Designing of a biometric fingerprint scanner-based, secure and low-cost electronic voting machine for India

Shubhranil Chakraborty[a], Debabrata Bej[b], Dootam Roy[c], and Sekh Arif Mahammad[a]

[a]Department of Electronics and Communication Engineering, Jalpaiguri Government Engineering College, Jalpaiguri, West Bengal 735102, India.

[b]Department of Electronics and Communication Engineering, National Institute of Technology (NIT) Durgapur, Durgapur, West Bengal 713209, India.

[c]Department of Information Technology, Jalpaiguri Government Engineering College, Jalpaiguri, West Bengal 735102, India.

Abstract

A reliable Electronic Voting Machine (EVM) is proposed and implemented in this study, which is integrated with a biometric fingerprint scanner to ensure a secure election process. This biometric EVM includes features such as an interactive user interface, hack-free design and master lock. The EVM system has the capability of registering user data and storing them in a database through proper authentication. Moreover, the system proposed lowers the requirement for human resources. This paper provides a detailed description of the systematic development of the hardware and software used. The software part includes algorithm development and implementation. A thorough and in-depth understanding of the data and the communication protocols along with the pathways used for storage of data in the devices is provided. Additionally, the cost of the system is 62.82% less than the officially existing EVM machines of India. Furthermore, this study seeks to demonstrate the benefits of such an approach from a technological and a social standpoint.

Keywords: Electronic Voting Machine; biometric fingerprint authentication; embedded systems applications; electronic voting technology; user friendly environment; system oriented approach

1. Introduction

Voting is a regular occurrence in most democratic nations, and it serves a crucial function. According to [1], there are two sorts of voting systems: controlled voting and uncontrolled voting. Controlled voting occurs within the polling station with the presence of an election commission (EC) authority. In contrast, uncontrolled voting occurs outside of the polling station and is referred to as remote voting. In general, two types of mediums are utilized to gather votes in both controlled and uncontrolled voting systems. These are paper-based voting and electronic-based voting. In paper-based voting, traditional paper ballots are being used at the polling station in controlled voting. In contrast, in uncontrolled voting, paper ballots are cast from a remote place, or it can be defined as postal voting. In electronic-based voting, e-voting is utilized at the polling station in the controlled voting. In contrast, online voting is being used from the outside of the polling station by using a computer or mobile phone in uncontrolled voting. However, a paper-based voting system has limitations as low voting speed, low tallying speed and scope for booth capturing [2]. In this context, an electronic-based online voting system can be a helpful solution.

An electronic-based online voting system has the following advantages: portability, mobility, high voting speed, reusability, flexibility, etc. On the other side, this system faces some difficulties from the complicated design of the system and vulnerability to online threats [2]. In this context, electronic voting (E-Voting) at the polling station is the more acceptable solution because of its convenience, high tallying speed, and flexibility [2]. However, it faces with few difficulties like attack vulnerability and inequality [2]. Moreover, according to [3], there are also some issues with ballot secrecy and software integrity. In [4], the authors have reasoned about the currently deployed e-voting systems of the USA, named Election Systems & Software (ES & S). As a case study of India, about 85 million names on India's electoral rolls were fake or duplicated [5]. In India, a common allegation by various groups is that the electronic voting machine (EVM) is hacked or there are malpractices in the election process. As a vote represents an individual's voice, and voting is an essential aspect of sustaining integrity, its security remains the most pressing demand of the overall election system. The protection community regards EVMs as defective since they are entirely dependent on the physical security offered. An individual with access to such systems may sabotage them, causing all of the votes to be moved by tampering with the mechanism. To avoid this problem, a web-based solution has been provided in [6]. However, this system faces complexity and security issues. To solve these faults in e-voting / EVM systems, researchers suggested to use blockchain technology and cryptography.

Many researchers incorporated the blockchain technology into the EVM system to solve the said issues. In [7], the authors included this concept by connecting all the EVMs in a network. The EVMs (termed as the active nodes) procure the votes, store the chains, and authenticates the other nodes' transactions. The authors have designed an algorithm solely based on blockchain technology. In [8], the authors integrated blockchain technology as a subpart of the existing voting process. The genesis block of the blockchain would store the personal information of the voters. The voting day would witness the voters casting their vote after verification of their choice from a list as blocks. After casting, this information was broadcasted to a peer-to-peer network. On checking the validity of both the information by private miners, the actual data would be sent to a central network. In [9], the authors proposed a system that uses several tools such as ganache, truffle framework, metamask, and Node Package Manager (NPM). The designed algorithm was used Ether, Ethereum’s cryptocurrency, to have an account with a wallet address and write the transaction to the blockchain. The votes got processed by several nodes on a network of miners. The miners compete for completion of the transaction, the winner getting rewarded by Ether from the user. However, blockchain technology has many disadvantages, such as scalability, energy consumption, and expense of implementation. Also, these voting techniques may introduce unexpected security concerns and vulnerabilities and so, need a more advanced software architecture and management expertise [19].

Cryptography is another technique on which many researchers have worked to solve the issues of faulty e-voting. In [10], the authors proposed an algorithm based on the classic cryptographic technique of using a standard public-key cryptosystem, scattering entities, and disjoining the responsibilities to avoid critical security points. Features such as voting coercion, vote materialization, voting receipts, vote trade, the voting process and voter anonymity are covered in that approach. The authors devised web services and a proposed standard for election, Election Markup Language to show the proposal's viability. In [11], the authors addressed the issue by introducing cryptography for message exchange between polling stations. The authors also

reasoned that the messages exchanged are different from each other and have different security needs. The architecture involved a base station, several Polling Stations (PSs) and included several e-voting devices. All the PSs were connected to the base station, which acts as a server via a private local network. The base station monitored and managed all the activities of the PSs using some predefined techniques to open and close sessions for voting. The votes were then transmitted and stored in a database of the base station. In [12], the authors discussed cryptographic techniques in a web-based voting scenario. This technique has limitations, such as the necessity of employing a key, and disclosing it to any unwanted person, whether purposefully or inadvertently, would allow access to a cornucopia of personal data. Moreover, implementing such a design is complicated and time-consuming. Also, most of the literature requires the devices to be connected to a network, threatening the system's security.

