ISSN 2394-739X

IJRSET MAY Volume 9 Issue 5

International Journal for Research in Science Engineering & Technology (IJRSET)

https://www.doi.org/10.5281/zenodo.6556149

BALLOT CHAIN FOR SECURE AND TRANSPARENT E-VOTING MECHANISM USING AIIOT AND BLOCKCHAIN TECHNOLOGY

[1] Mr.R.Sathish Kumar, [2] M.Sanjay, [3] P.K. Pranav, [4] S.Suriya, [5] N.Shri Heamnath
[1, 2, 3, 4, 5] Electronics and Communication Engineering,
[1, 2, 3, 4, 5] NS COLLEGE OF TECHNOLOGY,
[1, 2, 3, 4, 5] Vazhiyampalayam, Coimbatore, Tamil Nadu 641035.

ABSTRACT - Artificial intelligence (AI) has shown colossal potential in an assortment of genuine applications. Nonetheless, a few huge contemplations like decency, transparency and trustworthiness are as yet testing while applying AI to trust-situated applications, for example, E-voting. The innovation can guarantee the safety of each and every vote, better and quicker and substantially more exact counting and programmed counting. In this paper intend to work with the combination of AI ecosystems by fostering a blockchain-based recognizable self-counting e-voting system the proposed system presents an original voting system by utilizing QR and Fingerprint of Aadhaar card. Whenever the e-voting system is coordinated with the Internet of Things, any qualified voter can vote from anyplace as there will be at least two degrees of validness checks. The proposed instrument of voting utilizing Blockchain serves the election directing bodies as well as the voters who get told in the event of any interfering with their votes before the counting announcement.

Keywords: [Artificial intelligence, IOT, Voting System, Fingerprint, Aadhaar card, Blockchain.]

1. INTRODUCTION

India is the biggest democratic and Republic country on the planet. In any democratic and republican country elections are important and furthermore a heart to the majority rules government. In a vote based system people have the honor of being administered willingly. People pick their agents through elections which are the ordinary highlights of popular governments from one side of the planet to the other. In any case, these elections ought to be held freely, fairly, transparently and impartially. For this reason, the constitution of India furnishes an Election Commission with independent (Art 324-329), comprising a Chief Election Commissioner and other Election Commissioners (at present two other election commissioners).

Indian Electoral System

The Constitution of India has vested in the Election Commission of India the Superintendence, heading and control of the whole interaction for direct of elections to Parliament and Legislature of each and every State and to the workplaces of President and Vice-President of India. The Indian Electoral system has been extensively partitioned into two; they are immediate election in view of territorial constituencies and proportional portrayal through a single transferable vote. The primary system is followed for the election of the members of Lok Sabha, State Assemblies and UnionTerritories assemblies. The second, election hung based on proportional portrayal through a single transferable vote for the President and the Vice-President of India, member's of Rajya Sabha and members of Legislative councils.

