

Smart Voting System using Deep Learning Techniques and Facial Authentication

Bala Krishnan, Gibran and Sathish Kumar

Abstract- Online voting system in which the election data is stored and processed. To achieve higher level of security, one levels of authentication techniques are used. The authentication technique used is a Face Detection and Recognition system. In this method of authentication, the voters face image captured during the registration is compared with the image captured by the webcam at the time of casting vote. After the first level of authentication is done a voter can casting the vote. These techniques provide a more secure platform thus overcoming vulnerabilities of the traditional voting system. We use Opencv, Flask are the python package and HaarCascade Algorithm.

1. INTRODUCTION

In Democratic countries like India, the voting system plays a major role during elections. Traditionally, the election commission in India uses electronic voting machines which need more manpower, time-consuming and also they are less trustworthy. As we know, in every country Election is a basic process of democracy which allows people to show their opinions by selecting their candidate. India is spending huge money to improve our whole voting system to provide a better government to citizens. In India, voting system should be honest, translucent and fully secure for the better democracy. The current system is used to less transparency because there could be chances of cheating at the voting time. Authentication of Voters, smartness of the voting process, protecting voted data these are the main challenges of current Election voting. Thats why it is necessary to generate a smart election voting system. As the modern communications and Internet, today are almost accessible electronically, the computer technology users, brings the increasing need for electronic services and their security. Usages of new technology in the voting process improve the elections in natural. After the industrialisation more number of people leave their native places and come to the cities for the job sake. But many of them still have their voter ids in the address of their native places. On the day of voting they cant able

to go their places so they dont cast their valuable vote. this is the main reason for reduction of voting percentage in our country. Our government also keep on working to find out a best solution for this circumstance.

2. OBJECTIVE

This system provides a better security as it ensures that no voter is allowed to vote more than once. Also the system takes care that no voter can determine for whom anyone else voted and no voter can duplicate anyone else vote. Every voter can make sure his/her vote is cast.

3. LITERATURE-SURVEY

Title - A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption

Author - Xuechao Yang; Xun Yi; Surya Nepal; Andrei Kelarev; Fengling Han, IEEE Access, March 2018

Advanced security methods are necessary to introduce effective online voting in the whole world. Elections conducted on paper consume a lot of resources and contribute to the destruction of forests, which leads to climate deterioration. Recent online voting experiences in countries, such as the United States, India, and Brazil, demonstrated that further research is needed to improve security guarantees for future elections, to ensure the confidentiality of votes and enable the verification of their integrity and validity

Title - Electronic Voting Using Blockchain And Smart Contracts: Proof Of Concept

Author - Fábio D. Giraldo; Barbosa Milton C.; Carlos E. Gamboa, IEEE Latin America Transactions 10, October 2020

Blockchain technology has been presented as a support for trust needs between transactions in electronic information systems. Its successful use in cryptocurrencies has allowed it to explore its

capabilities in commercial, industrial, and service systems, backed by the operational alternatives offered by Ethereum Smart Contracts and the cryptographic security of public and private key.

Title - A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature

Author - Mahender Kumar; Satish Chand; C. P. Katti , IEEE Systems Journal , June 2020)

The end-to-end (E2E) verification enables a voter to check if his ballot is recorded as he intended and the public to check if the system has correctly counted all of the recorded ballots. The Internet voting systems based on the principle of E2E verifiability have many challenges; the most important is its security. Several E2E voting systems have been discussed in the last decade in terms of analyzing the e-voting system and formalizing its security requirements. This article presents an E2E verifiable internet voting system that provides mobility to a voter and allows him to cast his vote secretly in public computer with the benefit of early voting. The proposed system aims to support the election process universally by using the voter's unique identification and biometric features. We propose a new identity-based blind signature scheme that ensures the voter's anonymity.

