Eng. Sci., 2021, **16**, 341–353

Engineered Science

DOI: https://dx.doi.org/10.30919/es8d585

# Face Detection using Deep Learning to ensure a Coercion Resistant Blockchain-based Electronic Voting

Pooja S,[1] Laiju K Raju,[2] Utkarsh Chhapekar[1] and Chandrakala C.B[1,*]

## Abstract

An election is a powerful tool of any democratic country, which allows every citizen to exercise their right to vote. Though in-person voting is the most widely used medium for a citizen to vote, circumstances like a pandemic, natural disasters, or other location-based issues could deter an individual from doing so. This work proposes an architecture for a mobile-based internet voting application that could be downloaded on a smartphone, allowing citizens to vote remotely. Existing web-based online voting systems are complicated for novice users, requiring a complex key management process and a lack of coercion resistance voting system. The proposed work is a mobile application, which ensures more population coverage. The work also suggests a key management system for regional election officers, thus freeing novice users from the complications of key management. A face detector is proposed to provide coercion resistance in this online voting system. Face detection uses a deep learning-based multi-task cascaded convolutional neural network (MTCNN). The proposed model has also incorporated multi-factor authentication, blockchain technology, and asymmetric encryption standards to ensure security features required in a voting system while providing a hassle-free voting experience to the voter.

*Keywords:* Blockchain; CNN; Face Detection; Paillier Threshold System; Remote electronic voting.
Received: 11 September 2021; Accepted: 6 December 2021.
Article type: Research article.

## 1. Introduction

According to the election commission of India, for the 2019 elections, there were over 912 million[1] registered voters in the country, out of which a record 67.4% voted. Though this may seem like a significant number, it also means that nearly 298 million people did not vote in this election. A citizen can only cast his ballot at the assigned polling booth near his registered address in India.[2] This increases the difficulty for many people who usually migrate to the cities searching for work and are not present in their hometown.

Nearly 1.3 million army service personnel cannot vote due to their different posting locations[3] Remote Electronic Voting (REV) can be the perfect alternative that, if used wisely, can increase voter coverage and ensure faster results by its digital nature. However, it is not without its issues. REVs bring up new challenges like electronic verifiability, privacy risks concerning voter coercion by criminal elements of the society, forced abstention, and threats to the personal voting device like browser vulnerability.

The present work proposes a new architecture for Remote Electronic Voting (REV) systems that address these fundamental issues for implementing a REV system. It offers to implement the solution in a mobile operating system (OS) like Android OS to cover the maximum possible population since a computer is accessible to only 4% of the rural populace in India.[4] The work's main contribution is to free the user from the hassles of key management, unlike in other existing work[5,6,7] where the user has to perform the key management but the users struggle with the management of keys.[8] The proposed work requires key management training only to the regional elections officers who are small in number. The work aims to provide users with the same voting experience as physical voting, thus ensuring coercion resistance. This is addressed by using multi-task cascaded convolutional neural network (MTCNN) based face detector, which detects the presence of multiple faces in the camera, ensuring that the coercer cannot verify whom the voter has voted for. The application would immediately exit if another person comes in the viewport of the device.

[1] *Department of Information & Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka, 576104, India.*

[2] *Senior Software Engineer, QuEST Global, Trivandrum, Kerala, 695581, India.*

**E-mail:* chandrakala.cb@manipal.edu ( Chandrakala C.B)

This system uses a two-tier authentication using fingerprint and one-time password (OTP), both of which can be verified from the government-approved Aadhar database[9] to ensure verifiability. The use of a face detection system ensures that the authenticated voter is always in view. Blockchain technology ensures the integrity of the stored data. The distributed ledger technology provides immutability to the system. It protects it from a single point of failure (SPoF) attack on a centralized system like the current Electronic Voting Machines (EVM) systems. Homomorphic encryption provides end-to-end privacy and verifiability. It allows for secure multi-party communication with solid resistance to attacks like SPoF, distributed denial of service (DDoS), *etc*.

Killer *et al*.[5] proposed a blockchain-based electronic voting system called Provotum. It uses a public permissioned Blockchain (BC) as a Public Bulletin Board (PBB), where only authorized entities can sign blocks, while the public can verify all BC data. It uses a permission-less Proof-of-Authority (PoA) based Public Blockchain(PB) where the captured vote is securely transmitted in the system. But this proposed model does not offer any coercion-resistance or receipt-freeness(RF). Another drawback of this system is that only a yes or no vote can be cast, but no other information can be stored.

Agarwal *et al*.[10] proposed a method to curb the problem of 'rigging', wherein multiple votes are cast by the same person, by developing a prototype for fingerprint-based authenticity for biometric-based voting. The disadvantage of this method is that the fingerprint scanner designed using the ARM controller needs to be installed at each voting machine and hence does not contribute to the concept of remote voting.

Manikandan *et al*.[6] proposed using methods like candidate verifiability and the use of a One Time Password (OTP) for internet-based voting, which helps in ensuring the authenticity of the vote. The author has not stated how each candidate's public and private keys would be securely transferred to the user, otherwise leading to man-in-the-middle attacks. This system also proposes no verification for the impersonation of a voter. Mansingh *et al*.[11] proposed using (Radio Frequency Identification tags(RFID) tags and Fingerprint scanning as two-factor authentication to curb the issue of impersonating a voter. This method improves authentication for the EVM systems.

Zhang *et al*.[12] proposed a blockchain-enabled voting system that employs the use of smart contracts in the application. The system proposes scalability, privacy enhancement, universal verifiability, end-to-end verifiability, vote–and–go, un-reusability, affordability, fairness, robustness and requires each voter to have a unique public and private key. But it lacks an explanation of the secure distribution of these keys to many users who are not technologically capable of understanding how to deal with them.

Baudier *et al*.[13] proposes to analyze the use of Blockchain systems for secure e-voting. It has been concluded that blockchain can reduce fraud, increase transparency. Digital technology increases the level of participation, and the move to a sustainable solution (*i.e.*, refusal to use paper) is the need of the hour. Khutkyy *et al*.[14] explores the technical implementations of different e-voting schemes implemented in Ukraine. Elections held in a limited setting with only a few participants. In this study the use of blockchain technology was investigated by the election commission, where each user is given credentials to login into the network, but it does not mention how the cryptographic key would be securely distributed to the population. Estaji[15] proposed a method to avoid coercion in the election. It is necessary for remote voting, but it increases the complexity of tallying to weed out fake votes. The paper lacks proof of security for the presented NV12 scheme.

Tolosana *et al*.[16] highlighted different types of facial manipulations, benchmark databases for research in face manipulations, and face detection. The work by Zhang *et al*.[17] has more stable detections and face alignment. Although Guo *et al*.[18] proposed that the Multi-Task Cascaded Convolution Networks[17] do not work with small face images, the proposed work requires the use of the primary camera, which involves face detection at a close distance. Iftekhar *et al*.[19] proposed detecting human object interaction by utilizing relative spatial configurations object semantics. Guided Transformation Network (GTNet) uses self-attention to encode spatial contextual information in human and object visual features.

Our work aims to present a proof of concept for designing a Remote Electronic Voting system(REVS). The REV system uses an amalgamation of technologies to provide a highly secure and hassle-free voting experience for administrators and novice voters. The system ensures the capability to vote securely from a remote location. By using cryptographic mechanisms and a blockchain-based distributed ledger, it also aims to achieve a secure voting process and vote verification. This system's security measures can increase the population coverage during an election while also ensuring a valid vote capture. This works aims to provide a complete online voting system that incorporates user registration, secure vote capturing, vote tallying, and the vote publishing process. The key aspects such as ensuring non-repudiation through multi-factor authentication using biometric and One Time Password (OTP) for verification is addressed implicitly. Coercion prevention ensures that multiple people are not present when a user is attempting to vote. An encryption system that ensures secure communication between all the stakeholders involved. Resistance to man-in-the-middle attacks by using the asymmetric encryption standard. The work ensures integrity of each vote by using a blockchain system that stores the hash of the voting content. The system ensures ease of key distribution to Regional Election Officers (REO) who will manage the data center and act as the validator nodes of the blockchain.

## 2. Design and methodology

The system architecture for the proposed work is emphasized

 

in the below subsection 2.1. The architecture has addressed fundamental components[5] required in an electronic voting system. Subsection 2.2 emphasizes the methodology used to incorporate the functionalities specified by each module in the proposed architecture.

