VOTE FROM ANY CONSTITUENCY BASED ON BIOMETRIC AND FACIAL RECOGNITION USING BLOCK CHAIN

Ashoka S G[1], Mohammed Hannan Baig[2], Guruprasad Gowda M P[3],
Yashwanth Kumar H S[4], Rakshitha R[5]
[1,2,3,4]Students, [5]Assistant professor, Department of Computer Science and Engineering
Vidya Vikas Institute of Engineering and Technology, Mysuru, Karnataka, India.

Abstract: The foremost goal of the democracy is "vote" by which the people can elect the candidates for forming an efficient government to satisfy their needs & requests such that their standard living can be improved. Electronic Voting System is a simple. Using the Biometric identification, we can get the better results and it is also trustworthy. Every citizen of India is allowed to exercise their right to vote. Security is a heart of voting system. Our main objective is to develop a compatible voting system that simplifies the Election Procedure. Finger prints of the voters are used as the main authentication resource. The fingerprint pattern of each human Being is different thus making it unique & the voter can easily authenticate. Fingerprint scanning is used for authentication. In this voting system there are no more ballot papers, ballot boxes, stamping, etc. all these are condensed in a simple box called ballot unit of the electronic voting system. In our proposed system biometric plays the main goal of identification as it cannot be easily misplaced, shared, etc. It is considered more reliable for recognition than traditional token. The voting system based on current technologies viz., biometric system and facial recognition & block chain technologies. In facial recognition voter's face who is going to cast his/her vote is Detected, Captured & Stored in the local or cloud database then match the captured image with the image which is already stored on database to recognize the person. Block chain technology which is used in crypto currencies is being used in our voting system. In this paper we will show how block chain can be used to store or transfer votes between two peers.

Keyword: Voting, Fingerprint recognition, facial recognition, Block chain.

I. INTRODUCTION

The Abraham Lincoln famously quoted democracy as "Democracy is for the people, by the people, of the people". Having an elected representative in democracy is the utmost feature of it. The elections play a crucial part in choosing the capable leader which in-turn can impact the entire nation. India has become a role model to other countries in terms of Democracy. Fingerprints of the voters are used as the main authentication resource. The finger pattern of each human being is different, thus the voter can be easily authenticated. Fingerprint scanning is used for authentication. In this voting system there is no more use of ballot papers, ballot boxes, stamping, etc. all these are condensed in a simple system called Electronic voting system. In our proposed system biometric and Facial Recognition plays the main goal of the identification which cannot be easily misplaced, shared, etc. It is considered more reliable for recognition than traditional token used during elections.

II. LITERATURE SURVEY

The Previous work done in this domain involves reviewing the already present algorithms & assessment of these algorithms based on various features & conditions such as the kind of database used, and neural network-based image processing system used for the identification of the facial features. The amount of distortion and attenuation plays a big role in producing a clear and transparent image in a localized area of the image frequency as it would be vital feature while capturing the image & processing of it to accurately match it with one that is present in the database.

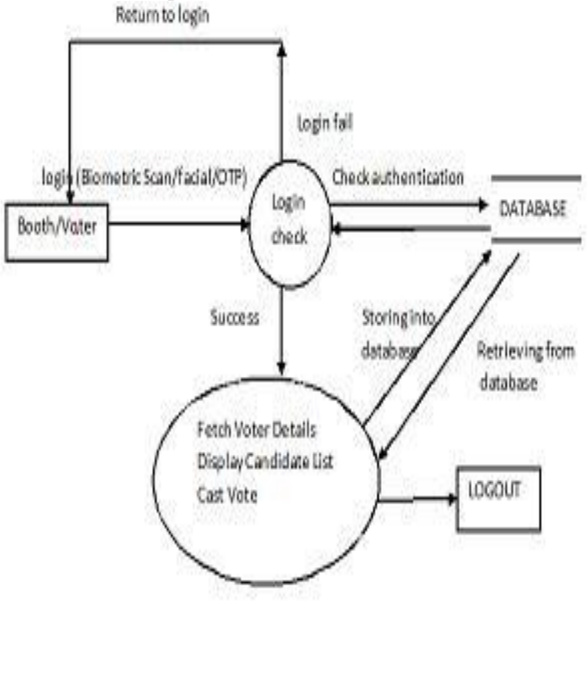


Fig 1 data flow diagram.

