Dual Authentication Voting System with Facial Recognition and Fingerprint using CNN

-Vidhya VB

-Dr. P Asha, M.E., Ph.D.

Computer Science and Engineering Department

Sathyabama institute of science and technology

ABSTRACT

Voting is one of the notably common and basic right of all citizens of the country. In the latest lok sabha election 2019, conducted in India, only 67.1% vote was being recorded. Conducting election in a democratic country like India, have major challenges of security threads, false voting, manipulation in recording vote and authentication of voter. Our country India employs the EVM(Electronic Voting Machine) since 1982. The system also has its flaws as vote rigging is a possibility. Hence, in this paper we give a solution to the voting problem.The data for the project can be acquired from the dataset of Aadhar card that contain the photo. By using CNN (Convolutional Neural Network) the face of the voter is detected and compared to the Aadhar dataset. This will be the first step of the authentication. Then the vote is casted through fingerprint, which is sensed through sensor and is authenticated. This will allow the voter to vote only once and to only one person. The recorded vote is saved in the cloud server and is counted immediately. This makes the system more efficient and authenticated and avoids rigging of vote, than the existing system of voting .

Keywords: Facial Recognition, Fingerprint, Authentication, CNN, Authentication, Voting System.

I. INTRODUCTION:

"Voting is a civic duty". Elections and voting are the systems that are stretches in the world far back in time. From Ancient Greece till today's modern technological world voting is prevailing. It is considered that the voting protects the democracy. When it comes to election every sin gee vote matters. The countries have its proper forms by the social agendas and the country's economy, that are being shaped by voting procedures. Voting hols the leaders accountable as its the key of the citizens. It is the elections conducted in a country and the percentage of vote that's impacts the present and the future of the country. In India, population and voting mannerism could affect nation's future widely. Ergo, the elections plays vital role.

In today's digitalising world, **biometrics** techniques are generally used as the key to identify a person using on some of the particular strands of unique physical or behavioural characteristics. Biometrics include finger/palm prints, hand geometry, DNA, blood types, facial measurements, iris recognition, voice and speech inflections, walk gaits, etc. One of the earliest and most fundamental biometric technologies that falls under the category of digital forensics is the fingerprint. Facial recognition is the most natural biometric technological method used. Facial recognition is used from prehistoric times, as every identification is documents of a person was done using the photographs attached of its bearer, comparing the actual face with the photo in the document.

The world, had solved a lot of mysteries using the biometric technologies. Ensuing 9/11 terrorist incident, instead wide applications of face recognition in typical public spaces like airports, official meetings, malls, etc, increased as the means of detecting faces and reducing threads. CCTVs in public places, and offices records images, accountability algorithms are then utilised for a matching exercise with a database of images already in existence. It gives rise to find criminals and unauthorised targets. In the same way fingerprints are used to find the felon or culprits from the crime scene. Therefore, fingerprints are routinely employed in forensic departments across the world for criminal investigations.

Fingerprints and Facial recognition, biometric techniques can be used primely for authentication purposes. In this paper, I have proposed the theory of using the fingerprints and face recognition methods to record vote, i.e., dual authentication using Convolutional Neural Network(CNN) of Deep Learning. Today's technologies, A subfield of artificial intelligence called "**machine learning**" trains computers without explicitly programming them to learn from past data or experiences. The development of intelligent systems that can mimic human intelligence is made possible by **artificial intelligence**. Wherein **Deep learning** is field that integrates AI and ML. Deep Learning (DL) is mainly involved in the construction of Neural Networks. Deep learning branches such as Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN) is used in fields such as computer vision, speech recognition, shape recognition, Natural Language Processing (NLP),and image analysis and recognition and is still being used. To summarise, we can say that Artificial Intelligence is the parent node, and Machine Learning and Deep Learning are the subdomains of this field, achieving AI.

Encryption and decryption process of an image is based on features using deep learning. For the system authentication and to adequately record votes, the matching database should be as vast and inclusive as feasible. The face is recorded by the camera and is compared to the dataset using the trained algorithm. When the face is recognised the voter is authenticated and is let to vote. The voter ID number, name and time of voting is also recorded. In the next step the voter is allowed to vote for only one candidate, only once. The vote is recorded using the fingerprint that is also compared for authentication. The vote is recored by dual authentication. The recorded vote is immediately counted and the result of the election is stored in the could. The cloud id protected by using zero trust framework. **Zero trust** determines the address specific cloud security authentication challenges. By these means the system would give better experiences and authenticated voting experience.

