ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse188932020.pdf
https://doi.org/10.30534/ijatcse/2020/188932020

Multilevel Voter Identity Protocol for Secure Online Voting

Rina Damdoo[1], Kanak Kalyani[2]
[1]Assistant Professor, ShriRamdeobaba College of Engg.& Management, Nagpur, India, damdoor@rknec.edu
[2]Assistant Professor, ShriRamdeobaba College of Engg.& Management, Nagpur, India, kalyanik@rknec.edu

ABSTRACT

The word vote means to choose from a list, to elect or to agree on. The main goal of voting, in a scenario involving the citizens of a given country, is to come up with leaders of the people's choice.

Some of the problems involved in existing voting systems include vote rigging during election, insecure or inaccessible polling stations, inadequate polling materials and also inexperienced personnel. In the era of Internet of Things/Everything, it is decadent to say online voting is not secure.Rather we have to arise with Aadhaar as an enabler. Unique Identification Authority of India (UIDAI) ensures and slogs so that its ecosystem adopts measures to keep Central Identities Data Repository (CIDR) up to dateand safe. Also, in current situation where almost whole world is facing pandemic situation because of COVID-19, only E-services like E-Banking, E-Learning, E-voting are unaffectedly operational.

Proposed system seeks to address these issues. Voters can vote from anywhere around the globe online, satisfying the condition that they have a valid Aadhaar card and they are registered voters. We are proposing multilevel voter identity protocol for secure online voting. We are naming our proposed work as COVID (Consolidate Online Voter IDentification) as it is merging CIDR with E-voting system. In this, the Aadhaar number authenticates Demographic details and fingerprints to develop an online identity service system. The paper is complemented with algorithms for Multiple Face detection, Eye-blinking detection or eye-tracking as a countermeasure against spoofing in face recognition systems.

Objective of this work includes online voting system to automate the data flow and validating the system to ensure that only legible voters are permitted to vote and only once. Considering enormity of CIDR, scope of the work can be extended by incorporating iris detection system for authenticating voters. On the other hand, major challenge is to provide end to end security of Demographic details from CIDR to voting devices.

Key words: Unique Identification Authority of India (UIDAI), Central Identities *Data* Repository (CIDR), AADHAAR card, fingerprint detection, Multiple Face detection

1. INTRODUCTION

The Aadhaar project is the world's largest national identity project launched by government of India. It collects the biometric and demographic data of residents of India and provides a unique identification number (UID) to them. This number is unique and is linked to an individual's unique biometric and demographic information. This collected data stored in the central database known as Central Identity Data Repository (CIDR).
These days there is a need for an online system that will help a person to cast his vote even when he is away from his constituency or wish to maintain social distancing. This will reduce his effort and save his travelling time. Proposed system will enable the Election Commission of India (ECI) to manage elections easily and securely. It will use the data which is already present with, in the form of Aadhaar unique identification. It contains personal identity along with his biometric information. With the help of steganography we can try to provide a biometric as well as password security to our vote. The system will make a decision whether the voter is the authenticated person or not. If the former, securely vote can be casted.

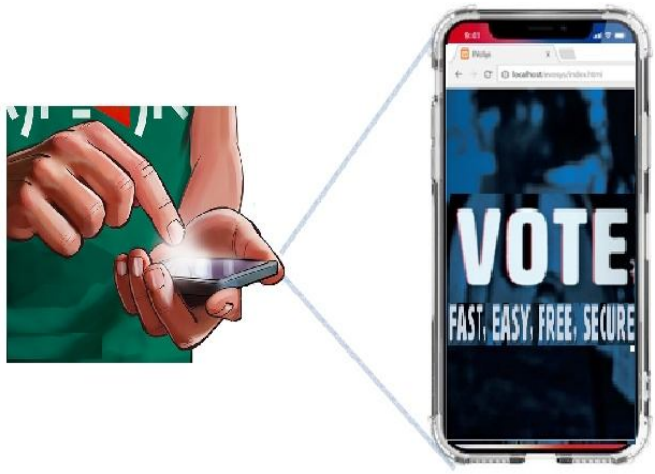

Figure 1: COVID (Consolidate Online Voter IDentification) System

A voting system should be so hard to tamper with and so resistant to failure that no commercial system is likely to ever meet the requirements, and developing a suitable custom system would be extremely difficult and prohibitively expensive.

