M.KUMARASAMY COLLEGE OF ENGINEERING
NAAC Accredited Autonomous Institution
Approved by AICTE & Affiliated to Anna University
ISO 9001:2015 Certified Institution
Thalavapalayam, Karur – 639 113.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

18ECP105L-MINOR PROJECT- III
SECOND REVIEW

ENHANCING SECURITY IN VOTING SYSTEM

YEAR/SEMESTER-III/V

BATCH NUMBER-02

DATE-06.09.2024

PRESENTED BY

1. ASWIN A(927622BEC019)
2. BALAGURU MADHAVAN G(927622BEC021)
3. BALAMURUGAN R(927622BEC022)
4. GOKUL K(927622BEC056)

GUIDED BY

Mrs.P.Yuvarani M.E.,

ABSTRACT

Voting is everyone’s right whether he or she who are age of 18 and above has the right to vote for our political leaders. In India voting system plays a major role.Over 40 to 50 years before paper ballot voting system is used but sometimes were prone to fraudulent voting with pre-filled fake paper ballots. In order to avoid the paper ballot voting system, the E-voting system (EVMs) is used had brought in the year of 1977 which reduces the time of counting the vote to enable faster announcement of results and eliminate the malpractices. But, in this E-voting system some malpractices taken place. To solve this problem permanently, our project aims to provide a secure and user-friendly online voting system with created database and collected fingerprints are used in this web-based online voting system to provide high performance and high security and which lowers the number of fake votes.

Keywords: Paper ballot Voting system, E-voting system, high performance, high security.

INTRODUCTION

- This project aims to develop the E-voting system into the biometric voting system that leverages fingerprint authentication to verify voter identify whether he/she has voted to prevent from malpractices.
- The system utilizes the MFS110(L1) fingerprint scanner which is used to scan the fingerprints and safely stored in PostgreSQL database and used verify the voters during the election process.
- This system is capable of handling large database making it adaptable for use in elections with large populations. By integrating MFS110(L1) and PostgreSQL this solution delivers a secure, reliable and transparent voting process, greatly enhancing the integrity of elections and it aims to contribute to more equitable and transparent electoral results.

MFS110(L1) FINGERPRINT SCANNER

POSTGRESQL DATABASE LOGO

LITERATURE SURVEY

1.	K.SELVI, 1/3,7TH STREET, GANDHINAGAR,VELAYUTHAMPALAYAM, PINCODE-639117	Points discussed on the use of Internet to control the home appliances from anywhere	9987124574	K. Selvi.

EXISTING METHOD

- Fingerprint-based biometric smart electronic voting systems using Arduino have been proposed as a way to improve the security and efficiency of elections.
- These systems use fingerprint sensors to identify voters and allow them to cast their votes electronically. Fig:1.a. Fingerprint voting system using Arduino Another study found that a fingerprint-based voting system using Arduino was able to resist a variety of attacks, including voter impersonation, coercion, and vote buying.
- The system was also able to provide a transparent audit trail, which could be used to verify the integrity of the election results. However, there are also some challenges associated with fingerprint-based voting systems. One challenge is that fingerprint sensors can be fooled by fake fingerprints.

- Another challenge is that fingerprint data can be used to track individuals, which could raise privacy concerns. Here are some additional details about the experimental results of fingerprint-based biometric smart electronic voting systems using Arduino.
- The accuracy of these systems is typically very high, with FARs and FRRs of less than 1%. The voting process is usually very fast, with voting times of less than 10 seconds per voter. These systems can be resistant to a variety of attacks, including voter impersonation, coercion, and vote buying[4]. The disadvantage of fingerprint voting system is that data can be hacked easily and it can’t properly detect the voting whether it is true or false.

