INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND LATEST TRENDS

ISSN 3011-3030 Vol.12, Issue.4, March 2024, Pages: 2691-2695

A Secure online E-voting System using Majority voting classifier

Dr D.Suneetha[1], NVVDD Lokesh[2], Paladugu Lakshmi kamakshi[3], Mandapaka Rama Krishna[4]

[1] *M. Tech., NRI INSTITUTE OF TECHNOLOGY, POTHAVARAPPADU, AGIRIPALLI, VIJAYAWADA. AP, India,* hodcsenriit@gmail.com

[2] *B. Tech NRI INSTITUTE OF TECHNOLOGY, POTHAVARAPPADU, AGIRIPALLI, VIJAYAWADA. AP, India,* devalokesh2329@gmail.com

[3] *B. Tech., NRI INSTITUTE OF TECHNOLOGY, POTHAVARAPPADU, AGIRIPALLI, VIJAYAWADA AP, India,* paladugulakshmi733@gmail.com

[4] *B. Tech., NRI INSTITUTE OF TECHNOLOGY, POTHAVARAPPADU, AGIRIPALLI, VIJAYAWADA. AP, India,* ramki1607@gmail.com

Abstract:- This report describes an online voting system designed to meet the needs of colleges and universities. Voting is a widely spread, democratic way of making decisions and can be used for electing student presidents and class representatives at the college level. The main aim of the project is to provide a secured and user-friendly voting system. The process of voting is critical in terms of safety and security. The system deals with the design and development of an electronic voting system by using face recognition. The proposed system allows the voters to scan their faces, which is then matched with the already saved images within the database. Unlike the traditional method, this system conceals the voter's choice from any unauthorized party. By using face recognition, it provides enough security to eradicate the dummy votes. The system also provides clear visualization of data regarding the percentage of total votes cast, the percentage of votes each party secured, and the final winner in the election.

Introduction:-

Elections are inevitable happenings in a democratic society and it is the soul responsibility of both the government and the citizens to make sure that it happens in a safe and secure way and also it take place smoothly. By means of this system the person is required to record his face before the election and the same is taken to account to compare while voting. In offline the data recorded through offline is sent through the microcontroller to the Web after reading the details. Application by means of serial terminal The program for the web application manages the Individual Database. If a citizen casts his vote, the website sends a confirmation message as ‘voted successfully’ that the vote is successfully registered. In the process of voting, voicing their choices or articulating views The main goal of this project is to make sure a voting system is designed using face recognition technology and OTP system to vote from any place on earth where internet is available. The Voting information is stored in the server database. As the world is changing day by day and is essential to adapt to the electronic world inorder to survive and meet world standards. This new technology refers to electronic voting systems where election is conducted online and offline but has a central database for smooth data transfers and result calculation. Therefore an e-voting system has to be designed and employed for a fair election to take place.Online voting system is contemplated as an interesting topic in information security research. Online voting system is a way that helps public to select their representatives and express their preferences for how they will be governed. Naturally, the belief of the election process is utmost important [1]. Election process has strong media coverage, particularly if something goes wrong. This system will increase the level of security and also the trust of voters. The problems of Maoist affected places for the voting has been addressed in [2] while [3] describe the genesis of Maoist violence and showed that public needs a more secure way of casting their vote. Online voting system definition given in [4] states that Online voting systems offer advantages compared to other voting processes. An Online voting system may be involved in any one of a number of steps in the setup, voting, collecting, distributing and counting of ballots. The question of who gets to count your vote was addressed in [5] while in [6] the voting security has been analysed. The same problem has also been addressed in [7] more abstractly to ponder over its perception and reality. The question of faith on the electronic voting has been discussed in [8]. It is hard to make the voting system trustworthy only because it has high security requirements: confidentiality and integrity. Confidentiality means all voters get assured about the privacy of votes and prevent selling of votes. Integrity means the assurance of election results and the votes are counted correctly. Integrity is easy to get through a public show of hands, but this dissipatesconfidentiality and confidentiality comes from the secret ballots, but this fails the integrity. The proposed system provides peoples to vote in a secure manner without any fear. The online voting system also provides the security to the voter's by storing the vote in a secure digital form, if the voter votes against malevolent candidate. This system also guarantees not to leak the vote in front of anybody. Section 2 of the paper briefly discusses the overview of the proposed online voting system.

Literature Survey:- In the paper 'secure and privacy preserving remote polling with untrusted computing devices" author "AMNA QURESHI", describes, to design a polling system which is flexible in polling, using fingerprint devices to provide an extra step of authentication, allow different devices which is available to the voter, no usage of polling sheets and to generate poll tags[1].In the paper "Secure and Hassle Free EVM through deep learning face recognition" author "Ishani Mondal", used neural networks after extracting the facial features of the voter and with that a reference to vote during election. If the details matches the existing details the user is allowed to vote [2].In the paper "VOT-EL: Three Tier Secured State-OfThe-Art EVM Design Using Pragmatic Fingerprint Detection Annexed With NFC Enabled Voter -ID Card" author", Anooshmita Das", proposed design, along with biometrics NFC technology is also taken into account.[3].In the paper "Secure and Electronic polling system", the authors AMNA QURESHI, DAVID MEGÍAS, HELENA RIFA-POUS described Se-VEP, an e-polling system enabled by Internet which provides and protects the voter's integrity, security, voters unique details, poll integrity, third party breaching, prevention of double voting , fairness in election, and coercion resistance, and preventing devices with virus which change the users decision in voting and giving false results which leads to lot of problems [4].