### 2.1 Remote electronic voting system (REVS) architecture

The proposed REVS system incorporates the fundamental components[5] of an electronic voting system, such as user registration, vote capturing, vote tallying, and result publishing. The flow of each component with respect to the proposed work is shown in Fig. 1. The system does not require an explicit voter/user registration if the Aadhar database is linked to the proposed voting system for verification. Since the Aadhar database has the date of birth stored for each user, it can be used to check whether the intended user is eligible to vote. The system starts with the user authentication module, where the user verification is done using fingerprint authentication and one time password. It is assumed that once access to the Aadhar database is granted, the fingerprint can be authenticated from the Aadhar gateway. Once user authentication is successfully completed, a pre-vote capturing module is created to guarantee that the user does not have to deal with the underlying complexity of key management. Before the user casts a vote, the user vote capturing module is proposed to check if the user is observed or under coercion. Once the user's vote is cast, a vote verification module is offered to check if the vote casted has reached the nodal centers tamper-free. Once the vote capturing process is over, a vote tallying module is proposed to compute totaling of the vote. The last module explains the result publishing process. Only after the successful completion of each module, the process is fed to the next module. The module specification is illustrated in the below subsection.

The use-case diagram shown using Fig. 2 represents the interaction of different actors of the system with the different modules stated in Fig. 1.

#### 2.1.1 User authentication module

The User Authentication Module consists of a biometric-based and One Time Password (OTP) verification. Fingerprint-based biometric authentication is used in the proposed work. The fingerprint is scanned from the user's personal device and verified with any existing Biometric databases. The most suitable solution for the Indian scenario is extending the UIDAI Aadhar database portal[9] for biometric verification. As per Aadhar Act 2016,[20] Aadhar verification can be either done using physical or electronic way of authentication. This work proposes extending the fingerprint authentication with the Aadhar database to ensure that an eligible citizen participates in the voting process. Thus, it removes the need for the electoral roll process required in the existing ballot-based voting system.[21] The proposed user authentication module is shown in Fig. 3.

Biometric authentication ensures non-repudiation, which is a must-have security feature in the proposed work. Fingerprint-based biometric authentication is favored over other biometric authentication types such as iris scans or face recognition because of its ease of use and the abundance of fingerprint scanners in today's smartphones. The uniqueness of a fingerprint scan and its high success rate has favored it to using other types of biometric scans.

OTP verification ensures user's liveness and is it uses the registered mobile number linked with the Aadhar database. There can be multiple people registered with the same mobile number. Thus, the multi-factor authentication includes OTP and biometric authentication, ensuring non-repudiation. The biometric and OTP verification further ensure that only one user can vote once using his registered sim card linked with his Aadhar. This process ensures that everyone can vote, even if only a single smartphone is available in the family. This contributes to reducing absentees in the voting process.

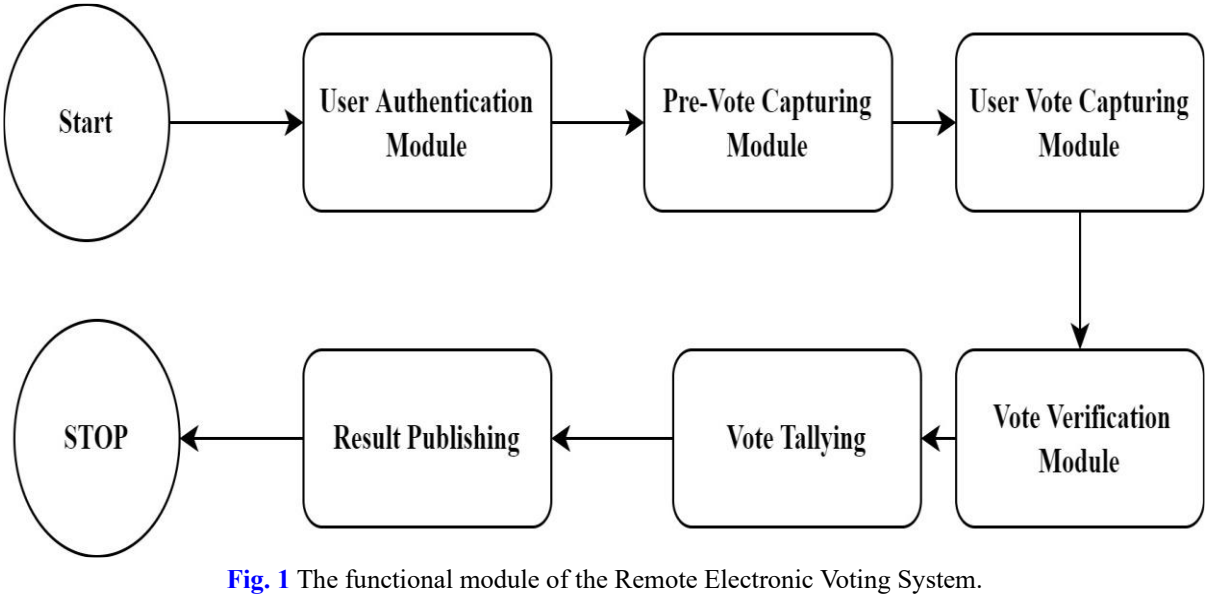


**Fig. 1** The functional module of the Remote Electronic Voting System.

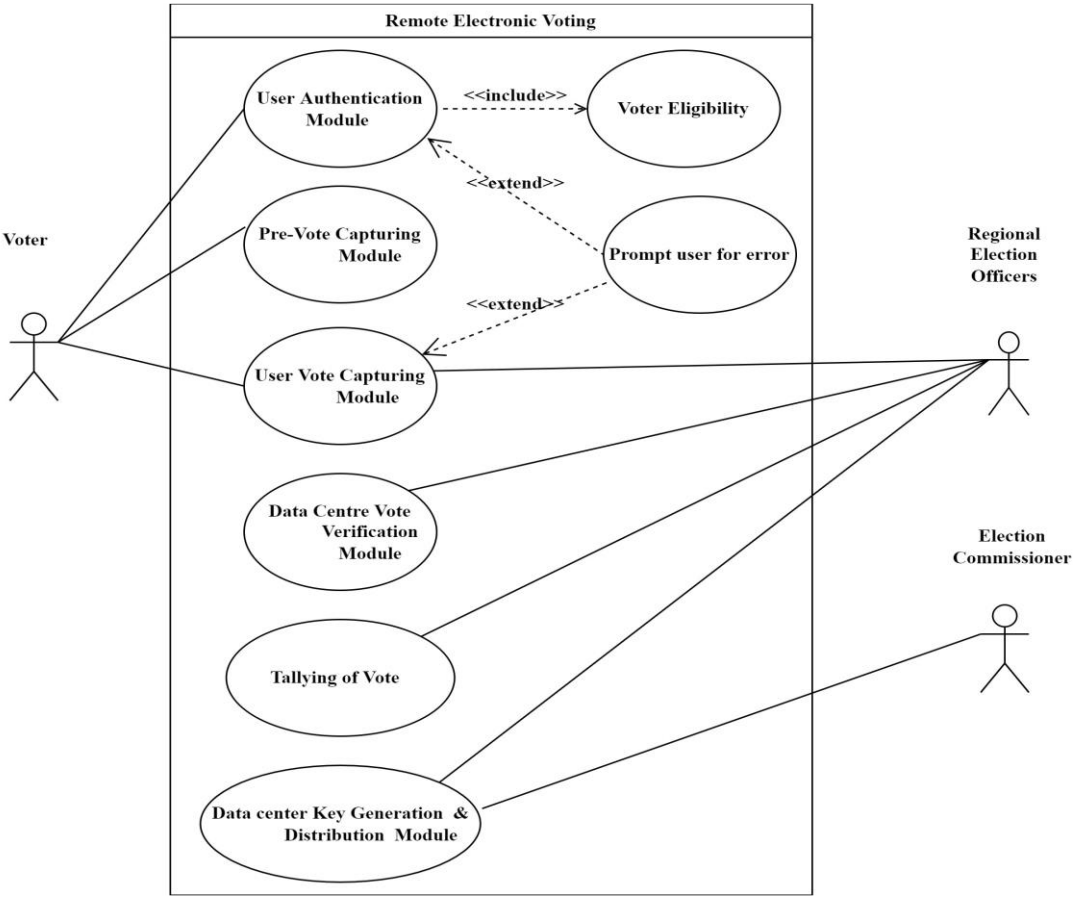


**Fig. 2** Use-case diagram of the Remote Electronic Voting system.

### 2.1.2 Pre-vote capturing module

The pre-vote capturing module is initiated only after successful user authentication. User input is required for region selection. Region selection initiates the transfer of the public key required for encryption to the client application. Two public keys are transferred from the selected regional data center. The global Paillier Threshold public key denoted by $K_T$, and the asymmetric public key, which is specific for each regional data center, 'i' is represented by $PK_i$. In the application, the camera detects the number of faces in the background. The criteria to start the vote capturing module is that only a single face should be visible in the camera. The module uses face detection based on a multi-task cascaded convolutional neural network (MTCNN)[17] which localizes the face using a bounding box and aligns the same. This concept detects if the user is interacting with other, thus ensuring the coercion-resistant security feature to the voting application, lacking in other existing works.[22] The flow chart of this module is shown in Fig. 4.