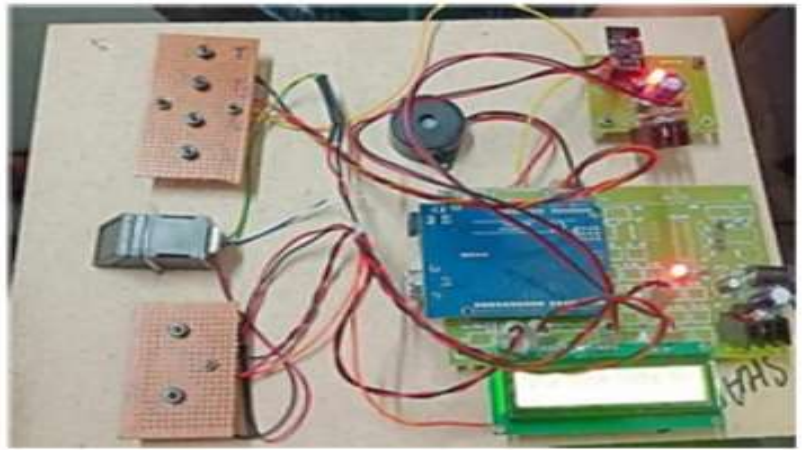
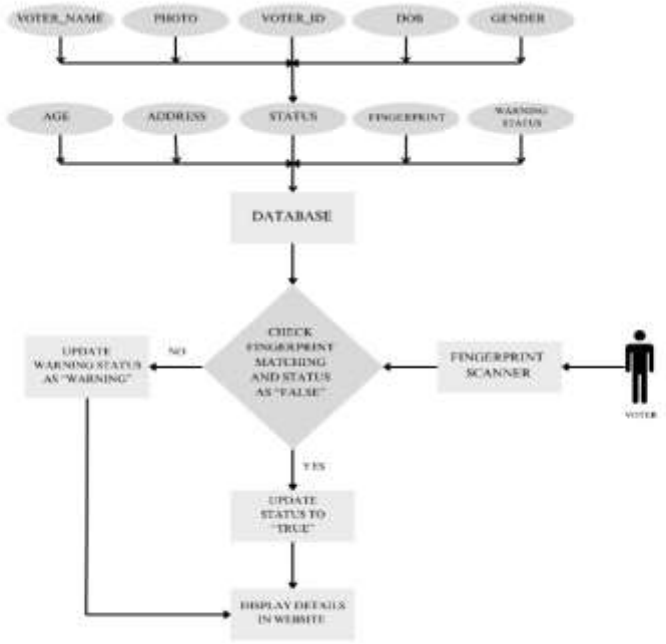


Fig:1.(a) Fingerprint voting system using Arduino

PROPOSED METHOD

This block diagram illustrates the steps involved in verifying a voter's fingerprint and ensuring that each voter can only cast a single vote. Here's a breakdown of the entire voting process which is given below in fig.

BLOCK DIAGRAM



RESULT & DISSCUSSION

RESULTS

Enhancing security in voting systems is critical to ensuring the integrity of elections, preventing fraud, and protecting voter privacy. There are several methods and technologies that can be employed to strengthen the security of voting systems. Here are the results and potential benefits of various strategies aimed at enhancing voting security system

