCTION

Embedded Systems:

An embedded system is a combination of software and hardware to perform a dedicated task. Some of the main devices used in embedded products are Microprocessors and Microcontrollers. Microprocessors are commonly referred to as general purpose processors as they simply accept the inputs, process it and give the output. In contrast, a microcontroller not only accepts the data as inputs but also manipulates it, interfaces the data with various devices, controls the data and thus finally gives the result.

An embedded system can be defined as a computing device that does a specific focused job. Appliances such as the air-conditioner, VCD player, DVD player, printer, fax machine, mobile phone etc. are examples of embedded systems. Each of these appliances will have a processor and special hardware to meet the specific requirement of the application along with the embedded software that is executed by the processor for meeting that

DOI: https://doi-ds.org/doilink/05.2024-45368588

specific requirement. The embedded software is also called “firm ware”. The desktop/laptop computer is a general purpose computer.

Embedded systems do a very specific task they cannot be programmed to do different things. Embedded systems have very limited resources, particularly the memory. Generally, they do not have secondary storage devices such as the CDROM or the floppy disk. Embedded systems have to work against some deadlines. A specific job has to be completed within a specific time. In some embedded systems, called real-time systems, the deadlines are stringent. Missing a deadline may cause a catastrophe-loss of life or damage to property. Embedded systems are constrained for power. As many embedded systems operate through a battery, the power consumption has to be very low. Some embedded systems have to operate in extreme environmental conditions such as very high temperatures and humidity.

PROJECT INTRODUCTION

AIM:

The main aim of this project is to develop RFID based smart electronic voting system for reducing electrol frauds

Existing Technology

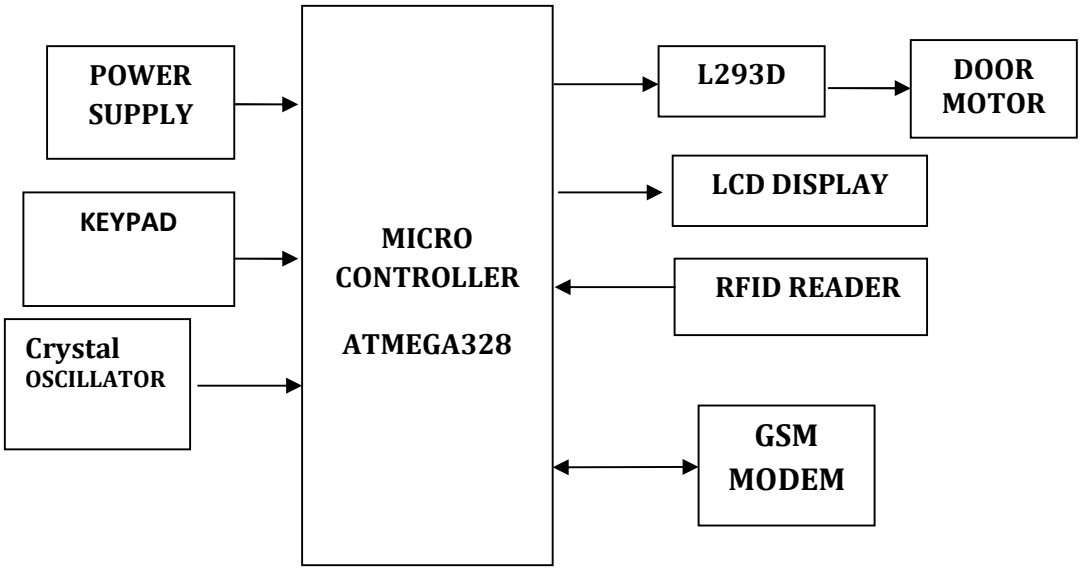
In EVM’s, the existing technology is having some flaws, such as mis-recording of votes leading to unscrupulous officials or 'helpers' to record an elector's vote differently from their intentions. Voters who require assistance to cast their votes are particularly vulnerable to having their votes stolen in this way. This is similar to the misuse of proxy votes; however, in this case, the voter will be under the impression that they have voted with the assistance of the other person, rather than having the other person voting on their behalf. Where votes are recorded through electronic or mechanical means, the voting machinery may be altered so that a vote intended for one candidate is recorded for another. Proxy voting is particularly vulnerable to election fraud, due to the amount of trust placed in the person who casts the vote. In several countries, there have been allegations of retirement home residents being asked to fill out 'absentee voter' forms. When the forms are signed and gathered, they are secretly rewritten as applications for proxy votes, naming party activists or their friends and relatives as the proxies. These people, unknown to the voter, cast the vote for the party of their choice. One of the simplest methods of electoral fraud is to destroy ballots for an opposing candidate or party. While mass destruction of ballots can be difficult to execute without drawing attention, in a very close election, it may be possible to destroy a very small number of ballot papers without detection, thereby changing the overall result. Blatant destruction of ballot papers can render an election invalid and force it to be rerun. If a party can improve its vote on the re-run election, it can benefit from such destruction as long as it is not linked to it. Tampering with electronic voting machines leads to all voting systems face threats of some form of electoral fraud. The types of threats that affect voting machines vary.