II. LITERATURE SURVEY:

There are many researches done for the betterment of the voting system worldwide. Vote manipulation, increasing of vote percent and securing of the vote have played main roles to develop new system. Here are few of the researches.

(1)Yr 2020, Vivek S K, et.al; develop e-voting system with Hyperledger Sawtooth blockchain framework. This system does not allow vote manipulation. The platform used were Angular 8, Node.js, and Sawtooth blockchain, Python, Docker technology, Amazon Web Services (AWS). No vote manipulation was recorded.
(2)Yr 2020, Dr. Nicolae Goga, Haider Abdullah Ali1, Naseer Abdulkarim Jaber Al-Habeeb, Sarmad Monadel Sabree Al-Gayar researchers together developed the idea of "mobile technology voting system" during the lockdown of COVID condition. Platform used were Android Studio and PHP.
(3)Yr 2020, Roopak T M, Dr. R Sumathi suggested an e-voting system using blockchain with Aadhar data set that would prevent duplication of vote. It used biometrics(fingerprint or iris) and User ID. Also uses digital signature as key for encryption of vote in the block.
(4)Yr 2020, Shaikh Mohammad Bilal, Prince Ramesh Maurya developed Voting System using Android Application with GUI board for

casting a ballot framework. The vote can be casted using smartphones. The system has conventional strategy for tallying.

(5)Yr 2020, Ramya Govindaraj, Kumaresan P, K.Sree Harshitha developed online voting system with features that could save our time and can vote from anywhere through online. The technology used were C# programming language, Microsoft SQL server and Microsoft azure cloud.

(6)Yr 2021, Awsan A. H. Othman developed a system with the solution that prevented vote information leakage and ensured data privacy using IoT and blockchain. Votes are encrypted on the blockchain to prevent vote fraud. Blockchain and IoT are used to construct the system.

(7)Yr 2020, G. Thomson had suggested using training datasets as a model for deep learning. With the addition of hidden layers, Deep learning is thought to generate the most accurate approximation of a complex function. As a consequence, the system would be able to recognise faces with accuracy.

(8)Yr 2019 Virtanen, T.; Chang, S.; Li, B.; Sainath; Purwins, H, The most common scientific technique is deep learning, used for signal processing, pattern identification, and graphic modelling. Convolutional Neural Networks are used in pattern recognition to identify fingerprints and recognise faces.

(9)Yr 2021 S. Jehovah Jireh Arputhamoni, Dr. A. Gnana Aravanan, An For electoral purposes, an online website has a blocked IP address. The name and address of the voter should be entered on the voting website. It is inconvenient because the existing voting method requires voter physical attendance. It takes less time to finish the process, which is done entirely online.

(10)Yr 2021 Mohamed Ibrahim, et.al., constructed a voting system that utilises its own blockchain, runs on a centralised network of nodes, and includes biometric scanners to securely record vote totals and discern between real and fraudulent voters. The security of the user was increased by using an independent blockchain network as a voting platform.

III. EXISTING SYSTEM

An electronic device used to register votes is known as an Electronic Voting Machine (EVM). Ballot papers system used earlier for recording votes were replaced by the EVMs. Since 2001 there were a lot of issues faced by the votes recorded in the EVMs regarding the manipulation of votes.

EVMs are mainly used in developed and developing countries like ours. Previously vote recording and paper ballot sheets were used for the vote tally, but via progression of technologies EVMs came into the picture to decide the fate of the nations since 1982. EVMs are designed to maintain the track of the total number and specifics of the casted votes. The data in it is secured for longer period, which could be used for future references which might also get manipulated and forged.