Absentee voting

An absentee ballot is a vote cast by someone who is unable or unwilling to attend the official polling station to which the voter is normally allocated. Numerous methods have been devised to facilitate this. Increasing the ease of access to absentee ballots is seen by many as one way to improve voter turnout, though some countries require a valid reason, such as infirmity or travel, be given before a voter can participate in an absentee ballot. Currently, India does not have an absentee ballot system for all citizens except in few exceptions. Section:19of The Representation ofthe PeopleAct (RPA)-1950allows a person to register to vote if he or she is above 18 years of age and is an 'ordinary resident' of the residing constituency i.e. living at the current address for 6 months or longer. Section 20 of the above Act disqualifies a non-resident Indian (NRI) from getting his/her name registered in the electoral rolls. Consequently, it also prevents a NRI from casting his/her vote in elections to the Parliament and to the State Legislatures. In August 2010, Representation of the People (Amendment) Bill-2010 which allows voting rights to NRI's was passed in both LokSabha with subsequent gazette notifications on 24 November 2010. With this NRI's are now able to vote in Indian elections but have to be physically present at the time of voting. Several civic society organizations have urged the government to amend the RPA act to allow NRI's and people on the move to cast their vote through absentee ballot system. So, if permitted online voting system is a good solution over physical presence systems.

2. LITERATURE REVIEW

Literature articulates, the numbers of voting systems have been adopted all over the world with the passage of time starting from paper ballot system to the recently adopted electronic voting system. Smart Voting System [2] addresses improving E-governance in developing countries. It helps in digitalizing the system. The system covers the people facing any disability to vote in person. The system also addresses the security issues.

Avinash Pratap Budaragade et.al.[2] propose providing magnetic strip voter ID cards for every voter. At the polling center these cards are used for authentication. Once they are verified another level of security is created by using biometric fingerprint as an authentication of voter. At every instance these data are stored in the server through internet. In our approach magnetic strip voter ID cards are replaced by Aadhaar cards.

Manjusha Amritkar et.al.[3] Supports Secure Online Voting System that can help to increase number of voters as individuals will find it easier and more convenient to vote especially those who are abroad. Their work can be used for those who do not have issued and registered for their voter ID card. It can increase user level security using pulse rate detection to avoid black mailing and bullying. It can help reduce manual process, human errors while calculation of votes, man power required at voting booths, time consumed and can help to save resources.

B. Swaminathan et.al.[4]Enforced a method for integrating Cryptography and Steganography to present a highly secure Online Voting System. The security stage of the system is greatly improved by the new idea of random cover image generation for each voter. The user authentication process of the system is improved by adding both biometric and password security. The Steganography portion of the system is secured by random distribution of message bits into the cover image.

It is the strong contention of Andrew Wolfe et.al.[5]that only by viewing the issues that surround e-voting in a full system approach we will not achieve a complete solution. The base for any additional work that we recommendshould be viewed as being suggested in the context of how thatarea for research would be influenced by all three legs of the E-voting stool of authentication, integrity, and public perception.

Anita Titus et. al. [6] proposes, after checking for validity of cards by the authorized personnel, the voter is again validated by his/her RFID card to proceed with the voting task. The fingerprint can be stored in databases and cross-validated using an internet-based Client Server Topology. In their work, the votes are tallied using the number of votes that are counted from the image captured by the camera using the steganography image processing, with the votes that, voter put at the time of voting using EVMS. steganography is the art of hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused data in regular computer files (such as images, sound, text etc) with bits of different, invisible information. Thus using this it can be checked whether the votes using both processes are equal or not.

