International Journal of Engineering Innovations in Advanced Technology

ISSN: 2582-1431 (Online), Volume-4 Issue-4, December 2022

A Survey On New Innovative EVM For India Voting With Biometrics

[1]M.V. Sheela Devi, [2]M. Gnana Tulasi, [3]M. Deva Priya, [4]M. Bhavani, [5]M. Bhavya Sri

[1]Assistant Professor, Department of CSE, KKR & KSR institute of technology and Sciences
[2,3,4,5]B. Tech Students, Department of CSE, KKR & KSR institute of technology and Sciences

***Abstract*—To avoid rigging completely. Electronic voting systems have come into picture to prevent rigging up to the maximum extent. But even there may be some malfunctions during elections. Thus, fingerprint based electronic voting system has been designed. According to ancient Greek scripts BIOMETRICS means study of life. Biometrics studies commonly include fingerprint, face, iris, voice, signature, and hand geometry recognition and verification. Many other modalities are in various stages of development and assessment. Among these available biometric traits, Finger Print proves to be one of the best traits providing good mismatch ratio and also reliable. To provide perfect security and to make our work easier, we are taking the help of two different technologies viz. EMBEDDED SYSTEMS and BIOMETRICS. Firstly, discussing about Biometrics, we are concentrating on Fingerprint scanning. For this, we are using FIM 3030N high voltage module as a scanner. This module has in-built ROM, DSP and RAM. In this, we can store the fingerprints of up to 100 users. This module can operate in 2 modes i.e., Master mode and User mode. We will be using Master mode to register the fingerprints which will be stored in the ROM present on the scanner with a unique id. When a person wants to register himself in the voter list, he has to provide his complete details along with his fingerprint image. Thus, when the same person comes to poll his vote during the elections, he needs to give his fingerprint image before polling his vote. Thus, the system scans his fingerprint image, compares the image with the already stored image. If both the images are matched, the person can eligible to pole his vote. If the fingerprint was not matched then the buzzer will give us the alert sound and that person can't be eligible to cast his vote. By this way we can avoid the rigging. After the polling was over there is switch named "results" get the final results. All this voting information was sent to the predefined web server by using the Wi-Fi module and we should provide the internet connection to that Wi-Fi module.**

***Key Words*—Internet of Things, Biometric, Finger print authentication, embedded system, voting system.**

Manuscript received November 17, 2022; Revised December 12, 2022; Accepted December 14, 2022

I. INTRODUCTION

Electronic voting reefer's to voting using electronic means to either aid or take care of the chores of casting and counting votes depending on the particular implementation ,e-voting may use standalone electronic machine (also called EVM)or computer to the internet .This concept describe an online electoral system for Indian election is proposed for 1st time there are number of voting system develop all over the world with each of them having it's limitation's this system uses the fingerprint sensor to scan thumb of the voter's in order to provide high performance with high security to the voting counter also as we using internet of thing i.e.(IOT)to make the voting system more practical. This system used to display the data-base of the user (voter). After receiving the Instruction from the polling officer, also the voter can use the touch screen to poll his/her vote.

The internet of things (IOT) is the inter-networking of physical devices, vehicles, building and other items embedded with electronics, software, sensors, actuators and network connectivity which enables these objects to collect and exchange data. The IOT allows objects to sense or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based system, and resulting in improve efficiency, accuracy and economic benefit in addition to reduce human intervention. In the broadest sense, the IOT encompasses everything connected to the internet, but it is increasingly being use to define objects that "talk" to each other. Simply, the Internet of things is made up of device - from simple sensors to smart phones and wearable's - connected together. For making an IOT infrastructure where we configure the hardware with software and control the devices over the internet this can be with help of raspberry pi and Arduino. The raspberry pi and arduino is platform for developing the internet of things environment. Fingerprint electronic voting system has provided a range of advantages to the voting process. It assists perform voting in much more successful and efficient way, such a minimizing the cost of the ballot's printing and employing more staff.

Fingerprint Election system also can make voting tallies faster as well as much more effectively than tired polling staff; they minimize human being mistakes in voting final result as well as minimize the expenses of the election. The significant advantages of electronic election might be reviewing in the following points: much more participation, fast process, lower costs, and precision placing and better access and versatility for the disable. Essential reason fingerprint readers are widely used is, they offer a fast, simple, powerful, and secure access by means of a person with the good access rights can authenticate. The advocate of electronic voting provides that the comfort, flexibility, speed, cost effectiveness, and versatility and these are the main advantages of the electronic voting machine. Considering that this system has every one of these properties, it can be used almost everywhere, by the government authorities, organizations, courts, shopping malls even in the colleges and universities.

