E-Voting System within IOT Enabled Smart Cities

B.Bala Abirami[1], T.JayaPriya[2], Nakka Kalyani[3], R.Revathi[4]
[1] *Assistant Professor, Department of Computer Science Engineering*
[2,3,4] *UG Student, Department of Computer Science and Engineering' Panimalar Institute of Technology, Chennai 600123*

***Abstract*—The primary goal of this project is to create a smart voting system that will give a more secure voting platform, eliminating the flaws in the current voting system. Two levels of authentication processes are employed in order to attain a better level of security. Techniques like Face Recognition and OTP Verification are utilized to guarantee user login authentication. Voters' faces are photographed and stored as images during the registration process, and when casting a ballot, our system uses a deep CNN-based face recognizer to capture avower's facial image. If the result of the comparison is positive, the system as sum esthete voter is legitimate and sends a One-time password (OTP) to their registered mail address. The user will be able to vote once they've enter etherish password. After casting a ball at, the voter's facial alignment is removed from the system, ensuring that they only cast one ballot.**

***Keywords*— Deep Learning, Face Recognition , OTP authentication ,Secure Authentication.**

I. INTRODUCTION

Elections in democratic nations like India heavily rely on the voting process. India's electoral commission has always relied on electronic voting machines, which are more labor- intensive, time-consuming, and less reliable. India is spending a lot of money to upgrade its entire electoral process so that its population can have better governance. For a stronger democracy, India's voting system needs to be fair, transparent, and completely secure. Because there is a possibility of voting fraud, the existing system is less transparent.

The key difficulties in the current election voting process are voter authentication, voting process intelligence, and data protection. Because of this, developing an intelligent voting system for elections is important.

As modern communications and the Internet are now mostly electronically accessible, users of computer technology have an increasing need for electronic services and their security. Employing new technology in the voting process naturally improves elections. After industrialization, more and more people left their homes and came to cities in search of work. However, many of them still have their voter ID on their home address. No vote takes place because they could not leave their home town son the day of the vote. This is the main reason for the decline in voting rights in our country. Also, fake polls are another issue that needs to be monitored. Our government continue to work to find the best solution to this situation.

Therefore, to overcome this challenge, we created this system that provides greater security by preventing voters from voting more than once. The system also ensures that voters cannot tell who someone else voted for, and that voters cannot duplicate another vote. All voters can ensure their votes are cast. The developed application is based on his intelligent-oriented electronic voting method for IoT- enabled cities. Convolutional Neural Networks (CNN) and his LSB are techniques used for face recognition.

The face analysis uses the Haarcascade Adaboost learning algorithm. Images of voters are captured by webcam. This image is used as input to the face detection algorithm. This is achieved through the image stored in the user's record during registration. Once the user is verified, they can vote. Votes are then stored in a database and used for tallying after the voting period is over.

II. RELATED WORK

A relatively new idea is facial recognition. In 2001, Viola and Jones [1] first proposed her Adaboost framework of cascading to make facial recognition real-time. More recently, convolutional neural networks have been used in computer vision and pattern recognition to accomplish the same thing. Many CNN-based object detection methods have been proposed [2-8]. [9] improved her region proposal- based CNN method and proposed the Faster R-CNN framework. This 110 framework introduced an anchor method to make region proposal a CNN classification problem that can be trained on the entire grid during the training phase. The continuously trainable Faster R-CNN network is faster and more powerful, achieving 73% mAP on the VOC2007 dataset using VGG-net. [10] used the Faster R- CNN framework to accelerate face recognition with promising results.

Most face recognition methods used oriented faces as input. Employing orientation in the test phase was shown to improve recognition accuracy by 1% on the LFW dataset [11]. The usual method of face matching was to predict facial features from the detected field of view, such as eyes, nose, and mouth. A geometric transformation between the predicted facial cues and the predefined cue positions was then applied to the facial spots. Aligned faces with known face identities are then fed into a deep network, which uses the intermediate bottleneck layer as a representation to train a discernible feature extractor for final classification. Categorized by layers.