N.L.Clarkea et.al[7] Propose, Mobile phones are now an accepted part of everyday life, with users becoming more reliant on the services that they can provide. In the vast majority of systems, the only security to prevent unauthorized use of the handset is a four digit Personal Identification Number (PIN). In their work they discuss the findings of a survey into the opinions of subscribers regarding the need for security in mobile devices, their use of current methods, and their attitudes towards alternative approaches that could be employed in the future. Although the need for security is understood and appreciated, the current PIN-based approach is under-utilized and can, therefore, be considered to provide inadequate protection in many cases. Authors thus suggest, alternative methods of authentication, such as fingerprint scanning and voice verification based upon findings, a

non-intrusive, hybrid method of authentication would best satisfy the needs of future subscribers.

[8] Strains security of the data stored by the Aadhaar project with the minimum storage of space in the direction of encryption and steganography. In this, a new efficient security model based on the combination of Arnold's transformation and least significant bit is presented that provides two key level securities. Two keys make the system highly secured and it deals with the demographic data only.

In practice, the placement of finger on the scanner for authentication is not done with the utmost care as when placed during the enrollment and this result in rejections of genuine users [1]. Moreover, user behavior and environmental conditions decrease the genuine acceptance rate (GAR) for authentication of fingerprints. To overcome these limitations, an efficient preprocessing algorithm has been proposed to achieve good vertical orientation and high ridge curvature area around the core point for fingerprint authentication and analysis. The algorithm is implemented in two stages. The process of obtaining the vertical oriented fingerprint image is carried out in the first step. This is followed by core point detection of a fingerprint. Core point detection is efficiently identified for any type of fingerprints. P. Gnanasivam et. al. developed algorithm which they tested using a line based feature extraction algorithm with a large internal database and samples of fingerprint verification competition (FVC).

3. PROPOSED WORK

3.1 System Overview

According to guidelines laid by Election commission of India the identification of voter is very necessary step. Hence Online voting system is divided in two phases.

- First phase deals with the authentication of voter identity and the information provided by the elector.
- Second phase deals with the actual voting process where the voter will give the vote and the vote will be stored in secure database

3.1.1Authentication of Elector

In online voting system, the information of each voter is uploaded in the database of Election Commission according to AADHAAR Identity Number. The AADHAAR Identity number is unique for every citizen or voter of India. AADHAAR Identity number has been introduced by government of India and this also recognizes the constituency of the voter. The module will scan the AADHAAR QR code and check in the database if a proper record is in the database exists. If the user exists then the module checks if the voter id is generated by the election commission. If the voter id exists then the system will prompt the user to scan the fingerprint through the fingerprint module [1]. The fingerprint of the voter is authenticated by the AADHAAR database. To verify the mobile number the system generates the OTP to be sent to the AADHAAR registered mobile number. Once the phone number is verified by the system, the authentication process is complete. The system will automatically log off when the elector is found to be not registered [22].

