Decentralised Voting System Based on Regions Using Facial Recognition

Pratiksha Bankar**, Apurva Dhoble**,Nikita Jadhav**,Sakshi Tingare**
*(Prof.G.G.Taware,Computer Engineering,SVPM's College Of Engineering Malegaon(BK),Baramati
Email: hodcomp@engg.svpm.org.in)
** (UG Students,Computer Engineering,SVPM's College Of Engineering Malegaon(BK),Baramati
Email:
pratikshab0202@gmail.com,apurvadhoble7@gmail.com,nikitajadhav4124@gmail.com,sakshitingare1091@gmail.com)

Abstract:

Online voting system is an arising conception that has run gradually important in present's digital world. The technique is expected to enhance namer participation, minimize charges and add the effectiveness of the voting procedure. even so, the security of online voting networks is a biggest concern, as it's open to hacking and cyber attacks. In this paper, we bounce an online voting technique that incorporates face discovery and blockchain technology to deliver a secure and transparent voting system. The suggested system uses facial recognition to authenticate voters and blockchain technology to encrypt and store the votes, icing their security and integrity. The facial recognition technique was elaborated operating Python's inbuilt library, HOG algorithm, and was trained on authorized voter images to descry and match images during the voting procedure. SHA256 encryption was operated to cipher sensitive data, like as voter credentials and offering data, and insure secure storehouse and transmission. The executed technique was secure, tamper- evidence, and efficient in maintaining the integrity of the voting data. coming advancements could contain fresh security measures and developing the usage of blockchain technology. This system has the possible to revise the voting process by making it more secure, transparent, and accessible.

Keywords — Blockchain, Face Detection,HOG,SHA256.

I. INTRODUCTION

Now a daytime in india two kinds of system are applied for voting. The premier system is secret ballot paper, in which many of paper are used and another system is EVM(electronic voting machine) which is used since 2003. We've to bounce a system or way for online voting that's further secure than the exsiting system. India is the largest popular country in the world. So it's necessary to make sure that the governing body is chose through a fair election. India has only offline proposing system which isn't effective and upto the mark as it requires largish man manpower and it also requires additional time to reuse and display the results. so, to be produced effective, the system needs a change, which overcomes these drawbacks. The substitute system doesn't force the person's physical appearance to bounce, which makes the effects easier. This paper focusses on a system where the voter can vote ever from anywhere operating his/ her computer or mobile phone and does not bear the person to got to the polling booth through two step authentication of face recognition and blockchain security. Suppose you're an eligible person who goes to polling booth and cast vote using EVM(Electronic Voting Machine). But since it's a circuitry after all and if someone tampers with microchip, you may not know that did your vote reach to person for whom you want to voted or was diverted into another seeker's account? Since there's no tracing reverse of your vote. But, if you apply blockchain- it stores everything as a transaction t and hence gives you a receipt of your vote(in a form of a transaction ID) and you can use it to insure that your vote has been counted securely. Now suppose a digital voting system(website/ app) has been began to digitize process and all confidential data is kept on a single admin garçon/ machine, if someone tries to hack it or meddle over it, he she can change voters's vote count- from 2 to 22! You may noway know that hacker installs malware or performs clickjacking attacks to steal or negate your vote or simply attacks central machine. To avoid this, if network is integrated with blockchain- a one-off property called invariability protects system. Consider SQL, PHP, or any distinct traditional database systems. You can fit , update, or cancel votes. But in a blockchain you can just fit data but can not modernize or cancel. Hence when you fit something, it stays there ever and no one can change it- therefore name immutable ledger. But creating a blockchain system isn't enough. It should be decentralizedi.e if one server goes down or something happens on a particular node, other nodes can serve normally and don't have to stay for victim node's recovery. We use Face detection and Recognition Technology for authentication of citizens that he she is the proper consumer or not. We give numerous modules in which admin can login withinside the tool and show the

multitudinousoperations.Also voters can login in the system and use their right to vote. When the Voter uses the system, the system will capture his/ her image using a web camera & try to match with the image stored in the database. If both images are the same also the namer can cast his/ her vote.