Having mentioned the literature available in this field of study, it is important to state forward the problem for which this paper proposes a simple yet effective solution. India is a country of 136.64 crore people as of census done in 2019 [13]. Thus, a general election of any kind is a pretty big task which the Election Commission (EC) undertakes. Although, the EC does a pretty good job in completing the task, however, cases of booth capturing and registering fraudulent votes by impersonation of original voters are quite common and most frequent in village areas. Addressing such a problem on just the communication front or even the fact of securely storing the registered votes using cryptography are not enough. This issue must be addressed while casting the votes.

In this context, biometric technologies may be used in e-voting systems to validate voters' identities and reduce fraud. Election officials can use biometrics to check the authenticity of voters during the voting process [14]. The authors of [15] presented a simple architecture and logic flow for voting based on biometric data and sought to integrate the pre-existing Aadhaar database. However, there was a lack of planning for storing data and no means to check for integrity and the system comprised of the same unit for configuration and logging of votes. In [16], the author proposed a method to provide the second layer of security in the EVM system by integrating a Near Field Communication (NFC) card with a biometric sensor. As the NFC card records whether a person has voted or not, tampering/losing of the card may have significant consequences, such as voters' inability to vote. In [17], the author proposed a secure and fair biometric voting system and an automation method of the manual vote-counting process by utilizing the Lab-view software. However, a change in source code or workflow of Lab-View code might have disastrous effects on vote counting. Moreover, automating the process without supervision has drawbacks of making it difficult to trace back the fault in the case of a mistake.

In this context, the authors of this paper propose a system-oriented architecture of the biometric EVM machine. In this approach, voters must enter their information into the system by scanning their fingerprints using a biometric fingerprint sensor on a pre-election day in the presence of observers/commissioners. Voter information, together with a unique ID is stored in a database incorporated into the system. On voting day, voters must scan their fingerprints to the sensor, and the machine will retrieve their registered data based on ID matching. Voting is either disallowed or permitted based on this. If voting is allowed to one voter, the system will enable him or her to cast a vote. He or she then casts his or her vote. The result is shown on the screen, and data is delivered to a database included in the system. The system provides a user-friendly user interface (UI) for quick access to configuration, voter information input, and voting. This system is highly

secure and has a master lock option. The system is broken down into two sub-systems, similar to the present EVM system, with one designed for setup and another one for voter registration and voting. The two modules communicate with each other through UART communication. The novelty of such a machine is the fact that it does not entirely scrap away the EVM machine which is still deployed and used, but it builds upon the crevices of the older machine. The proposed machine exploits the fact that connecting to any type of external or even internal network provides a potential risk of unauthorized access by hackers who can steal data and/or contaminate the vote counts. Even the secured blockchain technology, which was discussed in the previous paragraphs, are not immune to such attacks. The problem of using blockchain technology or even connecting to an external network is addressed and presented in [18]; some of those problems are unwanted malware attacks, Denial of Service (DoS), etc. Thus, each unit acting as an individual system would be beneficial in a delicate job like a nationwide voting process.

The remainder of the paper is organized into sections that detail the design methodology. Section 2 presents the proposed EVM system. Section 3 explains the components and procedures utilized to create the proposed EVM. Section 4 presents the findings and perspectives. Finally, Section 5 concludes the paper.

2. Proposed electronic voting machine

2.1. Proposed EVM system overview

In the proposed EVM system, individuals' fingerprint impression is used for their identity and authenticity. Fingerprint impression is the cheapest and unique way of identification. Each prototype designed has a database that will be created which would store the voter's name and relevant details prior to the election day as a pre-poll procedure. During elections, the finger impression of a voter is entered as an input to the system, which is then compared with the records available in the database. If the particular pattern of the fingerprint matches with a record, then access to voting is granted. If the pattern does not match with the records stored in the database, the access to cast a vote is denied. The prototype has two units, a ballot unit, and a control unit, both of which communicates via the serial port (UART) communication, and the result is instantaneous. It is important to point out that each EVM machine is designed to hold the information of a maximum of 200 voters, which is the limit of the fingerprint module used [22]. This paper explains the working of one such prototype. Deploying this machine on a nationwide scale would require each machine to be independently designed with different set of fingerprints. This would further secure the process as no two machines would have the ability to authorize the voting process for the same individual.

The e-voting systems which stores the data in cloud or an external server can be easily hacked. Therefore, it is always favorable that EVMs are isolated from any external network. So, the data in the presented prototype is stored in its internal electrically erasable programmable read-only memory (EEPROM). It is still favorable for any system to be as interactive as possible. When it comes to EVM, the priority for this demand is foremost. A complicated process of voting can lead to the wrong selection of the candidate by the voter. An LED display in the prototype would guide the voters during the election process, thus making the system user-friendly. Keeping in mind all the necessities, this prototype is secure, easy-to-operate, and, most importantly, cost-effective.

The architecture devised addresses the lacunae of the present EVM machines and strives towards correcting them to provide a hassle-free and trustworthy voting process. The proposed biometric EVM consists of two parts: (a) Control Unit (CU) and (b) Ballot Unit (BU). The subsequent section provides an in-depth view of both units.