Related Work:-

The system model for our proposed e-voting scheme is shown in Fig. 1. It can be observed that the system contains multiple E-voting stations that are connected to the public block chain. Other than that, we have a database that stores the citizen 's record for the entire city to decide whether or not an elector is eligible to cast a vote at a particular polling station. In each E-voting station, we have servers (which can access data from the primary database if required), voters and voting machines. In our system, we use the concept of both public and private block chain, as shown in Fig. 1, E-voting stations use a private block chain to register the voters and count the votes for a specific cause or a specific candidate. The reason for using a private blockchain is that it's inexpensive and a bit faster than the public. In addition, it does not pollute the public block chain with raw data because it was designed to be used only for a digital currency, not for data storage, and it also holds the record of our desired transactions in a separate and filtered form, which can provide a great deal of assistance when auditing the voting system. Whereas, on the other hand, the public blockchain is used to share the root hash given by the Merle tree in order to ensure the integrity of the data and distribute the final results of each polling station so that it is freely accessible to everyone. There are a few steps in our system to vote; first, an elector sends a request for registration to his / her corresponding E-voting station by submitting some personal information , e.g. name, CNIC, father's name, place of birth and date of birth. When the registration server receives the information, it hashes the data and then requests the primary data center to provide the correspondence to the requested user. If hashes get the match , the elector must register and be entitled to cast a ballot on the election day. Until we delve deeply into the proposed methodology, we need to identify the design criteria for Evoting.

Design Requirements for E-VOTING

In this section, we have mentioned the design requirement for an efficient E-voting system.

- ➢ It should be able to avoid multiple votes by a single person.
- ➢ It should be able to provide integrity to citizen data.
- ➢ It should be able to provide integrity to the votes cast by citizens.
- ➢ The procedure should be easy to follow.
- ➢ It should be robust.
- ➢ It should be able to detect intrusions within the network

- It should be able to allow us to detect the external threats so we could plan countermeasures against it.

Merkle Root To ensure the integrity of our citizen's record that is stored at the primary data center (where the citizen's record is saved), we use the Merkle tree hashing algorithm to get the hash of the data and save the root hash of the Merkle tree to the public blockchain to provide an extra layer of data integrity. Merkle tree is a key algorithm to store data with a lot of security and integrity. Each leaf in the Merkle tree contains a cryptographic hash (which takes the citizen 's record as input and in return gives a unique hash). Merkle tree keeps merging it from step 1 to root hash, as shown in Fig. 2. Then we need to protect the root hash to ensure the integrity of the data. Merkle root has the following two essential properties.

- Non-Membership Proof.
- Membership Proof

Proposed System:-

The proposed system allows the voters to scan their faces, which is then matched with the already saved images within the database. Unlike the traditional method, this system conceals the voter's choice from any unauthorized party. By using face recognition, it provides enough security to eradicate the dummy votes. The system also provides clear visualization of data regarding the percentage of total votes cast, the percentage of votes each party secured, and the final winner in the election.

Problem Statement: The existing system of university elections is running manually. The voter has to cast his/her votes through a paper-based system where the voter has to tick off to who they would like to vote and then hand over the paper to the officials. This might lead to the tampering of votes or a person can cast votes multiple times or on behalf of others.

• Approach: Face detection using artificial intelligence, data visualization using machine learning, and data mining techniques are used in this system. The first step involves creating a data set containing the photos of the students within a class. The second step involves using face recognition and ensuring a fair voting process and result prediction.

Results: The system will ensure that no voter will get to cast multiple votes and also ensures that only students from a particular class will be able to take part in their representative election. In the end, the contestant with the highest number of votes will be represented as the winner. Also, a graphical representation of the votes obtained by each contestant will be displayed.

Conclusion The main aim of the project is to ensure a more secure and transparent voting system. By using artificial intelligence, the proposed system ensures the tampering happening within the current voting system are minimized if not completely eradicated. The voting system is proposed to create a stable and efficient E-voting system architecture. This proposed system not only deals with the integrity of votes but also secures citizens' data as an Evoting station network. We used two machine learning models with a different set of settings. One is the Gaussian Vector Support Machine, and the other is the linear Vector Support Machine. A comparison is made between these two classifiers by measuring their accuracy and AUC (area under the curve). The idea of a smart contract is used to register voters and to receive votes as well. Where the Merkle root algorithm has been used to get the root hash to ensure the integrity of the data stored at the citizen's data centre. We believe that this voting architecture can be extended as an I (internet voting) where users can vote through a secure application or secure web servers. We did not focus servers generating addresses for users that we use to register and process blockchain that could be part of our future projects towards an efficient smart voting system using blockchain and machine learning. In addition, in the future, we will be able to look at the counter-measures of the various attacks once we have detected them.