Title - A Smart Contract System for Decentralized Borda Count Voting

Author - Somnath Panja; Samiran Bag; Feng Hao; Bimal Roy, IEEE Transactions on Engineering Management , Nov. 2020

In this article, we propose the first self-tallying decentralized e-voting protocol for a ranked-choice voting system based on Borda count. Our protocol does not need any trusted setup or tallying authority to compute the tally. The voters interact through a publicly accessible bulletin board for executing the protocol in a way that is publicly verifiable. Our main protocol consists of two rounds. In the first round, the voters publish their public keys, and in the second round they publish their randomized ballots. All voters provide Non-interactive Zero-Knowledge (NIZK) proofs to show that they have been following the protocol specification honestly without revealing their secret votes. At the end of the election, anyone including a third-party observer will be able to compute the tally without needing any tallying authority.

Title - Modeling Reliability of Threshold Weighted Indecisive Voting Systems

Author - Hainan Zhang; Hoang Pham, IEEE Transactions on Computational Social Systems ,Feb 2020

In industry, the method of hypothesis acceptance based on available information is widely used in applications such as system modeling. Xie and Pham modeled the reliability of weighted threshold voting systems with a general recursive reliability function in human organization systems. As an extended study, we introduce a generalized weighted indecisive-voting n-unit system using a new decision rule consisting both a threshold parameter τ and a new indecisive parameter θ . In general, indecision happens due to limited information, and an indecisive parameter is then applied if no decision is made. System reliability R is calculated to show the system performance.

Title : SecEVS : Secure Electronic Voting System Using Blockchain Technology

Authors:Ashish Singh; Kakali Chatterjee , 2018 International Conference on Computing, Power and Communication Technologies (GUCON)

In today's digital environment, the voting system moves from paper-based to a digital system. A digital e-voting system has many properties such as transparency, decentralization, irreversibility, and non-repudiation. The growth in digital e-voting system arises many security and transparency issues. In this paper, we used the blockchain technology in digital e-voting system to solve the security issues and fulfill the system requirements. It offers new opportunities to deploy a secure e-voting system in any organization or country. The solution is far better as compared to other solutions because it is a decentralized system, contains the results in the form of bit-coins, having different locations. We will also analyze the security of our proposed voting system, which shows our protocol is more secure as compared to other solutions.

Title : An Approach to the Efficient Security Algorithms Used in Voting Scanning in an Electoral Process

Authors:Segundo Moisés Toapanta Toapanta; Josue Andrés Tamayo Lamar; Javier Gonzalo Ortiz Rojas; Luis Enrique Mafla Gallegos, 2019 2nd International Conference on Safety Produce Informatization (IICSPI)

It was considered that the security of information is an important factor in an electoral process in a country; for the frequent problems that have been detected in the scanning of votes to expedite the count. The objective is to analyze a method of vote scanning that allows improving security, administration, and implementation so that vote counting is faster and more secure compared to the traditional voting system. The deductive method and the exploratory investigation were used to analyze the information of the articles of the reference. It turned out to be a prototype of a voting scan algorithm based on the OCR reader scanner that was proposed and analyzed; for the scanning of the votes and projection of results via the internet for the next elections to improve the integrity of the information. It was concluded that a prototype of an adequate algorithm for vote scanning is an alternative to improve a traditional system that will be integrated into a voting system.

Title : Decentralized E-Voting Portal Using Blockchain

Authors:Kriti Patidar; Swapnil Jain, 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)

Online voting is an alternative to age old paper ballot system and the currently popular electronic voting machines (EVM). An electronic voting portal should offer security and integrity along with the transparency of votes and privacy of voters. This paper proposes an e-voting system based on blockchain that eliminates some of the limitations in existing voting systems. The paper also presents state of art of some blockchain frameworks for e-voting. The presented implementation is suitable for small scale elections like inside corporate houses, board rooms etc. The implementation uses smart contract from Ethereum. Truffle framework is used in this paper for development, testing and deploying smart contracts. Ganache is used as Ethereum client for testing. Here Meta-mask is used as browser wallet.