II. LITERATURE SURVEY

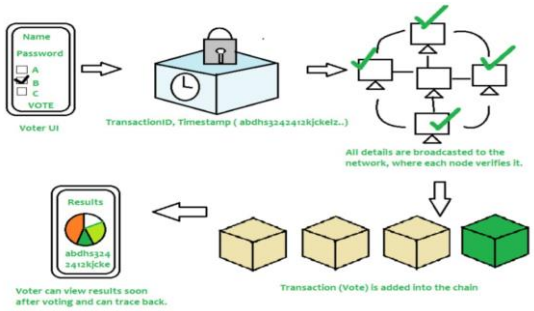
A. *Blockchain For The Security Purposes-*

if system is integrated with blockchain- a special property called invariability protects system. Consider SQL, PHP, or any other traditional database systems. You can fit , update, or cancel votes. But in a blockchain you can just fit data but can not modernize or cancel. Hence when you fit commodity, it stays there ever and no one can manipulate it- therefore name inmutable ledger. But crecting a blockchain system isn't enough. It should be decentralizedi.e if one server goes down or commodity happens on a particular node, other can serve typically and don't have to stay for victim node recovery. So a list of advantages are listed below •

You can bounce anytime/ anywhere(During Afflictions like COVID- 19 where it's insolvable to hold choices physically)

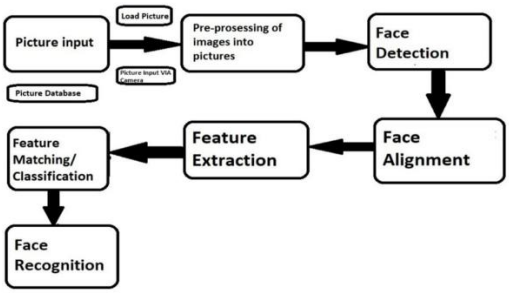
• Secure • inflexible • Faster • Transparent

B. *SHA256 For Enceyption Of An User Information-*



user needs to add his/ her credentials in order to vote. All data is then encrypted and kept as a transaction. This transaction is then circulate to every node in network, which in turn is thenverified.However, it's stored in a block and added to chain, If network approves transaction. Note that formerly a block is added into chain, it stays there ever and ca n't be updated. voter can now see results and also trace back transaction if they want. Since current voting systems do n't serve to security requirements of ultramodern generation, there's a need to make a system that leverages security, convenience, and trust involved in voting process. Hence advancing systems make use of Blockchain technology to add an redundant subcaste of security and encourage people to bounce from any time, anywhere without any hassle and makes voting process more cost-effective and time- saving.

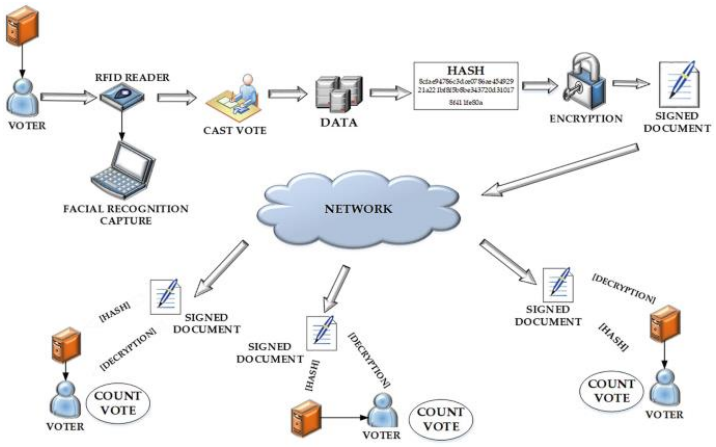
C. HOG For Detection Of Face At The Time Of Voting.-



This is grounded on the HOG(Histogram of Oriented Gradients) point descriptor with a linear SVM machine learning algorithm to perform face discovery. HOG is a simple and important point descriptor.overeater is robust for object detection because object shape is characterized using the local intensity grade distribution and edge direction

	encrypt the voter data so that no one can temper with it.		
3	For decting the face and this face can be match with the voter face photo.	HOG(Histogram Of Oriented Gradients) Supports the CNN.	level-2 heading, level-3 heading, 87%

III.TECHNICAL DETAILS.



SR. NO	ALGORITHMS APPLIED		
	Title	**Algorithm**	**Accuracy**
1	Blockchain technology are used to secure the voter information that they are used for voting.	Immutable ledger	75%
2	Algorithm can be used to	SHA256	85%

A.Dataset.

1. Voters Informations like voter name, addhaar no,phone no,address,voter id,username and password.
2. Voter face are used for the authentication of user.

B.Model Building.

The Following are the steps are used to build a model.

