ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (51-56), Month: October - December 2021, Available at: www.researchpublish.com

SMART ONLINE VOTING SYSTEM USING IOT

Nischal Raghuram Puvvala[1], Aditya Asok Nair[2], Puneet Chawla[3]

[1]Department of Computer Science and Engineering, SRMIST Ramapuram Chennai. [UG Scholar]

[2]Department of Computer Science and Engineering, SRMIST Ramapuram Chennai. [UG Scholar]

[3]Department of Computer Science and Engineering, SRMIST Ramapuram Chennai. [UG Scholar]

Abstract: **It is essential that administrators of the country are elected by an honest election. Therefore it is important to ensure safe and secure election methods. The proposed new method of E-voting uses modern technologies like the internet of things and it does not require the voter's physical presence. People can vote from the comfort of their homes using mobile and web applications. Every vote will be made secure with a series of facial recognition and encryption algorithms. Offline voting system is implemented using a web application & mobile application which incorporates the Aadhar card and the voter ID.**

Keywords: **Secure election methods, Internet of Things, Mobile and Web Applications, E-Voting, Facial Recognition, Encryption Algorithms, Adhaar Card, Voter ID, Web Application, Mobile Application.**

1. INTRODUCTION

India is currently the most substantial democracy of the world with the most diverse voter bank of the world; consisting of 912 million people from various demographics like religions and ideologies. It is imperative that such a country have a secure and accessible election so that people of every demographic can participate in electing their chosen candidate and see their representation in the political sphere. It is important that the fate of 1.36 billion people is spear-headed by representatives that are responsible and have been put there by fair means. It is vital to the spirit of democracy that the country is headed by someone the people trust and not some tyrant that seized power from the people by ill-begotten means[1].

India currently uses offline voting methods like ballot boxes and EVMs to conduct voting. EVMs were introduced in India in the early 1980s and Ballot boxes were introduced in the late 1990s, and while these may have been the best methods to conduct elections at the time with current technology the voting experience can be improved exponentially and it's many shortcomings remedied. Elections as they exist now require a huge amount of man-power and resources like venues, which are often requisitioned from educational institutions like schools and colleges. Law enforcement authorities like the police department are directed towards the election duties which leaves certain areas unsupervised.

Places that house the venues for the elections are often subject to overcrowding and congestion which causes inconveniences to the locals and the public at large. All these factors lead to the venue being unhygienic subjecting the voters to potential hygiene risks. This makes conducting traditional elections at times of crisis inconvenient at best and inconceivable at worst.

With the advent of modern sciences like IoT, big data and data structures, our election methods can be improved to a point where all the concerns about manpower and hygiene will be null and void. This is what we aim to accomplish. By using substantiated systems, such as per-existing databases and two-factor authentication, we can overhaul the convenience and security of polling to ensure that every person can exercise his/her fundamental right to vote [6].

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (51-56), Month: October - December 2021, Available at: www.researchpublish.com

In short, the current election system is outdated and unoptimised and is a waste of human resources and time. The electoral system is open to malpractices and manipulation which undermines the core principles of a democracy.

Our objective is to make elections more streamlined and accessible to voters which will increase the percentage of voting turnout with the help of mobile and web applications. By using concepts like the Internet Of Things to connect devices for voting. It uses Big Data to access pre-existing databases like Aadhar[3] and Voter Id[6] while using binary search algorithm to help optimise the verification process for voters hence facilitating ease of access to the voting system.

Facial recognition software[2] (Normalized Pixel Difference (NPD)[7] and Deep Convolutional Neural Network (DCNN)[7], etc) are used to verify the voter's authenticity before and during the voting process. After the vote is cast, it is encrypted using Public key (RSA)[8] encryption algorithm. The encrypted data is stored till the counting day and the Public key RSA[8] decryption algorithm is used to decrypt the votes. The votes are then counted.