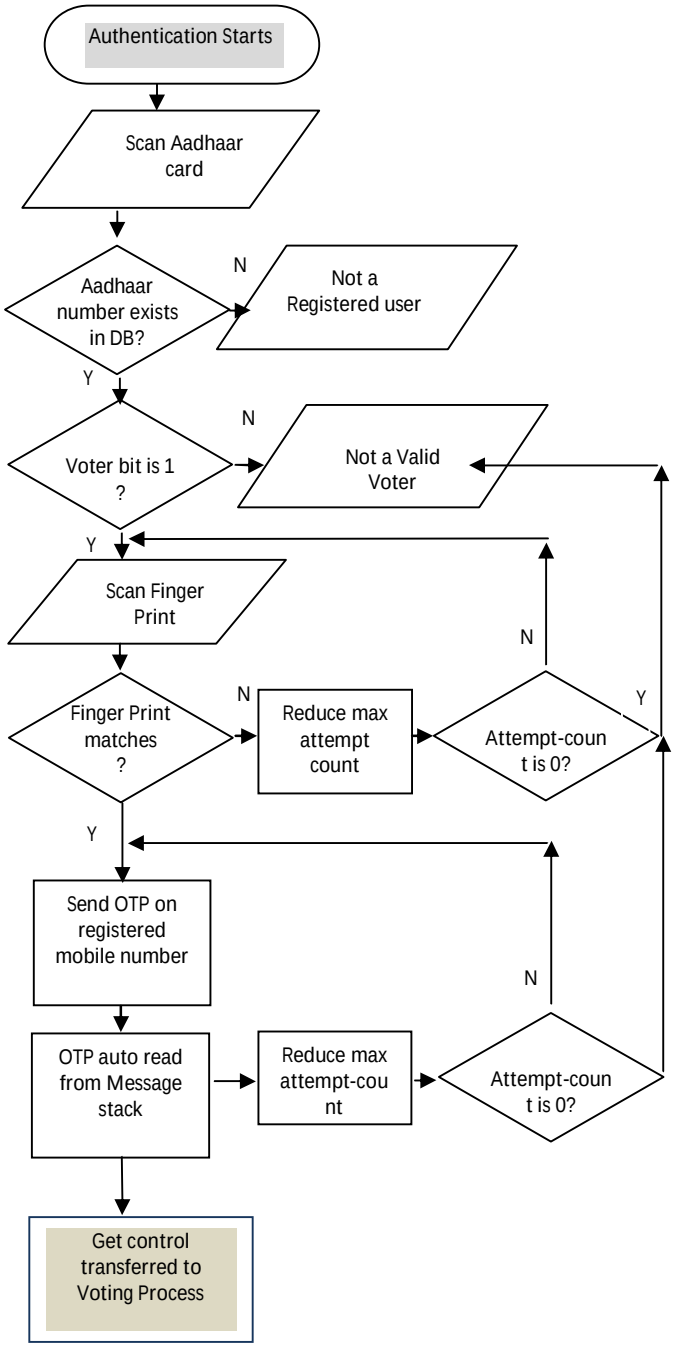

Figure 2: Authentication of Voter Identity

3.1.2 Voting Process

On the day of Election the module "Give Vote" will be activated. As per the guidelines laid of Election Commission of India, when the elector proceeds to give vote, physical identification should be complete and the voter machine/ EVM should not be visible to any other person apart from the Elector.

According to the guidelines the system first verifies the face and liveness of the person standing in front of camera. Liveness Identification is very important as it is easy to mislead the system by still picture. For detection of live face, camera module captures the face at certain interval unknown to user. If the system detects the live face it will check for number of faces.

As per rules, when the elector gives vote the voting information should not be seen by any other person. Hence the system identifies whether multiple faces can be detected. If a single live face is detected the user will be directed to page similar to EVM where the elector can cast the vote.

Face identification and recognition plays a vital role in online voting system. Also it is very essential to authenticate the correct person gives the vote.