The matching algorithm going to be designed in this project will support the system with additional advantages. The fingerprint matching algorithm combine both local and global information are used for the purpose of fingerprint feature extraction. The result of the algorithm will be finger code which is short length fixed code that will be stored in the system's database and it will be used during the matching. The finger code provides another advantage to the system by making the matching process faster, by taking the Euclidean distance between two finger codes. In the existing system, the election process was preceding like cast the vote by showing the voter ID card at the polling booth and by pressing the button against the party symbol. But in that there is a chance of rigging. So, to avoid this we are incorporating the embedded systems into the election system by registering the fingerprints of every voter before election. Voting process is known as a process for a group by means of a meeting or democratic vote in orders to take a free decision. This manner considers as the best normally found in republic and democratic governments (IDEA international, 2012) Common elections systems already exist for hundred years ago.

All those earlier election systems, however they had been considered being acceptable in past days, they started to reveal its disadvantages, day after day. These disadvantages, lead to a huge development in the design and style of electronic voting machine. Previously back to 1960, the election systems used were all run manually. This involves, the election system that use paper, were the voters' votes casted and counted by hands. During 1961, the design of voting systems developed from manual base to electronic base where the first electronic voting system was the electronic punch card system (Giovanni, 2008). In the proposed system, we are incorporating the fingerprint module and by using this system, before election we are going to register the fingerprint of every voter and at the time of voting one must show his finger at the fingerprint module to cast his vote.

Since finger print was unique for every person and there is no chance of rigging and once the fingerprint was matched then only the person can able to cast his vote. The project requires the voter to submit his/her Fingerprint at the election place. The Fingerprint technology will be used in this project to create the system. The primary goal of the project is to make a system that requests the voter to give his/her Fingerprint as a personality proof. The fingerprint voting system reads the fingerprint's data and compares it with the data previously stored inside the database. If the data exists in the database meets with the previously stored data, the voting system will enable the voter to enter into the system and give his/her vote. If the data of the Finger didn't meet with the stored data, then the system will instantly trigger the display and the authorities will come to take an action. In order to achieve the primary goal of this project, matching algorithm need to be designed in efficient way in order to increase system's accuracy.

The proposed matching based on Gabor liner filter bank which consists of 8 filters which will extract the local and global feature of the fingerprint and convert the extracted information into variant vector (finger code). The performance of liner filters is not accurate if the fingerprint image not clear. For that another objective is added to this project which is reducing the noise of the fingerprint image using sectorization and normalization. Voting machines are the total combination of mechanical, electro-mechanical, or electronic equipment (including software, firmware, and documentation required to program control, and support equipment), that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information.

The first voting machines were mechanical but it is increasingly more common to use electronic voting machines. A voting system includes the practices and associated documentation used to identify system components and versions of such components; to test the system during its development and maintenance; to maintain records of system errors or defects; to determine specific changes made after initial certification; and to make available any materials to the voter (such as notices, instructions, forms, or paper ballots). Traditionally, a voting machine has been defined by the mechanism the system uses to cast votes and further categorized by the location where the system tabulates the votes. Voting machines have different levels of usability, security, efficiency and accuracy.

Certain systems may be more or less accessible toall voters, or not accessible to those voters with certain types of disabilities. They can also have an effect on the public's ability to oversee elections. Electronic voting systems may offer advantages compared to other voting techniques. An electronic voting system can be involved in any one of a number of steps in the setup, distributing, voting, collecting, and counting of ballots, and thus may or may not introduce advantages into any of these steps. Moreover, it is also important that a false entry should not be made so for this one of the most secure methods for voting is using a biometric sensor like a fingerprint reader. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints.

II. LITERATURE REVIEW

[1] Suggests the use of GSM modules along with the biometric system for voting. A touch screen is implemented to overcome the button problem in a regular EVM and also to select suitable candidates during voting. The GSM module is used to send the results to the corresponding authority. A PC is used to store the details of people in the database. If a match is not found an alarm/buzzer is used to generate the error message. Although the system can be considered to be secure and reliable, it may not cater to a system that intends to conduct voting in multiple locations simultaneously.

[2] Suggests a model that implements a biometric voting system using an EVM. Here the fingerprint is scanned and checked with the database. If the user exists, he/she is allowed to cast his vote using the EVM. In this system each EVM is used for a particular location and the winner candidate is declared by the EVM itself after a particular period of time.

[3] This uses Aadhar card information for the election process. Two databases are maintained, one central and another local. The unique aadhar card number and fingerprint is used to authenticate the user. As each vote is casted, it will be updated onto the local database.

