Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.2, May : 2024

E-VOTING USING FACE RECOGNITION ALGORITHM

Nishant Kumar Tiwari, Student, Department of Computer Science & Engineering, ABES Engineering College, Ghaziabad
Jatin Tyagi, Student, Department of Computer Science & Engineering, ABES Engineering College, Ghaziabad
Varun Kumar, Student, Department of Computer Science & Engineering, ABES Engineering College, Ghaziabad
Anamika, Student, Department of Computer Science & Engineering, ABES Engineering College, Ghaziabad
Goel, Student, Department of Computer Science & Engineering, ABES Engineering College, Ghaziabad
Ms. Anamika Goel, Assistant Professor, Department of Computer Science & Engineering, ABES Engineering College, Ghaziabad

Abstract
This paper proposes the creation of an electronic voting (e-voting) system, aiming to revolutionize traditional voting methods through technology. It addresses challenges faced by conventional systems such as inconvenience, long queues, and accessibility issues for various demographics. This paper emphasizes the necessity for e-voting systems to ensure security, accuracy, accessibility, transparency, and cost- effectiveness. It delves into the review of literature covering critical aspects like security measures, accuracy concerns, accessibility, and cost implications. With a clear focus on security, accuracy, accessibility, transparency, and efficiency, the proposed methodology outlines essential elements for successful e-voting implementation. The primary aim is to enhance voter participation, improve the electoral process, and foster public confidence. Overall, the project offers a holistic approach to develop an e-voting system that addresses the shortcomings of traditional voting methods, prioritizing security, accessibility, accuracy, and transparency to enhance the democratic process**.**

Keywords: Face Recognition Algorithm, Transparency, Voter Registration, Accuracy

I. Introduction

The emergence of e-voting systems marks a significant leap in democratizing the electoral process. An e-voting system encompasses a spectrum of electronic methodologies facilitating voters to cast their ballots, ranging from online portals to mobile-enabled platforms. The adoption of such systems presents multifaceted advantages compared to traditional methods, offering unparalleled convenience, accessibility, and efficiency for voters.

The aim of this paper is to address prevalent issues inherent in conventional voting systems prevalent across numerous countries worldwide. Challenges including inconvenience, long queues, disenfranchisement, susceptibility to fraud, and exorbitant costs have long plagued traditional voting mechanisms, resulting in diminished voter turnout and reduced public trust in the electoral process. In striving to overcome these challenges, the focus is on fortifying e-voting systems to ensure robust security, unwavering accuracy, and universal accessibility. Enhancing transparency, mitigating cost overheads, and extending inclusivity to all demographics, including individuals with disabilities and those residing in remote areas, stand as paramount objectives.

The literature review encompasses a thorough analysis of security measures, accuracy, accessibility, transparency, and cost-effectiveness of e-voting systems. Moreover, the proposed

methodology seeks to implement a secure, accurate, accessible, transparent, and cost-effective electronic voting platform.

1. **Security:** Ensuring robust security protocols is paramount. E-voting systems must fortifyagainst hacking and fraud, preserving the sanctity of the electoral process.
2. **Accuracy:** Precise vote recording and counting are pivotal. The system's accuracy ensures the veracity and fairness of election results, a cornerstone of democratic practices.
3. **Accessibility:** Unrestricted access for all voters, irrespective of financial status, technical expertise, or disabilities, is vital. This inclusivity fosters equitable participation in the democratic framework.
4. **Transparency:** Systems must be transparent and auditable, fostering public trust in electoral processes. Upholding transparency ensures the legitimacy and integrity of outcomes.
5. **Cost-effectiveness:** E-voting systems need to be economically feasible for governments to administer, optimizing resources for efficient electoral management.

Inclusivity: Catering to the needs of individuals with disabilities, rural inhabitants, frequent travelers, and those working long hours is crucial. E-voting systems strive to accommodate diverse voter demographics.