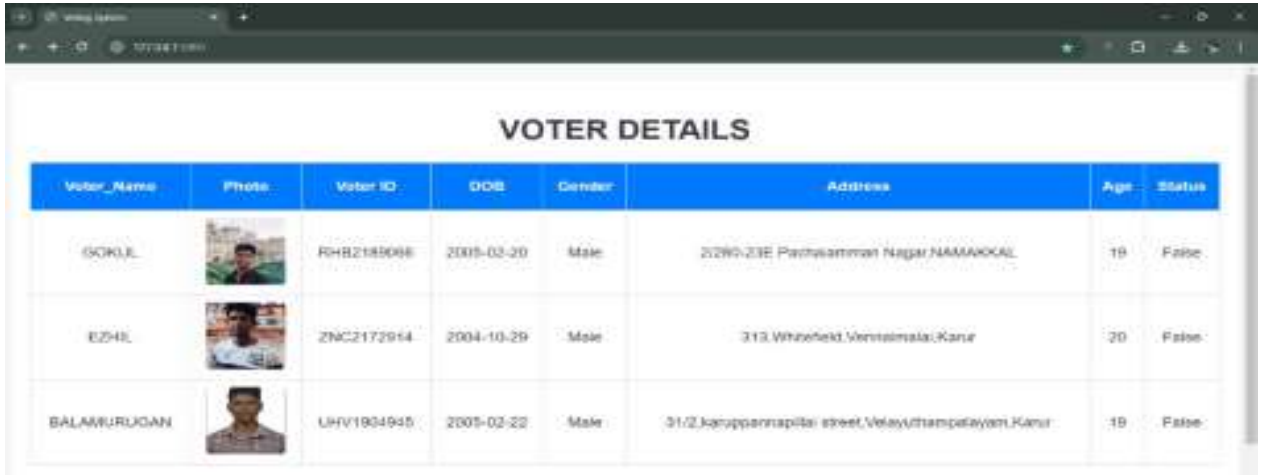


Fig.1 Inserting web page details in PostgreSQL Database

Fig:5.2 Inserting counts for advance information in PostgreSQL Database

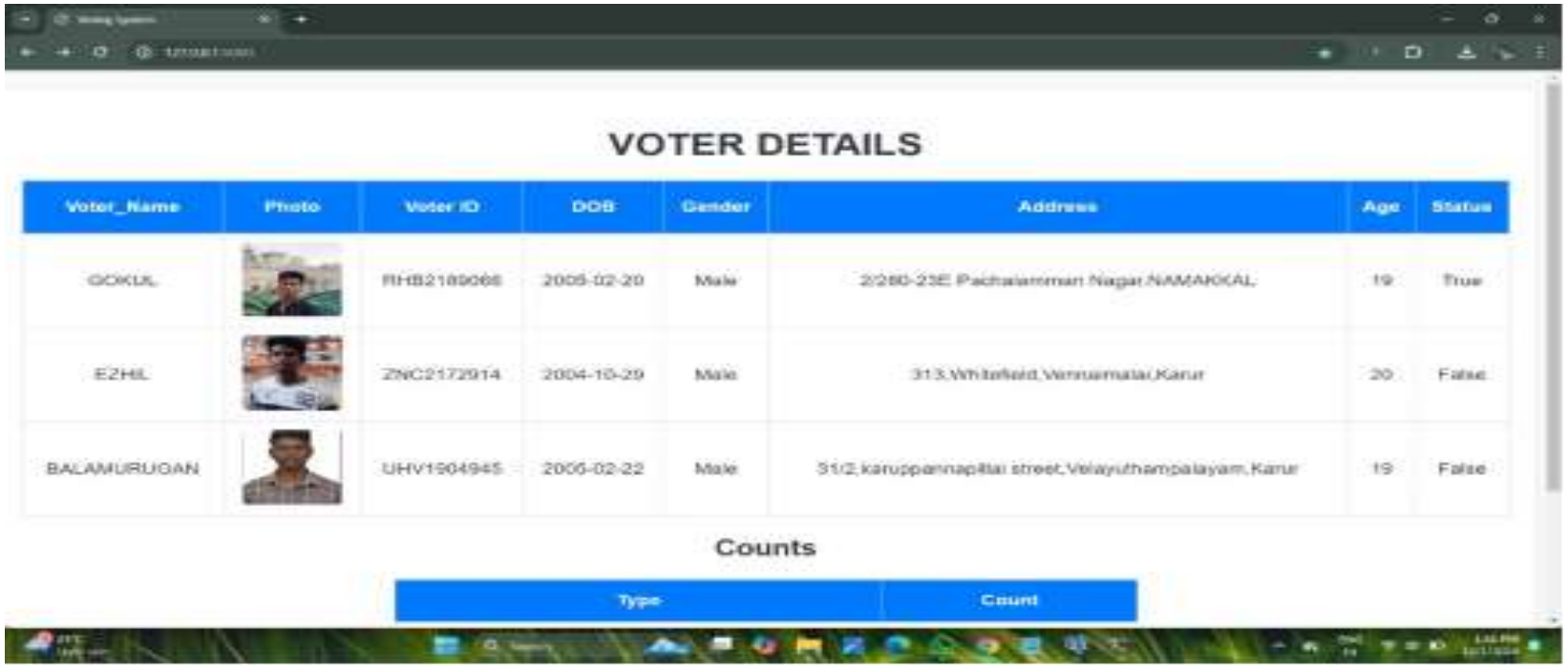


Fig:5.3 After insertion the fingerprint