



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

Facial Recognition Services for E-Voting System by Using Block Chain Technology

V.S. Kharanstephen*¹, P. Chandru*², B. Gokulnath*³, S. Avinash*⁴, Mrs. Anusuya. C*⁵

Department of Computer Science Engineering, Mahendra Institute of Technology, Mallasamudram, Namakkal, Tamilnadu, India

Assistant Professor, Department of Computer Science Engineering, Mahendra Institute of Technology, Mallasamudram, Namakkal, Tamilnadu, India

ABSTRACT: In this system a Face Detection and Recognition system (FDR) used as an Authentication technique in systematic voting, which one of electronic is voting types, is proposed. Web based voting allows the voter to vote from any place in state or out of state. The voter's image is captured and passed to a face detection algorithm (Eigenface or Gabor filter) which is used to detect his face from the image and save it as the first matching point. The voter's National identification card number is used to retrieve and return his saved photo from the database of the Supreme Council elections (SCE) which is passed to the same detection algorithm (Eigenface or Gabor filter) to detect face from it and save it as second matching point. The two matching points are used by a matching algorithm to check wither they are identical or not. If the results of the matching algorithm are two point match then checks wither this person has the right to vote or not. If he has right to vote then a voting form is presented to him.

KEYWORDS: Voting, Elections, Democracy, Application, Blockchain, Decentralized, E-voting, Voter Privacy, Face Recognition.

I. INTRODUCTION

Face Biometric based system is a voting system in which the election data is recorded, stored and processed primarily as digital information and it needs to address, obtain, mark, deliver, and count ballots via computer. Therefore voter identification and authentication techniques are essential for more secure platform mechanisms to overcome vulnerabilities of the client used by the voter to cast her vote. Security can be achieved using some of techniques of electronic voting such as Guidelines, only need to develop a list of instructions and then send it via email or put it on the election web page; Bootable CD, approach to overcome the secure platform problem was proposed by Otten (2005). She recommended developing a special voting operating system based on Knoppix. It is an operating system based on Debian that is designed to be booted and run directly from a CD or DVD; Smart Cards as Observers, in which an observer is a manipulation resistant piece of hardware which is owned by the voter. The idea is that the observer is not allowed to directly communicate with the Internet. All the communication needs to be forwarded by the voter; Code Sheets, the idea of code sheets is that the voter gets a piece of paper together with the general election information via post where each candidate or each party is linked to a particular code.

Now, in order to cast a voter the voter does not click on the candidate or party of her choice but enters the corresponding code; Trusted Computing, the idea is to use an appropriate security architecture based on a security kernel and on Trusted Computing elements. Such a solution is the only one that could efficiently overcome malicious software on the voting casting device as well as potential malicious voters installing malware on purpose on their device. However, currently, there are still open problems with Trusted computing itself and it is not widespread enough; Individual Verifiability, the idea is that you use one software to prepare a voter and a second one to verify that the vote has been properly prepared (encrypted).

Plus, you can also do the verification with an offline tool In this research, we proposed an authentication technique using a Face Detection and Recognition system in Face Biometric based to achieve the rules of Supreme Electoral Council as follow: Only eligible persons vote, No person gets to vote more than once, the vote is secret, and each (correctly cast) vote gets counted and to achieve the aims of Face Biometric based as follow: increase participation, lower the costs of running elections, and improve the accuracy of results. In general, an FDR system starts by

Interfacing with an image source for grabbing facial images, Automatic detection or manual selection of human face may be found within the scene, Manipulate (create, add, delete) a database of faces, Launching the recognition process by comparing the face previously detected with the database's faces.