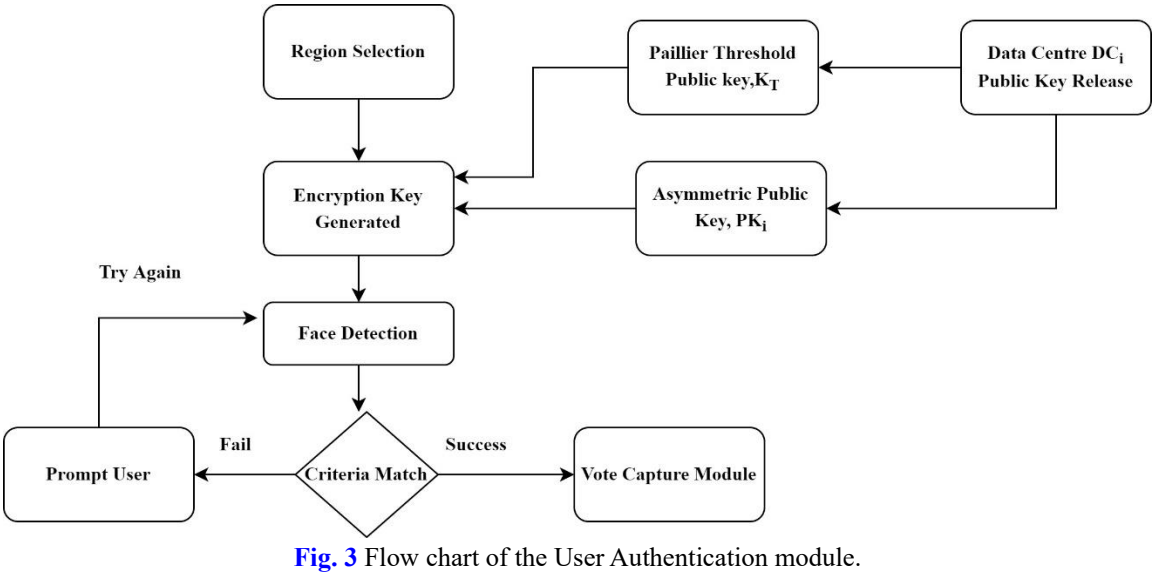


**Fig. 3** Flow chart of the User Authentication module.

 

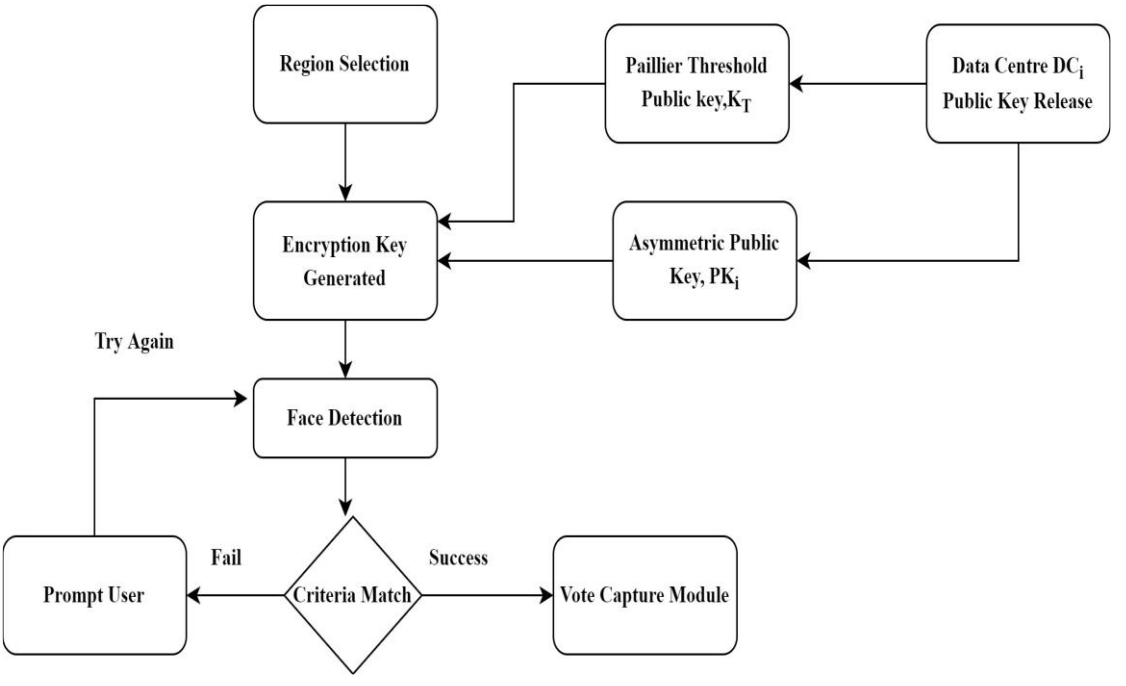


**Fig. 4** Flow chart of the Pre-Vote Capturing module

### 2.1.3 User vote capturing module

Once the user has casted his/her vote and it is captured in the application, the user vote capturing module gets triggered. Its flowchart is shown in Fig. 5. The encryption of the captured vote happens at the client-side application. The strategy proposed in this module is as follows.

The user's vote, V is encrypted to get the resultant ciphertext $C_1$ shown using equation (1) using the global threshold Paillier Public key, $K_T$ . The vote data structure consists of candidate id for which the user wishes to cast a vote, timestamp of vote capture, and the session key. The session key is established when the user selects the voting region. The session key is unique for each voter capturing session and is used to trace back to the user for prompting the user with a message if the vote capture was successful or not. The SHA-512 hash function is used to compute hash, $H_1$ of the cipher message $C_1$ as shown in equation (2).

$$C_1 = E_{K_T}(V) \quad (1)$$

$$H_1 = h(C_1) \quad (2)$$

The second encryption is done for the content, $C_1 || H_1$ using the asymmetric public key $PK_i$ and is shown using equation (3) $C_2$. The resulting ciphertext obtained is redirected to the selected data center. At the data center, verification of vote is initiated to ensure the vote has not been tampered with during the transit. Hash, $H_1$ is again encrypted using threshold Paillier Public key $K_T$. $CH_1$, the encrypted hash of $H_1$ is redirected to be stored at the BC is shown using equation (4).

$$C_2 = E_{PK_i}(C_1 || H_1) \quad (3)$$

$$CH_1 = E_{K_T}(H_1) \quad (4)$$

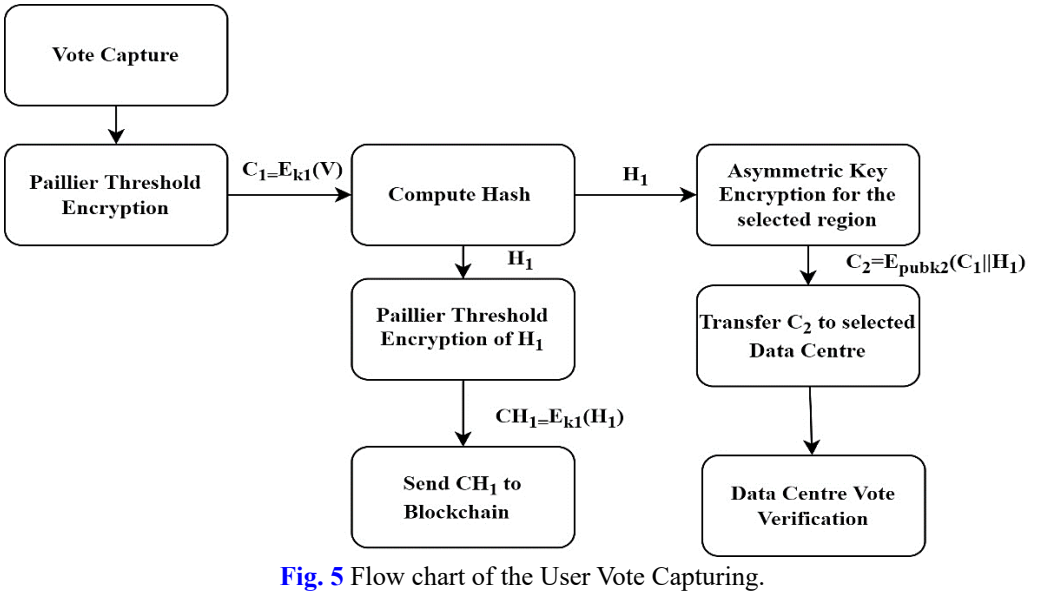


**Fig. 5** Flow chart of the User Vote Capturing.

### 2.1.4 Data center vote verification module

This module facilitates a receipt to the user for the successful capture of the vote or prompt the user for a vote capture again. This ensures end-to-end verifiability that their vote is captured and the equality of the hash is verified. Received ciphertext, $C_2$ is decrypted at the data center using its specific private key $PrK_i$, and the process is listed below as shown in Fig. 6.