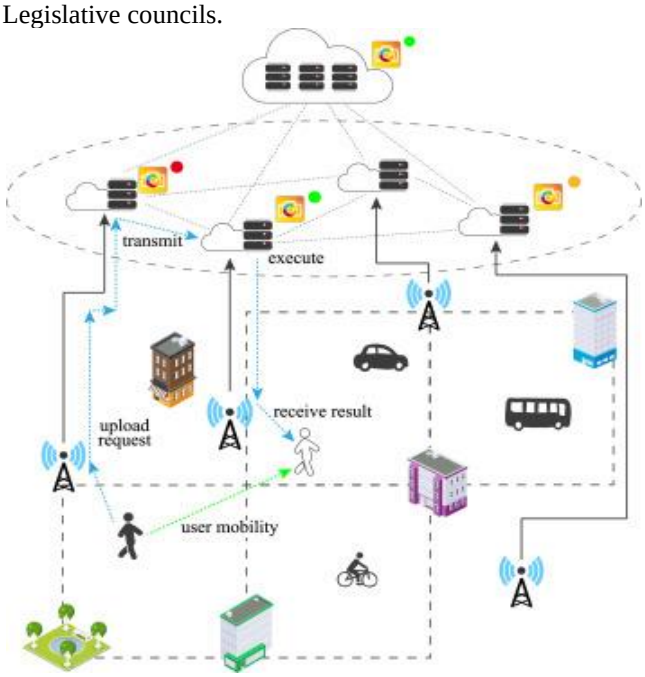

Figure 1.Blockchain and IoT

Building an IoT stage that is decentralized in nature will assist guarantee compatibility with a blockchain network, yet it tends to be a test to design IoT sensors to deal with their own computer and data storage, since they depend on focal register and storage assets. This use of blockchain technology permits endeavors to oversee data nervous devices in an IoT system, reducing costs related with IoT device support and data move. It lessens the dangers of overseeing data, since there is no concentrated data archive and the record isn't powerless against cyber attacks. It wipes out the IoT passage or some other middle device for data exchange and diminishes the time expected to handle the data. Blockchain forces undeniable level security by authenticating and authorizing encoded device-created data with the assistance of decentralized, appropriated

records. In a circulated record, data calculation and storage are spread across a large number of devices. Thus, the disappointment of a device, a server or the network won't influence the whole IoT ecosystem, as it could in the customary model. As a rule, the resiliency of a blockchain network will move toward adaptation to non-critical failure, where the network can keep working on the off chance that hubs are taken disconnected. Because of powerless access control and client/server models, numerous IoT ecosystems present easy objectives for criminals. Dispersed denial of service (DDoS) attacks to ordinary traffic to associated devices by overpowering the objective or encompassing foundation with a surge of internet traffic, have become more successive. The Mirai and Hajime IoT botnets uncovered the weakness of associated devices to DDoS attacks. IoT devices and networks can be shielded from botnet-driven DDoS attacks with the appropriated security engineering of a blockchain. In this engineering, each device in a network is freely gotten with a blockchain peer-to-peer network.

2. EXISTING METHODOLOGIES

1. S.Jehovah Jireh Arputhamoni A.Gnana Saravanan et.al proposed Online Smart Voting System Utilizing Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN. India being a democratic nation, actually leads its elections by utilizing voting machines, which includes significant expense and manual work. Web-based system empowers voter to project their votes from anyplace on the planet. The ongoing system requires the actual presence of voter, which is awkward to numerous voters. The cycle consumes less time also. Utilizing the detection of face and fingerprint images, the quantity of phony voters can be decreased. This proposed brilliant voting system utilizes face and Fingerprint acknowledgment by utilizing the image processing and CNN, which is more gotten than the current one. The fundamental security level is where the system perceives the face and fingerprint of the voter from the ongoing database of face images and Fingerprint images given by the election commission. Minutiae based Matching technique is for matching fingerprint images and image given by election commission. In the event that the image caught is coordinated and voter is permitted to vote.

2. S.Ganesh Prabhu, P Jayarajan et.al proposed Smart Online Voting System. The point of this undertaking is to permit the client to vote disconnected too in the event that he/she feels that is happy with utilizing radio frequency identification (RFID) labels. It is examined by a RFID card peruser and afterward analyzed in light of the subtleties put away in the database. The client if votes through disconnected should likewise go through the customary use instances of fingerprints and voter id. The voting system during the election is totally through the internet and is empowered exclusively during the booked season of election. During the election time goes through two step verifications. The first is through facial recognition. At the point when the client has enrolled his/her vote and is a legitimate voter the client is gone before to the subsequent stage of verification. In the subsequent stage of confirmation, the client gets an OTP to his/her enlisted versatile number. The client is then provoked to enter that OTP in the system to make a choice. Presently assuming that the OTP matches and every one of the certifications are correct the client is prepared to vote. The client can choose a party and cast a vote. In this way, the voting system is finished effectively.

3. Ramya Govindaraj, Kumaresan P, K.Sreeharshitha et.al proposed Online Voting System Using Cloud. The point of this task is to execute online voting system with highlights like the plans that the particular party has carried out, in view of the elements will vote. Before days there was voting system with papers. Presently, this electronic system has no need of ballot papers and so forth. Every one of the approved and qualified people can enroll through online and can vote by signing into their own systems. There is no tedious for the clients. The significant benefit is that the client has no need of coming to the voting lobbies, as they can vote from anyplace. This article proposes online voting system with highlights like the plans that the particular party has executed, in view of the elements will vote. The fundamental motivation to move from ordinary voting system to online voting system is that it can consume time and can vote from anyplace through online.