II. LITERATURE REVIEW

TITLE: A SECURE END-TO-END VERIFIABLE INTERNET-VOTING SYSTEM USING IDENTITY-BASED BLIND SIGNATURE AUTHOR

NAME: MAHENDER KUMAR

DESCRIPTION:

End-to-end (E2E) verification allows voters to confirm that their votes are recorded as they intended and the general public to confirm that the system has accurately tallied all of the recorded votes. The security of the E2E verifiability-based Internet voting systems faces numerous difficulties, with security ranking as the most significant. In order to analyze the e-voting system and formalize its security needs, a number of E2E voting systems have been discussed over the past ten years. This article introduces an E2E verifiable internet voting system that gives voters mobility and enables them to covertly cast their ballots on public computers while enjoying the advantages of early voting. The suggested technology makes use of the voter's distinctive identification and biometric characteristics to help the electoral process globally. We suggest a brand-new identity-based blind signing system that guarantees the voter's privacy. We use the Boneh-Lynn-Shacham short signature technique, which protects the confidentiality of votes while using a small ballot size. The technology gives each voter a digital witness that allows them to verify that their vote was recorded as they intended and the general public to verify that all recorded ballots was correctly counted. Under the well-known elliptic curve discrete logarithm and gap Diffie-Hellman assumptions, the proposed system achieves privacy.

TITLE: WE VOTING: BLOCKCHAIN-BASED WEIGHTED E-VOTING WITH VOTER ANONYMITY AND USABILITY

AUTHOR NAME: ZIKAI WANG

DESCRIPTION

E-voting is essential for ensuring and advancing social justice and democracy. However, traditional e-voting systems rely on a centralised structure, which causes a crisis of confidence in the results of the vote-counting. Researchers have developed blockchain to enable decentralised e-voting in response to this issue, but doing so also raises additional problems with regard to flexibility, privacy, and usability. WeVoting, which offers weight based flexibility with strong anonymity and improves usability by inventing a voter-independent on-chain counting mechanism, is the solution we suggest in this work. To accomplish voting anonymity with weight, we specifically use distributed ElGamal homomorphic encryption and zero-knowledge proof. Additionally, WeVoting creates a counterbased counting mechanism in place of those self-tallying systems in order to improve usability. We Voting can ensure a proper counting outcome even in the presence of dishonest counters by carefully creating an honesty-and-activity-based reward system. We Voting achieves strong anonymity in weighted voting, according to our security and performance evaluations, on the assumption that it satisfies the essential security standards for electronic voting. Additionally, its counting system has reasonable overhead and is adequate for practical needs.

TITLE: AVEC VOTING: ANONYMOUS AND VERIFIABLE E-VOTING WITH UNTRUSTWORTHY COUNTERS ON BLOCKCHAIN

AUTHOR NAME: MEIQI LI

DESCRIPTION

E-voting is essential to contemporary social life. Traditional e-voting systems, on the other hand, frequently rely on a reliable third party, making them non-verifiable and vulnerable to a single point of failure. Many researchers have attempted to use block chain in recent years to fix the flaws in e-voting systems. Blockchain-based electronic voting, however, has a significant negative impact on performance and introduces new issues with maintaining the

confidentiality of ballots and the privacy of voters. In this work, we suggest AvecVoting, a highly secure and efficient block chain based anonymous and verifiable e-voting mechanism. To specifically safeguard voters' privacy and the secrecy of ballots, we employ threshold encryption and one-time ring signing. Additionally, we introduce the term "counter" to count the votes in order to improve performance. The reputationbased PayOff algorithms based on smart contracts and the carefully crafted RandomS ortition algorithms allow Avec Voting to achieve accurate counting regardless of whether some counters are unreliable. Our safety and efficacy analyses demonstrate that AvecVoting offers high security features like anonymity, non-repeatability, secrecy, verifiability, etc., while also resolving blockchain-related performance difficulties and offering good efficiency during the voting and counting stages.

III. METHODOLOGY

EXISTING SYSTEM

In existing system, if you wish to vote for someone, then you have to go to the destination where the voting procedure is going on and then only you can vote for him or her. In existing system the results will be modified easily by third parties. There is no way to protect data in server. Server can be hacked by third parties and fake results will be announced easily. So the existing approach does not provide trusted environment for online voting process. The voter has to visit Booths to vote a candidate so there is wastage of time. The voter has to manually register into the voter list. Also vote counting has to be done manually. Voter must be present in his/her constituency to give his/her vote. In current system after voting if any technical problem or damage occurs with the machines it may leads to the re election.