$C_2$ is decrypted using datacenter specific private key, $PrK_i$ which yields in $C_1 || H_1$. Hash of $C_1$ is computed using hashing algorithm shown using equation (5). Compare the equality of two hashes *i.e.* $H'_1$ and $H_1$. If both are identical r, a response is sent back to the user with the message, "Vote is captured successfully" and encrypted vote, $C_1$ is stored at the data center. Else, user is prompted to vote again.

$$H'_1 = h(C_1) \tag{5}$$

### 2.1.5 Tallying of vote

The vote tallying module on successful completion of the process publishes the result. The process is described below and is shown in Fig. 7. From the data center, each encrypted vote $C_1$ is collected and passed to a hashing algorithm to obtain $H'_1$. For this transaction id, the corresponding hash value is retrieved and stored in blockchain, $H_1$. Then the equality of both the hashes is compared. If both the hashes are identical, $C_1$ is decrypted to yield partial decryption shares. The actual tally of the vote is computed by decrypting the threshold number of partial decryption shares.

### 2.1.6 Datacenter key generation & distribution module

This is an offline module where the generation of asymmetric key pairs and distribution of the Threshold Paillier Encryption System is carried out by the Election Commissioner (EC). The data centers are managed by regional election officers (REO). The data centers can be on a virtual private cloud, which can either be leased or government-owned. For each state, there can be multiple nodal centers storing the vote of designated areas. Thus data centers are distributed.

Regional Election Officer's (REO) are also the validator nodes of the blockchain who store the hash of each voting transaction. The key generation by EC is carried out using the key generation process explained in the Paillier Encryption System described in sections 3.1 and 3.2. While using the Threshold Paillier encryption system, if there is $l$ number of REOs, then that many number of partial secret shares, denoted by $s_i$ are generated and shared with the REO. The keys are transmitted to the REO's using a smart card. The smart card is programmed with the Regional Election officer's identification information like user-id, biometric information for authentication, and keys required for the voting process. The smart card used is a contact-based secure microcontroller, which includes a RAM, ROM, input/output functionality, and user memory.[32] The security protection of the smart card is described in detail in Smart-Card Alliance.[23] The manufacturer can delete the stored data if the smart card is penetrated without proper authentication.

The functionalities are described below and are represented in Fig. 8.

1. EC securely distributes keys to all the registered and trained regional election officers.
2. The threshold Paillier private key shares are computed by EC and are distributed securely offline to the REO.
3. EC also distributes the asymmetric key pair to each of the REO.

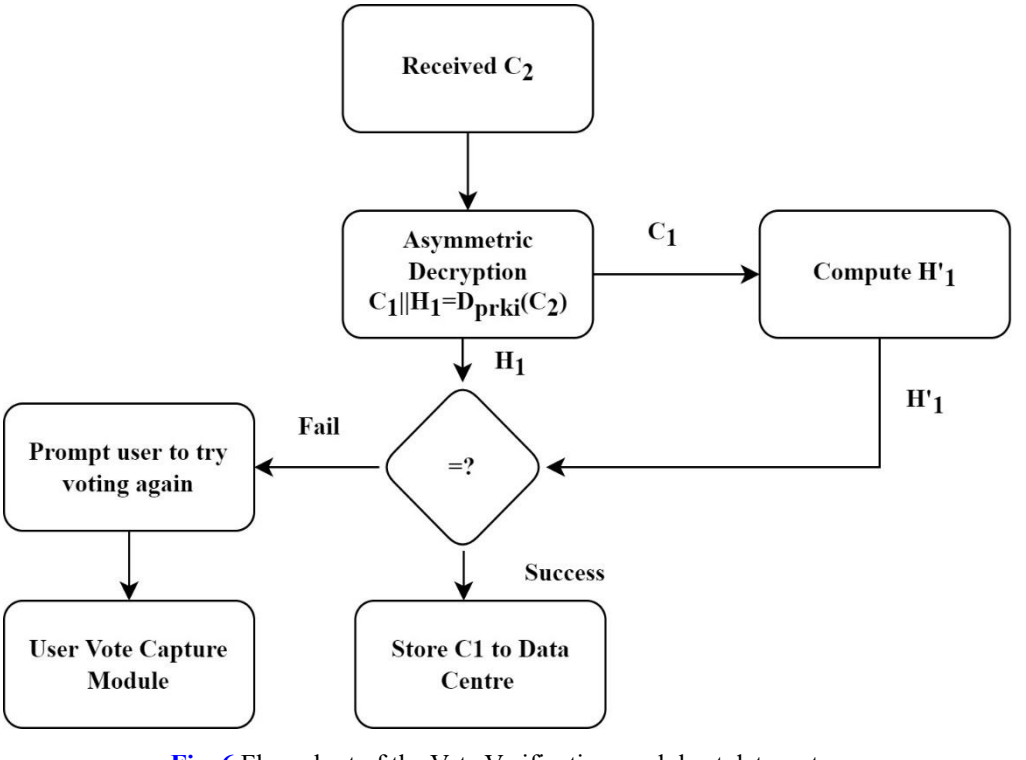


**Fig. 6** Flow chart of the Vote Verification module at datacenter.

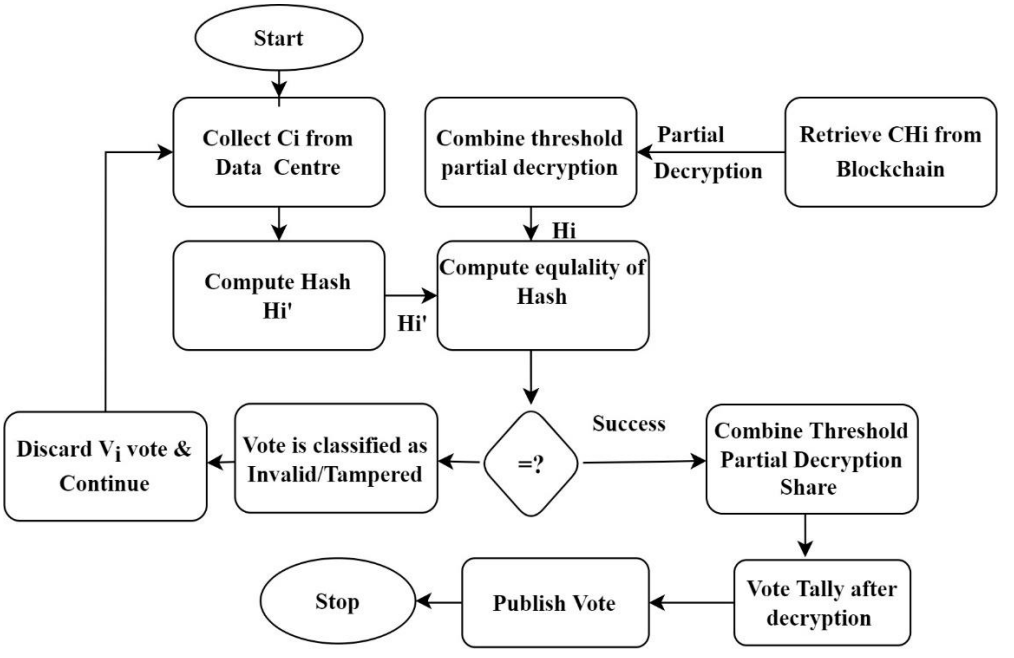


**Fig. 7** Flow chart of the Tallying of Vote module.

## 2.2 Proposed methodology

### 2.2.1 Secure multiparty communication using paillier encryption system

The system adopts the public key cryptography Paillier cryptosystem[24] for encryption which follows a probabilistic algorithm. Initially, the system proposed to use single public-key encryption based on the Paillier cryptosystem. The main drawback of this approach is that the vote decryptions will be based on private keys associated with single data centers/REO's. If the REO private key is compromised, this leads to a single point of failure (SPoF). This situation can even lead to the nullification of an election[25] which destroys the whole purpose of the online voting system. The existing system[7] relies either on single public-key encryption or a symmetric standard. Thus, it lead to nullification of election in those centers where keys are compromised. To avoid such situations, the proposed work uses the Threshold Paillier encryption system, which requires the participation of $l$ number of nodal centers for decryption. This ensures that the attacker compromises at least $l$ number of nodal centers, which is a tedious process. Also, in the existing system,[23] novices users must manage the keys through a smart card. Thus, if the smart card is lost, the user cannot cast his vote. The proposed work does not require novice or any other user's to manage the keys. The system ensures that on the selection of a voting region, the public keys of the Threshold and Paillier encryption system get transmitted to the user secure network protected by IPsec layer.