III. VOTING PROCESS

A. Functional requirements:

Biometric scan:

Biometrics is automated means of recognizing a person based on a physiological or behavioural characteristic. Scanning of biometrics is measured for fingerprints in this application.

Facial Detection:
In facial detection concept of viola jones algorithm is to follow appearance-based approach for face detection

Fetch voter details:
Biometric data are separate and distinct from personal information through which voters details can be easily fetched.

Display candidate list:
List of Candidates who are to be elected in the voting procedure is displayed.

Vote:
Voters cast vote for candidates they want through biometric system & facial recognition. Voting information is hashed using block chain concept & stored in cloud database.

Non-functional requirements:
This application provides confidence & participation, enabling all the citizens to actively participate in the elections from any voting booth in the Constituency & can cast their votes. Independently improving the Usability & Performance of the system.

Our application helps the voters to cast their votes trouble-free and also proceed with their daily routines hence making it more reliable. Also the quick & rapid counting process helps the election commission to announce the result as soon as the elections being conducted comes to an end. Hence the risk of Cost & maintenance of huge security force for the safety of all casted votes and plus the Time for manually counting all those votes can be prevented. Therefore it acts as a commanding tool in field of voting system.

The application also provides other specifications like ability to add future functionality in case of any new technologies & Has ability to be reused in future elections.

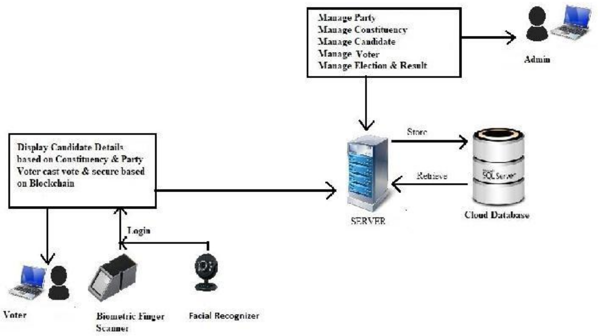
IV. EXISTING SYSTEM

People in an area will be allotted different voting booths. On reaching the voting booth, people have to submit their voter's identification card. The election committee will verify the person with their ID details. People who are voting will be marked the simple way by just using a sheet in their registers. This is not quick and convenient. And it takes long time to mark out each person. The voting machines will contain the list of candidates out of which a person has to choose one and vote for him. After the voting time, finally all votes are calculated & winner is declared. Nonetheless, this system could be outdated & is difficult to maintain. It can easily get misplaced as there will be only one saved copy of it and it is inconvenient if it gets lost. If voting time is approaching & no proper security is provided, one can vote in the name of others. There is a possibility of power going in the wrong hands.

V. PROPOSED SYSTEM

The objective of voting is to let voters to exercise their right to express their choices regarding specific issues, pieces of legislation, citizen initiatives, constitutional amendments, recalls and/or to choose their government and political representatives. Technology is being used more & more as a tool to assist voters to cast their votes. Voter identification is required during two phases of the democratic process: first for voter registration in order to establish the right to vote & afterwards at voting time, let a citizen to exercise their right to vote by verifying, if the person fulfills all the requirements needed to vote (authentication). For this purpose, biometrics & facial recognition is used. Fingerprint authentication is one of the finest biometric authentications that can be used for this purpose. Fingerprint authentication refers to the automated method of validating a match between two human fingerprints. Authentication by biometric verification is becoming more and more common in commercial and public security systems and applications. We propose a system where we use biometric & also facial recognition for elections. Voting using biometric & facial recognition is a new application for people. During voter registration, the voter fingerprints are scanned & facial data collected and saved in database after hashing it using blockchain concept. On the voting day, when the person arrives to vote, our application will match the fingerprints & recognized facial data with the database. Thus one person can only cast one vote. Any person who is not validated by the system can't vote. Thus eliminating any chance of proxy votes. This will prevent the misuse of voting powers. On the end of voting day, our application will calculate the votes & declare the winner. System records vote of people based on registered fingerprints and their facial data in hashes using blockchain concept thus making it secure.