Title : Increasing Participation and Security in Student Elections through Online Voting: The Case of Kabarak University

Authors:Moses M THIGA , 2020 IST-Africa Conference (IST-Africa)

Electronic voting systems have enhanced efficiency in student elections management in universities, supporting such elections to

become less expensive, logistically simple, with higher accuracy levels as compared to manually conducted elections. However, e-voting systems that are confined to campus hall voting inhibits access to eligible voters who are away from campus. This study examined the challenges of lack of wide access and impersonation of voter in the student elections of 2018 in Kabarak University. The main objective of this study was therefore to upgrade the offline electronic voting system through developing a secure online voting system and deploying the system for use in the 2019 student elections at Kabarak University. The resultant system and development process employed demonstrate the applicability of a secure online voting not only in the higher education context, but also in other democracies where infusion of online access and authentication in the voting processes is a requisite.

Title : From Conventional Voting to Blockchain Voting: Categorization of Different Voting Mechanisms

Authors:SyadaTasmiaAlvi; Mohammed Nasir Uddin; Linta Islam; Sajib Ahamed , 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)

For the development of society and the enhancement of citizen's civic knowledge, voting plays an incredibly important role in many forms of practice as a guiding factor for the true growth of democracy. The world's electoral mechanism has been marked by several structural problems, leading in an election being held by a dishonest candidate. Scientists were mentally, psychologically, socially and critically worried about the mismanagement of electoral processes documented at various stages of selecting a leader. Deal with the question about how to protect dishonest participants in elections from unethical practices such as bribery and spoofing are a great concern. The results of making a dishonest participant a winner are bad administration, uncertainty and diversification for the financial benefit of public funds. Approaches ought to be created to fix the issues of the electoral processes. Thus, this paper concentrated on a systematic analysis of multiple forms of voting with blockchain and without blockchain by numerous researchers as a forum to find vulnerabilities or weaknesses and propose a perfect voting mechanism to fulfill all the properties requires in voting system.

4.EXISTING-SYSTEM

This system isolates the malicious devices by eliminating the threats encountered during communication and path formation process by computing the weighted trust of each device. Moreover, to ensure transparency in the polling mechanism, a blockchain is maintained that includes IoT devices to further formulate a secure polling process. IoT devices are used record and collect the vote.

Limitations

- It Use an Iot Based hardware for Casting the vote
- The IoT devices are either legitimate or malicious
- Malicious devices and not be able to add in the blockchain

5.PROPOSED SYSTEM

System is used cast your vote through online via website using facial authentication and machine learning techniques . To get a high degree of accuracy from what is called “training data”. Haar Cascades use the Adaboost learning algorithm. which selects a small number of important features from a large set to give an efficient result of classifiers. Initially, the algorithm needs a lot of positive images (images of faces) and negative images (images without faces) to train the classifier. Then we need to extract features from it. For this, haar features shown in below image are used. They are just like our convolutional kernel. Each feature is a single value obtained by subtracting sum of pixels under white rectangle from sum of pixels under black rectangle.

A. Setup

The registrar and moderator each generate a key pair. They select a secret key $x_r \in_r Z_p^*$ and $x_m \in_r Z_p^*$ and then compute their corresponding public keys as $y_r = g^{x_r} \pmod{p}$ and $y_m = g^{x_m} \pmod{p}$, respectively.

Protocol 1 Voter Registration

Input: Public key y_i of v_i ; hash function h .

Output: Digital Signature EG-Sign _{y} (y_i).

Setup: (Registrar R)

- 1: Randomly select secret key $x_r \in_r Z_p^*$.
- 2: Compute public key as $y_r = g^{x_r} \pmod{p}$.

Registration Request: (Voter v_i)

- 1: Randomly select secret key $x_i \in_r Z_p^*$.
- 2: Compute public key as $y_i = g^{x_i} \pmod{p}$.
- 3: Send y_i to R.

Authentication: (Registrar R) If v_i is eligible:

- 1: Randomly select u_i with $1 < u_i < p-1$ and $\gcd(u_i, p-1) = 1$.
- 2: Compute $w_i = g^{u_i} \pmod{p}$.
- 3: Compute $s_i = (h(y_i) - x_r w_i) \mu^{-1} \pmod{p}$.
- 4: Send (w_i, s_i) to v_i .

