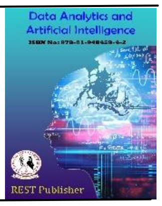
DOI: https://doi.org/10.46632/daai/2/4/29

Data Analytics and Artificial Intelligence
Vol: 2(4), 2022
REST Publisher; ISBN: 978-81-948459-4-2
Website:http://restpublisher.com/book-series/data-analytics-and-artificial-intelligence/



Ai Based Dual Authentication System

*S. Gopinath, S. Pragadeswaran, P. Subaranjani, R. Mounitha, N. Parameshwari
Karpagam Institute of Technology Coimbatore, Tamil Nadu, India
*Corresponding author Email: drgopi9hd1985@gmail.com

Abstract: Artificial intelligence (AI) has demonstrated huge potential in a various real-world applications. However, some significant considerations like fairness, transparency and trustworthiness are still challenging when applying AI to trust-oriented applications such as E-voting. In this project, we aim to facilitate the consolidation of AI ecosystems by developing a blockchain-based traceable self-tallying E-voting system. The proposed system presents a novel voting system by using Fingerprint of Aadhar card. In E-voting system an voter can vote from anywhere as there will be two or more levels of authenticity checks. The system will act as registering module on activating switch by the super admin. For registering module, followed by the fingerprint verification. The system permits the elector to cast their vote, block chain technology comes into existence that is integrated within the machine. Each vote is added into each block encrypted by 256-bit SHA hash codes, the hashed block cannot be tampered by any individual as more security is added to the system. By adopting Blockchain within the distribution of information will scale back one in every of the cheating sources of database manipulation. The proposed mechanism of voting using Blockchain not only serves the election conducting bodies but also the voters who get notified in case of any meddling with their votes before the counting announcement.

Keywords: Dual Authentication voting, Self-tallying Voting System, Ballotchain, AI Based Voting, Aadhar Card Based Voting..

1. Introduction

India is the largest democratic and Republic country in the world. In any democratic and republican country elections are necessary and also a heart to the democracy. In a democracy people have the privilege of being ruled by a government of their own choice. The Electronic Voting Machines (EVMs) were used for the first time in part of Parur Assembly Constituency in Kerala in 1982, on experimental basis. Later, the extensive use of EVMs started in 1998. The EVMs were used at all polling stations in the country in the14th General Elections to the Lok Sabha in 2004 for the first time. Since then, all elections to Lok Sabha and Legislative Assemblies have been held using EVMs. Building an IoT platform that is decentralized in nature will help ensure compatibility with a blockchain network, but it can be a challenge to configure IoT sensors to handle their own computer and data storage, since they rely on central compute and storage resources.This application of blockchain technology allows enterprises to manage data on edge devices in an IoT system, reducing costs associated with IoT device maintenance and data transfer. It reduces the risks of managing data, because there is no centralized data repository and the ledger is not vulnerable to cyberattacks. It eliminates the IoT gateway or any other intermediate device for data exchange and reduces the time required to process the data.Blockchain imposes high-level security by authenticating and authorizing encrypted device-generated data with the help of decentralized, distributed ledgers. In a distributed ledger, data computation and storage are spread across millions of devices. As a result, the failure of a device, a server or the network will not affect the entire IoT ecosystem, as it might in the traditional model. In many cases, the resiliency of a blockchain network will approach fault tolerance, where the network can continue operating if nodes are taken offline. Due to weak access control and client/server architectures, many IoT ecosystems present soft targets for hijackers. Distributed denial of service (DDoS) attacks, which disrupt normal traffic to connected devices by overwhelming the target or surrounding infrastructure with a flood of internet traffic, have become more frequent. The Mirai and Hajime IoT botnets exposed the vulnerability of connected devices to DDoS attacks.