Even if EVMs reduce the complications of the paper ballots, many software developers suggests that those are vulnerable to malicious programming and would be easily affected by any hacker, who could hack the machine and can alter the vote counts easily. Despite any number of data are stored in EVMs, a single virus attack enough to malfunction of the existing voting system. The EVMs used during the elections are suspected to damage which results in loss of data.The preponderance of the electronic voting gadgets used in the nation were produced internationally, which ensures that the secret codes that operate the electronic voting machines are in the hands of westerners and may be manipulated to sway the outcome of elections. Fake display units which are easily available in the markets, could be managed to install in the voting machines to manipulated numbers. There is no requirement for a hacker to carry out this technique to compromise the programme. Fake voters can cast any number of fake votes in the EVMs as there is no technology in it to identify the fake voters or repeated votes. Hence the existing system is considered to have its faults that would never give accurate votes which is greatest fault of this technology.

IV. PROPOSED SYSTEM

Face recognition and fingerprint scanning techniques addresses the issue of voter authentication. The photo of the voter is fed to the system by the Aadhar card picture dataset and its trained prior which is then used during the election and at the time of voting. Biometric fingerprint and camera devices are used in the Voting process for voter verification. The voter have to first enroll himself/herself using his/her face scanned for facial recognition through a capturing device. The face is compared with the Aadhar photo dataset and face of the voter is recognised and authenticated to vote. At the time of voting, the voter provides fingerprint through fingerprint scanning device, it allows fingerprint acquisition from the voter which serves as a unique proof of a person. The data id fetched by the controller from the device that reads the fingerprint and compares the read data with the already existing data in the database which is stored during the registration of the voters (via voters ID or Aadhar ID)(Fig.1.). The system checks for the data matches with the pre-processed data of the registered fingerprint of the voter, if it matches then the voter is allowed to cast his vote. Else, the vote is not record and considered along with it a warning is also generated.

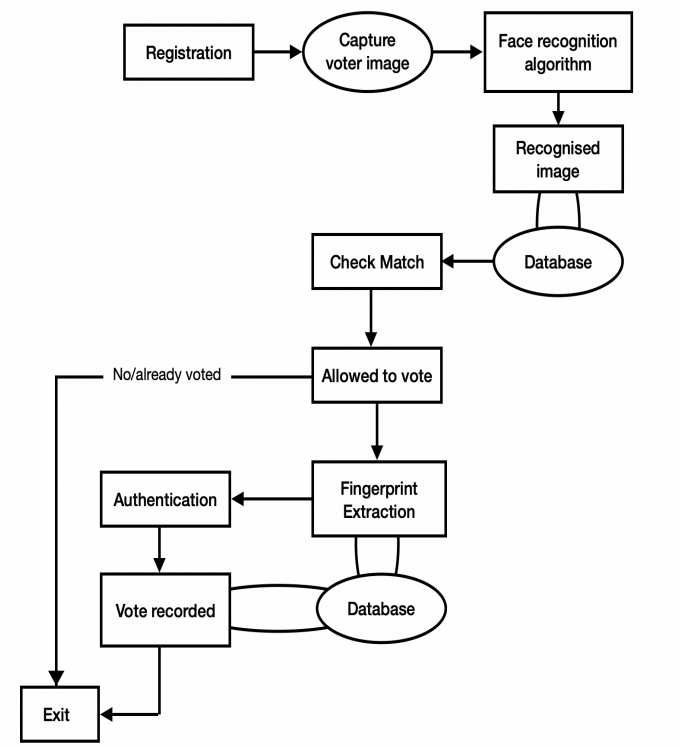

Fig.1. Working of the proposed system

This voting system is based on facial recognition and fingerprint authentication. The voter is recognised using face recognition as the ID's photo. After matching of faces the voter is allowed to choose the candidate to vote. Only one candidate can be selected by the voter. After choosing the candidate vote is casted through the fingerprint. After capturing the finger print the vote is taken in count. The time of the vote casted by the voter is recorded and the casted votes are stored in cloud that is being protected by zero trust algorithm.

In this proposed system the online system with facial recognition and fingerprint authentication will facilitate the voters so as to reduce the frauds, accuracy of the voting is increased, most reliable form of voting, minimum time lags, increasing voters percentage as it provides better, reliable and secure voting environment. The development of an improved authenticated voting system is anticipated in near future.

