****

**MINI-PROJECT**

**On**

**“FINGERPRINT BASED FRAUD DETECTION VOTING SYSTEM”**

**BACHELOR OF ENGINEERING**

**IN**

**INFORMATION SCIENCE AND ENGINEERING**

**Submitted by**

**Nisarga K(1DS20IS065)**

**Nithya M (1DS20IS067)**

**Saijyoti G M (1DS20IS085)**

**Sanjana H Goud (1DS20IS092)**

**Under the guidance of**

**Dr Chandrakala B M**

**(Associate professor)**

**Department Of Information Science and Engineering**

**DAYANANDA SAGAR COLLEGE OF ENGINEERING**

S M Hills, Kumara Swamy Layout, Bengaluru-560078

**2022-23**

**Abstract**

Currently, the voting system in India is inefficient and vulnerable to outside threats, the only thing that the security checks is a voter ID card, which these days are faked by many. It is slow and counting the votes manually can take a long time. In some rural areas, where there is not much security available, polling booths are captured and often most ballots are destroyed. So, the development of such a system which is online will cut out these possibilities and many votes can be saved through this system, even if such incidents occur. Biometric Fingerprint devices are used in the Electronic Voting machine for voter verification. We have designed a fingerprint-based voting machine where there is no need for the user to carry his ID which contains his required details. The person at the polling booth needs only to place his Finger on the device, thus allowing the acquisition of an on-spot fingerprint from the voter which serves as an identification. This Fingerprint reader reads the details from the tag. This data is passed onto the controlling unit for the verification. The controller fetches the data from the reader and compares this data with the already existing data stored during the registration of the voters. If the data matches with the pre-stored information of the registered fingerprint, the person is allowed to cast his vote. If not, a warning message is displayed on LCD and the person is barred from polling his vote. The vote casting mechanism is carried out manually using the push buttons. LCD is used to display the related messages, warnings and ensuring results. This application also ensures that the voting is anonymous, after the login, each user is given a unique and random id which will have no ties to the user’s details, therefore there is no way to find out which user voted for which candidate. A simple, user-friendly interface is used, which will help even the illiterate voters. The focus in more on the visual representation of data, and no unnecessary links are used, the interface is made as simple as possible with only basic functionalities

**CONTENTS**

Abstract

Chapter1 Introduction….………………………………Pg No.

* 1. Introduction
  2. Problem statement
  3. Objectives and Scope of Project
  4. Motivation of Project

Chapter 2 Literature Survey…………………………….Pg No.

Chapter 3 Requirements …………………………………Pg No.

3.1 Software Requirements

3.2 Hardware Requirements

Chapter 4 System Design …………………………………Pg No.

4.1 Existing system

4.2 Proposed system

4.3 System Architecture

Chapter 5 Conclusion ……….……………………………Pg No.

References

**Chapter 1**

**Introduction**

**1.1 Introduction**

Biometrics is the science and technology of measuring and analyzing biological data. Biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, for authentication purposes. The field of biometrics was formed and has since expanded on too many types of physical identification. Among the several human fingerprints remain a very common identifier and the biometric method of choice among law enforcement. These concepts of human identification have led to the development of fingerprint scanners that serve to quickly identify individuals and assign access privileges. The basic point of these devices is also to examine the fingerprint data of an individual and compare it to a database of other fingerprints. In our project we have used fingerprints for the purpose of voter identification or authentication. As the thumb impression of every individual is unique, it helps in minimizing the error. A database is created containing the fingerprint images of all the voters as required. Illegal votes and repetition of votes is checked for in this system with accurate coding. Hence with the application of this fingerprint based EVM system elections could be made fair and free from rigging. Further that the elections would no longer be a tedious and expensive job.

**1.2 Problem statement**

The current voting system in India is slow and vulnerable in the authentication of voters, where the only thing that the security checks is a voter ID card, which these days are faked by many. And identity verifications are done manually which requires more manpower. In the present system there must be people assigned to check whether EVM’s are busy or not. It is slow and counting the votes manually can take a long time.

**1.3 Objectives and Scope of Project**

* The possible solution is, if a person is identified using his/her fingerprint rules out the possibility of fake votes and it provides the result immediately after the voting process is completed. The whole process is done automatically by the voting machine.
* The environment of this voting system is designed in such a way that it won't allow voters inside the voting room if another voter is casting his vote.
* Biometric Enrollment: Develop a system to enroll voters' fingerprints and associate them with their voting credentials (e.g., voter ID or unique identifier).
* Fingerprint Verification: Implement a fingerprint recognition algorithm to verify the identity of voters during the voting process.
* Fraud Detection: Incorporate fraud detection mechanisms to identify and prevent fraudulent activities, such as attempting to vote multiple times or using fake fingerprints.