B. Voter Registration

At this phase, voters are required to prove their voting eligibility to the registrar by providing evidence such as their identities. After validation, voters are added to the electoral roll. Protocol 1 summarizes this process.

1) *Voter Key Generation and Registration:* Each voter v_i selects a secret key $x_i \in_r Z_p^*$ and then computes the corresponding public key as $y_i = g^{x_i} \pmod{p}$. Public keys are shared with the registrar during registration.

2) *Signing Voter's Public Key:* The registrar verifies the eligibility of the voters and signs their public keys. It selects u_i randomly where $1 < u_i < p-1$ and $\gcd(u_i, p-1) = 1$ then computes the following:

$$w_i = g^{u_i} \pmod{p}, \quad s_i = (h(y_i) - x_r w_i) \mu^{-1} \pmod{p},$$

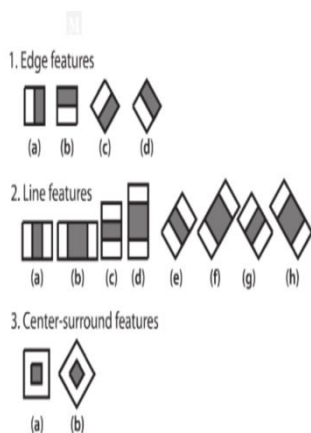
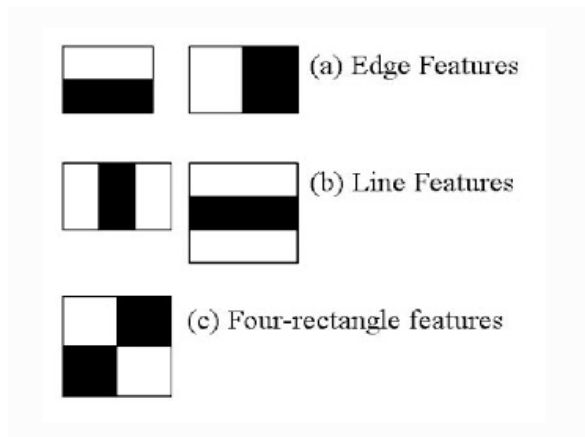
(2) where (w_i, s_i) is the signature. The registrar adds

$y_i (w_i, s_i)$

to the electoral list which it discloses once the registration phase is complete.

6.ALGORITHMS

Haarcascade algorithm



Face Detection determines the locations and sizes of human faces in arbitrary (digital) images.

In **Face Recognition**, the use of Face Detection comes first to determine and isolate a face before it can be recognized.

ADVANTAGE

- The key advantage of a Haar-like feature over most other features is its calculation speed.
- Haar Cascade is a machine learning object detection algorithm used to identify objects in an image or video
- Haar Cascades use the Adaboost learning algorithm which selects a small number of important features from a large set to give an efficient result of classifiers.

CNN

Convolutional neural network (ConvNets or CNNs) is one of the main categories to do images recognition, images classifications. Objects detections, recognition faces etc., are some of the areas where CNNs are widely used. In work project we are going to detect and classify drone in video using CNN algorithm.

Steps

- ☐ Provide input image into convolution layer
- ☐ Choose parameters, apply filters with strides, padding if requires. Perform convolution on the image and apply ReLU activation to the matrix.
- ☐ Perform pooling to reduce dimensionality size
- ☐ Add as many convolutional layers until satisfied
- ☐ Flatten the output and feed into a fully connected layer (FC Layer)
- Output the class using an activation function and classifies images.