PROPOSED SYSTEM

- We are going to select voting system by FACE RECOGNITION.
- It very secure. Only authenticated person can casting vote.
- Once person voted he removed from list by admin.
- Voter also views available candidates.
- Admin check give accept for authenticated person otherwise reject that person.

IV. MODELING AND ANALYSIS

This system contains six different modules. They are:

- Voter Registration
- Face Recognition
- Candidate Registration
- Admin Panel
- Voting Phase
- Counting and Resulting

V. MODULE DESCRIPTION

5.1 Voter Registration

- Voter register details before election.
- Registration contain name, e-mail Id, username, password.
- Browse photo and voter id card.
- Details are stored in voter list.

5.2 Face Recognition

After fill detail in page then give submit camera is recognize voter face in different way.

5.3 Candidate Registration

- Candidate also registers details.
- Details contain name, id , number of member support, photo and logo.
- It stored in the candidate list.

5.4 Admin Panel

- Admin maintain the detail of both voter list and candidate list.
- Check only authenticated person can cast vote.

5.5 Voting Phase

- Election is start voter enter user name and password automatically open camera
- Admin check face view the available candidate then voter select their candidate and cast vote
- Once person voted admin remove they details in list.

5.6 Counting and Resulting

- Voter casted voting automatically count increases.
- Finally result announced.

V. RESULTS AND DISCUSSION

The result of enforcing a decentralized voting system using blockchain and face recognition technology would be a more secure, transparent, and accessible voting process. The use of blockchain technology would ensure the integrity of the voting process by furnishing a tamper-evidence and auditable tally, while face recognition technology would give an accessible and accessible way to corroborate the identity of choosers while guarding their sequestration. By enforcing a decentralized voting system using blockchain and face recognition, it would be possible to help fraud, manipulation, and hacking in the voting process. This would increase the delicacy and translucency of election results, thereby promoting trust in the voting process and the popular system as a whole. Also, the use of face recognition technology would make the voting process more accessible to all eligible choosers, including those with disabilities or limited access to technology. The technology could also reduce the need for physical polling stations, making it more accessible for choosers to cast their vote from anywhere at any time. Still, the perpetration of a decentralized advancing system using blockchain and face recognition technology isn't without its challenges. Technical, cost, and scalability enterprises must be addressed to ensure the technology is a feasible and extensively espoused result for secure and accessible voting. Sequestration enterprises associated with the use of face recognition technology must also be addressed to cover the obscurity of choosers and help abuse of particular data. Overall, the result of enforcing a decentralized advancing system using blockchain and face recognition technology would be a more secure, transparent, and accessible voting process that promotes trust in the popular system and ensures accurate and fair election results.