V. PROPOSED METHODOLOGY

A. CONVOLUTIONAL NEURAL NETWORK (CNN)

Biometric authentication is used in many fields for security reasons. The face recognition and fingerprint matching uses techniques that are machine learning based as they bestow higher accuracy as compared with other techniques. CNN of deep learning is said to pull off a best as near as a function through many number of hidden layers. Feature extraction is the pre-step for recognition and identification before matching. Deep Learning has the child node that is Convolutional Neural Network (CNN) which is mainly used for facial recognition. CNN is a multi-layer network that performs specific tasks using trained dataset classification. Facial recognition using CNN has an accuracy of 98%

B. FACIAL RECOGNITION

To do face recognition, the input of the voters face is scanned by a webcam or camera that is to be detected and verified. Following the input is taken by the web cam, and faces are allowed to be detected. Recognition starts when the CNN classifier is trained, it can be utilised to work.(Fig.2.).

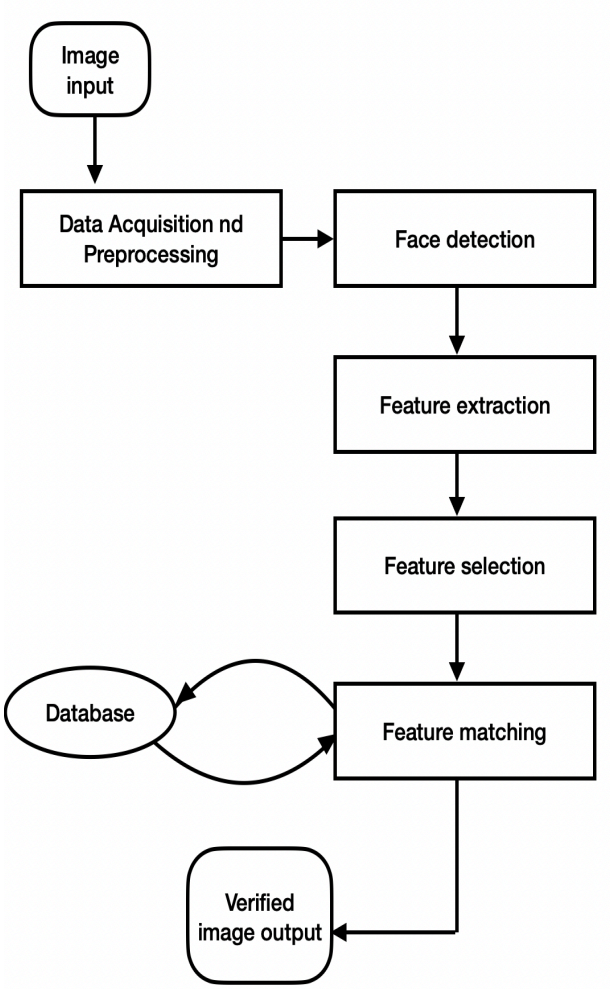

Fig.2. Flow chart of Facial Recognition

The Aadhar card photo dataset is used to train the system and then CNN classifier is used. Face is obtained by the camera, libraries are imported, image processing is done using CNN, the model is trained and tested. The face is recognised and then is the model is used for authentication.

C. FINGERPRINT AUTHENTICATION

Fingerprint extracting has two steps, fingerprint enlistment and matching. The user enters their finger through an optical sensor to check for fingerprint matching, at which point the system creates a template of their finger and compares and contrasts it to templates from the finger library dataset acquired from the Aadhar fingerprint dataset (Fig.3.). Scale Invariant Feature Transform (SIFT) object is used for fingerprint comparison.