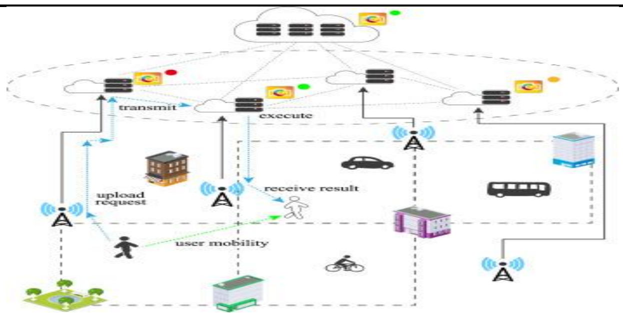


FIGURE 1. Block chain

2. Related Works

i) **Kiosk Voting:** Voting machines would be located away from traditional polling places, in such convenient locations as malls, libraries, or schools. The voting platforms would still be under the control of election officials, and the physical environment could be modified as needed and monitored (e.g., by election officials, volunteers, or even cameras) to address security and privacy concerns, and prevent coercion or other forms of intervention.

ii) **Remote Internet Voting:** It seeks to maximize the convenience and access of the voters by enabling them to cast ballots from virtually any location that is Internet accessible. While this concept is attractive and offers significant benefits, it also poses substantial security risks and other concerns relative to civic culture. Current and near-term technologies are inadequate to address these risks.

iii) **Design of Secured E-Voting System:** It is able to desire with the widespread use of computers and embedded systems. Security is the essential problem should be considered in such systems. This method proposes a new e-voting system that fulfils the security requirements of e-voting. It is based on homomorphism property and blind signature plan. The suggest system is executed on an embedded system which serves as a voting machine. The system employees RFID to store all conditions that comply with the rule of the government to check voter eligibility.

iv) **A Hybrid Biometric Based E-Voting System:** Information technology changes and gives shape to networked society all over the world today & its solutions are becoming main drivers in almost all field of human life activity. Although the acceptance rate of government applications is increasing e-voting is hardly accepted as main tool in its field because its shortages in offering good solutions to common problems like fraud, bribery, anonymous character of the vote and absence of good independent monitoring.

v) **Techniques for Feature in Speech Recognition System:** The time domain waveform of a speech signal carries all of the auditory information. From the phonological point of view, very little can be said on the basis of the waveform itself. However, past research in mathematics, acoustics, and speech technology have provided many methods for converting data that can be considered as information if interpreted correctly. In order to find some statistically relevant information from incoming data, it is important to have mechanisms for reducing the information of each segment in the audio signal into a relatively small number of parameters, or features. These features should describe each segmenting such a characteristic way that other similar segments can be grouped together by comparing their features. There are enormous interesting and exceptional ways to describe the speech signal in terms of parameters. Though, they all have their strengths and weaknesses, we have presented some of the most used methods with their importance.

vi) **Development of Ant rigging Voting System Using Biometrics Based on Andhra Card Numbering:** Nowadays' voting process is exercised by using EVM (Electronic voting machine). In this paper we present and use implementation is to execute the progress of anti-rigging voting system using finger print. The purpose of the project and implementation is to provide a safety and good environment to the customers is to electing the candidates by using the intelligent electronic voting machine by providing a rival naming to every user using the Fingerprint identification technology. It involves microcontroller and interfaces. Intelligent EVM has been particularly designed to collect, record, store, count and display cent percent accurately.

3. Proposed Work

In the proposed solution, all the activities are managed using a Block chain based mechanism. We have proposed a two-end mechanism in which all the activities are coordinated by the national and state bodies at various levels and voters play an equal part in it. The integration of Block chain mechanism and voting system may reduce the risks with transparent and decentralized feature of Block chain technology.

Poll-Site Internet Voting: According to the title above, it offers the promise of greater convenience and efficiency in that voters could cast their ballots from any poll site using their Andhra card, and the tallying process would be both fast and certain.

QR and Fingerprint Based Voter Verification System: The proposed method uses the QR code and fingerprint biometric authentication provided by the Aadhar card in India.

Andhra QR Verification: Aadhar card contains a citizen information, Aadhar number, QR code. In that, Aadhar QR code contains a valid Aadhar number. By decoding the QR code, the Aadhar number is obtained. The citizen information can be accessed by using the Aadhar number. The citizen information contains an iris data, fingerprint data, address, etc. Based on the Aadhar QR code, a virtual voting System using diary technique is developed. The AVS allows the citizen Aadhar QR code. The Aadhar number is extracted by the decoding of QR code. Extract the citizen information and fingerprint fromthe database based on the Aadhar number.