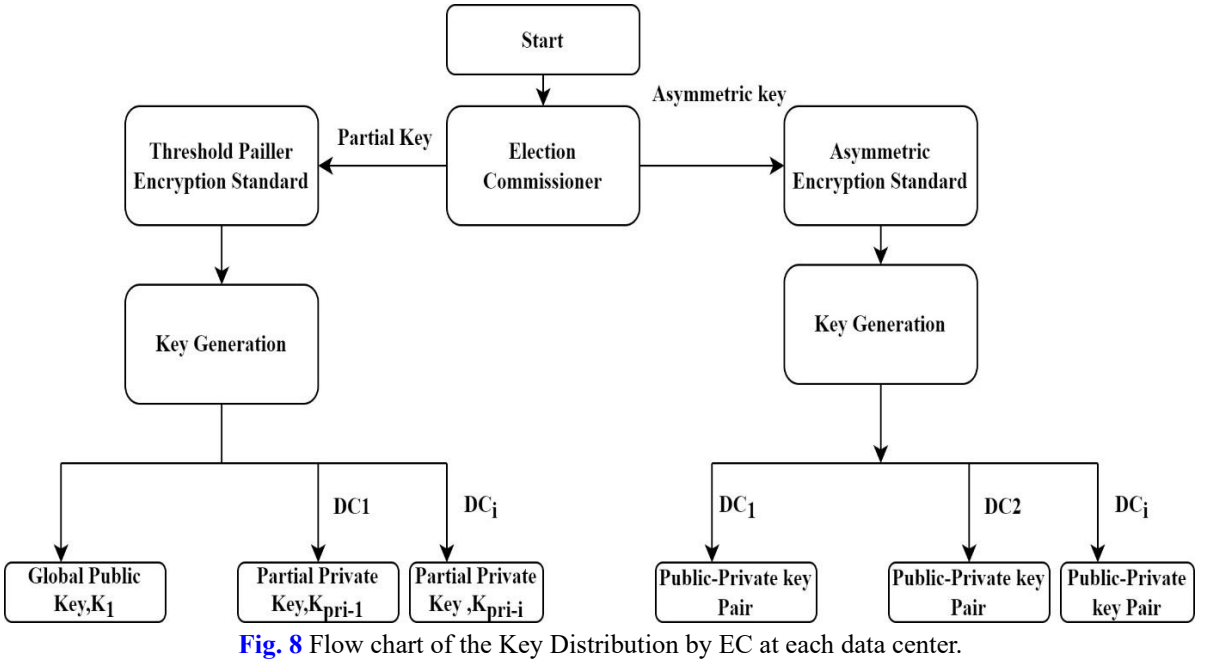


**Fig. 8** Flow chart of the Key Distribution by EC at each data center.

Paillier homomorphic encryption satisfies the following properties suggested by Cramer *et al.*[26] For the plaintext's addition, from encryption $\bar{a}$ and $\bar{b}$, it is easy to compute the encryption of $a + b$. For multiplication with a constant, from the encryption $\bar{a}$ and $a$ constant k $\epsilon z$ and $k.a$, random encryption is easy to compute. For proving knowledge of plaintext, it is easy to give zero-knowledge proof for a process that has created an encryption $\bar{a}$ that it knows 'a'. Each server can share its partial decryption for the threshold decryption and decrypt the encrypted text using a single public key share by all servers.

The Paillier cryptosystem has computations from the group $z_{n^2}$ where the RSA modulus is indicated by n. The public keys are generated by choosing a unique prime number of length k-bits denoted by $p$ and $q$, such that $n = p * q$. One of the private keys is the least common multiple, as shown in equation (6).[24] The random number g is selected such that, g $\epsilon z^*_{n^2}$. The public key for encryption, PubK2 $= (n,\ g)$. The private key for decryption, PrK $= (\lambda, \mu)$, where $\mu$ and L(x) is shown using equations (7)[24] and (8),[24] respectively.

$$\lambda(n) = lcm(p-1, q-1) \quad (6)$$

$$\mu = \mathrm{L}(g^{\lambda} mod\ n^2)^{-1}\ mod\ n \quad (7)$$

$$\mathrm{L(x)} = \frac{x-1}{n} \quad (8)$$

The message $m$ needs to be encrypted where $0 \leq m < n$. The random integer $r$ is selected such that r $\epsilon z^*_{n^2}$. The ciphertext $c$ obtained is shown using equation (9).[24]

$$c[m, r] = g^m\ r^n\ mod\ n^2 \quad (9)$$

In the decryption process, the ciphertext obtained from equation (9) should be such that c $\epsilon z^*_{n^2}$. The original text, $m$ is retrieved using equation (10).[24]

$$m = L(c^{\lambda}\ n^2)\mu\ mod\ n \quad (10)$$

### 2.2.2 Threshold paillier encryption

A threshold variant of the Paillier Encryption Scheme[27] is used in the proposed system to allow secure multi-party communication. The work has modules for key generation and encryption/decryption process, which is adopted for the proposed work.

The key generation of threshold variant[28] is obtained from four unique prime numbers denoted by $p$, $q$, $p'$, $q'$ and should satisfy $p = 2p' + 1$ and $q = 2q' + 1$. Modulus, $n = p * q$, and $m = p' * q'$. Random number g is picked such that, g $\epsilon z^*_{n^2}$. The value 'd' is picked such that it should be $d \equiv 0\ mod\ m$ and $d \equiv 1\ mod\ n$. Using the Chinese Remainder Theorem, the value can be computed using equation (11).[28] Hiding polynomial, $f(x)$ coefficients is expressed using equation (12).[28] where $a_0 = d$, hiding $a_0$ as the secret key. $a_i$ for $0 < i < w$ is a random value from $[0, nm)$. Each share is denoted by $s_i = f(i)$ for the $ith$ partial key. These partial keys need to be distributed in a secure way. Other public verification values, $v = v^{\Delta s_i}\ mod\ n^2$, where $\Delta = l!$. $l$ is the total number of servers who are sharing the secret key, and $w$ is the threshold number of servers required to decrypt the ciphertext. It is usually given as $w = \frac{l}{2}$.

$$d = m\ *(\ m^{-1}\ mod\ n) \quad (11)$$

$$f(x) = \sum_{i=0}^{w-1} a_i\ x^i \quad (12)$$

The encryption process of the Paillier Threshold cryptosystem is for the given modulus value, $n$ and $l$ denoted by the total number of participating servers, and $w$ denoting the threshold number of servers required to decrypt the cipher. Public keys $k1 = (n, g)$ will be published. Plaint text, $m$ is encrypted to yield $c$ using equation (13)[28]

$$c = (n+1)^m\ r^n\ mod\ n^2 \quad (13)$$

The decryption process of the Paillier Threshold cryptosystem needs a threshold number of participants. The threshold number of partial decryptions $c_i$shown using equation (14)[28] needs to be shared and combined at data centers to retrieve the original content using the Lagrange interpolation technique. Combination shares are combined to form $c'$ as shown in equation (15).[28] Message $m$ can be recovered using equation (16)[28]

$$c_i = c^{2\Delta s_i}\ mod\ n^2 \quad (14)$$

$$c' = \Delta\ \prod_{i \epsilon\ s} c_i^{2\lambda^S_{0,i}}\ mod\ n^2 \quad (15)$$

where $\lambda^S_{x,i} = \Delta \prod_{i' \epsilon\ S \setminus \{i\}} \frac{-i}{i-i'}$.

$$m = 4\ \Delta^2\ \ \frac{(c'-1)}{n}\ \ mod^{-1}\ n \quad (16)$$

where $c' = 1 + n^{4\Delta^2 m}$, the threshold encryption requires a pre-determined number of servers to collaborate to decrypt an encrypted message. Decryption is not achieved if collaboration has any number less than the threshold. In layman's terms, the encryption environment will have one public key and $n$ shares of private keys created with a threshold of $w$. The decryption server must receive $w$ private shares, which will successfully help in retrieving the original plain text. It can be further illustrated using two stages of pre-authentication and authentication phases.

#### a. Pre-authentication phase

The Election Commissioner (EC) is responsible for generating a public key for threshold Paillier encryption system and shared private keys denoted by, $s_i$. It is distributed among the validators/regional election officers. Threshold value $w$ is decided for the complete decryption of the original text.

#### b. Authentication phase

If an EC wants to communicate a message among the validator nodes, the session key is encrypted, and a hash of the key is sent to all the dealer nodes. After collecting the threshold number of partial decryption shares - $PDS_i$ from other nodes, it can combine them to retrieve the original intended message. EC can use this communication to communicate session keys.

### 2.2.3 Blockchain distributed ledger

Byzantine Agreement Protocols can be used as consensus in a blockchain[5] platform like Ethereum. But it has security issues like susceptibility to Sybil attacks. Proof of Work has the issue of intensive mathematical computation and hence is more

resource-intensive. Our proposed work uses a Proof of Authority consensus. Set of authorities called validators or sealers decide the creation of the block. The validators/sealers here will be personnel's responsible for each voting station/ area/region. This has the advantage of block creation at steady intervals.