7.SYSTEM SPECIFICATION

HARDWARE REQUIREMENTS

The most common set of requirements defined by any operating system or software application is the physical computer resources, also known as hardware. The minimal hardware requirements are as follows,

1. Processor: Pentium IV
2. RAM: 8 GB
3. Processor: 2.4 GHz
4. Main Memory: 8GB RAM
5. Hard Disk Drive: 1tb
6. Keyboard: 104 Keys

SOFTWARE REQUIREMENTS

Software requirements deals with defining resource requirements and prerequisites that needs to be installed on a computer to provide functioning of an application. The minimal software requirements are as follows,

1. Front end: python
2. Dataset: csv
3. IDE: anaconda
4. Operating System: Windows 10

8.MODULE DESCRIPTION

Register

Registration module is the starting point of this project where a user gone make use of this system by registering him self

into it. In this module user will have a unique voter ID and user gone register with some basic information about him after the user gone complete the registration by giving his face as input and system will read the face and load it in datasets after that registration process is completed.

Data Preprocessing

In this module the collected dataset from user in the time of registration will be stored in folder and all image are resized to standard and unique size and the image are converted to gray scale image and noise are removed.

Feature Extraction

In this feature extraction module we extract the feature from registered user datasets folder

Admin upload candidates and assign election

Admin is the one who monitor the entire system. First admin has a standard login id and password. Admin can upload election candidates the candidates list must be in a csv file where the candidates detail like part name email and area the he gone compete with this detail the file will be uploaded from data the details will be uploaded to system. Admin can also monitor the registered user. Admin can also assign election on the upcoming dates.

Login

Now the register user will login in this system with registered information if information give by the user matches the database the user will be allowed to login into this system. After the user successfully logged in now the user can see the upcoming election if the election was assigned and user can also see the candidates list.

Face Recognition

Every time a new user register or the existing user vote his face will be recognition to check whether user is authorized or not.

Voting

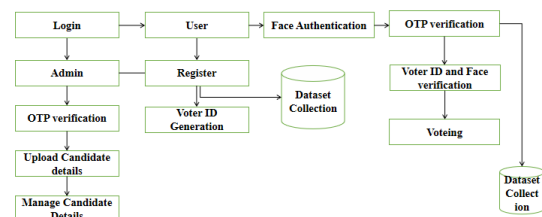
After user logged in now user can vote for his area. After selecting the party he can vote in that time user face will be recognized and check whether he is a authorized registered user or not if the user

is unauthorized user will not allowed to vote his vote will not be registered.

See the result

After the user voted his vote now the result will be automatic updated with the vote count.