Fingerprint Biometric: In order to prevent identity theft and multiple voting, biometric technology can be used at polling stations to confirm the identity and eligibility of voters. Biometrics is the best technology to identify and authenticate individuals reliably and quickly based on their unique physical characteristics, such as fingerprints, to cite just the most well-known example.

DCNN Based Biometric Verification: The individual's biometric features are captured and compared to previously captured and confirmed biometric featuresof that individual. All biometric data is first captured by a sensor as an image. This image is then further processed into a biometric template. DCNN Algorithm used for verification and de-duplication are based on comparing these biometric templates.

Ballotchain: The recorded vote must be the same as the one the voter intended to cast.The fundamental idea of the Ballotchain solution is to match a Bitcoin transaction to a vote cast by an elector in support of the candidate selected by the voter.Every vote therefore benefits from the characteristics of a Blockchain transaction, namely: It is non-modifiable; It is non-repudiable; It cannot be registered in multiple ways; All nodes possess a valid copy.

Self-tallying: The tally must be the same as the sum of the recorded votes. Satisfying this crucial requirement without tallying authorities is the main contribution. This is because the last voter to cast a ballot is able to compute the election result before choosing his/hervote and casting the final ballot.

Endcore Counting: Artificial Intelligence applied to the electoral count using Counting Sort Decision Algorithm. It is the most vital and robust module that has been developed to run on the Election Day for counting of votes, monitoring of end-to-end process and declaration of Results by the System. The Application is designed in a way that the series of work to be done by the Returning Officer in the System will automatically be popped up one after another.

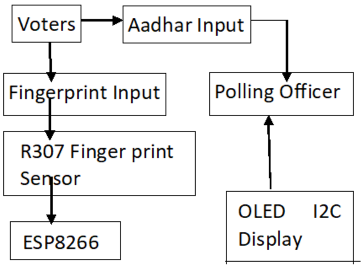


FIGURE 2.

4. Results and Discussion

In this section, the performance of our proposed e-voting system is analysed. The prevoting phase has no computation, which only distributes the numbers of the voters and candidates. Thus, we mainly analyse the computation cost of the voting phase and postvoting phase. Moreover, we also, respectively, test the total time cost for the different numbers of voters and candidates by using the 1024-bit session key and the 512-bit shared secret on a laptop.

Performance Analysis of Voting Phase: In the voting phase, the five steps are as follows: registering identification for voters, negotiating session keys among voters, generating masked values, constructing shared polynomials, and computing shares. Meanwhile, the computation cost mainly concentrates upon generating masked values and computing shares. Assume that the computation costs of one masked value and one share are separately expressed as $\text{cost}_{\text{mask}}$and $\text{cost}_{\text{share.}}$

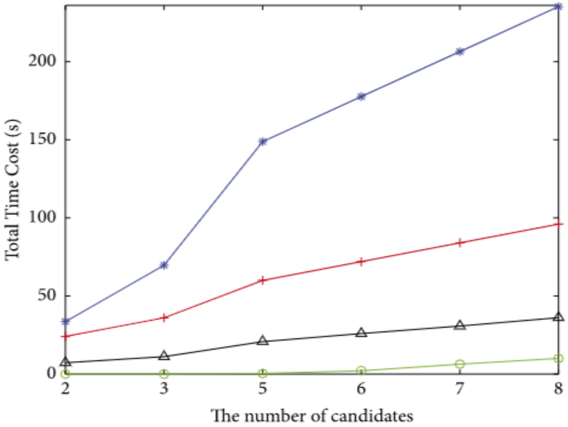


FIGURE 3. Total Time Cost Comparison of 5 Candidates

Performance Analysis of the Post voting Phase: Inpostvoting phase, VS and candidates are responsible for computing the sum of shares and then publish. Each participant reconstructs a polynomial to obtain the tallying result and then verifies it. Meanwhile, computing the sum of shares, recovering polynomial, and verifying the tallying result are the main computation cost in this phase. Assume that they are separately expressed as cost$_{mask}$, cost$_{share}$ and cost$_{verify.}$