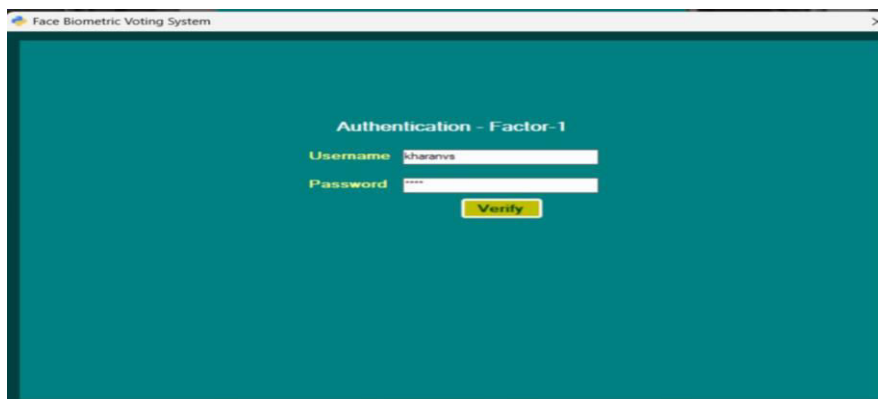


Fig.Login Page

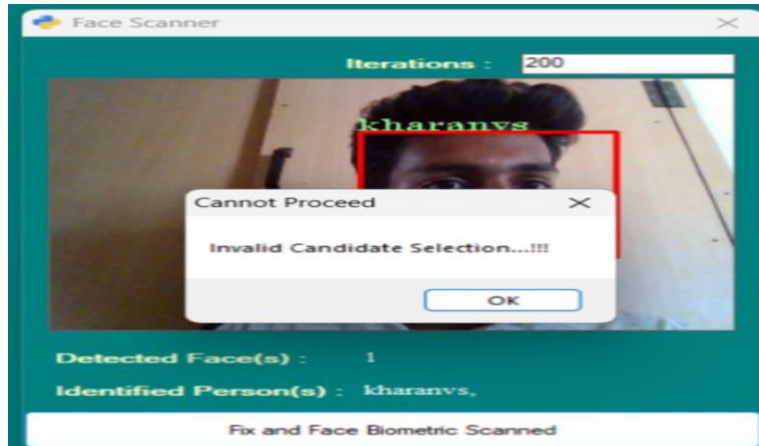


Fig. invalid candidate



Fig. Voter registration.