2.1.1. Control Unit

The CU is the brain of the biometric EVM. The district authority can solely operate this unit under the Officer-in-Charge (OC) election. This unit configures the BU, stores the number of votes cast, and displays the result on the Thin Film Transistor (TFT) Liquid Crystal Display (LCD) display. The CU has three buttons used to perform the following operations: (a) Reset - It clears the BU and CU data and the EEPROMs of the respective units. (b) Settings - Settings are used to configure the EVM to act on candidates' division into categories and subcategories. The EVM has an option to choose between three categories and a combination of subcategories. It has a provision for six candidates with a different choice for None of the Above (NOTA). Thus, the categories and subcategories can be divided as in Table 1. The corresponding set of instructions and protocols and conveyed to the BU is now ready to be used in the election.

Table 1

Categories and subcategories of candidates/voters

Sl. No.	Categories of voters	Subcategories of voters
1	1	0-6
2	2	0-4,0-2 / 0-2,0-4
3	3	0-3,0-3

2.1.2. Ballot Unit

The BU is a device that registers the votes of individuals. The BU comprises a biometric sensor for verification; a TFT LED screen shows the party an individual has voted for and push-pull switches to register the votes. After an individual has cast a vote, the corresponding result relies on the EEPROMs of both the BU and CU. This is done to ensure and safe case the votes cast in case of any damage to either of the units.

2.2. Block diagram of the proposed EVM

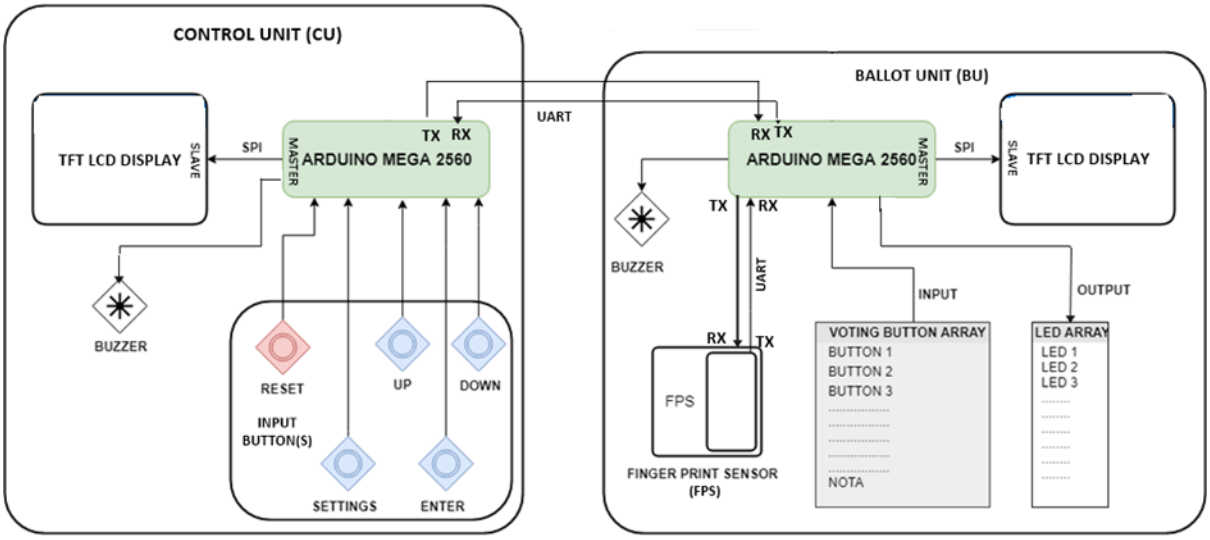

Fig. 1. Block diagram of proposed EVM

The decisive and the most important CU component is the Arduino Mega 2560 [20] microcontroller. It controls all the instructions which it receives through the digital input of the push and pull switches. A total of 5 digital inputs are connected for the functions explained in the previous section. A buzzer is connected through the digital output pin to signal if the device is getting reset. A TFT LCD screen is connected through the Serial Peripheral Interface (SPI) communication port. Similarly, the central unit on the BU is an Arduino Mega 2560 microcontroller. The device receives three types of inputs. Foremost, it receives data from the CU through the Universal Asynchronous Receiver/Transmitter (UART) port, which sets the working of the BU. The second type of input the BU receives is through another UART port. This input is connected to the Fingerprint Sensor GT-511C3 [21], which validates if a particular fingerprint is present or not. It passes the corresponding result to the microcontroller through the UART port. The third input it receives is through the push buttons on the digital pins for the corresponding candidates voted. The Block diagram of the proposed EVM system is presented in Fig. 1.

2.3. Working principle of the proposed EVM

A flow chart of the proposed EVM system is presented in Fig. 2.

2.3.1. Registration of the voters

The GT-511C3 fingerprint sensor stores the fingerprints according to index positions. So, to map the respective fingerprints to the details of the voters, such as their name, age, gender, and ID, the respective details of a voter are written on a text file during the registration process and saved in the EEPROM of the CU and BU. When a new voter is registered, the *.txt* file is appended with the new details fed from a specially designed on-screen keyboard on the BU. This process repeats until the n number of specified users are registered. An important point to note here is that the registration process can be initiated only by authorized personnel. The EEPROM of the CU and the memory of the fingerprint sensor store the information about the authorized personnel from the time of manufacturing (before the EVM is functional and set for public use). This is one of the functionalities of the master-lock feature stated above. For voter registration, Algorithm 1 is used.