2. PROPOSED METHODOLOGY

i. Register

Before the voter is allowed to enter the platform, they have to apply to the platform. This will be done using the entrants Aadhar number[3] and Voter ID. This is to legitimise the identity of the voter as efficiently as we can. Once this step is cleared, the voter can log in and vote when the polling is taking place.

ii. Login

The voter uses voter id as his username and phone number to sign in. The data of the voter is fetched using a binary search algorithm[9] from the existing aadhar and voter id databases and an otp is sent to the voter's mobile phone which will act as a means to authenticate the voter. After the voter has been verified facial recognition is required to proceed further. The facial recognition system uses multiple algorithms such as Normalized Pixel Difference (NPD), Skin Detection Using Two Color Spaces HSV and YCGCR, Real-Time Multi-Face Detection System and Deep Convolutional Neural Network (DCNN) to cross reference the photo existing in the latest photo of voter in aadhar and election databases and the current recording[3].

iii. Binary Search Algorithm

Binary Search Algorithm is implemented to find the voter id number in the database. The voter id number is a series of 8 alphanumeric characters. As the central voter database is already sorted the search algorithm will look for the midpoint of the database and verify if the entered voter id is smaller or greater than the voter id in the middle index. If the voter ids are a perfect match the algorithm will return the voter id details. If it is smaller than the midpoint the algorithm will continue the same process in the lower half of the dataset and if the voter id entered is greater than the midpoint, the algorithm continues the same process in the upper half of the data set until it finds a perfect match for entered voter id. As voter id number is unique to every voter the database will not have any repetitions and the binary search algorithm will return the details of the voter linked to the entered voter id number[3].

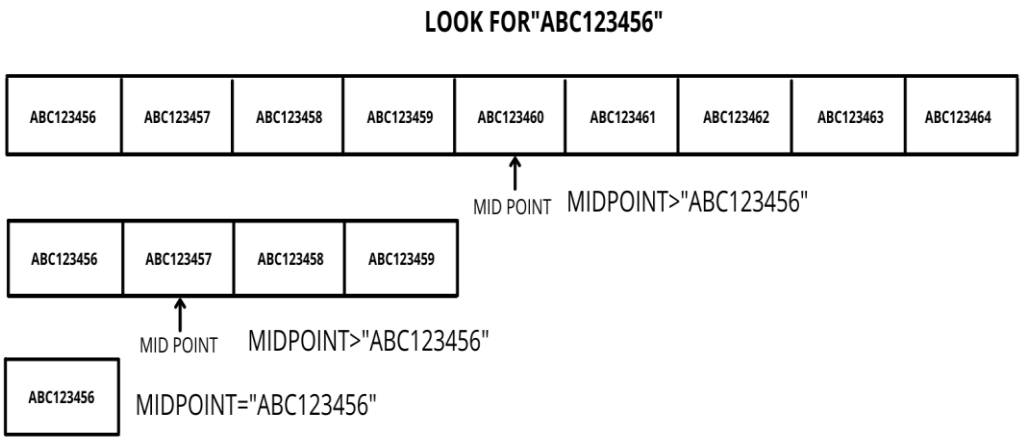

Fig 1. Algorithm Searching For A Certain Entry

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (51-56), Month: October - December 2021, Available at: www.researchpublish.com

iv. Normalized Pixel Difference (NPD)