BC makes use of the Merkle Hash tree[29] to store the hashes more securely. It was initially introduced to provide secure authentication using a hash. Every leaf node is labeled with the hash of the data block, and the non-leaf node is labeled with the hash of its child node.

### 2.2.4 SHA-512 hashing algorithm

Hashing is used because of its one-way function. It is impossible to obtain the input message if the attacker gets hold of the hash message. SHA-512[30] operates on eight 64-bit words. The message is padded so that it results in lengths of multiples of 1024-bits. Each 1024-bit block is passed iteratively to return the final hash digest of 512-bits.

### 2.2.5 Face detection using multi-task cascaded convolution network

Face Detection is the prime requisite for face recognition and facial emotion analysis. Face recognition requires access to the Aadhar database, where the biometric given by the user for authentication can be mapped to the user whose vote is being captured. Thus the system ensures non-repudiation. The proposed work mentions face detection with the possibility of adding face recognition in the future once the Aadhar database is accessible.

For face detection, state-of-the-art techniques based on machine learning and deep learning are available. The method based on Viola Jones[31] face detector, is the fastest and works best on resource constraint devices such as mobile devices. It detects only full frontal face. The deep learning based face detection technique's such as Multi-task cascaded convolutional neural network(MTCNN),[17] Faster R-CNN,[32] MobileNet Single Shot Multibox Detector(SSD),[33] You only Look once Yolov3[34] are more accurate in face detection compared to the Viola Jones based face detector.

The proposed work requires key facial features such as eye, nose, and mouth for facial emotion analysis as future work. Thus the proposed work has adopted MTCNN face detection work based on Zhang. *et al*.[17] Also other face detection methods based on Facenet[35] use face alignment defined in the MTCNN model. There are three stages of the convolutional network that recognize faces and landmark locations, such as two points for the eye, nose, and two corners of the mouth. It makes use of multi-task learning. The first stages use a shallow convolutional neural network (CNN) to produce the candidate window. The second stage refines the obtained candidate window using a more complex CNN. The third CNN, which is the most complex, refines and outputs facial landmark position. For the proposed work, only a bounding box is kept for each face.

The images are scaled to different sizes and is fed into the 3 stages known by Proposal network (P-Net), Refine network(R-Net) and Output network(O-net). The three tasks of the CNN detectors are: Face classification, Bounding Box Regression and facial landmark localization. Face classification uses cross-entropy loss,[17] given by equation (17)[17]:

$$L_i^{det} = -(y_i^{det} \log(p_i) + (1 - y_i{}^{det})(1 - \log(p_i))) \quad (17)$$

Where $p_i$ is the probability that indicates sample $x_i$ is a face. Ground truth level is denoted by $y_i \epsilon\{0,1\}$ .Bounding Box Regression[17] employs Euclidean loss for each sample $x_i$ is shown using equation (18),[17] where $y_i^{\wedge box}$ is the regression target obtained from network and $y_i^{box}$ is the ground-truth co-ordinate. Facial Landmark Regression,[17] the loss function is the Euclidean distance is shown using equation (19).[17]

$$L_i^{box} = \left\| y_i^{\wedge box} - y_i^{box} \right\|_2^2 \quad (18)$$

$$L_i^{landmark} = \left\| y_i^{\wedge landmark} - y_i^{landmark} \right\|_2^2 \quad (19)$$

### 2.2.6 Screenshots of the user interface(UI)

The MTCNN based face detector can use pre-trained models and can extended to the android mobile operating system environment. Other mobile operating systems can be explored as future work. The code from the GitHub link for MTCNN for android,[36,37] an open-source and public link, is used for the proposed work. The UI screenshot designed using android studio here is shown in the below figures Fig. 9 and Fig.10. Fig. 9a shows the integration of the fingerprint module designed using public Github.[38] Fig. 9b shows the UI for OTP generation. Fig. 9c shows the UI screenshot for detecting the face using a bounding box. Fig. 10a shows the UI screenshot for the error message that gets prompted if the user /voter is not found voting in solitude. Fig. 10b shows the Region selection which the user has to select, which shows the candidate contesting at that voting area. Thus area selection enables the user to see the candidate list. Fig. 10c shows the UI screenshot where the user has made his selection. This verifies the applicability of the MTCNN model in an android environment for face detection. The underlying integration with blockchain is also underway. The UI screenshot uses the image downloaded from Unsplash Photos[39] for everyone, which is free to use.[40]

The fingerprint authentication prompt is extended from Open source Github Link[38] and is integrated with MTCNN based face detector to include the authentication process. Once OTP verification is completed, region selection is made by the user, which starts the face capturing process.

## 3. Results and discussion

The system is qualitatively analyzed for the security aspects such as privacy (ballot secrecy), resistance to single point of failures (SPoF), distributed denial of service (DDoS) attacks, and coercion attacks. The proposed work uses secure multi-

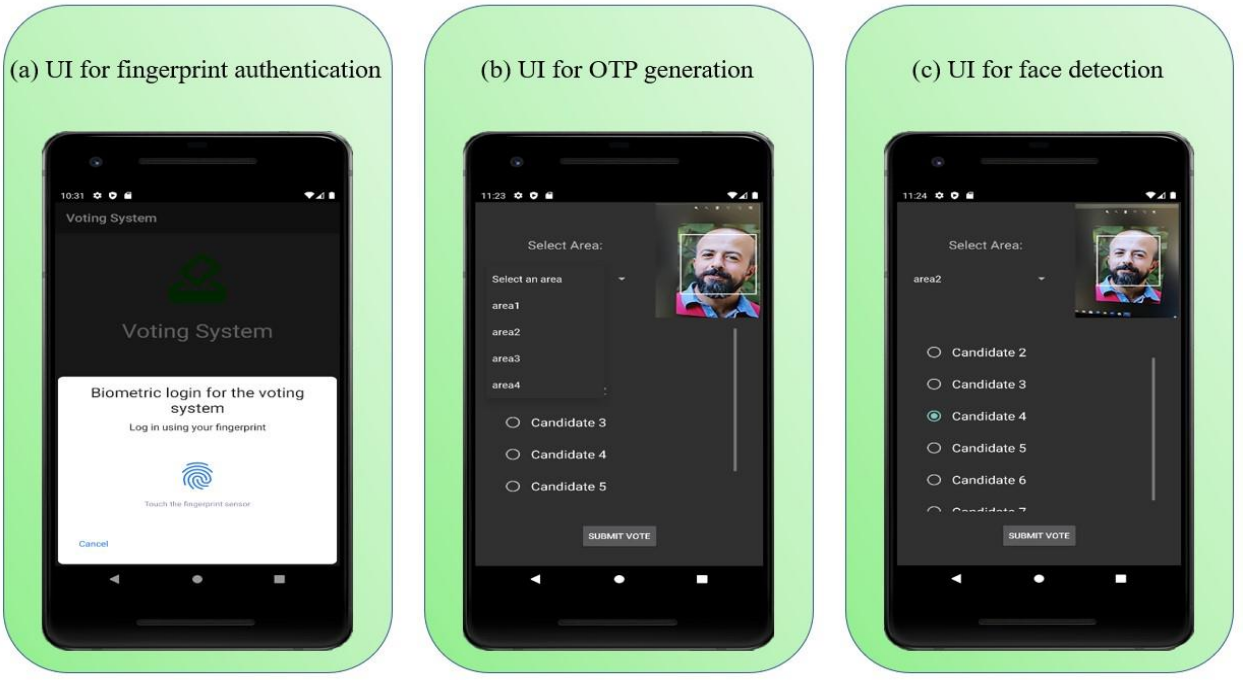


**Fig. 9** UI for finger print authentication, OTP generation, and face detection.

party communication (SMC) and ensures end-to-end verifiability and ease of key distribution. These are detailed below and show in Table 1.

**Table 1**. Qualitative analysis of the security features of the proposed REV system

| Security Features | Proposed work | [5] | [6] | [7] | [12] |
|---|---|---|---|---|---|
| Ballot Secrecy | ✓ | ✓ | ✓ | ✓ | ✓ |
| Resistance to SpoF | ✓ | ✓ | ✓ | ✓ | ✓ |
| Resistance to DDoS | ✓ | ✓ | ✓ | ✓ | ✓ |
| Coercion resistant | ✓ | × | × | × | × |
| Non-repudiation | ✓ | ✓ | ✓ | ✓ | ✓ |
| Receipt-Freeness (RF) | ✓ | × | × | × | × |
| SMC | ✓ | × | × | × | ✓ |
| End-to-end verifiability | ✓ | ✓ | ✓ | ✓ | ✓ |
| Ease of key distribution | ✓ | × | × | × | × |

The system also has various advantages to the existing electronic ballot voting system. Setup time required for the existing election system[21] requires preparation of electoral rolls, deployment of polling personnel, police personnel training, checking EVM's, segregation of EVM's, database management. Deployment of polling personnel is done through a three-stage randomization process. Thus, a time duration of 6 months is required for the setup phase only. The proposed work only distributes threshold shared private keys and asymmetric keys to the polling officer/validating node. The tallying time in EVM is based on the number of constituencies, which usually take up to 3 to 4 hours. In the Paillier threshold system, the decryption depends on the number of key shares. For 100 shares for decryption, it might take 60 seconds.[41] The user can vote from any location using his mobile device and is the most significant advantage of the proposed work. The comparisons between our work and the EVM system are summarized in Table 2.