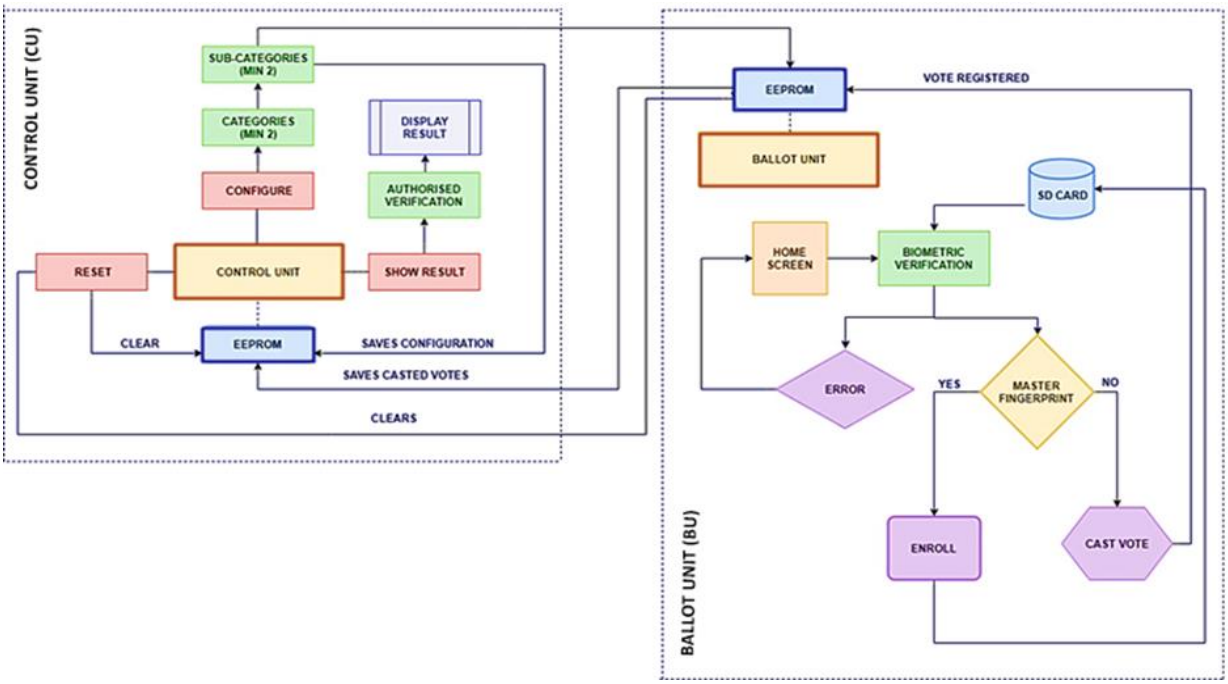

Fig. 2. Flow chart of proposed EVM

Algorithm 1: Algorithm for Registration of voters
INPUT: auth_fingerprint, voter_fingerprint
OUTPUT: flag
Initialization:
1: Activation of fingerprint sensor
2: Authentication initiated
3: flag := 0
4: if auth_fingerprint = true
Activate fingerprint sensor for voter
Capture fingerprint, assign an id (implicitly)
name := Enter voter name
gender := Enter voter sex
age := Enter voter age
write id, name, gender, age to voter_info
write voter_info to EEPROM
ready data packet for voter_info to send to CU
send data packet to CU through UART
flag := 1
5: end if
6: if flag = 1
display 'Registration successful'
else
display 'Registration failed'
7: end if

2.3.2. Setting up and working of BU and CU

The flow of our algorithm originates in the CU. Foremost, the CU needs to be configured. For example, the CU would ask for the number of categories and subcategories on starting up the

device. Then, depending on the number of candidates participating in the election, the appropriate number must be selected from the combination as stated in Table 1. The selected configuration is now forwarded to the BU, and a copy is sent to the EEPROM of the CU. The pseudocode for the CU is provided below in Algorithm 2.

Algorithm 2: Algorithm for Control Unit (CU)
INPUT: category, sub_category
OUTPUT: result
Initialization:
1: Setup categories, sub_catrgories
2: append data frame
3: send data frame via UART
LOOP PROCESS
4: data := listen for incoming data
5: if data = true
category := extract category from data
sub_category := extract sub-category from data
increment corresponding sub_category field in result
6: end if
7: display result

The next step of the algorithm is to register the users who can vote on a particular EVM. The BU algorithm is designed so that a new person cannot be registered until and unless the OC or any authorized personnel validates his fingerprint for registering new biometrics. The information about people registered to vote on a particular EVM is stored inside the fingerprint sensor module. Once all the users have been registered, the voting process can be initiated.

The BU has a touchscreen LCD that must be pressed each time users want to cast their vote. On touching the screen, the fingerprint module is activated. On authenticating with the correct fingerprint, the BU redirects to the function for casting a vote. A message is displayed on the screen, and the user is asked to cast their vote. On casting their vote, the party voted for is displayed on the screen sometimes, and the voting process is complete. The results are stored in the EEPROM of the Arduino Mega of the BU, an external Secure Digital (SD) card attached to the BU, and the EEPROM of the Arduino Mega of the CU, which is communicated through the UART port. The pseudocode for the BU is provided in Algorithm 3, and data retrieval during casting of the vote is based on Algorithm 4.

When a voter tries to cast his vote during the voting process, the foremost step is to get their fingerprints authenticated. When the fingerprint sensor feeds in the fingerprint from a voter, the BU fetches the file from the EEPROM. The corresponding details for the particular index, which is matched with the index of the sensor, are displayed on the screen on the successful matching of the fingerprint pattern. Fig. 3 shows the working steps of the proposed EVM system.