[4] Describes that raspberry pi is used as host. This minicomputer has the ability of image processing and control complete voting machine system. A camera is used to take picture of citizens' national ID card and identify that this user is valid voter for that region. If the citizen is valid and also didn't vote then the person is allowed to submit his/her vote. Each voting machine is locked by finger print access module. The user is identified his/her finger print is sent to a specific machine for voting. Each voting machine is networked with central Raspberry pi voting identification system.

[5] Summarizes all the necessary electronics to allow you to store, delete, and verify fingerprints with just the touch of a button. Stored fingerprints are retained even in the event of complete power failure or battery drain. Biometric voting has made the voting procedure simpler. It is a revolutionary method preferred to traditional EVM voting, as it is risk defective.

[6] Describes that creation of a database consisting of the thumb impressions of all the eligible voters in a constituency is done as a pre-poll procedure. During elections, the thumb impression of a voter is entered as input to the system. This is then compared with the available records in the database. If the particular pattern matches with anyone in the available record, access to cast a vote is granted. But in case the pattern doesn't match with the records of the database or in case of repetition, access to cast a vote is denied or the vote gets rejected. The result is instantaneous and counting is done. The overall cost for conducting elections gets reduced and so does the maintenance cost of the systems. The postal type of voting is not convenient for everyone.

[7] Describes to improve the security performance in the voting machine as well as to provide easy access to cast the vote by using finger print. Fingerprint is one of the unique identities of a human being which is being used in the aadhar system. By using arduino software and by using image processing we capture the finger print of every individual and the face of the individual is being captured. The polling of the vote is transmitted to PC through arduino communication. Face of the person captured is compared to aadhar details using Lab VIEW.

[8] Describes that advance method of voting system in Indian Election commission. The

casting a ballot framework is overseen easily as the clients need to login by Unique Identification Authority of India(UIDAI) and secret phrase and snap on individuals ideal possibility to make their choice. This shows that highly secured secret key is affirmed in advance to each individual acknowledged in the fundamental database of Electronics Corporation of Israel (ECI). The elector can guarantee that his/her vote has polled to the address as such saving a huge time and facultative ECI to result at between times.

[9] Massod Ahmed said that in electronic voting authentication scheme, every polling station is responsible to support three different types of keys. These are global key, pair wise key, and individual key. The global keys are public keys shared with all polling stations in the voting network. The pair wise key can be used for communication with polling stations. Individual keys will be used for communication with the server. To ensure authentication of local broadcast, electronic voting authentication scheme uses one-way key chains in a well-organized way. The support of source authentication is a visible advantage of this scheme. We examine the authentication of electronic voting authentication scheme on numerous attack models. The measurement demonstrates that electronic voting authentication scheme is very operative in protecting against numerous elegant attacks such as wormhole attack, Sybil attack, and HELLO Flood attack. The proposed system is evaluated and the results demonstrate that the proposed system is practical and secure as compared to the direct recording electronic and manual systems.

[10] 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.

[11] 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 more advanced software architecture and management expertise

[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

[13 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.

[14] 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.

III. CONCLUSION

For over a century, fingerprints have been one of the most highly used methods for human recognition; automated biometric systems have only been available in recent years. This work is successfully implemented and evaluated. The arrived results were significant and more comparable. It proves the fact that the fingerprint image enhancement will certainly improve the verification performance of the fingerprint-based recognition system. Because fingerprints have a generally broad acceptance with the general public, law enforcement and the forensic science community, they will continue to be used with many governments legacy systems and will be utilized in new systems for evolving applications that require a reliable biometric. This biometric voting system would enable hosting of fair elections in India. This will preclude the illegal practices like rigging. The citizens can be sure that they alone can choose their leaders, thus exercising their right in the democracy.

REFERENCES

[1] Ashok Kumar D., Ummal Sariba Begum T., A Novel design of Electronic Voting System Using Fingerprint,International Journal of Innovative Technology & Creative Engineering (ISSN:2045- 8711),Vol.1,No.1. pp: 12 19, January 2017.

[2] 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, 2018.

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

[4] Chaum D., Secret-ballot receipts: True voter-verifiable elections, IEEE Security and Privacy38-47, 2014.

[5] Darcy, R., & McAllister, I., Ballot Position Effects, Electoral Studies, 9(1), pp.5-17, 2000.

[6] Gritzalis D., [Editor]., Secure Electronic Voting, Springer-Verlag, Berlin Germany, 2013.

[7] 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, 2018.

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

[9] 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.

[10] 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, 2016.

[11] R. Hite, All Levels of Government are needed to Address Electronic Voting System Challenges, Technical report, GAO, 2017