4. Samiran Bag; Feng Hao et.al proposed E2E Verifiable Electronic Voting System for Shareholders. The point of this venture is an end-to-end (E2E) verifiable online shareholder voting system utilizing individualized computing device, say a PDA. In a public corporation, shareholders have specific freedoms relating to their value venture. These incorporate the option to vote on specific corporate issues connected with the working of that company. This article proposes SHE, an e-voting plan that permits shareholders of a company to vote remotely (or on location) on specific corporate issues. SHE plot is end-to-end verifiable as per the thought gave in the writing. Also, these article major areas of strength for gives of the voter privacy. While the voting server is totally compromised, what the attacker can realize is restricted to the halfway count at the hour of the split the difference, which is least data spillage and furthermore shown that this article brings about sensible computational and correspondence load on the election the executives system which makes it appropriate for genuine deployment.

3. PROPOSED METHODOLOGY

In the proposed technique, every one of the exercises is overseen utilizing a Blockchain based system. The proposed two-end systems wherein every one of the exercises is facilitated by the public and state bodies at different levels and voters have an equivalent impact in it. The mix of Blockchain instrument and voting system might decrease the dangers with straightforward and decentralized element of Blockchain technology.

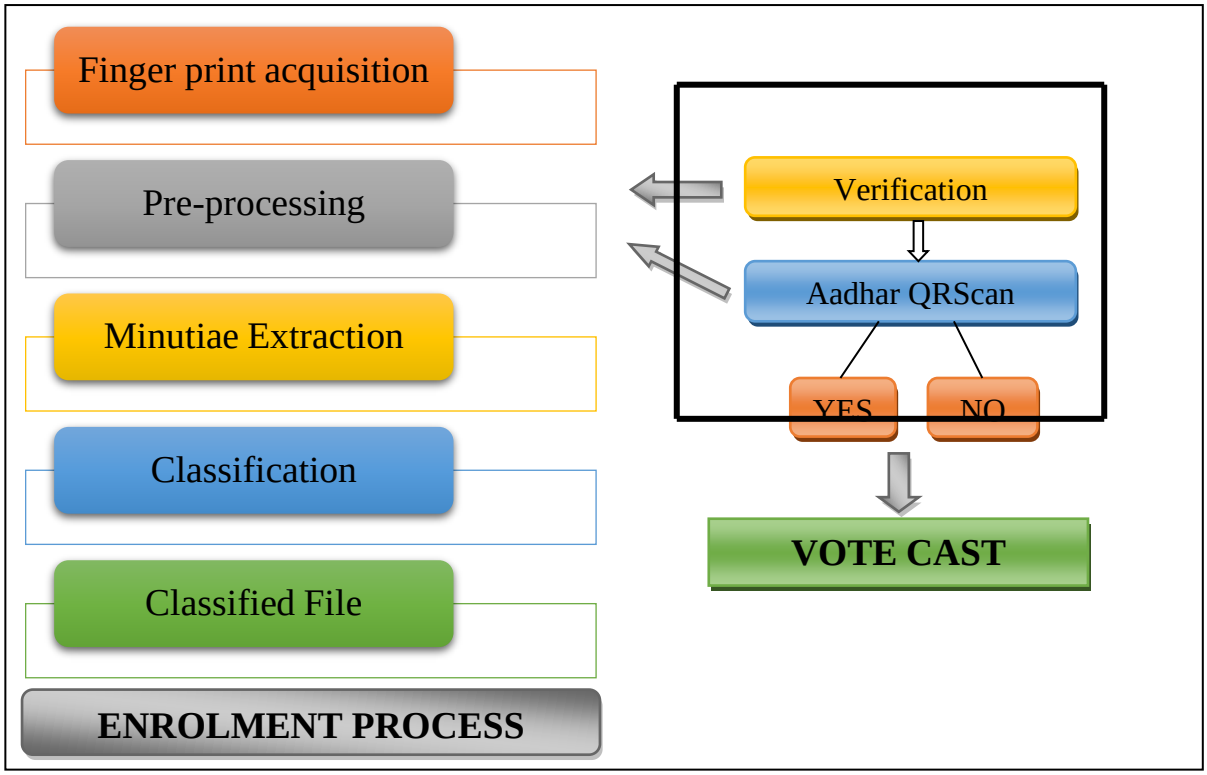

Figure 1.Voter Verification Module

3.1 Blockchain-Based Electronic Voting System

Poll-site Internet voting

It offers the guarantee of more noteworthy accommodation and proficiency in that voters could project their ballots from any poll site utilizing their Aadhar card, and the counting system would be both quick and certain.