Proposed system architecture



A voting machine with fingerprint scanner & facial scanning will be used by the voter by using windows application in a computer to cast vote after getting authenticated. First, the user has to login to the system through the fingerprint recognition. Authentication will be granted once the fingerprint matches Aadhar fingerprint database. If the fingerprint matches, then the user has to go through the authentication process of facial recognition. Once both fingerprint & Facial data is authenticated and matched, then the user will be allowed to cast their vote for their desired candidate. The casted vote will be updated at each instance of time in the database. The election results can be published on the website in the same day with high accuracy and efficiency.

VI. CONCLUSION

Face recognition has been since its advent a more secure & trustworthy form of authentication by including this feature with our present voting system we could enhance the capabilities of the system and can make it more secure and free from false voting.

Thus the onset of this biometric thumb impression voting system would enable hosting of fair elections in India. In this paper, we introduced a unique, blockchain-based electronic voting system that employs smart contracts to enable secure and cost efficient election while guaranteeing voters privacy.

REFERENCES

[1] Baumberg, “Reliable feature matching across widely separated views”, in CVPR, 2000

[2] F. Song, D. Zhang, J. Wang, H. Liu, and Q. Tao, "A parameterized direct LDA and its application to face recognition," Neuro computing, Vol.71, 2007

[3] KashifHussainMemon, Dileep Kumar and Syed Muhammad Usman, “Next Generation A Secure E-Voting System Based On Biometric Fingerprint Method”, 2011.

[4] P. Viola and M. J. Jones, "Robust real-time face detection," International Journal of Computer Vision, Vol. 57, pp. 137-154, 2004.

[5] Nicholas Weaver. (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/secure-vote-today.

[6] TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it [Online]. Available at: https://techcrunch.Com/2018/02/24/liquid-democracy-uses-blockchain.

[7] Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth. ethereum.org/

[8] Vitalik Buterin. (2015). Ethereum White Paper. Available at: https:// github.com/ethereum/wiki/wiki/White-Paper.

[9] Nca.tandfonline.com. (2015). Pirates on the Liquid Shores of Liberal Democracy: Movement Frames of European Pirate Parties. [Online]. Available at: https://nca.tandfonline.com/doi/abs/10.1080/ 13183222.2015.1017264#.Wr0zCnVl8YR

[10] Feng Hao, P.Y.A. Ryan and Piotr Zielinski. (2008). Anonymous voting by two-round public discussion. Available at: http://homepages.cs.ncl.ac. uk/feng.hao/files/OpenVote_IET.pdf [8] Feng Hao and Piotr Zielinski. A 2-Round Anonymous Veto Protocol Available at: http://homepages.cs.ncl.ac.uk/feng.hao/files/av_net. pdf.

[11] The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Available at: https://users.ece.cmu.edu/~{}adrian/ 731-sp04/readings/dcnets.html.

[12] Ronald Cramer, Rosario Gennaro and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme Available at: http://www.win.tue.nl/~berry/papers/euro97.pdf

[13] Jonathan Alexander, Steven Landers and Ben Howerton (2018). Netvote: A Decentralized Voting Network Available at: https://netvote. io/wp-content/uploads/2018/02/Netvote-White-Paper-v7.pdf

[14] Agora (2017). Agora: Bringing our voting systems into the 21st century Available at: https://agora.vote/Agora_Whitepaper_v0.1.pdf

[15] Kirill Nikitin, Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, Justin Cappos and Bryan Ford (2017). CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds Available at: https://www.usenix. org/system/files/conference/usenixsecurity17/sec17-nikitin.pdf

[16] Alin Tomescu and Srinivas Devadas (2017). Catena: Efficient Nonequivocation via Bitcoin Available at: https://people.csail.mit.edu/ alinush/papers/catena-sp2017.pdf

[17] Michael del Castillo (2018). Sierra Leone Secretly Holds First Block chain-Audited Presidential Vote Available at: https://www.coindesk.com/ sierra-leone-secretly-holds-first-blockchain-powered-presidential-vote/

[18] Ethereum Blog. (2018). On Public and Private Block chains Ethereum Blog. Available at: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains/

[19] Bitfury.com. (2018). Digital Assets on Public Blockchains Available at: http://bitfury.com/content/5-white-papers-research/bitfury-digital_ assets_on_public_blockchains-1.pdf