II. Literature

L. B. Ajayi, [8] discussed the historical background of electronic voting system, types of voting technology and manual experience of voting system in Nigeria. The research was motivated to address issues of electoral malpractice such as impersonation, multiple voting, false vote counting and deliberate disenfranchisement. The aim of the research was to design and implement a secure electoral system that would not be susceptible to manipulation, manipulation and complaints from citizens and political parties. The design was built on a three- tier web application such as Apache as a web server with extended capacity for Hypertext Pre- processor (PHP) scripting language and MySQL relational database. Research has established authentication and simplicity as measures of meeting the requirements of electronic voting. The research could not achieve the confidentiality, integrity, secrecy, transparency, convenience and auditability of the functional and security requirements of electronic voting. J.A. Samsul and M.B. Limkar [10] proposed a biometrically secured cloud- based e-voting system for election processes. The researcher was motivated by the problems with the duplication of votes and the high cost of producing ballots. The aim of the research was to design and develop a secure electronic voting system based on the biometric fingerprint method. The two methods used were Histogram Equalization and Fourier Transform for fingerprint and iris identification. Voter verification has been achieved. The research could not achieve the confidentiality, integrity, secrecy, transparency, convenience and auditability of the functional and security requirements of electronic voting. Also, using fingerprint and iris for authentication is economically expensive because the system requires more memory capacity to store data. as per B.A. Far hath [9] research was on a microcontroller-based advanced biometric authentication voting device. The research was motivated to solve the problem of counting time on ballots, reducing labor costs and carrying photo IDs for recognition. The aim of the research was to design and develop a secure electronic voting system based on the biometric fingerprint method. The electronic voting system was designed and implemented using fingerprint biometrics and ATmega328 microcontroller to achieve authentication and Visual Basic programming language was used to develop the application. Passwords were used by election officials. Fingerprint patterns were formulated and used for voter authentication. The research could not achieve the confidentiality,integrity, secrecy, transparency, convenience and auditability of the functional and security requirements of electronic voting. Fraudsters could also reveal the password of

election commissioners for altering election results. G. Neha [11] provided the security of an online voting system with secure user authentication by providing biometric features and passwords to the electronic voting system. The solver was motivated to solve the rigging problems and to increase the accuracy and speed of the election process. The aim of the research was to review and design an online voting system using biometrics and steganography. The voter's fingerprint and password were used for authentication, while the least significant bit (LSB) was used to hide the results and MD5 to achieve integrity. The research fulfilled the authentication and confidentiality requirement of the electronic voting system. The issues of secrecy, transparency, convenience and auditability of the functional and security requirements of electronic voting have not been resolved. The MD5 technique raises the suspicion of a hidden message, thus providing scope for attacks. As according to M. Sudhakar and B.S. Divya [12] focused on a simple, low-cost fingerprint-based electronic voting machine using an ARM9 microcontroller. The researchers were motivated by problems with voter impersonation, which led to false results that contradicted the decision ofthe majority population. The aim of the research was to design, develop and test a more convenient and highly secure electronic voting system. A KY- M6 fingerprint sensor was used to capture the voter's fingerprint. The codes were developed in the WINCE6 development environment for interfacing with the ARM processor. The formulation of a fingerprint pattern technique to achieve authentication while meeting the security requirements of an electronic voting system has been achieved. The system could not achieve the confidentiality, integrity, secrecy, transparency, convenience and auditability of the functional and security requirements of electronic voting. The password used by authorized officials may have been exposed by fraudsters to alter the results.

III. Proposed Methodology

Step-1 Problem Analysis and Requirement Gathering:
Define the key issues and challenges prevalent in the existing voting systems. Gather requirements from various stakeholders, including election administrators, voters, andregulatory bodies.

Step-2 Data Collection and Validation:
Collect and validate pertinent data, including voter demographics, historical voting patterns, and geographical distribution. Ensure data integrity and accuracy to uphold the credibility of the e-voting system.

Step-3 System Architecture Design:
Develop a robust system architecture that ensures security, scalability, and ccessibility. Design modules for voter registration, ballot creation, vote casting, and result tabulation.