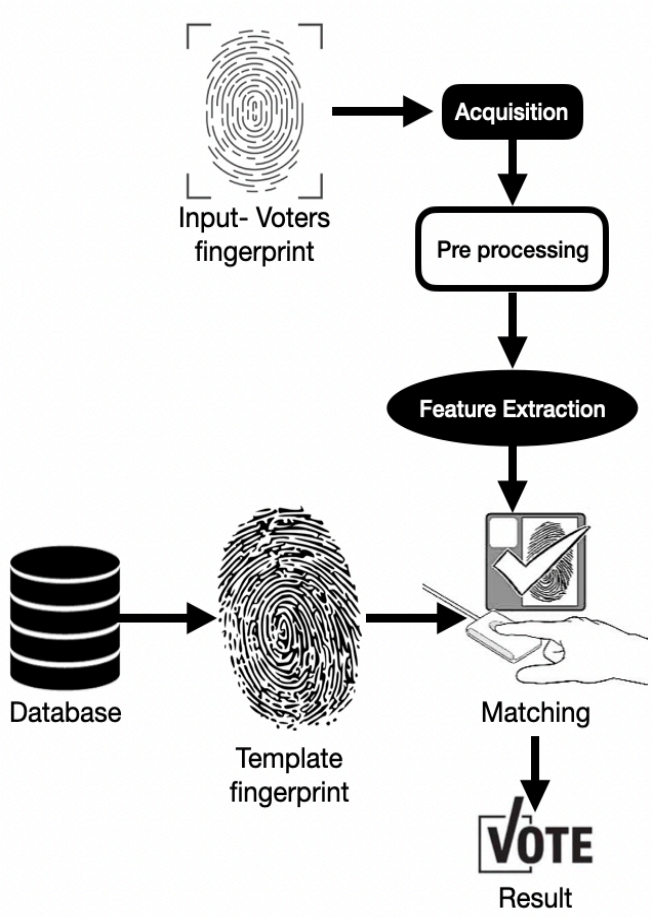

Fig.3. Flow chart of Fingerprint Recognition

The system provides the comparing result, that describes if the fingerprint matches or not. If success the voter's vote is casted for the particular candidate once and vote is stored.

D. ZERO TRUST SECURITY

The casted voting result is saved in the cloud is saved securely in cloud using zero trust cloud security. Zero trust is a framework for securing organisations in the cloud initiates that no users are trusted by default (Fig.4.). Cybersecurity strategy to secure data in cloud is done by zero trust algorithm. A zero trust

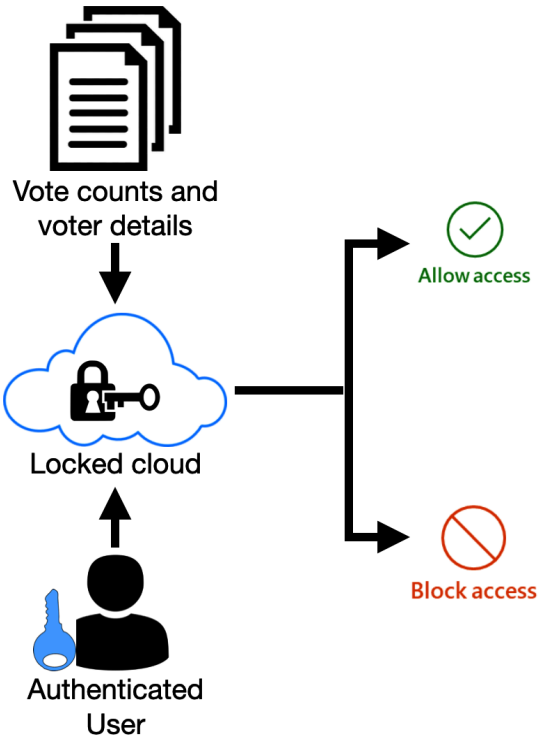

Fig.4. Working architecture of Zero Trust security.

architecture follows the maxim "never trust, always verify". The vote is saved in the cloud and is only retrieved by authenticated pupils.

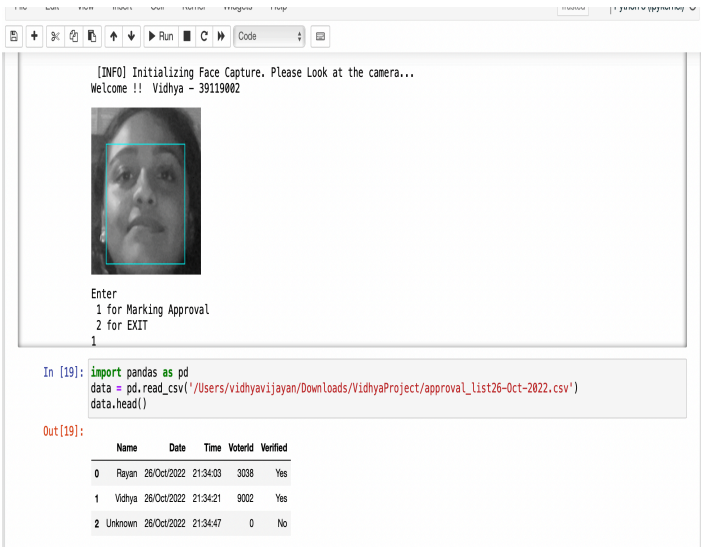

Fig.5. Output of Facial Recognition.