A huge collection of facial recognition, verification, and recognition is provided. The contributions in [12,13,14] all use multi-stage complex systems that use and merge the outputs of deep convolutional networks with PCA for dimensionality reduction and SVM for classification. Zhenyao et al. It uses a deep network to warp faces into canonical front views and learn about his CNN that classifies each face as belonging to a known identity. Tigerman et al.
[15] proposes a multi-step approach to align faces to 3D shape models[16].
We trained a multiclass network to perform face recognition tasks on a large number of entities.[17] We have also processed Siamese networks for experimental purposes, directly optimizing her L1 distance between two facial features[18]. They used an ensemble of three architectures to achieve the best performance (97.35%) on the LFW dataset[19].

III. TECHNIQUES USED

A. Overview of CNN architecture for face recognition

The ideas for our model are primarily derived from Google's Inception Architecture. The architecture can be described as follows.

A multi-layer feedforward layer consisting of 200 intermediate nodes with another L2 weighted regularization layer interspersed with convolutional layers. While training the model with the triplet loss function, the embedding f(x) of the image x is such that the relative distances measured between different pairs of samples are maximized and between similar pairs of samples are minimized. It is done as it should be. The purpose of the loss function is to separate the anchor record or current image x ai from the positive image x p i and the negative record x n i (any other person) by a fairly large distance, the edge being α.

$$L = \sum_{i=1}^{m} ||f(x_i^a) - f(x_i^p)||_2^2 - f(x_i^a) - f(x_i^n)||_2^2 + \alpha]_+$$

where [z]+ means max(z,0) and m is the number of triplets in the training set. We used a pre-trained model because the model was not trained completely from scratch as it would take considerable time and effort.

B. Facial Recognition

A subset of the entire LFW dataset was used to demonstrate the use of the model. The dataset consists of 100 images of 10 girlfriends. Later, we tested the system using pre-captured images of valid voters. Results and analysis are presented in the next section. Facet detection, transformation, and cropping were performed on the image. A 200-dimensional embedding vector is computed by feeding aligned and scaled images to a pretrained network. When calculating the distance between images of the same person, the distance should be relatively smaller than the distance between two different persons of her. This is the main advantage of using the triplet loss function. The same calculation was performed on a custom dataset of pre-captured images of voters ready to vote in an election. Hence the test image,
A person currently about to vote is compared to images in the database, and if the comparison score is below the optimal threshold.

C. Adaboost

Not only is there a lot of functionality, but sometimes it is irrelevant. Features that are part of the face. Adaboost selects both the best and weaker features and trains a classifier using them. A "strong" classifier is built by an algorithm and a "weak" classifier. Here, a strong classifier means one that has a low error rate and is definitely part of a face, and a "weak" classifier means an error rate of less than 50%. Facial area of the face. Therefore, we use Adaboost to combine these weak classifiers into strong classifiers for face detection.

IV. PROPOSED WORK

The system proposed here is used to vote online via a website using facial recognition using machine learning technology. To get a high level of accuracy from the "training data" Haar Cascades uses her Adaboost learning algorithm. We select a small number of significant features from a large set to provide efficient results for our classifier.

First, the algorithm needs a lot of positive images (images with faces) and negative images (images without faces) to train the classifier. After that, we must draw features from it. Images are processed using CNN image processing techniques.
During voting, one-time his password will be sent to the voter's email id. Provides additional authentication to your system. The main advantage of a Haar-like function over most other functions is its computational speed. Haar-Cascade's machine learning algorithms identify objects in images or videos. Hair cascade detection is shown in fig.1 below.