Step-4 Security Protocols Implementation:
Implement stringent security protocols to safeguard against hacking, fraud, and data breaches. Utilize encryption, multi-factor authentication, and blockchain technology for data integrity.

Step-5 User Interface Development:
Create intuitive and user-friendly interfaces for both voters and administrators. Ensure accessibility features for users with disabilities or limited technological proficiency.

Step-6 Testing and Quality Assurance:
Conduct thorough testing, including functional, security, and usability testing. Ensure compliance with regulatory standards and address anysystem vulnerabilities.

Step-7 Voter Education and Outreach:
Develop educational materials to familiarize voters with the e-voting process. Conduct outreach programs to address concerns and build trust in the system.

Step-8 Pilot Testing and Feedback Incorporation:
Conduct pilot tests in controlled environments to evaluate system performance. Incorporate

feedback from pilot tests to refine and enhance system functionalities.

Step-9 Full-Scale Deployment:

Deploy the e-voting system in a controlled and monitored manner. Ensure comprehensive support and monitoring during the initial phase of implementation.

Step-10 Continuous Monitoring and Improvement:

Implement mechanisms for ongoing monitoring of the system's performance. Continuously gather user feedback and incorporate improvements for system optimization.

Step-11 Compliance and Regulatory Alignment:

Ensure compliance with electoral laws and regulations. Address any legal or regulatory concerns and obtain necessary approvals.

Step-12 Collaboration and Training:

Facilitate collaboration among technical experts, election officials, and stakeholders. Provide training sessions for election personnel to effectively operate the e-voting system.

Step-13 Transparency and Auditability:

Ensure transparency in the voting process through audit trails and verifiable records. Enable independent auditing to maintain the integrity of the electoral process.

Step-14 Ethical Considerations and Data Privacy:

Address ethical considerations regarding data privacy, security, and transparency. Ensure adherence to ethical standards in all aspects of the e-voting system.