QR and Fingerprint based Voter Verification System

The proposed technique utilizes the QR code and fingerprint biometric confirmation given by the Aadhaar card in India.

Aadhar QR Verification

Aadhaar card contains a resident information, Aadhaar number, QR code. In that, Aadhaar QR code contains a substantial Aadhaar number. By decoding the QR code, the Aadhaar number is acquired. The resident information can be gotten to by utilizing the Aadhaar number. The resident information contains an iris data, fingerprint data, address, and so forth. In light of the Aadhaar QR code, a virtual voting System utilizing journal procedure is created. The AVS permits the resident Aadhaar QR code. The Aadhaar number is extricated by the decoding of QR code. Extricate the resident information and fingerprint from the database in light of the Aadhaar number.

Fingerprint Biometric

In order to prevent identity theft and multiple voting, biometric technology can be utilized at polling stations to affirm the character and qualification of voters. Biometrics is the best technology to recognize and verify people dependably and immediately founded on their special actual qualities, like fingerprints, to refer to only the most notable model.

DCNN Based Biometric Verification

The person's biometric highlights are caught and contrasted with recently caught and affirmed biometric elements of that person. All biometric data is first caught by a sensor as an image. This image is then additionally handled into a biometric format. DCNN Algorithm utilized for verification and de-duplication depend on looking at these biometric templates.

3.1.1 Ballot Chain

Cast as intended: The recorded vote must be the same as the one the voter intended to cast.

The principal thought of the Ballot chain arrangement is to match a Bitcoin transaction to a vote cast by an elector on the side of the competitor chose by the voter. Each vote subsequently profits by the qualities of a Blockchain transaction, to be specific: It is non-modifiable; It is non-repudiable; It can't be enlisted in more ways than one; All nodes have a legitimate copy.

Self-Tallying

Counted as cast: The tally must be the same as the sum of the recorded votes

Fulfilling this vital prerequisite without tallying specialists is the principal Contribution. This is on the grounds that the last voter to cast a ballot can figure the election result prior to picking his/her vote and casting the last ballot.

ENDCORE Counting

Artificial Intelligence applied to the electoral count utilizing Counting Sort Decision Algorithm. The

most indispensable and strong module has been created to run on the Election Day for counting of votes, monitoring of end-to-end cycle and statement of Results by the System. The Application is planned such that the series of work to be finished by the Returning Officer in the System will automatically be sprung up consistently.

At first, the election commission board set under registration process in server. In Under registration process, the Electoral Server is coordinated with Aadhar and Blockchain to securely direct election.

4. EXPERIMENT RESULTS

In this segment, the exhibition of our proposed e-voting system is dissected. The prevoting phase has no computation, which just conveys the numbers of the voters and competitors. Consequently, for the most part break down the computation cost of the voting phase and post voting phase. Also, separately test the complete time cost for the various numbers of voters and applicants by utilizing the 1024-bit session key and the 512-bit shared secret on a laptop.

Performance Analysis of the Voting Phase

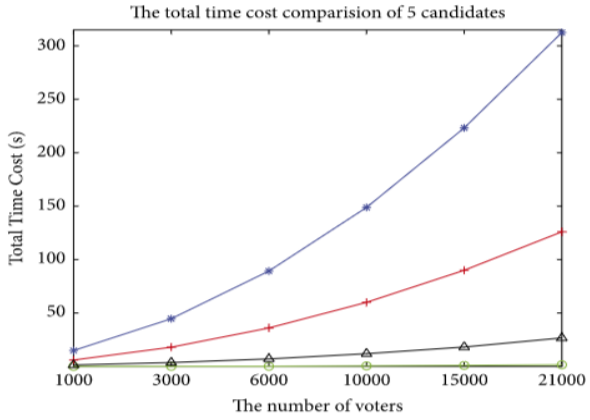

Figure 3.Performance Analysis of the Voting Phase

In the voting phase, the five steps are as per the following: enrolling identification for voters, arranging session keys among voters, creating covered values, developing shared polynomials, and processing shares. In the mean time, the computation cost for the most part thinks after producing veiled values and registering shares. Expect that the computation costs of one veiled worth and one offer are independently communicated as $cost_{mask}$ and $cost_{share}$.