Algorithm 3: Algorithm for Ballot Unit (BU)
INPUT: category, sub_category
OUTPUT: data packet
Initialization:

1: Fetch data from UART
2: Extract category and subcategories
LOOP PROCESS
3: index := listen for data from biometric module
4: authenticate the information according to the index value and set flag value accordingly (Algorithm 4)
5: if flag = true
vote := enter vote from particular category
write vote to EEPROM
ready data packet to send to CU
send data packet through UART
6: end if

Algorithm 4: Algorithm for retrieval of information during casting of vote
INPUT: voter_fingerprint
OUTPUT: flag
Initialization:
1: fetch index value for corresponding fingerprint from biometric module
2: Authentication initiated
3: flag := 0
4: fetch voter_info file from EEPROM of BU
5: ind := read index values from file
6: if ind = index
flag := 1
7: end if
8: return flag

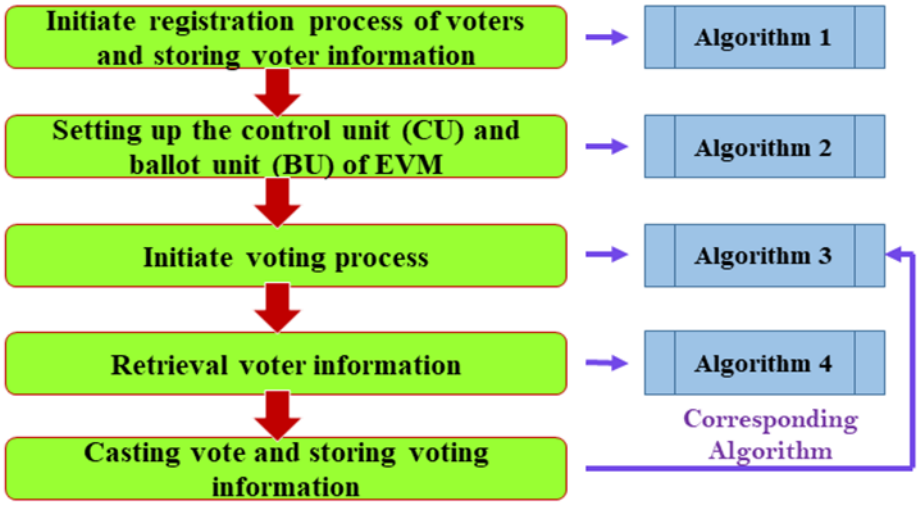

Fig. 3. Working step of proposed EVM

3. Components and techniques used to design the proposed EVM

3.1. Prototype development of the system

The following components are used to design the proposed system. The components of the proposed EVM system are shown in Fig. 4.

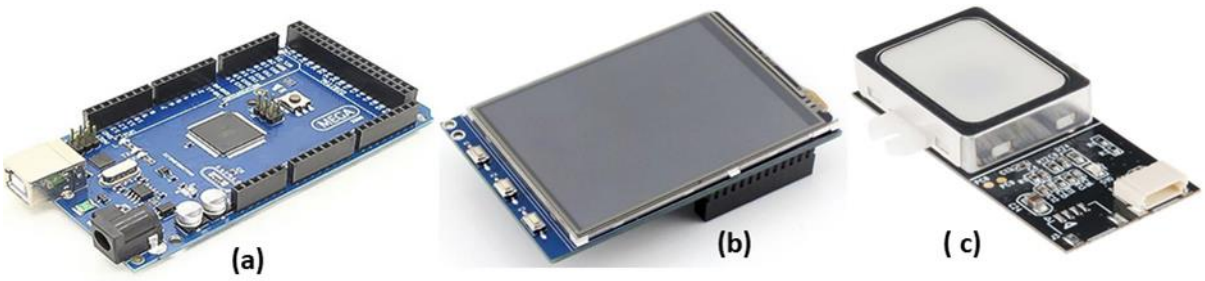

Fig. 4. Components of proposed EVM. (a) Arduino Mega 2560, (b) TFT LCD Screen, and (c) Optical Fingerprint Scanner (GT511C3)

3.1.1. Arduino Mega 2560

The Arduino Mega 2560 is a microcontroller board based on the ATmega2560. It comprises 54 digital IO pins, 16 analog inputs, a USB connection, an ICSP header, a 16 MHz crystal oscillator, a power jack, and a reset button. The said microcontroller is used as the brain of the proposed biometric EVM. Arduino Mega is responsible for all the communication, processing, and stacking of data.

3.1.2. TFT Display

The TFT displays are used as an interface both for displaying outputs and taking inputs. The display unit has a touch feature that we use to take the respected inputs. Both the display units are resistive touch.

3.1.3. Fingerprint Sensor (GT-511C3)

It is an independent unit that has its EEPROM storage for storing fingerprints. The fingerprint verification takes place within the unit using *SmackFinger 3.0* Algorithm [22]. The device can read and write fingerprint templates and databases. It communicates using the UART protocol at a baud rate of 9600. The device is capable of 1:1 Verification and 1:N Identification. When the fingerprints are matched, the respective information is sent to the main microcontrollers using UART.

3.1.4. Programming tools/ software

The Arduino Integrated Development Environment (IDE) 1.8.15 [23] is used to write and upload programs to Arduino Mega 2560 board.

3.2. Picture of the final prototype

The Control Unit and Ballot Unit are constructed using the modules stated above. The logic is implemented in C++ code in Arduino IDE. The finished product is encompassed inside cases designed using a 3D printer and polylactic acid (PLA), as shown in Fig. 5.