DOI: https://doi-ds.org/doilink/05.2024-45368588

Proposed Technology

Here in this project we present a voting machine which uses Radio Frequency Identification technology which helps to overcome the drawbacks of the above mentioned systems. RFID uses electromagnetic fields to track and detect objects. RFID reader transmits an encoded radio signal to detect the tag, emitting unique electronic product code. The main purpose of our project is to design an efficient and cost effective voting system. This system reduces the complications in e-voting machine and voting process is made more transparent. Here we use a RFID reader module which senses the RFID tags with unique identity. RFID tags with unique identity are allotted for different candidates in the election.

BLOCK DIAGRAM:



DESCRIPTION:

The proposed hardware design for the system is, the heart of the system is Arduino UNO. Along with it many components are used such as RFID, GSM, DC motor and motor drivers, etc are used.

SOFTWARES:

- ✓ Embedded C
- ✓ Arduino IDE

DOI: https://doi-ds.org/doilink/05.2024-45368588

- ✓ Express PCB

HARDWARES:

- ✓ Arduino Uno
- ✓ Power Supply
- ✓ GSM module
- ✓ LCD
- ✓ DC MOTOR
- ✓ RFID MODULE
- ✓ MAX 232
- ✓ L293D.

ARDUINO

Overview:

The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter. The Uno board has a resistor pulling the 8U2 HWB line to ground, making it easier to put into DFU mode.

The board has the following new features:

1.0 pinout: added SDA and SCL pins that are near to the AREF pin and two other new pins placed near to the RESET pin, the IOREF that allow the shields to adapt to the voltage provided from the board. In future, shields will be compatible with both the board that uses the AVR, which operates with 5V and with the Arduino Due that operates with 3.3V. The second one is a not connected pin, that is reserved for future purposes.

- Stronger RESET circuit.
- Atmega 16U2 replace the 8U2.

"Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version 1.0 will be the reference versions of Arduino, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform; for a comparison with previous versions, see the index of Arduino boards.

GSM

(GLOBAL SYSTEM FOR MOBILE COMMUNICATION)

DOI: https://doi-ds.org/doilink/05.2024-45368588

GSM (GLOPAL SYSTEM FOR MOBILE COMMUNICATION) is the most popular standard for mobile telephony systems in the world. The GSM Association, its promoting industry trade organization of mobile phone carriers and manufacturers, estimates that 80% of the global mobile market uses the standard. GSM is used by over 1.5 billion people across more than 212 countries and territories. This ubiquity means that subscribers can use their phones throughout the world, enabled by international roaming arrangements between mobile network operators. GSM differs from its predecessor technologies in that both signaling and speech channels are digital, and thus GSM is considered a second generation (2G) mobile phone system. This also facilitates the wide-spread implementation of data communication applications into the system.