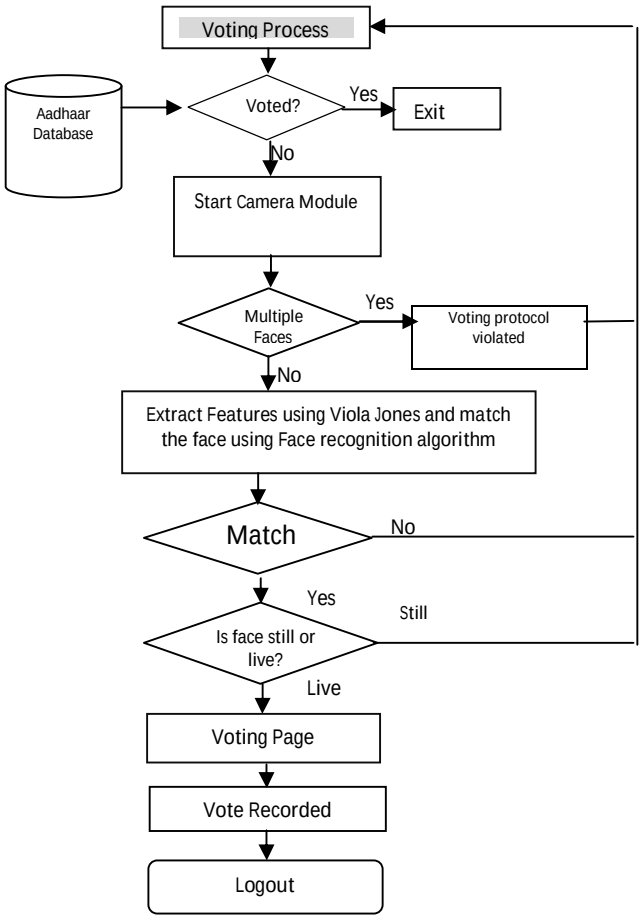

Figure 3: Voting Process on Election Day

Table 1shows various methods adopted to detect the face and identify expressions. These can be used as they form an important part to detect whether the image is live or not[20].

Kumar et al [9] proposes facial expression detection using using radial basis function. Feature extraction is carried out by Haar discrete wavelet transform and Gray-level difference method. Proposed work can be extended by incorporating facial expression recognition module to detect intimidation.

Table 1: Facial Expression Recognition Algorithms

Sr. No.	Method	Author	Description
1	Automatic facial expression recognition using features of salient facial patches[11]	Happy and Routray	Recognizes face deformation when there is change in expression Uses Constrained Local Model (CLM) and Discriminative Response Map Fitting (DRMF)
2	Image ratio features for facial expression recognition application[12]	Song et al	Skin wrinkle detection using binary classifiers
3	Facial expression feature extraction using hybrid PCA and LBP[13]	Luo et al	Uses geometry standardization, eight eyes division and vitality Standardization. PCA and LBP were utilized to extricate the global component of the facial expression.
4	A robust novel method for face recognition from 2D Depth Images using DWT and DCT Fusion[14]	Naveen and Moni	Encompasses unregistered 2D Depth Faces with orientations beginning from 10° to 40°
5	Local appearance-based face recognition using adaptive directional wavelet transform[15]	Muqeet and Holambe	2-D adaptive directional wavelet transform (2-D ADWT) and LDA subspace method
6	Detecting and aligning faces by image retrieval[16]	Shen et al	Detects facial feature point by Hough Transform.
7	An implicit shape model for combined object categorization and segmentation[17]	Smith et al	global shape regularization technique
8	Real-time facial feature detection usingconditionalregression forests.[18]	Dantone et al	Conditional Regression forest for detecting facial feature point

4.CONCLUSION

Online Voting or E-Voting system is the need of time. System can be made more secure by using Anti -Spyware programs to prevent remote access of electors' mobile phones. If E-Banking is preferred by citizens then E-Voting also will be preferred, provided we come up with authenticating, integrating, and public perception solution.In the era of Internet of Things online voting system should come up as smart living machine [21].