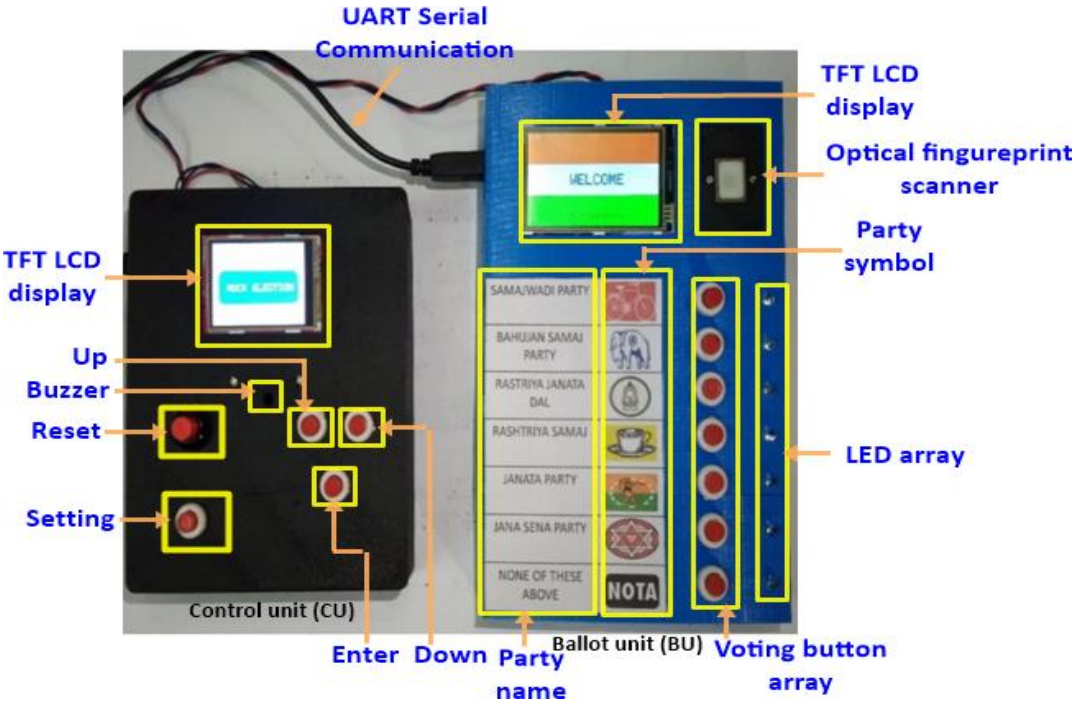

Fig. 5. Prototype of the proposed EVM

4. Results and discussions

4. 1. Results

The paper discusses the results in the following sub-sections. (a) Setting up the EVM, (b) Casting of votes, and (c) Displaying the results.

4.1.1. Setting up the EVM

The foremost step is setting up the biometric EVM. On pressing the settings button on the CU, the device is directed to the category and subcategory menu. Both of which can be selected from the combination shown in Table 1. After setting up the CU, the selected categories and subcategories are shown in the CU and BU, which is communicated using the UART comm. Port. The configuration processes and corresponding results are shown in Fig. 6.

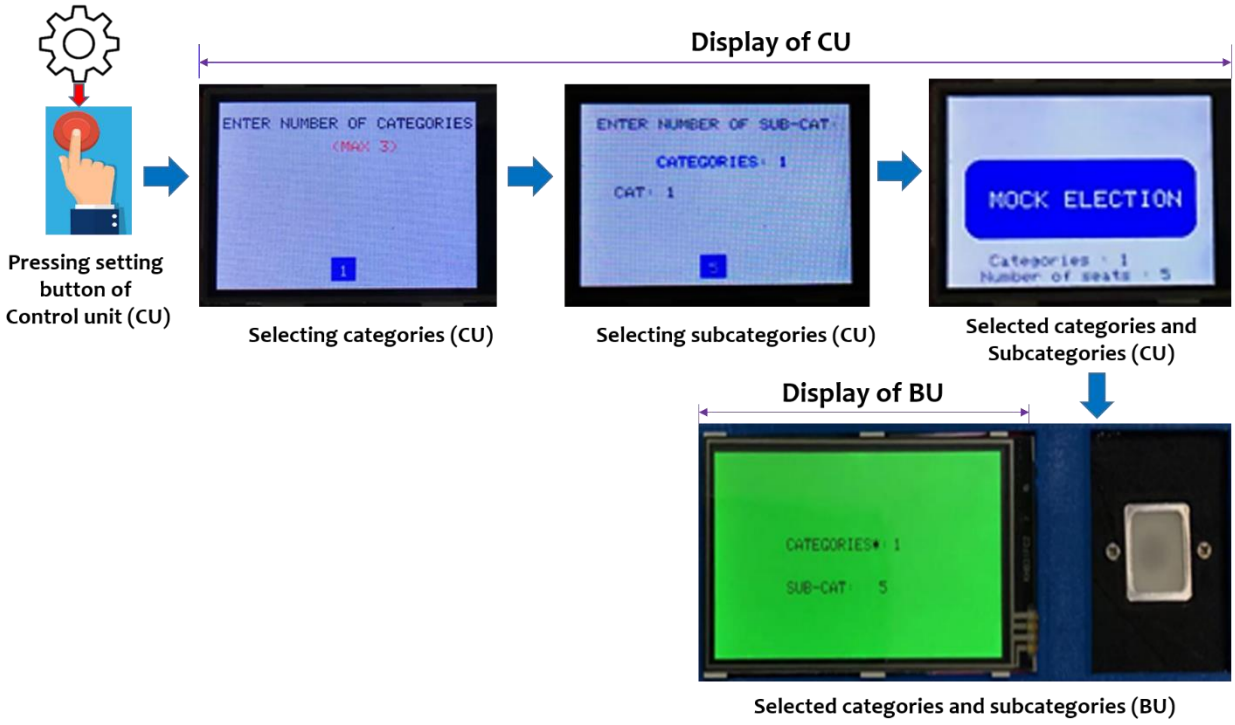

Fig. 6. Setting up and corresponding results of the proposed EVM

4.1.2. Casting of Votes

After configuring the devices, the next step is to cast the vote. For the trial, we have previously registered the users who are going to participate in the voting process. The instruction on the BU is to press the screen to proceed to the authentication menu. On touching the screen, the fingerprint sensor activates, and it asks the user to place the registered finger on the sensor. On successful authentication, the voter's details are displayed on the screen. After authentication, the screen redirects to a menu that presents the option to proceed to vote or exit. If there is some discrepancy in the details, the user can select exit and report the error to the concerning authority. If not, the user proceeds to vote. On proceeding to vote, the user presses one of the active buttons for each category selected. In this trial, we have shown the voting procedure for category – 1 and subcategories – 5. On registering their vote, the party voted for is shown on the screen sometimes for validation purposes. If a user tries to cast their vote for a second time, the device invalidates the trial and displays a message for the same. The different steps of vote casting and displaying results are shown in Fig. 7.