The GSM standard has been an advantage to both consumers, who may benefit from the ability to roam and switch carriers without replacing phones, and also to network operators, who can choose equipment from many GSM equipment vendors. GSM also pioneered low-cost implementation of the short message service (SMS), also called text messaging, which has since been supported on other mobile phone standards as well. The standard includes a worldwide emergency telephone number feature (112).

Newer versions of the standard were backward-compatible with the original GSM system. For example, Release '97 of the standard added packet data capabilities by means of General Packet Radio Service (GPRS). Release '99 introduced higher speed data transmission using Enhanced Data Rates for GSM Evolution (EDGE).

RFID

RFID (Radio Frequency Identification) technology has been around for many years. Prior to the year 2000, common uses for RF-ID in the USA included tollway passes, access ID cards and the tiny ID chips that are inserted in animals for identification. The recent introduction of RFID in the supply chain as well as several mandates has added to the awareness and value of this technology.

RFID tags operate at several different frequencies. The majority of RFID tags operate at either 13 MHZ or 900 MHZ. Think of these two frequencies as the AM and FM bands on your radio. Each one has its advantages. For example, one works better when surrounded by metal while the other will work better over long distances.

13 MHZ (HF) tags are generally better at penetrating liquids and are usually used for access control such as in security cards and wristbands. The read range at this frequency is about 3 feet or 1 meter.

900 MHZ (UHF) tags operate better when reading multiple tags simultaneously, and thus are generally the tag type of choice for inventory purposes. The read range at this frequency is about 3-10 feet or more depending on what type of reader, interrogator or access point is used.

Most RFID tags do not contain any data in them after they are manufactured; they are similar to a blank label waiting for information to be printed on them. To place information in the tag, an encoder must be used. One of the most popular methods of encoding is with an RFID Capable Label Printer that has a built-in encoder and RFID Capable Barcode Label Software.

There are basically three types (called classes) of tags:

Class 0 - these tags are like a license plate in that they are read only and are encoded with data when they are

DOI: https://doi-ds.org/doilink/05.2024-45368588

manufactured.

Class 1 - these tags allow you to write the data in the tag and are usually one time programmable (OTP). These are available in either HF or UHF versions and are known as GEN1.

Class 1 GEN2 EPC (GEN2) - these tags are the latest type of UHF tag and are the types of tags most referred to in this document. They are also the tags required for mandates by various suppliers such as Wal-Mart and the US Department of Defense (DOD). In the industry, we refer to these tags simply as GEN2. These tags are 96 bits or larger and contain advanced features such as lock after write and CRC read verification.

The following components are required to write data (encode) to class 1 tags:

Software Application à Encoder Software à Tag Encoder à RFID Tag

The following components are required to read data from the tag:

RFID Tag, Reader, Interrogator or Access Point à Decoding Software à Software Application

IDAutomation.com provides some components of this system including Software Applications, Encoder Software and Tag Writers.

LCD

Introduction

A liquid crystal display (**LCD**) is a thin, flat electronic visual display that uses the light modulating properties of liquid crystals (LCs). LCs does not emit light directly.

They are used in a wide range of applications including: computer monitors, television, instrument panels, aircraft cockpit displays, signal, etc. They are common in consumer devices such as video players, gaming devices, clocks, watches, calculators, and telephones. LCDs have displaced cathode ray tube (CRT) displays in most applications. They are usually more compact, lightweight, portable, less expensive, more reliable, and easier on the eyes. They are available in a wider range of screen sizes than CRT and plasma displays, and since they do not use phosphors, they cannot suffer image burn-in.