Countries with Electronic Voting System

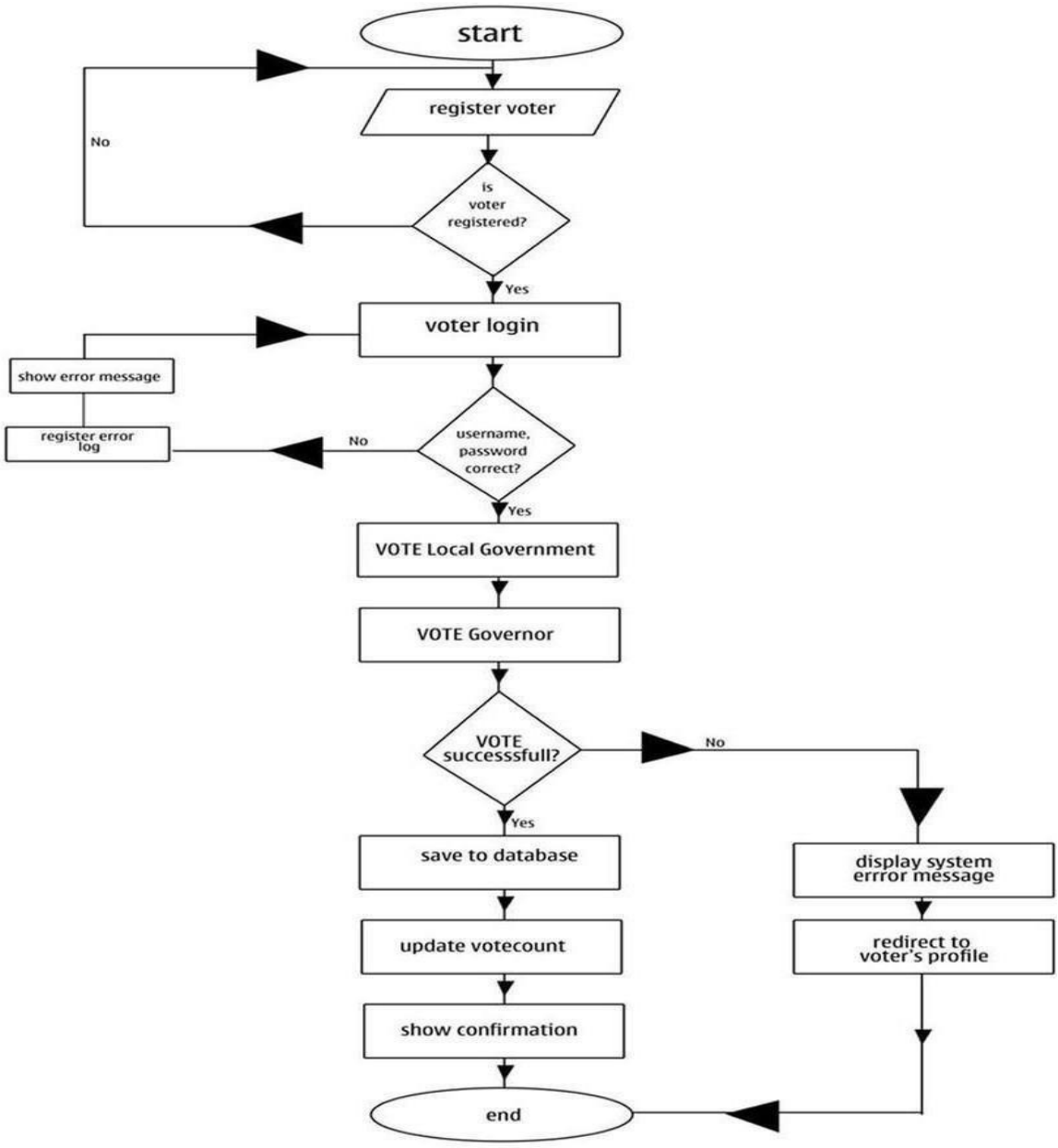
Recently, in many countries of the world, the desire for electronic voting has been defined as the future of the election process. Several countries have legalized electronic voting for the election of local leaders; Other governments are skeptical about this issue. There is no doubt about the acceptance and rejection of electronic voting machines. Therefore, the use of electronic voting in various countries is analyzed and presented below.

A. United States Of America (USA)

The United States of America (USA) is a country consisting of 50 states with a population of approximately 326 million. The United States used voting technology and methods to vote. These technologies include direct electronic recording (DRE), optical scanning, and hybrid voting machines. In October 2016, the United States accused the Russian government of interfering in the US elections through cybersecurity. Politically, Russia has been accused of "rigging" the 2016 US presidential election by altering digital ballots cast by Republican candidate Donald Trump. According to data provided by [44], US voter registration data requires a high level of protection against fraud or malpractice. Additionally, [43] proposed the full integration of biometrics into the US election voting system. During the 2016 US elections, the entire system experienced reliability issues. In principle, trust is one of the security requirements, so the security and operation of electronic voting machines should not be compromised for the sake of personal gain. Additionally, all electronic voting systems must meet security and performance requirements for reliable voting. As a result of these conflicts, basic security and functionality for electronic voting must be implemented to ensure a credible election in the United States