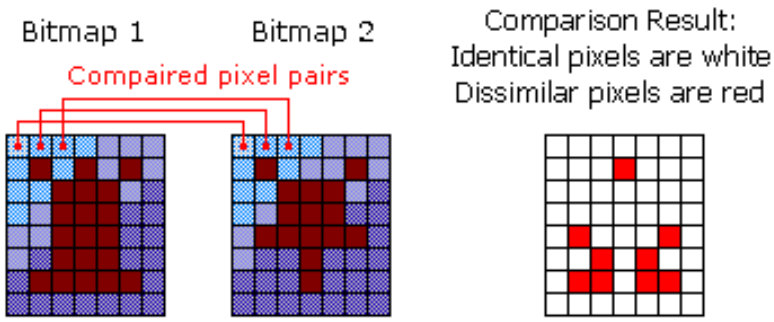

Fig 2. Comparing The Pixels Of The Newly Received Image To The Sample Image

Normalized Pixel Difference compares the pixels of the face using parameters such as brightness and darkness values. It includes scaling and allows the system to reassemble the image or the compared image. A deep quadratic tree beginner is constructed to find out the most appropriate set of NPD characteristics to increase their dissimilarities. A deep quadratic tree learning technique is used and a single soft-cascade AdaBoost classifier is built to pick up multiple composite faces and arbitrary posture and occlusion constraints. The map shows the position of a particular facial element given in the image for example hair, eyes, nose, mouth, and beard [7].

v. Deep Convolutional Neural Network (DCNN)

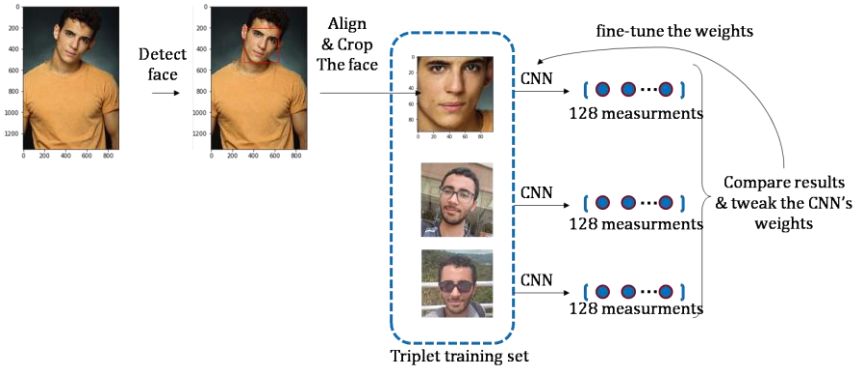

Fig 3. Picking Out Patterns In The Received Image And Comparing It To The Sample Image

Deep Convolutional Neural Network divides/compartmentalizes the facial scan into grids for ease of comparison. A complete image is given as input to a CNN to produce the part level response map for every face segment. The level response map is acquired by weighted mapping at its upper convolution layer. For every grid, patterns are identified and taken into consideration. It is also connected with a particular range and condition portions[7].

vi. Voting

Once the two step verification process is complete the voter is allowed to vote. The facial recognition software will be running throughout the voting process in order to make sure that a genuine voter is voting. Once the voter selects his/her preference in voting, the preference is encrypted using a Symmetric Key encryption algorithm and Public key RSA encryption algorithm. The voter id number of the voter will act as a symmetric key. Once the voting data is encrypted, it is stored in secure servers until the voting day.

vii. Public Private Key RSA encryption Algorithm and Symmetric Key Encryption Algorithm

The Symmetric Key Encryption algorithm uses a single code to encrypt as well as decrypt the vote. As soon as the vote is cast a 10 digit random integer is generated, which will be used as the symmetric field.

We then encrypt the symmetric key which was initially used to encrypt the vote with the public Private key RSA encryption, the symmetric key is encrypted using a code called public key. The public key we are using in this scenario is the voter id number. Once the vote is encrypted it can only be decrypted with a private key. The private key is a randomly

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (51-56), Month: October - December 2021, Available at: www.researchpublish.com

generated 20 alphanumeric characters for each ward. The private keys for the particular wards in a constituency will rest with the Election Commission officers. In order to keep the data more secure and increase the efficiency and security of the vote, it is first encrypted using a symmetric key algorithm. Then with voter id as the public key, the symmetric key is encrypted using a Public Private key RSA encryption algorithm. In this case, only a person with the private key for RSA Public Key algorithm can access the symmetric key and the symmetric key will decrypt the vote.[8]