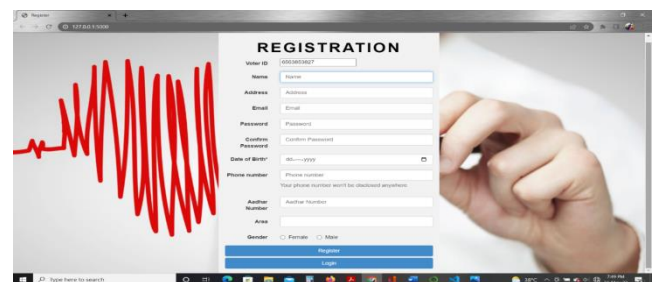
9. ARCHITECTURE DIAGRAM



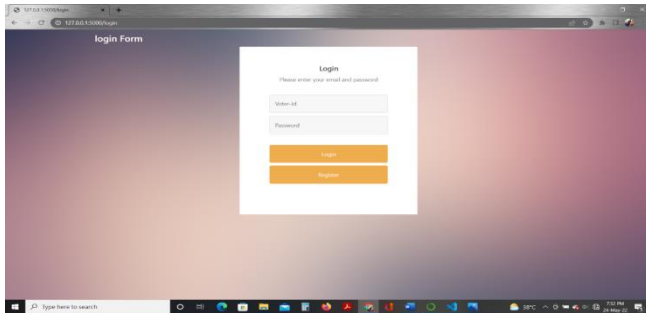
10. SCREENSHOTS

USER MODULE

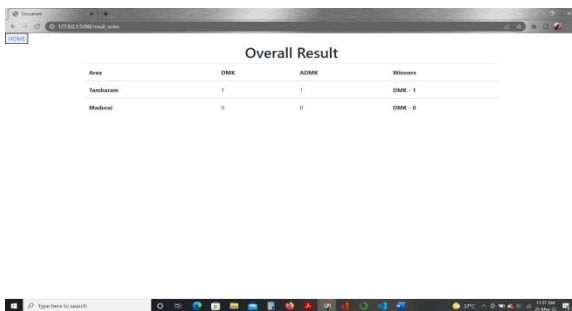
REGISTRATION FORM



LOGIN FORM

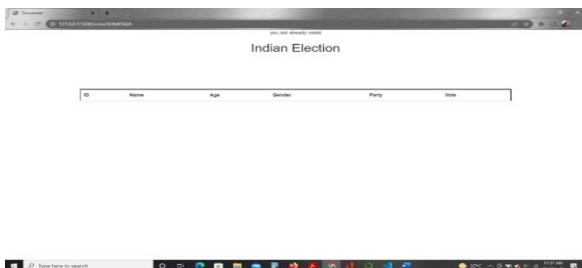


OVERALL RESULT PAGE



Area	DMK	AIADMK	Winner
Tambaram	1	1	DMK - 1
Madhav	0	0	DMK - 0

ALREADY VOTED USERS CAN'T VOTE AGAIN



11.CONCLUSION

Smart Voting is primarily responsible for the majority of India's city . It should be considered as the main issue for the majority of us. The existing methods for Voting involves manual work with lot of human work and man power and also if convert voting to online it need secured voting system to cast voters vote . The Machine Learning technique. Are use to recognize person face and check whether voter is a authorized or not.

12.REFERENCES

1. Title – Distributed Blockchain-based Anonymous Mobile Electronic Voting,Author – Ehab Zaghloul;Tongtong Li,IEEE,2021
2. Title - A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption,Author - Xuechao Yang; Xun Yi; Surya Nepal; Andrei Kelarev; FenglingHan,IEEE Access ,March 2018
3. Title - Electronic Voting Using Blockchain And Smart Contracts: Proof Of Concept,Author - Fáber D. Giraldo; Barbosa Milton C.; Carlos E. Gamboa ,IEEE Latin America Transactions 10, October 2020
4. Title - A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature,Author - Mahender Kumar; Satish Chand; C. P. Katti , IEEE Systems Journal , June 2020)
5. Title - A Smart Contract System for Decentralized Borda Count Voting,
6. Author - Somnath Panja; Samiran Bag; Feng Hao; Bimal Roy, IEEE Transactions on Engineering Management , Nov. 2020.
7. Title : A Comparative Analysis on E-Voting System Using Blockchain,
8. Authors:Kanika Garg; Pavi Saraswat; Sachin Bisht; Sahil Kr. Aggarwal; Sai Krishna Kothuri; Sahil Gupta, 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU).
9. Title :SecEVS : Secure Electronic Voting System Using Blockchain Technology,Authors:Ashish Singh; Kakali Chatterjee , 2018 International Conference on Computing, Power and Communication Technologies (GUCON).

10. Title : An Approach to the Efficient Security Algorithms Used in Voting Scanning in an Electoral Process,Authors:SegundoMoisésToapantaToapanta; Josue Andrés Tamayo Lamar; Javier Gonzalo Ortiz Rojas; Luis Enrique Mafla Gallegos, 2019 2nd International Conference on Safety Produce Informatization (IICSPI)
11. Title : Decentralized E-Voting Portal Using Blockchain,Authors:Kriti Patidar; Swapnil Jain, 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)
12. Title : Increasing Participation and Security in Student Elections through Online Voting: The Case of KabarakUniversity,Authors:Moses M THIGA , 2020 IST-Africa Conference (IST-Africa)
13. Title : From Conventional Voting to Blockchain Voting: Categorization of Different Voting Mechanisms,Authors:SyadaTasmiaAlvi; Mohammed Nasir Uddin; Linta Islam; Sajib Ahamed , 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)