**1.4 Motivation of Project**

* Enhancing Voter Confidence: By incorporating fingerprint-based fraud detection, the voting system aims to increase voter confidence in the electoral process. It provides voters with the assurance that their votes will not be tampered with or compromised by fraudulent activities, thereby fostering trust in the system.
* Strengthening Election Integrity: The use of fingerprint-based fraud detection strengthens the overall integrity of elections. It helps in minimizing the chances of unauthorized individuals manipulating the system or attempting to undermine the fairness of the voting process. This promotes a level playing field for all candidates and parties involved.
* Combating Electoral Fraud: Electoral fraud can have a significant impact on the legitimacy of election results. Fingerprint-based authentication acts as a deterrent against various types of fraud, such as voter impersonation, ballot stuffing, and the use of fake identities. By implementing this system, the aim is to minimize the occurrence of fraudulent activities and ensure the accuracy of the election outcome.

**Chapter 2**

**Literature Survey**

We have refereed various IEEE Research papers and other Research papers also. We have learnt the working principle of various components and the practical implementation of the code.

The concept of the fingerprint sensor and the way in which the sensor works and how that sensor can be used for detecting frauds in the EVM is all explained in [1].

The concept of the working of a system which has the domain as the Internet of Things where they are building Fingerprint Based Biometric Voting Machine using Arduino. IoT is the system of interrelated computing devices, mechanical and digital machines, objects, and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. These concepts are explained along with the risks that are possible while doing the EVM using IoTs are mentioned in [2].

The concept of how the fingerprints is stored in the database and the way of giving immediate intimation about the vote casted by the voter to increase transparency in the system and the way of giving results immediately after the election process gets finished are proposed in [3].

The concept of feeding data using fingerprint sensors without creating data of the person multiple times and the concept of casting votes online while sitting in their comfortable place are proposed in [4].

**Chapter 3**

**Requirements**

**3.1 Software Requirements**

1. Operating System: Windows, Linux, or macOS.
2. Database Management System: MySQL, PostgreSQL, or MongoDB.
3. Fingerprint Recognition Algorithm: minutiae-based matching or pattern-based matching.
4. Fraud Detection Mechanisms: fingerprint template matching, anomaly detection, or biometric fusion.
5. Arduino uno IDE

**3.2 Hardware Requirements**

1. Arduino Uno: A microcontroller board with digital and analog input/output pins, a USB connection, and various components, used for programming and controlling electronic devices.
2. Fingerprint Module: A module used for verifying identity by enrolling, verifying, and identifying fingerprints, typically communicating through a UART interface with external devices.
3. 16x2 LCD: A liquid crystal display module that can display 16 characters per line and has two lines, commonly used in electronic devices, with command and data registers to control the display of characters and symbols.
4. DC motor:A DC motor is an electrical device that converts direct current (DC) electrical energy into mechanical motion or rotational movement. It operates based on the principles of electromagnetism, with a rotating armature or rotor interacting with a fixed magnetic field to produce torque.

**Chapter 4**

**System Design**

**4.1 Existing system**

The existing system for fingerprint-based fraud detection in a voting system might involve traditional paper-based voting methods where individuals cast their votes by marking their preferences on paper ballots. This system typically relies on manual verification processes, such as signature verification or ID checks, to detect fraudulent activities. However, these methods are susceptible to human errors and can be easily manipulated, leading to potential voting fraud.

**4.2 Proposed system**

The proposed system is a fingerprint-based fraud detection voting system that leverages biometric technology to enhance the security and integrity of the voting process. In this system, each eligible voter's fingerprint is enrolled and stored in a database before the election. During the voting process, voters' fingerprints are captured and compared against the enrolled fingerprints to verify their identity and eligibility to vote.

The proposed system utilizes advanced fingerprint recognition algorithms to ensure accurate identification and prevent fraudulent activities, such as multiple voting or impersonation. It may also incorporate additional security measures, such as encryption techniques, to protect the integrity and privacy of the biometric data.

**4.3 System Architecture**

The system architecture of a fingerprint-based fraud detection voting system typically consists of several components working together to ensure a secure and reliable voting process. Here are the key components:

Fingerprint Capture Devices: These devices capture the fingerprints of voters during the registration and voting phases. They can be specialized fingerprint scanners or integrated into electronic voting machines.

Database: A central database stores the enrolled fingerprints of eligible voters, along with their corresponding voter information. It provides a repository for efficient retrieval and matching of fingerprints during the voting process.