VI. RESULT

To test the model images the trained directory is used. It contains of different images of the person whose images we used for the training purpose.

The voting time, voter ID is recorded along with the face recognised and verified as in Fig.5.

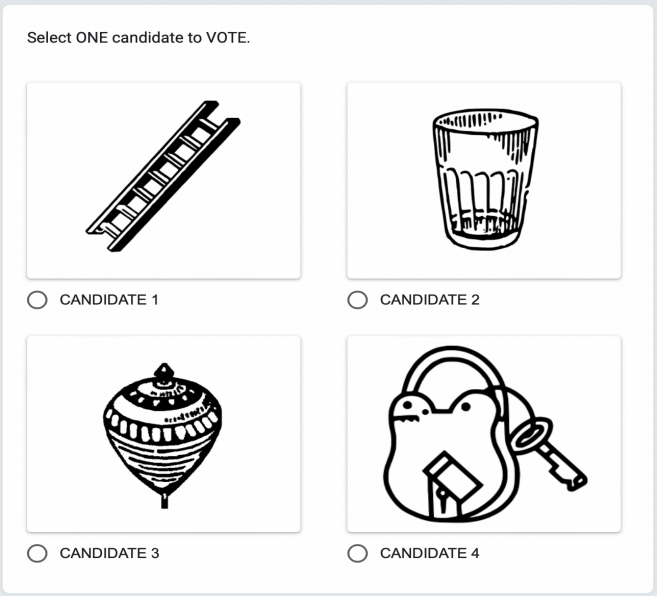

Fig.6. Voter to select the candidate.

Output that the model correctly recognises the face of the input image. Using real-time webcam photos, the system can recognise faces. The ID's photo of the voter and the face captured are compared and recognised.

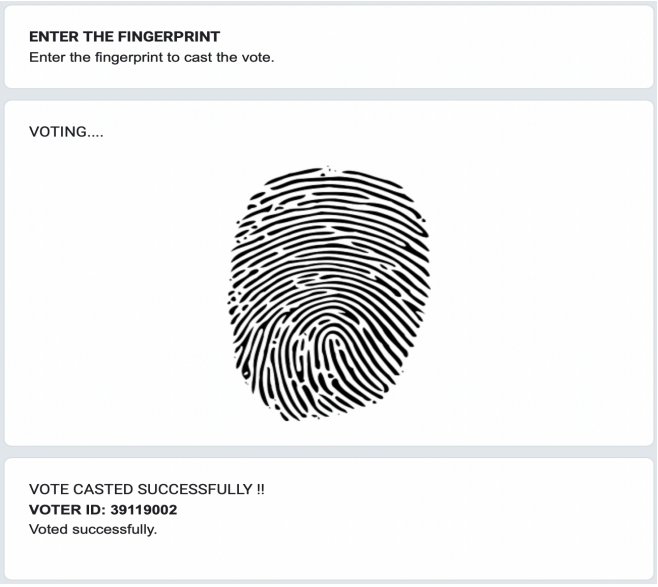

Fig.7. Scanning the Fingerprint to record vote.

The face is verified and moved to the next step for the voter to choose the candidates to vote. Only one candidate can be chosen

by the voter and no multiple voting is allowed (Fig.6.). In this step the voter have to choose the candidate.

After selecting the candidate of the election the voter have to scan their fingerprint in the optical scanner. (Fig.7.)

After scanning the fingerprint the finger print of the voter is compared to the existing data and then the vote is recorded.(Fig.8.)