References

[1] M. P. Wattenberg, Is voting for young people? Routledge, 2020.

[2] D. P. Redlawsk and M. W. Habegger, A Citizen's Guide to the Political Psychology of Voting. Routledge, 2020.

[3] C. Marsden, T. Meyer, and I. Brown, "Platform values and democratic elections: How can the law regulate digital disinformation?" Computer Law and Security Review, vol. 36, p. 105373, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S026736491930384X

[4] T. Dimitriou, "Efficient, coercion-free and universally verifiable blockchain-based voting," Computer Networks, vol. 174, p. 107234, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128619317414

[5] Y. Xiao, H. Deng, X. Lu, and J. Wu, "Optimal ballot-length in approval balloting-based multi-winner elections," Decision Support Systems, vol. 118, pp. 1 – 9, 2019. [Online]. Available:http://www.sciencedirect.com/science/article/pii/S0167923618301994

[6] J. Li, X. Wang, Z. Huang, L. Wang, and Y. Xiang, "Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing," Journal of Parallel and Distributed Computing, vol. 130, pp. 91 – 97, 2019. [Online]. Available: http://www.sciencedirect.com/ science/article/pii/S074373151930262X

[7] K. M. AboSamra, A. A. AbdelHafez, G. M. Assassa, and M. F. Mursi, "A practical, secure, and auditable e-voting system," Journal of Information Security and Applications, vol. 36, pp. 69 – 89, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/

[8] M. Warkentin, S. Sharma, D. Gefen, G. M. Rose, and P. Pavlou, "Social identity and trust in internet-based voting adoption," Government Information Quarterly, vol. 35, no. 2, pp. 195 – 209, 2018, agile Government and Adaptive Governance in the Public Sector. [Online]. Available: http://www.sciencedirect.com/science/article/pii/ S0740624X17301478

[9] S. S. More and P. P. Gaikwad, "Trust-based voting method for efficient malware detection," Procedia Computer Science, vol. 79, pp. 657 – 667, 2016, proceedings of International Conference on Communication, Computing and Virtualization (ICCCV) 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916002155

[10] A. B. Masood, M. Lestas, H. K. Qureshi, N. Christofides, N. Ashraf, and F. Mehmood, "Closing the loop in cyber-physical systems using blockchain: Microgrid frequency control example," in 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM). IEEE, 2019, pp. 1–6.

[11] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K.-K. R. Choo, "Neural-blockchain-based ultrareliable caching for edge-enabled uav networks," IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5723–5736, 2019.

[12] J. Gao, T. Wu, and X. Li, "Secure, fair and instant data trading scheme based on bitcoin," Journal of Information Security and Applications, vol. 53, p. 102511, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214212619309688

[13] P. Lafourcade and M. Lombard-Platet, "About blockchain interoperability," Information Processing Letters, vol. 161, p. 105976, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/ pii/S0020019020300636 [14] S. K. Lo, X. Xu, M. Staples, and L. Yao, "Reliability analysis for blockchain oracles," Computers and Electrical Engineering, vol. 83, p. 106582, 2020. [Online]. Available: http://www.sciencedirect.com/ science/article/pii/S0045790619316179

[15] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy in blockchain technology: A futuristic approach," Journal of Parallel and Distributed Computing, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0743731520303105

[16] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," Future Generation Computer Systems, vol. 105, pp. 13–26, 2020.

[17] ——, "Simulation of transaction malleability attack for block chain based e-voting," Computers and Electrical Engineering, vol. 83, 2020.

[18] J. P. Cruz and Y. Kaji, "E-voting system based on the bitcoin protocol and blind signatures," IPSJ Transactions on Mathematical Modeling and Its Applications, vol. 10, no. 1, pp. 14–22, 2017.

[19] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," International Journal of Network Security & Its Applications, vol. 9, no. 3, pp. 01–09, 2017.

Dr. D. Suneetha, a seasoned academic leader, is the Professor and Head of the CSE department at NRI Institute of Technology. With expertise in AI, ML, and Cloud Computing, she has published 31 papers and authored 4 books. Recognized for her excellence, she has received numerous awards including Best Teacher and Best HoD in 2021. Dr. Suneetha's commitment to education and research makes her an invaluable asset to her institution.

Neela veera venkata deva dhundi lokesh is a student of NRI INSTITUTE OF TECHNOLOGY, POTHAVARAPPADU, AGIRIPALLI, VIJAYAWADA. AP, India and He is pursuing B.tech Degree.

PALADUGU LAKSHMI KAMAKSHI is a student of NRI INSTITUTE OF TECHNOLOGY, POTHAVARAPPADU, AGIRIPALLI, VIJAYAWADA. AP, India and she is pursuing B.tech Degree.

Mandapaka Rama Krishna is a student of NRI INSTITUTE OF TECHNOLOGY, POTHAVARAPPADU, AGIRIPALLI, VIJAYAWADA. AP, India and he is pursuing B.tech Degree.