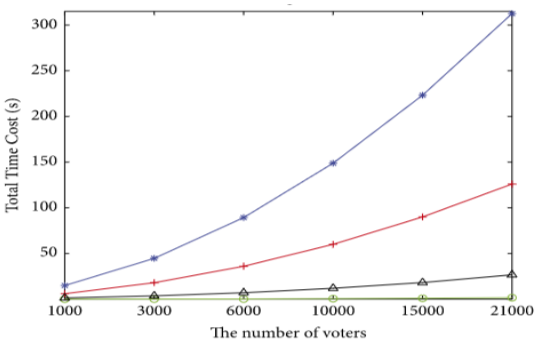


FIGURE 4. Total Time Cost Comparison of 10000 Voters

5. Conclusion

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions. In this project, we introduced a unique, blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. We have outlined the systems architecture, the design, and a security analysis of the system. By comparison to previous work, we have shown that the blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient election scheme, while increasing the security measures of the today's scheme and offer new possibilities of transparency. Using an Ballotchain private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain. For countries of greater size, some measures must be taken to withhold greater throughput of transactions per second, for example the parent & child architecture which reduces the number of transactions stored on the blockchain at a 1:100 ratio without compromising the networks security. Our election scheme allows individual voters to vote at a voting district of their choosing while guaranteeing that each individual voter's vote is counted from the correct district, which could potentially increase voter turnout.

References

1. Abuidris, Y., Hassan, A., Hadabi, A. and Elfadul, I. (2019)'Risks and opportunities of blockchain based on e-voting systems',16th International Computer Conference on Wavelet Active Media Technology and Information Processing, pp.365–368.
2. Al-Turjman, F. (2019) '5G-enabled devices and smart-spaces in social-IoT: An overview', Future Gener. Comput. Syst., vol. 92, pp.732-744.
3. Bai, S., Yang, G., Shi, J., Liu, G. and Min, Z. (2018) 'Privacy-Preserving oriented floating-point number fully homomorphic encryption scheme', Security and Communication Networks, vol. 2018, Article ID 2363928, 14 pages.

4. Cayamcela, M.E.M. and Lim, W. (2018) ‘Artificial intelligence in 5G technology: A survey’, Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC), pp.860-865.
5. Curran, K. (2018) ‘E-voting on the blockchain’, Journal of British Blockchain Association, vol. 1, no. 2, 6 pages.
6. Febriyanto, E., Triyono, Rahayu, N., Pangaribuan, K. and Sunarya, P. A. (2020) ‘Using Blockchain Data Security Management for E-Voting Systems’, 8th International Conference on Cyber and IT Service Management (CITSM), pp.1-4.
7. Ghosh, A., Gupta, S., Dua, A. and Kumar, N. (2020) ‘Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects’, Journal of Network and Computer Applications, vol. 163, Article ID 102635.
8. Gurubasavanna, M.G., Ulla Shariff, S., Mamatha, R. and Sathisha, N., (2018) ‘Multimode authentication based electronic voting kiosk using raspberry pi’, Second International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC, pp.528–535.
9. Hanifatunnisa, R. and Rahardjo, B. (2017) ‘Blockchain based e-voting recording system design’, 11th International Conference on Telecommunication Systems Services and Applications (TSSA), pp.1-6.
10. Komatineni, S. and Lingala, G. (2020) ‘Secured E-voting system using two-factor biometric authentication’, Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp.245–248.
11. Kshetri, N. and Voas, J. (2018) ‘Blockchain-enabled E-voting’, IEEE Softw., vol. 35, no. 4, pp.95-99.
12. Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M. and Guizani, S. (2017) ‘Internet-of-Things based smart cities: Recent advances and challenges’, IEEE Commun. Mag., vol. 55, no. 9, pp.16-24.
13. Monrat, A. A., Schelén, O. and Andersson, K. (2019) ‘A survey of blockchain from the perspectives of applications, challenges, and opportunities’, IEEE Access, vol. 7, pp.117134-117151.
14. Rathee, G., Iqbal, R., Waqar, O. and Bashir, A. K. (2021) ‘On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities’, IEEE Access, vol. 9, pp.34165-34176.