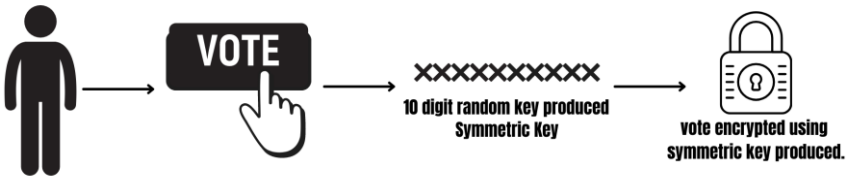

Fig 4. Encrypting Vote With Symmetric Key Algorithm

Fig 5. Encrypting Symmetric Key Using Public Private Key Algorithm

Fig 6. Decrypting Symmetric Key Using Public Private Key Algorithm

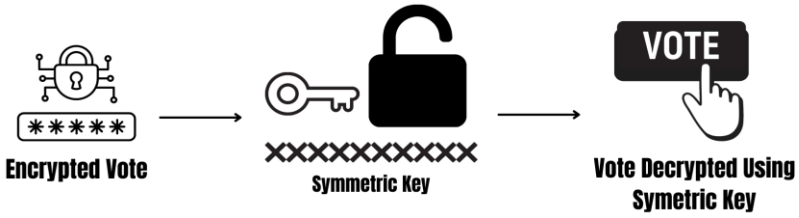

Fig 7. Decrypting Vote Using Symmetric Key Algorithm

viii. Counting

After the voting process is complete, the votes are decrypted using the Private key which is given to the election commission officers. As the votes are being decrypted they will be counted using search algorithms. The data is traversed and the count incremented for each vote to a candidate. After the traversal the number of votes are compared to verify the one with a majority.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (51-56), Month: October - December 2021, Available at: www.researchpublish.com

ix. Voting Centers Facility

Not everyone can have means to authenticate using a camera or an otp so the voting centers will have all the necessary tools for a voter to go and exercise his right to vote. It is not mandatory that a voter should have a mobile phone with integrated cameras advanced enough for facial recognition. So The voting centers will have a device to vote from with cameras sufficient to verify the voters with cabins for privacy during voting.

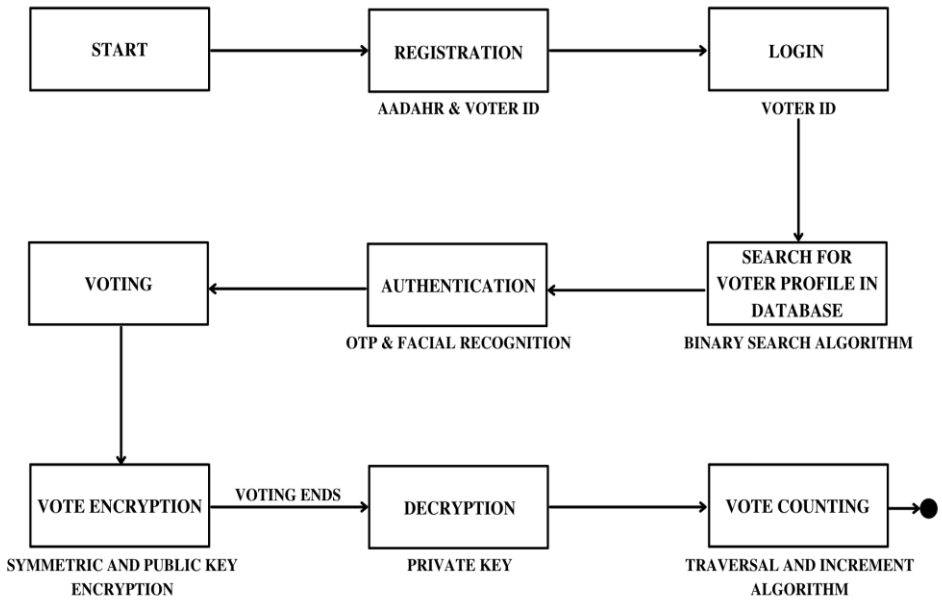

Fig 8. Methodology Flow Chart

3. RESULT

By combining security solutions like Facial Recognition algorithms and Encryption algorithms with the accessibility of modern tools like mobile phones and the internet, we have managed to overcome all of the downfalls of the existing voting system.