**a. Privacy**

Privacy can be termed as Coercion-Resistant (CR), Ballot Secrecy (BS), Receipt-Freeness (RF). Proposed work offers CR if the coercer cannot determine if the coerced voter complies with the demand. This is deployed using the face detection mechanism. Vote data structure does not store voter ID; hence BS is ensured, unlike in existing systems.[23] This also provides for the privacy of the ballot. RF intends to stop vote-selling a social issue involving the selling of votes. The receipt generated in the proposed work only shows a success message and does not reveal the choice of the vote.

**b. Resistant to SPoF and distributed denial of service (DDoS)**

Validator Nodes (VN) are distributed throughout regions. Any single VN cannot solely decrypt the voter's message because of the requirement of the threshold participation for decryption. This ensures resistance to SPoF. All the voting content is saved in a different data center according to user selection of a region, and only the hashes are saved in blockchain, thus avoiding SPoF. Hence, if VN is compromised, they still cannot compromise the system. Even if the attacker compromises the private key shares, the attacker should still be aware of the threshold variable. This threshold variable $l$ is secret information in the Threshold Paillier encryption system [27] and can be varied by the election officer. For DDoS attack to be successful, the attacker must compromise the minimum threshold number of validator nodes for decryption which is again a tedious effort for the attacker to guess the $l$ value.

 

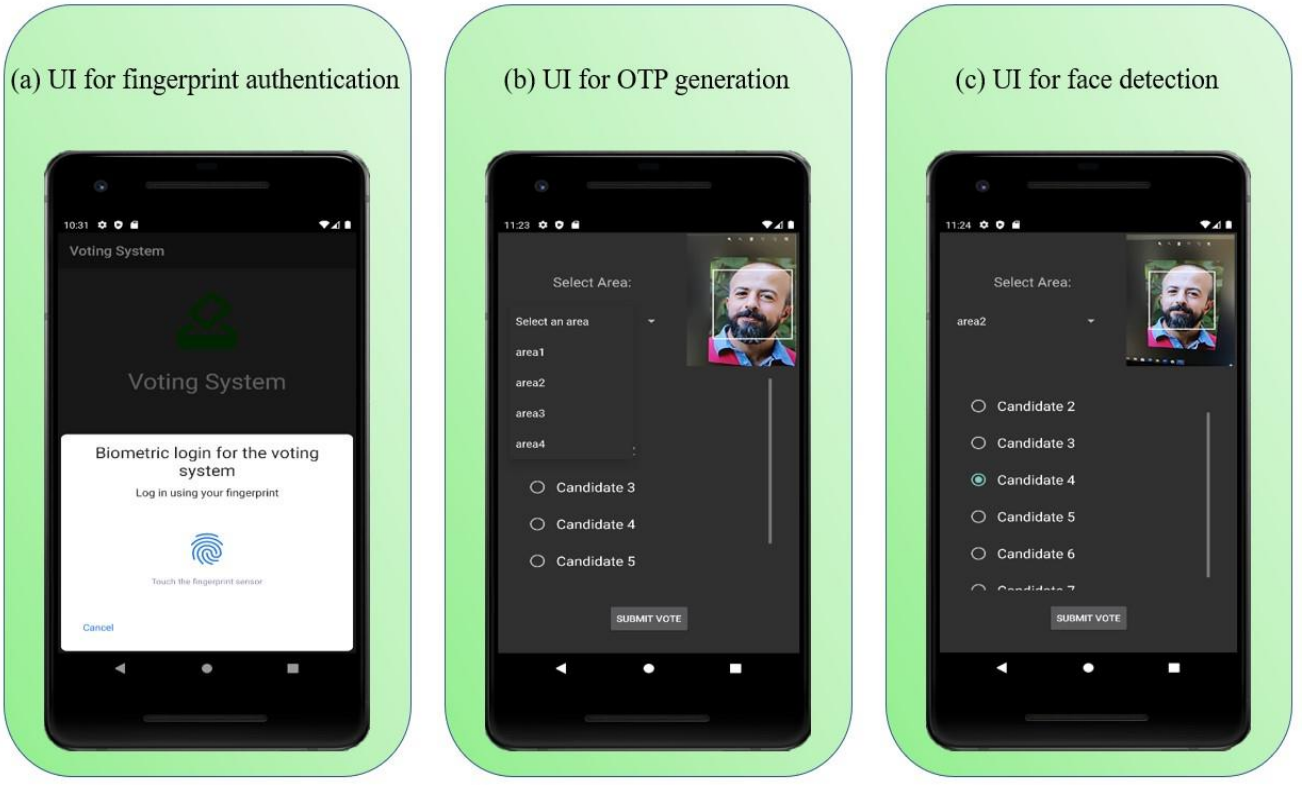


**Fig. 9** UI for finger print authentication, OTP generation, and face detection

**Table 2**. Comparison of existing EVM[21] system with the proposed REV system

| Parameters | Existing system | Proposed Work |
|---|---|---|
| Setup time | 6 months | Based on key size and number of shares. |
| Electoral rolls | More than 6 months before poll day | Not Applicable |
| Paper wasted | Equivalent to the number of voters | Almost negligible, every step is digitized |
| Flexibility | Voters can vote at their recognized polling station | Voters can vote from anywhere. |
| Tallying Time | Proportional to the number of voters and number of constituencies. | Based on the number of shares. |

**c. Secure multi party communication**

Since the public key is globally available and the shared private key is unavailable to the user, it helps in secure encryption. The inability of validator node/datacenters to decrypt the ciphertext ensures the voter's privacy. The requirement of a threshold number of validator nodes also prevents the system from being compromised and hence negates the danger of revealing voter's identity.

**d. End to end verifiability**

End-to-end verifiability is ensured by checking the equality of the hashes retrieved from the BC and with the corresponding partial decrypted shares. After the integrity check, the threshold number of validator nodes must join, decrypt, and publish the final tally of the votes.

**e. Ease of distribution of keys**

Existing work proposed issuance of public and private key pair to each user, which is not feasible with countries with a large population. But the distribution of keys to comparatively few datacenters is both feasible and manageable.

**f. Non-repudiation**

The proposed system uses fingerprint and OTP as a two-tier authentication. It ensures liveness and non-repudiation property. The fingerprint is unique for each user hence this biometric feature is incorporated into the system.

**e. Resistant to coercion-attacks**

Coercion resistance protect voters' privacy even if the adversary is trying to communicate with a voter.[42] Thus the system ensures that voters should vote in isolation. Isolation voting helps the voter to cast his choice of a candidate without being influenced by a coercer. This is made sure by ensuring that only one face is present that is , the voter's face, during the process. Detecting more than one face in the camera allows the system to check if the voter is observed and coerced to vote. Thus, the proposed work achieves the experience of voting in a booth but in a remote environment. If multiple faces are detected while casting a vote, the application times out. The user is prompted to vote again some other time when there is no background disturbance.

## 4. Conclusion

The proposed work aims to provide a coercion-resistant vote capturing experience to the user. Biometric-based authentication ensures non-repudiation. The use of cryptographic instruments like public-key cryptosystem and hashing algorithms ensures end-to-end verifiability. The system provides universal verifiability due to the incorporation of threshold variants to secure multi-party communication using the Threshold Paillier encryption system. Blockchain technology assures the integrity check, which verifies that the vote is not tampered with. The applicability of the proposed voting system for a mobile-based operating system ensures more population coverage.

## 5. Future work

The proposed work only has face detection and can be used integrated with face emotion analysis and facial tracking for better coercion detection. The current proposal is explored on android based mobile operating system devices. It can be adopted for other mobile-based operating systems in the future. The fingerprint authentication needs an extension of the Aadhar database for the system to be applied in real-time. This process needs access to the Aadhar database to provide two-tier authentication that promises to deliver a coercion-resistant system. As future work, face detection can be extended and be used for the face recognition process.

## Conflict of interest

There are no conflicts to declare.

## Supporting information

Not applicable.

## References


[1] Election Commission of India – Statistical Reports of General Election 2019, https://eci.gov.in/files/file/13585-10%C2%A0voters-information/.