process status updated to true in PostgreSQL Database

Fig:5.4 After insertion the fingerprint process status updated to true and count also updated in PostgreSQL Database

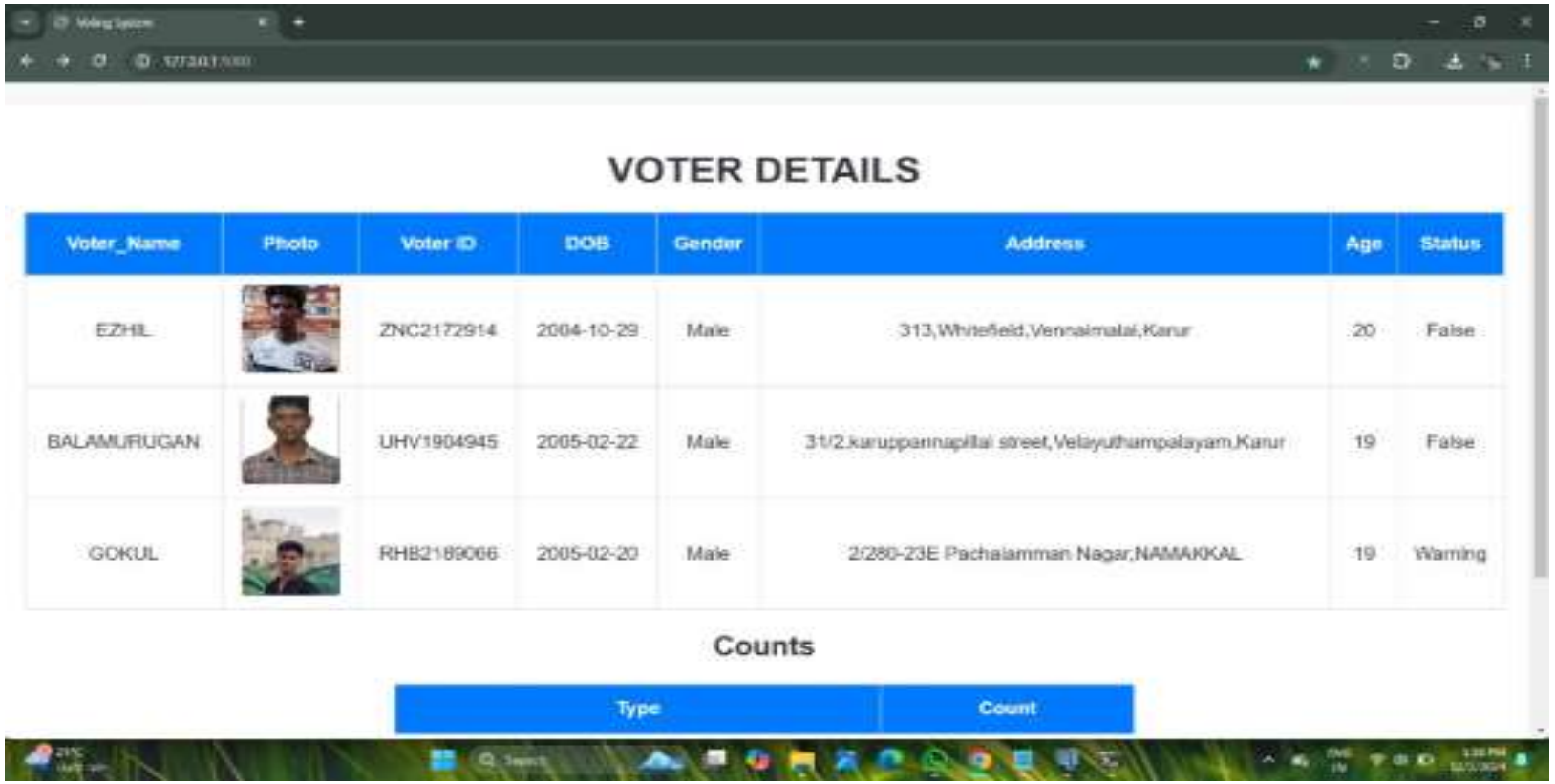
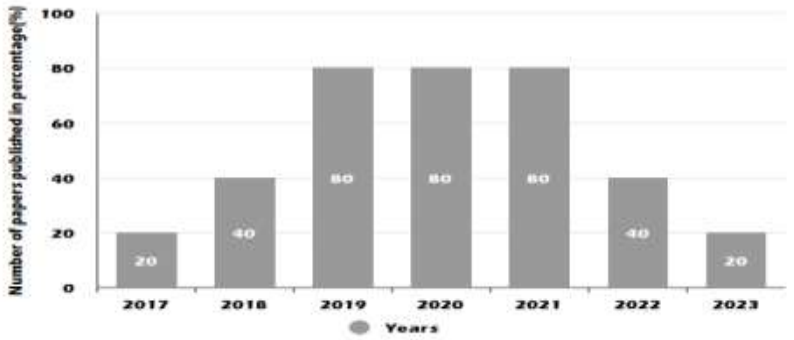