4. CONCLUSION

After considering various possibilities of translating the voting mechanism into the virtual world, we believe that having an end-to-end easy to access application as the new electoral system will not only improve the system exponentially but also facilitates an easy transition from offline to online voting.

The use of state-of-the-art security solutions like facial recognition and encryption not only ensures that our system will be insured against the normal pit-falls of online voting like security breaches and identity falsifications, but also makes it easier to build and integrate into existing systems so as to make the transition as smooth as possible. As more and more facilities move to the virtual world, moving the democratic process forward seems like the logical next step. Seeing as the electoral process is a cornerstone in any democracy, it should be made as convenient as possible while at the very least maintaining the security level of the offline sessions which our project more than accomplishes.

While this project may be technically sound, there is the issue of actually implementing it on a nation-wide scale, and so the biggest hurdle to overcome will be bureaucracy. This is mainly due to the public's scepticism towards such means. It is not unheard of for well established and reportedly secure platforms to get infiltrated, which for some sets the precedent that online platforms are not as reliable as the present method of elections, which has endured for as long as it has with seemingly no overt disruptions. It will be a herculean task to get this platform through the legal channels but once it's done it will just be a matter of improving upon the already sturdy framework of the project, with rigorous testing across multiple fields and constant improvement.

In an age where people rely on applications for anything, it would stand to reason that this is the most logical course of action in improving an antiquated system, and that is exactly what this paper aims to address.

5. FUTURE ENHANCEMENTS

While the existing system is relatively secure, it is not air-tight. This is a major area for improvement as the security of the system is one of the main attributes of our product. The privileged voting information needs to be protected and the current system, while effective, can be improved significantly. As such, the database servers of the election commission which store the votes need to be air gapped and fortified with the most effective security protocols possible. To ensure that all the security protocols are implemented, the software will be put through rigorous testing and will be improved accordingly. To reinforce it's security against external threats, it will be tested against the established and unorthodox hacking techniques. To keep the voter abreast of the situation, an integrated news feed will be used to display a live vote count and the latest results as they are revealed.

A major challenge to our product is integrating it into the mechanism of the elections not just physically but socially as well[10]. People will initially be apprehensive of the new system and as such we must take steps to ease their suspicions. To this end, distancing the system from seemingly corrupting influences such as ruling parties and private companies who may have certain political or ideological leanings. This is to ensure that the people behind the system are non-partisan and will not tamper with the votes. Further integrating it into the existing system without causing friction or excluding anyone from the voting process.

REFERENCES

[1] S Ganesh Prabhu, Smart Online Voting System, International Conference on Advanced Computing and Communication Systems, 2021

[2] S. Jehovah Jireh Arputhamoni, Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN, Third International Conference, 2021

[3] Himanshu Agarwal, Online voting system for India based on AADHAAR ID, Eleventh International Conference on ICT and Knowledge Engineering, 2013

[4] Kriti Patidar, Decentralized E-Voting Portal Using Blockchain, 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)

[5] Friðrik Þ. Hjálmarsson, Blockchain-Based E-Voting System, 2018 IEEE 11th International Conference on Cloud Computing (CLOUD)

[6] Bhuvanapriya R, Smart voting, 2017 2nd International Conference on Computing and Communications Technologies (ICCCT)

[7] Manisha Kasar, Face Detection Techniques using Database Images, International Journal of Control and Automation 12(6) : 17 - 34, June 2019

[8] Hayam K Al Anie, E-Voting Protocol based on Public-Key Cryptography, International Journal of Network Security and its Applications 3(4) : 87 - 98, July 2011

[9] Charles H. Davis, The Binary Search Algorithm, Published 1 April 1969, Corpus ID: 62128693

[10] Chrisanthi Avgerou, Trusting e-voting amid experiences of electoral malpractice: The case of Indian elections, September 1, 2019