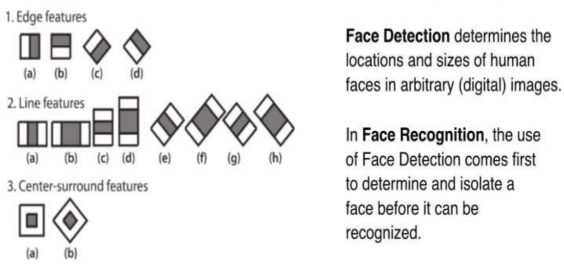

Fig.1 Haar-cascade

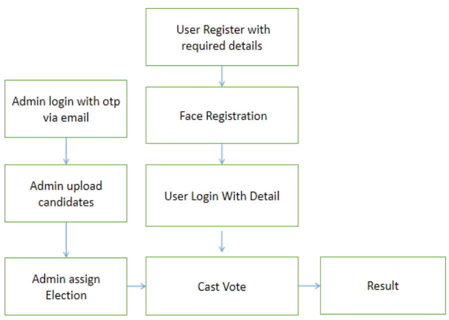

Fig. 2. Block Diagram of Proposed System

V. METHODOLOGY

A biometric method that analyses a person's distinctive facial features is facial recognition. From the properties of images and videos, recognition of faces can recognize individuals. Therefore, a face recognition system will recognize the characteristics of the face and compare the values to those in the knowledge base. Computational similarity matching is aided by some form of feature similarity measure, and as a result, the most predominant label is used as the image's label. The classification result will return false, i.e., the system will not be able to identify the individual, if the similarity metric value is less than a specific number. Face recognition works in this manner, and if two people have the same features, their resemblance is too great.

Since the suggested idea is a totally web-based system, the fundamental aspects of web-based technologies, such as database construction and image processing capabilities, govern the system's software requirements. By using this website, the voters will be able to cast their votes. After facial recognition, eligible voters will be permitted. Regardless of the device used to access the website, the voter's face will be captured. After that, the server will get the taken image. The server searches through each image in the database to see if any of the registered ones are a match. If a match is made, the voter is registered, acknowledged by the electoral commission.

Utilizing the Haar Cascade method, faces are detected. The website will state that the voter is not recognised and cannot vote if a match is not made. When the facial photos are identical, the image is stored on the server.The ten face image are taken and position of ten face, count are calculated. The proper voter face may be identified by comparing the two photos..

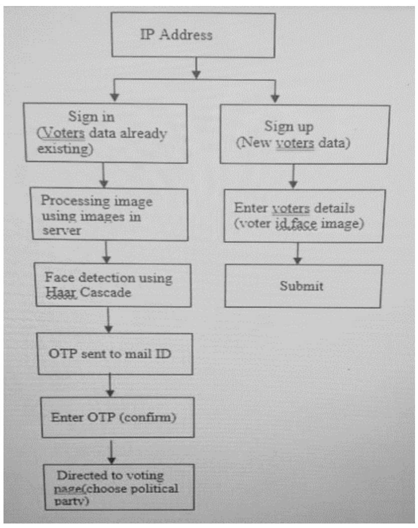

Fig. 3. Methodology of the system

VI. FACE DETECTION USING HAAR CASCADE

An algorithm is used to recognise items in an image or video, including faces. By using a series of square-shaped Haar characteristics, the algorithm is trained to recognise faces. Then, classifiers are used to identify the face (1) rather than the face (0). There are four phases involved in face detection. First, employing integral pictures to discover Haar features; second, integral images ;then Adaboost; and finally, a cascade of classifiers

A. Detecting Haar features

Haar wavelets, which identify faces by taking into account smaller portions of a face at once, compute their pixel intensities' sums, and then compare the sums, replace the time- consuming and labor-intensive usage of picture pixel intensities for face identification prior to Haar features. We have normalised greyscale for pixels in black and white images.

The key aspect in face recognition is detecting relevant features in human face like eyes, eyebrows, nose, lips. So how do we detect these features in real time/in an image? The answer is Haar Wavelets or Haar Features.

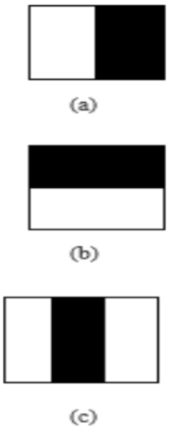

Fig. 4 Some common Haar features (a) Nose (b) Eyes (c) Mouth

Haar features are highly good in identifying rectangular characteristics, making them a very useful face identification method. Fig. 2(b) below can represent an eye. The eye is represented by the darker area, and the cheek region by the lighter area. Eyes are often recognised first since they are the darkest regions of the face in comparison to the rest of the face, whether in grey scale photos or not. Another illustration may be seen in figure 2 (a), where the nose's bridge is often higher and darker than the face's cheek region. This is how Haar features that look for lines and edges initially identify the face or different parts of the face.