4.1.3. Displaying of Results

After each vote is cast, each candidate's corresponding counter is incremented by 1 and is communicated the EEPROM of the CU, the EEPROM of the BU, and an external SD card. The result is displayed in the CU by pressing the display result button on this prototype. The proposed design has a master-lock feature implemented in it. The feature makes sure that no person other than the authorized people in question can view the results. This works similarly to authenticating the fingerprints. On pressing the button for displaying the results, the screen prompts the user for authentication. The authorized person must provide his/her biometric to the fingerprint sensor provided. On successful authentication, the results are displayed. The results are shown in Fig. 7.

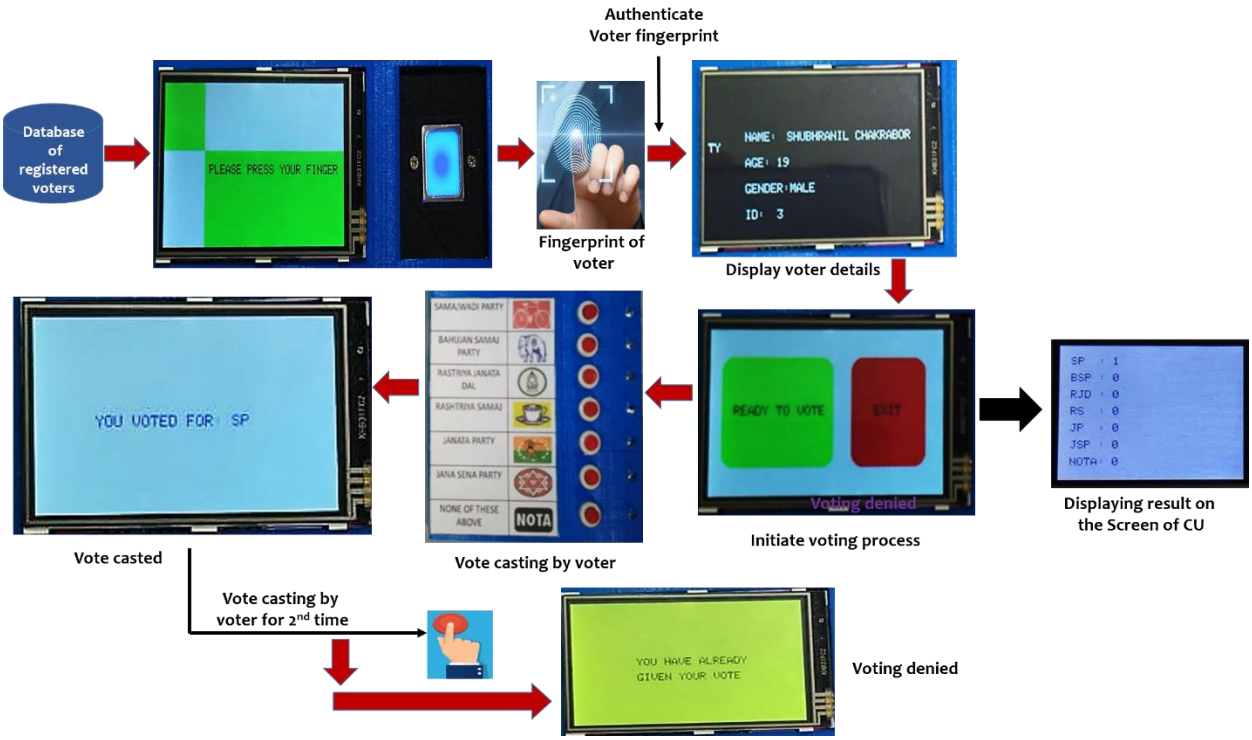

Fig. 7. Casting of the vote and displaying the result

4.2. Discussions

4.2.1. Performance comparison with existing EVM

A comparison has been drawn between the existing EVM system and the proposed biometric EVM system in Table 2 to show the improvements incorporated based on performance.

Table - 2

Performance comparison of the proposed EVM system with the existing EVM system

Parameters	Existing system [24]	Proposed system
Security	Tamper-proof (device gets locked out if any kind of tampering with the device is detected)	The device will get locked out on even suspicious button presses. Only the authorized person will then be able to unlock it afterward (master lock feature).
User Interface	Printed signs for different parties in the ballot unit.	User-friendly UI, virtual helping guides throughout the voting process in multiple languages, and structured tutorials.
Voter Verification	Voter ID card	Biometric voter verification
System Programming	Non-reprogrammable	Reprogrammable system

4.2.2. Cost Analysis of the proposed EVM system

As a case study, The Election Commission of India (ECI) states that the cost of manufacturing M2 EVMs (produced between 2006 and 2010) was Rs. 8,270 per unit (CU and BU). Moreover, the M3 EVMs, which are currently produced in the country, costs around Rs. 17,000 per unit [25]. The prototype proposed in the paper significantly reduces the cost of manufacturing a unit (CU and BU). The amount for producing the biometric EVM sums up to Rs. 6150, 25.63% less than the M2 EVMs and 63.82% less than the M3 EVMs. Table 3 breaks up the cost of producing the biometric EVM into the cost of individual components. A point to note here is the fact that the information provided regarding the cost of the EVM deployed by the ECI includes the overall cost and there is no breakup provided. Thus, the comparison is provided accordingly.