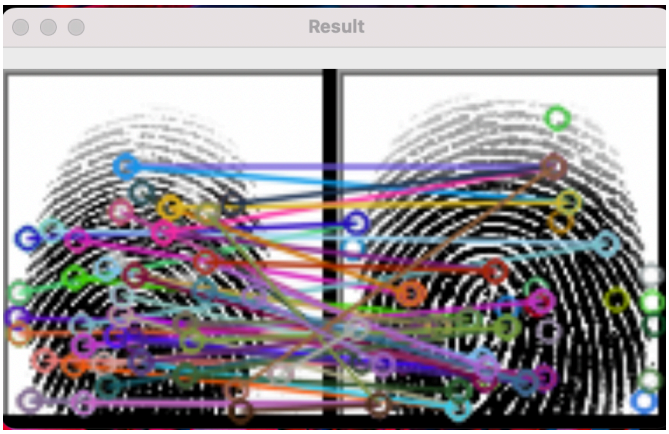

Fig.8. Fingerprint recognised compared using SIFT.

The result of the candidate is reviewed (Fig.9.).

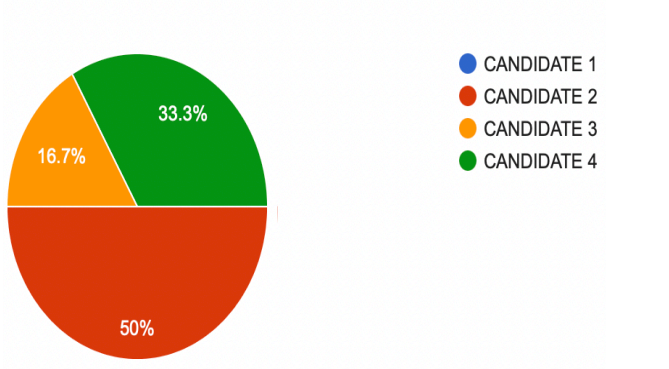

Fig.9. Result of the vote instantly being recorded.

It gives ten times faster than the existing system.

VII. CONCLUSION

World is turning over into completely digitised. As a part of digitisation, voting is also gets to be upgraded to digitised. One of the benefits of this project is that it reduces the time taken to announce the result and forgery complication. The system is made more secure by introducing face recognition and fingerprint authentication. This system allows a person to vote only once. Multiple voting is not allowed.The inconceivable nature of the voting and detains in results of the existing voting system is the key motivation to study for alternative and more secure methods of online voting.

The currently proposed system allows precisely the most effective authenticated voting, than the existing system or the mechanisms used by the government, as it identifies the person based on his/her fingerprint and recognises the voters face, by which it develops to be unique and more secure voting system. Limited expense, uses less power, employs fewer people, and is time-efficient, avoids invalid voting or vote manipulation and more acceptable and accessible for the voter to vote. It is dual authenticated and more secure. As the world is escalating to digital premises, voting should also be secure, transparent and digitalised as the proposed system.

Heeding to the references in India, as a consequence of the proposed system, it focuses to achieve a target of 80+ percent by the end of the year 2030.

VIII.REFERENCES

1. VivekSK,et.al.,“E-Voting System using Hyperledger Sawtooth blockchain framework”-2020.
2. Naseer Abdulkarim Jaber Al-Habeeb, Dr. Nicolae Goga, Haider Abdullah Ali1, Sarmad Monadel SabreeAl-Gayar,“New M-voting System for COVID-19 Special Situation in Iraq”,-2020.
3. Roopak T M, Dr. R Sumathi “Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology”-2020.
4. Shaikh Mohammad Bilal, Prince Ramesh Maurya, “Online Voting System via Smartphone”-2020.
5. Ramya Govindaraj, Kumaresan P, K.Sree Harshitha, “Online Voting System using Cloud”-2020.

6. Awsan A. H. Othman, et.al. “Online Voting System Based on IoT and Ethereum Blockchain”-2021.
7. Stanko I, Geoffrey Thomson Hinton. In: Skansi S. (eds) Guide to Deep Learning Basics. Springer, Cham -2020.
8. Purwins, H.; Li, B.; Virtanen, T.; Chang, S.; Sainath, T. Deep Learning for Audio Signal Processing. *IEEE J.*-2019.
9. S. Jehovah Jireh Arputhamoni, Dr. A. Gnana Aravanan, “Online Smart Voting System Using Biometrics”-2021.
10. Mohamed Ibrahim, et.al. “ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication”-2021.