Fig:5.5 If he or she place fingerprint more than one time the status updated to warning in PostgreSQL Database

Fig:5.5 If he or she place fingerprint more than one time the status updated to warning and count also updated in PostgreSQL Database

DISCUSSIONS



As per the research taken which is related to biometric voting systems over a period of past seven years, from 2017 to 2023. The number of papers were published on biometric-based voting systems has shown a gradually increasing trend over the years, with a notable rise from 2018 onwards. The highest number of papers were published in 2019, 2020, and 2021, indicating a peak period of research interest in this domain during these years. The surge in publications from 2018 to 2021 could be attributed to increased awareness and interest in biometric voting system and its potential applications in voting systems. This technology finds application across various domains, offering solutions that enhance transparency and security [6].

CONCLUSION

In conclusion, the exploration and implementation of fingerprint-based e-voting systems present a significant advancement in addressing the longstanding challenges faced by traditional electoral processes. By harnessing the unique and secure nature of fingerprint technology, these systems offer unparalleled security, transparency, and trustworthiness.

Despite these challenges, the potential benefits of fingerprint-based e-voting systems are undeniable. Moving forward, continued research, collaboration, and innovation are essential to overcome obstacles and realize the full potential of fingerprint technology in electoral processes[8].

REFERENCES

1. Lee JH. Systematic approach to analysing security and vulnerabilities of blockchain systems. Doctoral dissertation, Massachusetts Institute of Technology; 2019.

2. Zhang S, Wang L, Xiong H. Cha integrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. Int J Inf Secure. 2020;19:323–41.

3. Tyagi AK, Fernandez TF, Aswathy SU. Blockchain and Aadhar based electronic voting system. In: 2020 4th international con conference on electronics, communication and aerospace technology (ICECA); 2020 (pp. 498–504). IEEE.

4. CH Srilatha1, Dwaraka Chand Venigalla1, Sai Kaushik Tuttagunta1, Nallagatla Akshay1, Myasar Mundher adnan2, B Rajalakshmi3, H Pal Thethi4 and Ashwani Kumar5: Fingerprint-based biometric smart electronic voting machine using IoT and advanced interdisciplinary approaches. E3S Web of Conferences 507, 01037(2024).


Thank
you!