Performance Analysis of the Post voting Phase

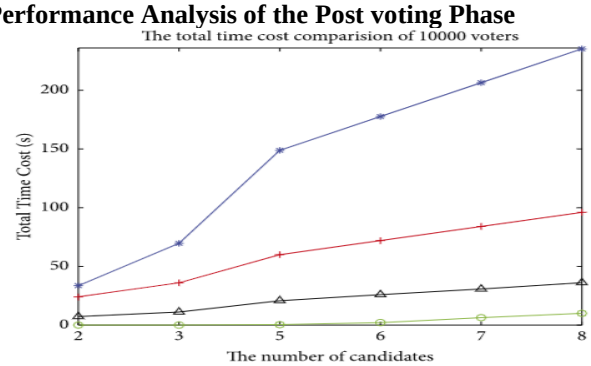

Figure 4.Performance Analysis of the Post voting Phase

In post voting phase, VS and up-and-comers are answerable for registering the amount of shares and afterward publish. Every member remakes a polynomial to get the tallying result and afterward confirms it. In the interim, figuring the amount of shares, recovering polynomial, and confirming the tallying result are the primary computation cost in this phase. Accept that they are independently communicated as $cost_{mask}$, $cost_{share}$ and $cost_{verify}$.

CONCLUSION

The idea of adapting digital voting systems to make the public electoral process less expensive, faster and easier, is a convincing one in present day culture. Making the electoral process modest and fast, standardizes it according to the voters, eliminates find out power obstruction between the voter and the chosen official and comes down on the chosen official. In this paper presented an extraordinary, blockchain-based electronic voting system that uses brilliant agreements to empower secure and cost-effective election while ensuring voters privacy. The election plot permits individual voters to vote at a voting locale fitting their personal preference while ensuring that every individual voter's vote is counted from the right area, which might actually increment voter turnout.

REFERENCES

[1]. S. Shukla, A. N. *asmiya, D. O. Shashank, and H. R. Mamatha,"Online voting application using ethereum blockchain," in 2018International Conference on Advances in Computing, Communicationsand Informatics (ICACCI), pp. 873–880, Bangalore,India, September 2018.

[2]. S. Komatineni and G. Lingala, "Secured E-voting system usingtwo-factor biometric authentication," in Proceedings of the2020 Fourth International Conference on Computing Methodologiesand Communication (ICCMC), pp. 245–248, Iccmc,Erode, India, March 2020.

[3]. M. G. Gurubasavanna, S. Ulla Shariff, R. Mamatha, andN. Sathisha, "Multimode authentication based electronicvoting kiosk using raspberry pi," in Proceedings of the InternationalConference on I-SMAC (IoT in Social, Mobile,Analytics and Cloud), I-SMAC, pp. 528–535, Palladam, India.,September 2018.

[4]. K. Curran, "E-voting on the blockchain," =e Journal ofBritish Blockchain Association, vol. 1, no. 22–7, 2018.

[5]. M. Audi Ghaffari, An E-Voting System Based on Blockchain and Ring Signature, School of Computer Science University of Birmingham, Birmingham, UK, 2017.

[6]. Y. Abuidris, A. Hassan, A. Hadabi, and I. Elfadul, "Risks and opportunities of blockchain based on e-voting systems," inProceedings of the 2019 16th International Computer Conference on Wavelet Active Media Technology and InformationProcessing, pp. 365–368, Chengdu, China, December 2019.

[7]. A. Ghosh, S. Gupta, A. Dua, and N. Kumar, "Security ofCryptocurrencies in blockchain technology: State-of-art,challenges and future prospects," Journal of Network andComputer Applications, vol. 163, Article ID 102635, 2020.

[8]. S. Bai, G. Yang, J. Shi, G. Liu, and Z. Min, "Privacy-Preserving oriented floating-point number fully

homomorphic encryptionscheme," Security and Communication Networks,vol. 2018, Article ID 2363928, 14 pages, 2018.
[9]. Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani,``Internet-of-Things-based smart cities: Recent advances and challenges,"IEEE Commun. Mag., vol. 55, no. 9, pp. 16-24, Sep. 2017.
[10]. M. E. M. CayamcelaandW. Lim, ``Artificial intelligence in 5G technology:A survey," in Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC),Oct. 2018, pp. 860-865.