Table - 3
Cost of the proposed biometric EVM system

Components	Cost (INR)
Arduino Mega	1600
Fingerprint Scanner	2000
PLA (3D printer filament)	700
Buttons, connecting wires, LEDs	250
LCD screens	1600
Total	**6150**

5. Conclusion

A lot of nations worldwide are on the high road to incorporate an e-government system. The proposed prototype can significantly speed up the voting process and reduce the amount of workforce required. Implementation of the biometric can safeguard the identities of the voters. The storage of data in more than one place can help authenticate if the data has been tampered with or not. The master-lock feature safeguards the information of how many votes have been aggregated from a particular poll station until and unless the authentication of authorized personnel officially counts the votes. Moreover, it proposes a significant price cut in producing a more advanced version of the existing EVM. Developing countries like India have introduced the Aadhaar card, a digital identity card for each person whose biometric features are linked. It would be quite insightful to observe how this digital identity card can be used for voting purposes. One approach may be to divide and conquer, i.e., to say that the prototype built above can store individual data of some population tapped from the Aadhar database. So, when an individual voter would come to cast their vote, it would be a hassle-free process. Moreover, the voters need not carry any extra identity proof, as the security concern would be tackled by the prototype suggested above. However, this is not an automated process, and it is not a replacement for the human proctored process. This is a comprehensive system of voter validation, vote input, vote recording and tabulation of election results in-situ, i.e., within the machine designed. Nonetheless, the machine would still require to be protected. However, the workforce can be reduced significantly, the voting percentage increased considerably, and a rigged-free election scenario is improved substantially.

References:

[1] Karokola, Geoffrey, Stewart Kowalski, and Louise Yngström. "Secure e-Government Services: Protection Profile for Electronic Voting–A Case of Tanzania." IST-Africa 2012 Conference Proceedings. 2012.

[2] Elbarbary, Enas Mohamed Mahmoud. Building Smart Multipurpose Electronic Voting System. Diss. October 6 University, 2016.

[3] Aranha, D. F., Barbosa, P. Y., Cardoso, T. N., Araújo, C. L., & Matias, P. (2019). The return of software vulnerabilities in the Brazilian voting machine. Computers & Security, 86, 335-349.

[4] Weldemariam, Komminist, Richard A. Kemmerer, and Adolfo Villafiorita. "Formal analysis of an electronic voting system: An experience report." Journal of Systems and Software 84.10 (2011): 1618-1637.

[5] Electronic Voting Machine of India. Available: https://eci.gov.in/faqs/evm/general-qa/electronic-voting-machine-r2/ [accessed on 8 September 2021]

[6] Warghade, Shrikant Subhash, and B. Karthikeyan. "Voting System for India." Intelligent Embedded Systems. Springer, Singapore, 2018. 59-65.

[7] Sudharsan, B., Nidhish Krishna MP, and M. Alagappan. "Secured electronic voting system using the concepts of blockchain." 2019 IEEE 10th Annual Information

Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2019.

[8] A. Indapwar, M. Chandak, and A. Jain, “E-voting system using blockchain technology,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 3, pp. 2775–2779, 2020.

[9] Khan, Saad, et al. "Implementation of Decentralized Blockchain E-voting." EAI Endorsed Transactions on Smart Cities 4.10 (2020).

[10] Santin, Altair O., Regivaldo G. Costa, and Carlos A. Maziero. "A three-ballot-based secure electronic voting system." IEEE Security & Privacy 6.3 (2008): 14-21.

[11] Ahmad, Masood, et al. "Security, usability, and biometric authentication scheme for electronic voting using multiple keys." International Journal of Distributed Sensor Networks 16.7 (2020): 1550147720944025.

[12] Pasquinucci, Andrea. "Web voting, security and cryptography." Computer Fraud & Security 2007.3 (2007): 5-8.

[13] Population of India (2019). Available: https://statisticstimes.com/demographics/country/india-population.php [accessed on 8 September 2021]

[14] Obaidat, Mohammad S., Tanmoy Maitra, and Debasis Giri. "Protecting the integrity of elections using biometrics." Biometric-Based Physical and Cybersecurity Systems. Springer, Cham, 2019. 513-533.

[15] Agarwal, Samarth, et al. "Biometric Based Secured Remote Electronic Voting System." 2020 7th International Conference on Smart Structures and Systems (ICSSS). IEEE, 2020.

[16] Hasan, Syed Mahmud, et al. "Development of electronic voting machine with the inclusion of Near Field Communication ID cards and biometric fingerprint identifier." 2014 17th International Conference on Computer and Information Technology (ICCIT). IEEE, 2014.

[17] Roopa, A. E., R. Hemavathi, and B. Pushpalatha. "Automated Biometric-EVM Implemented Using Lab-View." 2019 IEEE 5th International Conference for Convergence in Technology (I2CT). IEEE, 2019.

[18] National Academies of Sciences, Engineering, and Medicine. Securing the Vote: Protecting American Democracy. National Academies Press, 2018.

[19] Taş, Ruhi, and Ömer Özgür Tanrıöver. "A systematic review of challenges and opportunities of blockchain for E-voting." Symmetry 12.8 (2020): 1328.

[20] Barrett, Steven F. "Arduino microcontroller processing for everyone!." Synthesis Lectures on Digital Circuits and Systems 8.4 (2013): 1-513.

[21] Jatmiko, D. A., and S. U. Prini. "Orientation Recognition Performance Evaluation of GT-511C3 Fingerprint Sensor." IOP Conference Series: Materials Science and Engineering. Vol. 662. No. 2. IOP Publishing, 2019.

[22] Sapes, Jordi, and Francesc Solsona. "Fingerscanner: Embedding a fingerprint scanner in a raspberry pi." Sensors 16.2 (2016): 220.

[23] Arduino IDE. Available: https://www.arduino.cc/en/software [accessed on 6 June 2021]

[24] Shrivastava, Vishesh, and Girish Tere. "An analysis of electronic voting machine for its effectiveness." International Journal of Computing Experiments (IJCE) Vol 1 (2016): 8-12.

[25] Cost of EVM machine mentioned by Election commission of India (ECI). Available: https://eci.gov.in/faqs/evm/general-qa/electronic-voting-machine-r2/ [accessed on 6 June 2021]