[2] The Conduct of Elections Rules, Government of India., 2002, https://legislative.gov.in/sites/default/files/%282%29%20THE%20CONDUCT%20OF%20ELECTION%20RULES%2C%201961.pdf.

[3] News Article–India Today, 2019, https://www.indiatoday.in/elections/lok-sabha-2019/story/serving-army-personnel-being-denied-right-to-vote-at-place-of-posting-say-veterans-1476734-2019-03-13.

[4] Ministry of Statistics and Programme Implementation, Government of India. Schedule 25.2: Household Social Consumption: Education, 2019, http://mospi.nic.in/sites/default/files/NSS75250H/Chapter-5.pdf.

[5] C. Killer, B. Rodrigues, E. J. Scheid, M. Franco, M. Eck, N Zaugg, and B. Stiller, *IEEE 45th Conference on Local Computer Networks (LCN)*, 2020, 172-183, doi: 10.1109/LCN48667.2020.9314815.

[6] G. Manikandan, G. Anandaraju, and B. Karthikeyan, *6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2020, 783-786, doi: 10.1109/ICACCS48705.2020.9074158.

[7] J. E. Helm, *J. Inf. Technol.*, 2021, **36**, 128-153, doi: 10.1177/0268396220978983.

[8] A. Reuter, K. Boudaoud, M. Winckler, A. Abdelmaksoud, W. Lemrazzeq, 2020, **12063**, 36-46, doi: 10.1007/978-3-030-54455-3_3.

[9] UIDAI 'Why Aadhaar', https://uidai.gov.in/why-aadhaar.html.

[10] S. Agarwal, A. Haider, A. Jamwal, P. Dev, and R. Chandel, *7th International Conference on Smart Structures and Systems (ICSSS),* 2020, 1-5, doi: 10.1109/ICSSS49621.2020.9202212.

[11] P. B. Mansingh, T. J. Titus, and V. S. Devi, 2020, *6th International Conference on Advanced Computing and Communication Systems (ICACCS),* 1116-1119, doi: 10.1109/ICACCS48705.2020.9074281.

[12] S. Zhang, L. Wang, and H. Xiong, *Int. J. Inf. Secur.*, 2020, **19**, 323-341, doi: 10.1007/s10207-019-00465-8.

[13] P. Baudier, G. Kondrateva, C. Ammi, and E. Seulliet, *Technol. Forecast. Social Change*, 2021, **162**, 120397, doi: 10.1016/j.techfore.2020.120397

[14] D. Khutkyy, *E-Vote-ID*, 2020, **19,** 323–341, doi: 10.13140/RG.2.2.16935.57767.

[15] E. Estaji, T. Haines, K. Gjøsteen, P. B. Rønne, P. Y. Ryan, and N. Soroush, *International Joint Conference on Electronic Voting*, 2020, 50-66, doi:10.13140/RG.2.2.16935.57767.

[16] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, *Inform. Fusion*, 2020, **64**, 131-148, doi: 10.1016/j.inffus.2020.06.014

[17] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, *IEEE Signal Process. Lett.*, 2016, **23,** 1499-1503, doi:10.1109/LSP.2016.2603342.

[18] G. Guo, H. Wang, Y. Yan, J. Zheng, and B. Li, *Neurocomputing,* 2020, **395**, 128-137, doi: 10.1016/j.neucom.2018.02.110.

[19] A.S. M. Iftekhar, S. Kumar, R. A. McEver, S. You, and B.S. Manjunath, *Computer Vision and Pattern Recognition*, 2021.

[20] Right to Privacy Vis-A-Vis Data Protection With Special Reference To The Aadhaar (Targeted Delivery Of Financial And Other Subsidies, Benefits And Services) Act, 2016, 2018, http://kr.cup.edu.in/handle/32116/1911.

[21] The Functions (Electoral System of India), 2018, https://eci.gov.in/about/about-eci/the-functions-electoral-system-of-india-r2.

[22] N. Nigar, M. L. Nath, Islam, M. T., *JOIV: Int. J. Inform. Visualization*, 2020, **4,** 22-27, doi: 10.30630/joiv.4.1.283.

[23] Smart-Card-Alliance What Makes a Smart Card Secure? 2008, https://www.securetechalliance.org/resources/lib/Smart_Card_Security_WP_20081013.pdf.

[24] Paillier Threshold Encryption Toolbox, 2010, http://cs.utdallas.edu/dspl/cgi-bin/pailliertoolbox/manual.pdf.

[25] *Nullification of Elections*, 1970-1979, https://encyclopedia2.thefreedictionary.com/Nullification+of+Elections.

[26] R. Cramer, I. Damgård, and J. B. Nielsen, *International conference on the theory and applications of cryptographic techniquee-EUROCRYPT 2001,* 2001, **2045**, 280-300, doi: 10.1007/3-540-44987-6_18.

[27] T. Nishide, and K. Sakurai, *International Workshop on Information Security Applications, Springer,* 2010, **6513**, 44-60, doi: 10.1007/978-3-642-17955-6_4.
[28] I. Damgård, and M. Koprowski, *International Conference on the Theory and Applications of Cryptographic Techniques*, 2001**, 2045,** 152-165, doi: 10.1007/3-540-44987-6_10.
[29] R. C. Merkle, *IEEE Symposium on Security and Privacy, IEEE*, 1980, 122-122, doi: 10.1109/SP.1980.10006.
[30] H. N. Bhonge, M. K. Ambat, and B. R. Chandavarkar, *11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2020, 1-6, doi: 10.1109/ICCCNT49239.2020.9225559.
[31] P. Viola, and M. Jones, *Proceedings of the 2001 IEEE computer society conference on computer vision and pattern recognition, CVPR 2001 IEEE*, 2001, **1,** 1125-1134, doi: 10.1109/CVPR.2001.990517.
[32] S. Ren, K. He, R. Girshick, and J. Sun, *Adv. Neural Inf. Process. Syst,* 2015, **28**, 91-99, doi: https://arxiv.org/abs/1506.01497v3
[33] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C. Y. Fu, and A. C. Berg, *European conference on computer vision*, 2016, 21-37, doi: 10.1007/978-3-319-46448-0_2
[34] Bhuiyan, M. R., Khushbu, S. A., & Islam, M. S., *11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE*, 2020, 1-5, doi: 10.1109/ICCCNT49239.2020.9225384.
[35] F. Schroff, D. Kalenichenko, and J. Philbin, *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2015, 815-823, doi: 10.1109/CVPR.2015.7298682.
[36] Implementation of the MTCNN face detector for Keras in Python3.4+, 2017, https://github.com/ipazc/mtcnn
[37] MTCNN For Android Java, 2018, https://github.com/vcvycy/MTCNN4Android.
[38] Add fingerprint authentication to your app using Biometric Prompt., 2019, https://www.androidauthority.com/add-fingerprint-authentication-app-biometricprompt-943784/.
[39] Unsplash Photos for everyone, https://unsplash.com/phtos/eSjmZW97cH8.
[40] Unsplash Photos for everyone, https://unsplash.com/license.
[41] N. Kakade, and U. Patel, *11th International Conference on Computing, Communication and Networking Technologies (ICCCNT),* 2020, 1-7, doi: 10.1109/ICCCNT49239.2020.9225325.
[42] O. Kulyk, and S, Neumann, E-Vote-ID 2020, 2020.

## Author information

***Pooja S*** *received her post graduate degree in Cyber security from College of Engineering Trivandrum, Trivandrum, Kerla, India. Now she is pursuing her Ph.D degree in Cyber Securiy from Manipal Academy of Higher Education, Manipal, Karnataka, India. She also works as an Assistant Professor in Department of Information & Communication Technology at Manipal Institute of Technology, (MIT), Manipal Academy of Higher Education, India. Her research interests include blockchain, machine learning, deep learning, cryptography.*

***Laiju K Raju*** *received his Master's degree in Cyber Security from College of Engineering Trivandrum, Trivandrum, Kerala.He is a Senior Software Engineer in QuEST global. His research areas are Block chain, Computer Vision and Information Security.*

***Utkarsh Chhapekar****, has received his B.Tech degree in 2021 from the Department of Information and Communication Technology, Manipal and currently works as an Analyst with Deloitte USI. His current research interests include Artificial Intelligence, Natural Language Processing and Computer Vision.*

***Chandrakala C.B*** *graduated from Sri Jayachamarajendra College of Engineering, Mysore University, Karnataka, India in Electronics and Communication Engineering and obtained her Master's in Technology specializing in Software Engineering from SJCE, Mysore, VTU, Karnataka. She received PhD degree from MAHE, Manipal. She has experience of working both in Industry and academia. Currently she is working as Associate Professor-Senior in the department of Information Technology & Communication, Manipal Institute of Technology, MAHE, Manipal. Her research areas are Distributed Computing, Speech Processing and Recognition, Blockchain Technology, Software Engineering.*

**Publisher's Note:** Engineered Science Publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.