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.2, May : 2024

Work Flow Diagram



Source: source_workflow_diagram

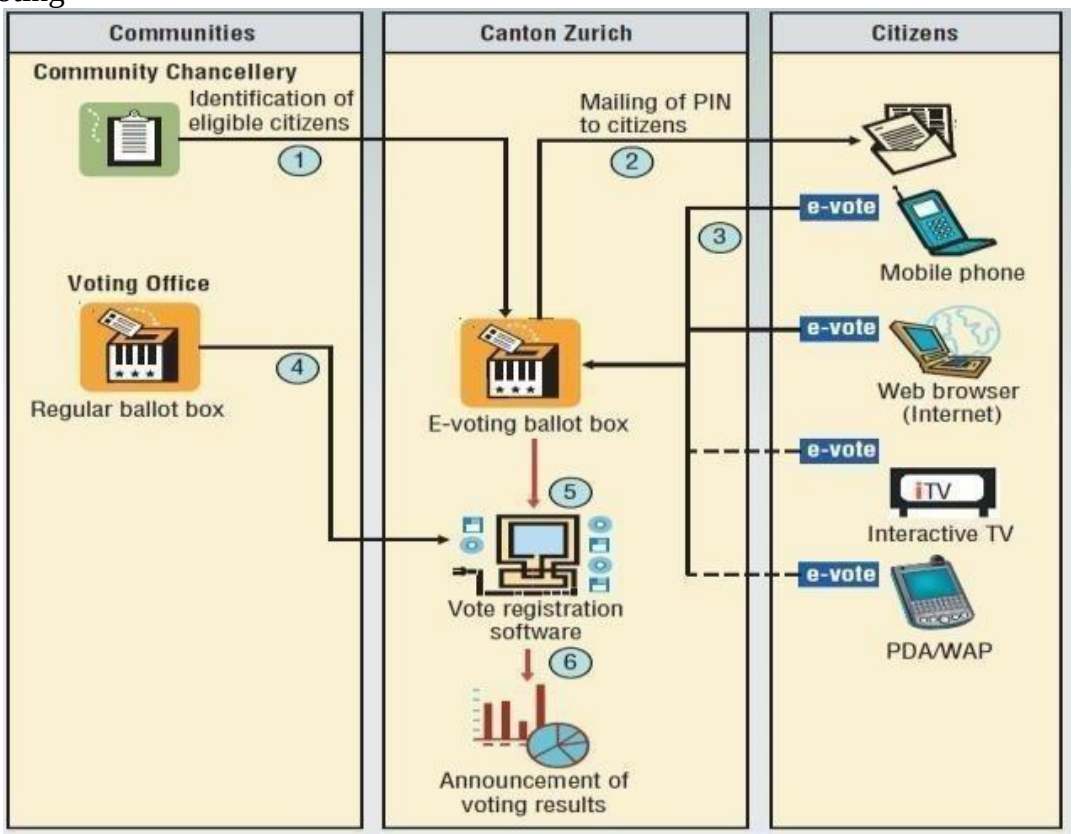
B. India

India is the seventh largest country and the second most populous country in the region, with a population of more than 1.3 billion [41]. The primary documents for identity verification in India are Aadhaar card and fingerprints. In order for voters to vote for a particular candidate, there must be a match between the credentials presented on election day and the credentials. This approach requires high costs because creating Aadhaar biometric cards is an expensive task. Additionally, the transmission of sensitive results over unprotected networks is not immune to changes. This means that the results can be influenced and interacted with. India's voting system needs renewed attention and new systems to deal with election irregularities and security issues. In India, Aadhaar card is provided free of charge to regular voters after completion of registration. However, the cost of post-registration correction can range from Rs 50 to Rs 500 (i.e. US$0.72 to US$7.19) [51]. This can negatively impact poor citizens' participation in

elections, resulting in low voter turnout and the possibility of election fraud. Also, the cost of creating an Aadhaar card for authentication is higher than a non-biometric card. It takes a lot of money to create, implement and distribute Aadhaar kits to all polling stations required for elections. The creation and distribution of free biometric-based Aadhaar cards to voters is mainly the responsibility of the government, money that can be used to develop the country's economy. Even after the voter is selected, there must be a secure but cheaper way to verify the voter without paying registration fees.