VII. RESULT

An online website is created using HTML and all the software codes are implemented using Visual Studio. The designed system is superior to the existing systems and is highly secure. The CNN algorithm used makes the system unique and efficient. OTP also gives extra authentication. It makes sure that the voter is validated before the voting process. By using the Smart Voting System the count of fake votes automatically reduce and may cease to occur and also makes the whole voting and counting of the votes easier, energy-efficient, accessible and more secure.

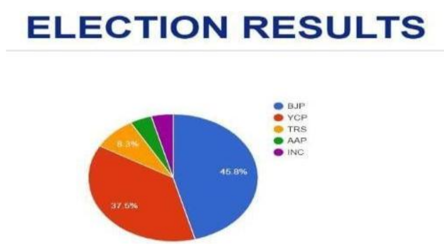

Fig 5. Result of vote election:

VIII. CONCLUSION

Auto-tuning with convolutional neural networks reduces human involvement in the process. The manual matching process is replaced by this automatic matching technology. This device creates new data at a rate of 1 million bytes per minute. That means less money and fewer people. Newly registered voters and deceased voters must be registered and removed from the database each year or before an election. Smart voting is mainly responsible for most of the Indian cities. It should be seen as the main problem for most of us. Existing voting methods are manual with a lot of manpower and labor, and even if voting goes online, there is a need for a secure voting system for voters to cast their ballots. machine learning technology. It is used to recognize a person's face and check if the voter has authority.

IX. FUTURE WORK

We have tested the suggested system using a biometric authentication mechanism at one level. By recording someone's image with a video camera, a face recognizer can analyse its features. The complete structure has been examined, including how close the eyes, nose, jaws, and mouth are to one another. The distinguishing characteristic used to identify a person is their relative distance.

When a user is in front of the camera, these measurements are compared to his identification in a database. To eliminate any security risks to India's general elections in the near future, we would like to implement fingerprint recognition as a second level of identification.

REFERENCES

[1] "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryptio" Xuechao Yang; Xun Yi; Surya Nepal; Andrei Kelarev, IEEE 2020.

[2] "Electronic Voting Using Blockchain And Smart Contracts: Proof Of Concept" Giraldo; Barbosa Milton C.;Carlos E. Gamboa ,IEEE October 2020

[3] "A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature" MahenderKumar; Satish Chand; C. P. Katti , IEEE Systems 2020

[4] "A Smart Contract System for Decentralized BordaCount Voting" Somnath Panja; Samiran, Bimal Roy, IEEETransactions on Engineering 2020.

[5] "A Comparitive Analysis on E-Voting System Using Blockchain"Kanika Garg; Pavi Saraswat; Sachin Bisht; Sahil Kr. Aggarwal; 2019 IoT-SIU.

[6] "SecEVS: Secure Electronic Voting System Using Blockchain Technology" Ashish Singh; Kakali Chatterjee.

[7] "An Approach to the Efficient Security Algorithms Used in Voting Scanning in an Electoral Process" Segundo Toapanta; Tamayo Lamar; Ortiz Rojas; 2019 IICSPI.

[8] "Decentralized E-Voting Portal Using Blockchain" Kriti Patidar; Swapnil Jain, 2019 10th ICCCNT.

[9] Cranor,L.(2004). Electronic Voting Hot List. Retrieved from http://lorrie.cranor.org/voting/hotlist.html.

[10] Dill,D.(2004),E-Voting misconceptions.Retrieved fromwww.verifiedvoting.org/article.php?id=2609.

[11] Dill,D. Lecture, October 14,UC Berkeley.

[12] Dugger,R.(2004).How they could steal the Election this time. The Nation, Retrieved from www.thenation.com/doc.mhtml?i=20040816&s-dugger,July 29,2004.

[13] [6:26 PM, 5/14/2025] Revathi Chand: Ben Adida. Advances in cryptographic voting systems. PhD thesis, Mas-sachusetts Institute of Technology, 2006.

[14] Ben Adida. Helios: Web-based open-audit voting. In USENIX Security Symposium, volume 17, pages 335–348, 2008.

[15] Ben Adida. Encrypting your vote in Javascript. In Rump Session for EVT/WOTE, 2011.

[16] Communities in America currently using proportional voting. The FairVote website archives. http://archive.fairvote.org/?page=2101.