REFERENCES

1. An efficient Algorithm for fingerprint preprocessing and feature extraction P.Gnanasivam, S. Muttan Centre for Medical Electroinics, CEG Campus, Anna University Chennai, Chennai-600041, India , ICEBT 2010
2. Smart and Secured Voting System using Magnetic Stripe Voter ID Card and Cloud Storage: A Client-Server Paradigm, AvinashPratapBudaragade, Vajrashri R. Biradar, IRJET, Volume: 06 Issue: 04, Apr 2019,pg 4089-4093
3. Secure Online Voting System, Manjusha Vijay Amritkar1,IJAR,2016, pg. 1648-1653 https://doi.org/10.21474/IJAR01/2257
4. Swaminathan B, and Dinesh J C D, "Highly secure online voting system with multi security using biometric and steganography," in International Journal of Advanced Scientific Research and Technology, vol 2(2), 195–203.
5. Smart Voting keys to e-Democracy,Andrew Wolfe, Arnold J. Sze, YaredBeyene, SAM,2019,48-55
6. Multi-factor authentication for secure electronic balloting credentials, Anita Titus, NithiyaPrincyRajam. B, IJARIIT, Volume 4, Issue 2,1923-1930
7. Acceptance of Subscriber Authentication Methods For Mobile Telephony Devices Author links open overlay panel, N.L.Clarkea, S.M.Furnella, P.M.Rodwella, P.L.Reynoldsb
8. International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307 295 Enhanced Security with Minimum Storage in Aadhaar Card,Jyoti Computer Science Department, IIMT College of Engineering, Greater Noida, Uttar Pradesh, India
9. Kumar, S., Singh, S. & Kumar, J. Live Detection of Face Using Machine Learning with Multi-feature Method. *Wireless PersCommun***103,** 2353–2375 (2018). https://doi.org/10.1007/s11277-018-5913-0
10. Reem Abdelkader, Moustafa Youssef, " UVote: Abiquitous E-Voting System", 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent
11. Happy, S. L., & Routray, A. (2013). Automatic facial expression recognition using features of salient facial patches. IEEE Transactions on Affective Computing. https://doi.org/10.1109/TAFFC.2014.2386334
12. Song, M., Tao, D., Liu, Z., Li, X., & Zhou, M. (2010). Image ratio features for facial expression recognition application. IEEE Transactions on Systems, Man, and Cybernetics. Part B, Cybernetics,n40(3), 779–788. https://doi.org/10.1109/TSMCB.2009.2029076
13. Luo, Y., Wu, C. M., & Zhang, Y. (2013). Facial expression feature extraction using hybrid PCA and LBP. The Journal of China Universities of Posts and Telecommunications, 20(2), 120–124
14. Naveen, S., & Moni, R. S. (2015). A robust novel method for face recognition from 2D Depth Images using DWT and DCT Fusion. Procedia Computer Science, 46, 1518–1528.
15. Muqeet, M. A., & Holambe, R. S. (2017). Local appearance-based face recognition using adaptive directional wavelet transform. In Proceedings of journal of King Saud University—Computer and information sciences (2017).
16. Shen, X., Lin, Z., Brandt, J., & Wu, Y. (2013). Detecting and aligning faces by image retrieval. In Proceedings of IEEE conference on computer vision and pattern recognition (pp. 3460–3467).
17. Smith, B., Brandt, J., Lin, Z., & Zhang, L. (2014). Nonparametric context modeling of local appearance for pose- and expression robust facial landmark localization. In Proceedings of IEEE conference on computer vision and pattern recognition (pp. 1741–1748) https://doi.org/10.1109/CVPR.2014.225
18. Dantone, M., Gall, J., Fanelli, G., & van Gool, L. (2012). Real-time facial feature detection using conditional regression forests. In Proceedings of IEEE conference on computer vision and pattern recognition (pp. 2578–2585).
19. Mobile Voting Using Finger Print Authentication Vijay Jumb, Jason Martin, Phyllis Figer, AniketRebello International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-4 Issue-4, April 2015
20. A Study on Various state of the art Face Recognition System using Deep Learning Techniques, Sukhada Chokkadi, Sannidhan M S, Sudeepa K B, Abhir Bhandary, IJATCSE, ISSN 2278-3091, Vol. 8 No. 4, 1590
21. N- Gram based Smart Living Machines(SLM) on IOT Platform, Rina Damdoo, IJITEE, ISSN: 2278-3075,Vol 8, Issue 8S3, 2019,293
22. Data Hiding using Meaningful Encryption Algorithm to Enhance Data Security, Devishree Naidu, Shubhangi Tirpude, Kanak Kalyani, Vrushali Bongirwar, , ISSN 2278-3091, Vol. 9 No. 2, 2408 https://doi.org/10.30534/ijatcse/2020/226922020