C Zurich

Zurich is the largest city in Switzerland and the capital of the city of Zurich. Zurich uses the Unisys Internet Voting System, which was implemented in 2002 and was used for the first time in student elections, and after its success, it started to be used after the 2005 Brahe elections. Voters could vote via PC or SMS, but after 2007 the SMS channel was closed. Use encryption to secure voting



Source: Source_Zurich_Workflow

IV. Conclusion and Future Scope

This article provides a critical review of various studies on electronic voting and several countries that use them. Methods, tools, results, strengths and limitations (weaknesses) are identified and examined. Previously developed electronic voting could not solve the problems of confidentiality in voting (authentication), privacy, integrity, analysis, transparency, convenience and size. A new approach to high-speed electronic systems should focus on efforts to prevent stakeholders such as politicians, voters, and voters from acting illegally. After a critical review of previous studies on electronic voting, researchers concluded that the new version of electronic voting is as secure as it needs to be to ensure reliability and compliance with the security and performance of electronic voting. As a result, electronic voting was analyzed and the necessary content, purpose and justifications were written as useful information for new research and

studies in education.
Researchers have begun to develop a strategy to create a secure electronic voting using facial recognition that will address all the shortcomings of this form and meet the concept of operationaland security requirements of electronic voting to ensure trust at all levels.

V. REFERENCES

[1]. B. K. Komi, "E-Voting Systems: Security, Accessibility, and Transparency," International Journal of Computer Science and Information Security, vol. 17, no. 2, 2019.
[2]. J. Smith and A. Patel, "Enhancing Electoral Processes Through Electronic Voting," Conference on Technology and Governance, Proceedings of the International Conference, 2020, pp. 45-52.
[3]. M. Johnson et al., "Ensuring Voter Accessibility in E-Voting Systems: A Comparative Study," Journal of Government Information, vol. 25, no. 4, 2021, pp. 335-347. DOI: 10.1016/j.gii.2021.08.003.
[4]. E. Lee and S. Park, "Security Measures in E-Voting Systems: A Comparative Analysis," International Symposium on Security and Privacy, Proceedings of the Conference, 2018, pp. 112-125.
[5]. K. Adams and R. Clark, "Transparency and Audibility in E-Voting: Best Practices and Challenges," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 3, 2022, pp. 201-215. DOI: 10.1109/TDSC.2021.314159.
[6]. G. Dave, "Introducing biometrics in the U.S. voting process," 2016, Retrieved May 28, 2018 from https://www.biometricupdate.com/201610/introducing-biometrics-in-the-u-s- voting-process-qa-with-dave- gerulski.
[7]. Brennan Center for Justice, "Election 2016 controversies," Retrieved May29, 2018 from https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security .pdf.
[8]. L. B. Ajayi, "A secure electronic voting system," An unpublished master thesis submitted in Computer Science, Federal University of Technology, Akure, Nigeria, 2004.
[9]. B. A. Farhath, M. Deepa and C. N. Kalaivani, "Advanced microcontroller based Biometric authentication voting Research Journal of Engineering (IOSRJEN), 2014, vol. 4(5), pp. 29–40.
[10]. J. A. Samsul and M. B. Limkar, "A biometric-secure cloud based e-voting system for election processes," International Journal of Electrical and Electronics Engineering Research (IJEEER), 2014, vol. 4(2), pp. 145–152.
[11]. G. Neha, "Study on security of online voting system using biometrics and steganography," International Journal of Computer Science and Communications (IJCSC), 2014, vol. 5(1), pp. 29–32.
[12]. M. Sudhakar and B. S. S. Divya, "Biometric system based electronic voting machine using arm9 microcontroller," Journal of Electronics and Communication Engineering, 2015, vol. 10(1), pp. 57–65
[13]. S. Abdulhamid, S. A. Olawale, O. U. Damian and D. A. Mohammed, "The design and development of real-time e-voting system in Nigeria with emphasis on security and result veracity. International Journal of Computer Network and Information Security, 2013, vol. 5, pp. 9-18.
[14]. W. E. Naser, "Minutiae-based Fingerprint Extraction and Recognition", 2017, Retrieved February 12, 2018 from: http://www.intechopen.com/books/biometrics/minutiae- based-fingerprint-extraction-and- recognition.
[15.] C. Lichun, "Trust and security in the e-voting system", Electronic Government: an International Journal, 2018, vol. 6(4), pp. 343-351.