LCDs are more energy efficient and offer safer disposal than CRTs. Its low electrical power consumption enables it to be used in battery-powered electronic equipment. It is an electronically-modulated optical device made up of any number of pixels filled with liquid crystals and arrayed in front of a light source (backlight) or reflector to produce images in color or monochrome. The earliest discovery leading to the development of LCD technology, the discovery of liquid crystals, dates from 1888. By 2008, worldwide sales of televisions with LCD screens had surpassed the sale of CRT units.

Each pixel of an LCD typically consists of a layer of molecules aligned between two transparent electrodes, and two polarizing filters the axes of transmission of which are (in most of the cases) perpendicular to each other. With no actual liquid crystal between the polarizing filters, light passing through the first filter would be blocked by the second (crossed) polarizer. In most of the cases the liquid crystal has double refraction

DOI: https://doi-ds.org/doilink/05.2024-45368588

Figure LCD diagram.

L293D

- 600mA OUTPUT CURRENT CAPABILITY PER CHANNEL
- 1.2A PEAK OUTPUT CURRENT (non repetitive) PER CHANNEL
- ENABLE FACILITY
- OVERTEMPERATURE PROTECTION
- LOGICAL "0" INPUT VOLTAGE UP TO 1.5 V
- (HIGH NOISE IMMUNITY)
- INTERNAL CLAMP DIODES

DC MOTOR

WORKING PRINCIPLE OF A DC MOTOR

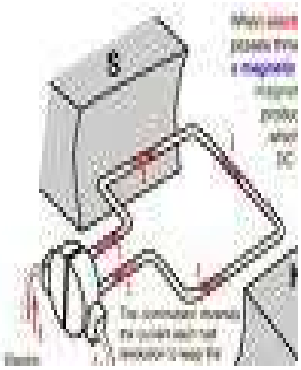
A DC motor is an electric motor that runs on DC electricity. It works on the principle of electromagnetism. A current carrying conductor when placed in an external magnetic field will experience a force proportional to the current in the conductor.

OPERATION OF A DC MOTOR

There are two magnetic fields produced in the motor. One magnetic field is produced by the permanent magnets and the other magnetic field is produced by the electrical current flowing in the motor windings. These two fields result in a torque which tends to rotate the rotor. As the rotor turns, the current in the windings is commutated to produce a continuous

Torque output this makes the motor to run.

DOI: https://doi-ds.org/doilink/05.2024-45368588



Arduino software

The Arduino Uno can be programmed with the Arduino software. Select "Arduino Uno from the Tools > Board menu (according to the microcontroller on your board).For details, see the reference and tutorials. The ATmega328 on the Arduino Uno comes preburned with a boot loader that allows you to upload new code to it without the use of an external hardware programmer. It communicates using the original STK500 protocol (reference, C header files).We can also bypass the boot loader and programs the microcontroller through the ICSP (In-Circuit Serial Programming) header; see these instructions for details. The ATmega16U2 (or 8U2 in the rev1 and rev2 boards) firmware source code is available. The ATmega16U2/8U2 is loaded with a DFU boot loader, which can be activated by:

- On Rev1 boards: connecting the solder jumper on the back of the board (near the map of Italy) and then resetting the 8U2.
- On Rev2 or later boards: there is a resistor that pulling the 8U2/16U2 HWB line to ground, making it easier to put into DFU mode.

The Arduino Uno has a number of facilities for communicating with a computer, another Arduino, or other microcontrollers. The ATmega328 provides UART TTL (5V) serial communication, which is available on digital pins 0 (RX) and 1 (TX). An ATmega16U2 on the board channels this serial communication over USB and appears as a virtual com port to software on the computer. The '16U2 firmware uses the standard USB COM drivers, and no external driver is needed. However, on Windows, an .information file is required. The Arduino software includes a serial monitor which allows simple textual data to be sent to and from the Arduino board. The RX and TX LEDs on the board will flash when data is being transmitted via the USB-to-serial chip and USB connection to the computer (but not for serial communication on pins 0 and 1). A Software Serial library allows for serial communication on any of the Uno's digital pins. The ATmega328 also supports I2C (TWI) and SPI communication. The Arduino software includes aWire library to simplify use of the I2C bus

FUTURE SCOPE

Anyone can carry the RFID card of someone being an imposter. To curb the menace of these imposters, an additional mechanism would be required to identify the voters like integrating the voting machine with fingerprint matching or face recognition. Another improvement that can be done is instead of storing the database locally on the

DOI: https://doi-ds.org/doilink/05.2024-45368588

EVM, the information of the voter can be retrieved from the server, where the server holds the database of all the registered users. This will allow any of the registered voters to vote from any polling booth.