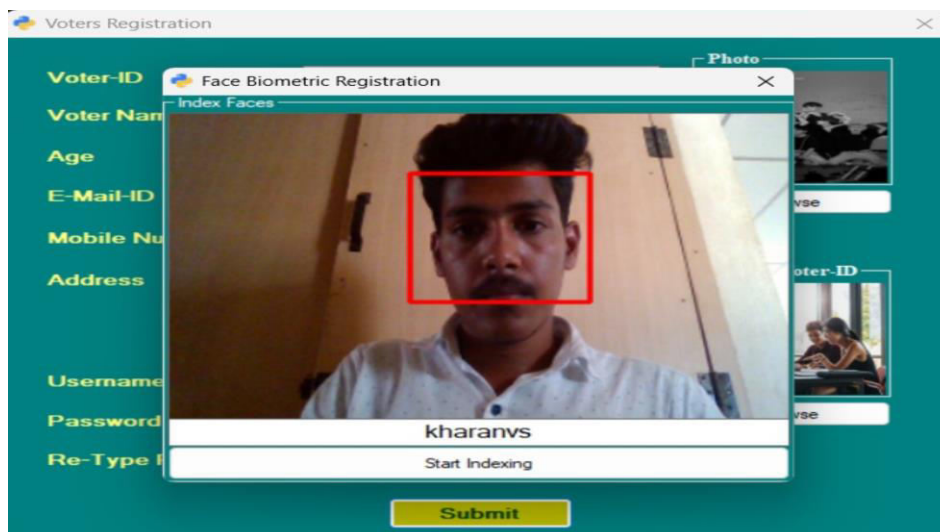


Fig. VotingWindow

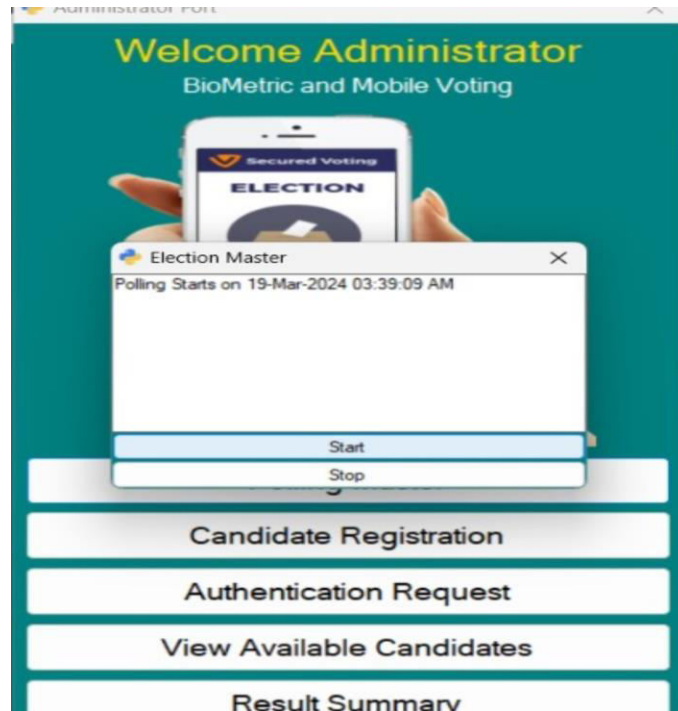


Fig. Polling Window

Age	E-Mail-ID	Mobile Number	Address	Username	
22	kharanstephen35@gm...	9080643233	tiruchengode	kharanvs	Accept
22	kharanstephen15@gm...	9080643233	tiruchengode	kharan	Accept

Fig. Result Window

VI. CONCLUSION

This voting system helps everybody to cast their votes without any problem. Voting application will increase the percentage of voting. Manual counting is not required. So by this we will get the very prominent, clear and fast result. By using this newly developed system we can overcome many problems of existing system. This system is more efficient than the existing one. Application voting allows the voter to vote from anywhere in his state or out of state.

FUTURE SCOPE

The use of block chain technology in e-voting systems offers several benefits such as increased transparency, security, and immutability. Linking application with Government Aadhar System (Digi locker System) and government voting system data. Local languages can be included which will play a vital role for people living in rural areas as well as

uneducated people. A Candidate's earlier social work and candidate qualifications can be added for a voter to have better choice. A complaint system can be included, that allows the people to file complaint against a candidate. Use of honey pots. More accessible to people with disabilities, such as visual or hearing impairments. This could lead to greater participation in the voting process by individuals who may have previously been excluded due to physical limitations.

REFERENCES

- [1] Kumar, Mahender, Satish Chand, and Chittaranjan Padmanabha Katti. "A secure end-to-end verifiable internet-voting system using identity-based blind signature." *IEEE Systems Journal* 14.2 (2020): 2032-2041.
- [2] Wang, Zikai, et al. "WeVoting: Blockchain-based Weighted E-Voting with Voter Anonymity and Usability." *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 2022. [3] Li, Meiqi, et al. "AvecVoting: Anonymous and verifiable E-voting with untrustworthy counters on blockchain." *ICC2022-IEEE International Conference on Communications*. IEEE, 2022.
- [4] Faruk, Md Jobair Hossain, et al. "Bie Vote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework." *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*. IEEE, 2022.
- [5] Ibitoye, Ayodeji Olusegun, Halleluyah O. Aworinde, and Esther T. Adekunle. "An enhanced multi-level authentication electronic voting system." *International Journal of Applied Sciences and Smart Technologies* 4.2 (2022): 149-158.
- [6] Neeru, Pathak, et al. "BIOMETRIC BASED ELECTRONIC VOTING SYSTEM." (2020).
- [7] Farooq, Muhammad Shoaib, Misbah Khan, and Adnan Abid., A framework to make charity collection transparent and auditable using blockchain technology, 2020
- [8] Ajish, S., and K. S. AnilKumar. Secure mobile internet voting system using biometric authentication and wavelet based AES, 2021
- [9]. Abayomi-Zannu, T. P., I. A. Odun-Ayo, and T. F. Barka. , A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication, 2019
- [10]. Ajish, S., and K. S. Anil Kumar, Secure I-Voting System with Modified Voting and Verification Protocol, 2020.



INNO  **SPACE**
SJIF Scientific Journal Impact Factor
Impact Factor: 8.379

doi[®]
CROSS **ref**

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 **9940 572 462**  **6381 907 438**  **ijircce@gmail.com**



www.ijircce.com

Scan to save the contact details