Fingerprint Recognition Module: This module contains algorithms and software that process the captured fingerprints and compare them with the enrolled fingerprints in the database. It performs biometric matching and verification to determine the identity and eligibility of the voter.

Voting Interface: This component includes the user interface through which voters interact with the system to cast their votes. It may be a touchscreen interface or a combination of physical buttons and displays.

Fraud Detection System: This system analyses the voting data and fingerprint patterns to detect any suspicious activities or anomalies that may indicate fraud, such as multiple votes from the same individual or mismatched fingerprints.

Security Measures: To ensure the integrity and confidentiality of the system, various security measures are implemented. These may include encryption of sensitive data, secure communication protocols, access control mechanisms, and audit trails for monitoring and tracking system activities.

Reporting and Result Generation: Once the voting process is complete, the system generates accurate and tamper-proof voting results based on the authenticated and verified votes. Reports and statistics can be generated for auditing and transparency purposes.

**Chapter 5**

**Conclusion**

The project "Fingerprint Based Fraud Detection voting system" was developed with the primary objective of creating an advanced Electronic Voting Machine (EVM) that incorporates fingerprint-based authentication. This innovative approach aimed to ensure a free and fair way of conducting elections, which forms the foundation of democratic countries like India.

By integrating biometric authentication, specifically fingerprint recognition, into the voting system, the project sought to provide a more efficient and secure method for casting votes. Fingerprint-based authentication adds an additional layer of trust and reliability to the voting process, as each person's unique fingerprint serves as a biometric identifier. This helps prevent fraud and impersonation attempts, ensuring that only eligible voters are able to participate in the election.

One of the notable advantages of the system is the online voting module, which allows voters to cast their votes from any location with internet connectivity. This feature not only enhances accessibility but also promotes convenience and flexibility for voters, eliminating the need to physically visit polling stations.

The use of fingerprint recognition technology in the voting system also strengthens the adherence to the fundamental principle of "one man, one vote." By linking each vote to a specific fingerprint, the system ensures that each voter can cast only one vote, further enhancing the integrity and fairness of the electoral process.

Moreover, the implementation of this system offers economic benefits. With the integration of biometric authentication, the need for physical voter identification cards or other forms of identification may be reduced, resulting in cost savings and increased efficiency in the overall election management.

In summary, the "Fingerprint Based Fraud Detection voting system" project aimed to create a technologically advanced voting system that guarantees secure, fraud-free, and trustworthy elections. By leveraging fingerprint recognition and online voting capabilities, the project aimed to enhance accessibility, ensure the integrity of the voting process, and reinforce the democratic principles of fair representation and one-person, one-vote.

**References**

Research papers:

1. Rudrappa B. Gujanatti1 , Shivaram N. Tolanur2 ,Murughendra S. Nemagoud3 , Shanta S. Reddy4 , Sangameshwar Neelagund5 , Assistant Professor 1 ,Electronics and Communication Department K. L. E. Dr. MSSCET, Belgaum, India1,2,3,4,5, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV4IS050948, Vol. 4 Issue 05, May- 2015 -“A Finger Print based Voting System”. Available: https://www.ijert.org/research/a-finger-print-based-voting-system-IJERTV4IS050948

2. Khadija Hasta1 ,Aditya Date2 ,Aparna Shrivastava3 ,Prajakta Jhade4 , S. N. Shelke5 , Computer Engineering (SPPU), Pune, India1,2,3,4,5 , Published in 2019 International Conference on Advances in Computing, Communication and Control (ICAC3). -“Fingerprint Based Secured Voting”. Available: <https://ieeexplore.ieee.org/document/9036777>

3. Mohammed Khasawneh1 ,Mohammad Malkawi2 ,Omar Al-Jarrah3 ,Laith Barakat4 ,Thaier S. Hayajneh5 ,Munzer.S.Ebaid6 , College of Engineering, University of Illinois, Urbana- Champaign, Urbana,IL,USA1 ,AIM Wireless2 , Jordan University of Science and Technology, Irbid, Jordan3,4 , School of Information Systems, University of Pittsburgh, Pittsburgh, PA, USA5 , King Abdullah II Design and Development Bureau, Amman, Jordan6 , Published in 2008 5th International Symposium on Mechatronics and Its Applications -“A biometric-secure e-voting system for election processes”. Available: <https://ieeexplore.ieee.org/document/4648818>

4. Oluwatosin Adesua, University of Ibadan, March 2015, Thesis for: B.Sc. (Hons) - “Online voting system with biometric authentication for ui elections”. Available:https://www.researchgate.net/publication/310597883\_ONLINE\_VOTI NG\_SYSTEM \_WITH\_BIOMETRIC\_AUTHENTICATION\_FOR\_UI\_ELECTIONS