CONCLUSION

In this project we have shown the implementation of a system that minimizes the possibility of rigging in elections and eliminates the need to do manual work. Cost of the EVM system is low and the system is convenient to use. It reduces the burden of the polling officers to identifying the voter. We have used database of 4 voters as a sample. In the real scenario, the number of voters will be quite large. In that case, storing them as array of strings might not work. We may need to employ a database management system to hold the record and retrieve the data quickly. Besides that, external memory will be required to hold such database. As Microcontroller is programmed over volatile memory, all the temporary data, like who has casted the vote and is reset. Although the total of the votes is stored, who has casted the vote and who has not, is lost. So, the EVM must remain in power on mode till the election is over.

REFERENCES

[1] K. Finkenzeller, "Introduction," in RFID Handbook, ed: John Wiley & Sons, Ltd, 2003, pp. 1-9.

[2] S. Merilampi, et al., "Analysis of Silver Ink Bow-Tie RFID Tag Antennas Printed on Paper Substrates," International Journal of Antennas and Propagation, vol. 2007, 2007.

[3] A. A. Babar, et al., "Performance of High-Permittivity Ceramic-Polymer Composite as a Substrate for UHF RFID Tag Antennas," International Journal of Antennas and Propagation, vol. 2012, p. 8, 2012.

[4] C. Sung-Lin and L. Ken-Huang, "A Slim RFID Tag Antenna Design for Metallic Object Applications," Antennas and Wireless Propagation Letters, IEEE, vol. 7, pp. 729-732, 2008.

[5] P. H. Yang, et al., "Compact Metallic RFID Tag Antennas With a Loop-Fed Method," Antennas and Propagation, IEEE Transactions on, vol. 59, pp. 4454- 4462, 2011.

[6] K. Tae-Wan, et al., "Design of a Label-Typed UHF RFID Tag Antenna for Metallic Objects," Antennas and Wireless Propagation Letters, IEEE, vol. 10, pp. 1010-1014, 2011.

[7] Z. Wenjing, et al., "Active E-Plate with Slot Antenna," in Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on, 2008, pp. 1-3.

[8] Z. Zhiguo, et al., "Design of New Type License Plates Based on RFID and its Secure Automatic Identification System," in Networked Computing and Advanced Information Management, 2008. NCM '08. Fourth International Conference on, 2008, pp. 298-302.

[9] H. Gi-Hyun, et al., "The development of UHF RFID metal tag applying to license plat," in Computer Engineering and Technology (ICCET), 2010 2nd International Conference on, 2010, pp. V3-271-V3- 274.

[10] K. Min-Seong, et al., "Directivity Design of RFID Tag Antenna Using Side-view Mirror for Vehicle," in Microwave Conference, 2008. APMC 2008. AsiaPacific, 2008, pp. 1-4.

DOI: https://doi-ds.org/doilink/05.2024-45368588

[11] L. M. a. C. Qin, "Tunable Compact UHF RFID Metal Tag Based on CPW Open Stub Feed PIFA Antenna," International Journal of Antennas and Propagation, vol. 2012, 2012.

[12] S. L. Chen, et al., "A metallic RFID tag design for steel-bar and wire-rod management application in the steel industry," Progress in Electromagnetics Research, vol. 91, pp. 195-212, 2009

DOI: https://doi-ds.org/doilink/05.2024-45368588