1. Admin-
   - Authority Of admin to login on their owm side
   - Add the candidates i.e the voter list who are eligible for the vote.
   - Manage the election i.e to add the voting start and end date, add the result date time.
   - View the voters.
2. Voter-

Voter need to registration by using the voter name, voter aadhar card no, voter address, voter face photo,voter id,username and password.(username can be generated on the hased format because the security of the blockchain)

- Login- voter need to login using the username and password.
- Face Recognition for the user authentication- user face is verfied when it match to the face images then the user has authority to vote.
- Vote- Voter have to vote the person that he/she want to voted.
- View the election result- Now voter can be see the result after the date of result decleration.

C.Technology and Tools Used-

The Following are the tools and technology are used to build the model.

1. PYTHON-
   Python are used for the coding purpose there different python inbuilt liberies are used for the face detection.
2. DLIB-
   It is a facial detector having the pre trainded models,itb is used to estimate the location of co-ordinators that maps the facial points on the person's face.so we we can map the image to identify the person is authenticate or not.
3. SHA256-
   It is encryption algorithm used in blockchain technology to encrypt the data so that no one can temper with this data.
4. PIL-
   It is in inbult python libries that can be used for the face detections.
5. Face_recognition_models-
   Python inbult function are used for face recognition.

IV.CONCLUSIONS

The thing of the present exploration is to produce a system that's further salutary and secure than former bones . also, the suggested result uses Blockchain technology to secure the voting process. Facial recognition must be a needed element of the online voting process in order to reap the maturity of the benefits. Because recognition failure disenfranchises the namer, this necessitates secure technology on both the system and namer ends. The nature of face recognition poses sequestration enterprises, which are particularly visible in the prospectivesemi-controlled remote voting setting, where the namer would have to demonstrate that the place is respectable for remote voting. likewise, collecting a videotape sluice for the purpose of liveness discovery begs the question of whether the quantum of sequestration violation is commensurable to the value achieved.

REFERENCES

[1] Amna Qureshi, David Megias and Helena Rifa-Pous, "SeVEP: verifiable secure and privacy-preserving remote polling with untrusted computing devices", *IEEE Access*, vol. 7, pp. 19266-19290, 2019.

[2] A. R. Syafeeza, M. Khalil-Hani, S. Liew and R. Bakhteri, "Convolutional neural network for face recognition with pose and illumination variation" in International Journal of Engineering and Technology, vol. 6, no. 1, pp. 44-57, 2014.

[3] Ishani Mondal and Sombuddha Chatterjee, "Secure and Hassle Free EVM through deep learning face recognition", *Proceeding in International Conference on Machine Learning Big Data Cloud and Parallel Computing (COMITCon) IEEE*, pp. 109-113, 2019.

[4] Y. Abuidris, A. Hassan, A. Hadabi and I. Elfadul, "Risks and Opportunities of Blockchain Based on E-Voting Systems", *2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing*, pp. 365-368, 2019.

[5] C. K. Adiputra, R. Hjort, H. Sato, S. M. Khan, A. Arahad, G. Mushtaq, et al., "A Proposal of Blockchain-Based Electronic Voting System", *2018 Second WorId Conference on Smart Trends in Systems*, vol. 4, no. 10, pp. 22-27, 2020.

[6] S. Agbesi and G. Asante, "Electronic Voting Recording System Based on Blockchain Technology", *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*, pp. 1-8, 2019.

[7] A.K. Maurya and A.K. Tripathi, "An edge priority-based clustering algorithm for multiprocessor environments", *Concurrency and Computation: Practice and Experience*, vol. 31, no. 11, pp. e5060, 2019.

[8] S. A. Adeshina and A. Ojo, "Maintaining Voting Integrity using Blockchain", *2019 15th International Conference on Electronics Computer and Computation (ICECCO)*, pp. 1-5, 2019.

[9] S. Bistarelli, I. Mercanti, P. Santancini and F. Santini, "End-to-end voting with non-permissioned and permissioned ledgers", *Journal of grid computing*, vol. 17, no. 1, pp. 97-118, 2019.

[10] C. K. Adiputra, R. Hjort, H. Sato, S. M. Khan, A. Arahad, G. Mushtaq, et al., "A Proposal of Blockchain-Based Electronic Voting System", *2018 Second WorId Conference on Smart Trends in Systems*, vol. 4, no. 10, pp. 22-27, 2020.

[11] S. Agbesi and G. Asante, "Electronic Voting Recording System Based on Blockchain Technology", *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*, pp. 1-8, 2019.*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.