SECURE VOTER AUTHENTICATION FOR RELIABLE VOTING PROCESS USING RFID AND BIOMETRIC

S.Bharath,
Final Year Students
bharathsampath2001@gmail.com
S.Tharun,
Final Year Students
tharunsridhar56@gmail.com
G.Kalanandhini
Assistant Professor,
g.kalanandhini.ece@psvpec.in
Department of Electronics & Communication Engineering,
Prince Shri Venkateshwara Padmavathy Engineering College, Chennai 127

ABSTRACT

Voting machines are the entire aggregate of mechanical, electromechanical, or digital equipment (including software, firmware, and documentation required to application manipulate and assist equipment), this is used to outline ballots to solid and rely votes to document or show election effects and to preserve and convey any audit path information. The first vote casting machines had been mechanical however it's far an increasing number of not unusual place to use digital vote casting machines. Moreover, it's also vital that a fake access must now no longer be made so for this one of the maximum stable techniques for vote casting is the usage of a biometric sensor like a fingerprint reader. In this project, a Fingerprint reader is getting used for presenting get entry to to the voter in addition to creating a log if the individual has voted or now no longer.

Keywords: Voting, IoT(Internet of Things), Wireless.

I INTRODUCTION

The Internet of Things is a tool of interrelated computing devices, mechanical and digital machines, objects, animals or people which may be provided with specific identifiers and the cap potential to interchange statistics over a network without requiring human-to-human or human-to-pc interaction. RFID stands for Radio Frequency Identification. [1]This rapidly-growing technology transmits statistics wirelessly thru the use of radio waves. RFID requires using a device known as a reader. The reader is needed to retrieve any statistics stored on a RFID tag. [2]The reader device carries an antenna and a small chip to transmit statistics through the radio-frequency electromagnetic field. The reader is answerable for deciding on up identifying statistics much like the suitable serial range from package deal tags. The statistics is picked up through the antenna which emits radio signs and receives signs decrease returned from package deal tags. [3] These signs are then transmitted in digital format to the first-class pc tool. Biometric Systems are automated techniques of verifying or recognizing the identity of a dwelling man or woman on the basis of some physiological tendencies like a fingerprint or face pattern or some additives of behavior like handwriting or keystroke patterns. The above era are interfaced in this mission to decorate the security. [4]The main aim of the project is to eliminate the security compromises in the existing voting system by introducing various authentication steps (Biometric, IOT and RFID).Votes are casted by just identification and casting process which lacks security. The existing voting system does not have security features as the votes can be casted by any other and lot of excess polls is recorded. Due to this disadvantage this model is proposed. In this proposed system the voting system is improved with security features to avoid various security issues like illegal voting's. [5]The proposed system consists of various security authentications by various election officers followed by the implementation of aadhar with voters ID which is for the voter's identification and the votes are casted by the voters using their fingerprints. The voters can get a notification of their casting as an alert SMS. [6]This intimates the voters and they can crosscheck whether they have voted or not. This can be implemented and can provide safe and secure voting. In this voting system, the first module is the authentication of the election officers by an IOT webpage which increases the security of the system. Here we use adafruit.io website to create IOT webpage. Adafruit.io is a cloud service by which we can create an IOT webpage for ourselves to switch on/off the voting machine. It is open source software and can be accessed through internet. Through the webpage the election officer initiates the start of the election. The prototype provided is activated by the command from the IOT webpage which is given by the officer. [7]The command from the webpage is received by the microcontroller (Arduino UNO) and the voting process is initiated, this process is followed by the RFID authentication. The second module which is followed by the IOT authentication is the authentication by the polling officers and they are in charge of the polling booth. The polling officer in the booth ensures their identity by RFID followed by their biometric, activates the prototype after the IOT authentication by the election officer. The polling officer has three types of access in voting machine. [8]The polling officer can check the total amount of vote casted, start and stop the voting. The voter also ensures their identity by the RFID and followed by their biometric to cast their votes. After the verification of the biometric there will be list of parties displayed in the LCD and votes are casted by the voters using the Keypad and a SMS is sent to the voters.

II RELATED DOCUMENTS

Santosh Kumar Shaw et al., proposed the paper titled "**Design and Implementation of Arduino Based Voting Machine**" that turned into posted with inside the year of 2018 via way of means of IJRITCC. In this paper, they've defined a secured gadget that may dispose of controversies regarding elections in our country. In their beyond paintings they've advanced a prototype and examined efficiently an Arduino UNO primarily based totally Aadhaar facilitated digital vote casting device owning a tier fingerprint safety. [9]The essential cause of this gadget is to provide a instantly and honest election and to reduce all different elements that have an effect on it. This intention has been done via way of means of supplying twin verification of the electorate primarily based totally on their fingerprint and particular identification. In this System all of the applicable facts are taken from the electorate and are saved with inside the database, and then they're furnished with particular ID. The procedure of verification includes matching of this identification and fingerprint from the database. This is a quicker and extra secured manner of keeping elections. [10]This gadget is secured, dependable and additionally cost- effective. The downside of current vote casting gadget is loss of safety troubles and there may be excessive threat for a couple of vote casting and the gadget is slow. In proposed vote casting procedure, verification for legal voter is completed with the assist of fingerprint scanner, which insures that voter is registered voter and handiest legal electorate are allowed to go into the vote casting room. [11]This additionally assures the bodily presence of the voter. Thus, this gadget gets rid of the possibilities of a couple of vote casting additionally which makes our gadget extra secured.

Adrià Rodríguez-Pérez proposed the paper titled “**Secret Suffrage in Remote Electronic Voting Systems**” that was published in the year of 2017 by IJRITCC. In this paper, Adrià Rodríguez-Pérez have described different forms of remote electronic voting since 2000, it has become apparent that internet voting fails at providing the privacy guarantees offered by traditional paper-based voting systems. Against this assumption, the current proposal suggests reviewing the traditional configuration of the principle of vote secrecy. [12]The Proposal will assess current accepted standards on voters’ anonymity for traditional and internet-based voting systems, Evaluate the core elements of lawful relaxations to the principle of secret suffrage, and especially those traditionally associated to different forms of remote voting, and assess whether they can be applied to internet voting and study how current technical developments in the field of elections may result in further relaxations of the principle of secret suffrage in the future. [13]Overall, the goal of the proposal is to approach the principle of secret suffrage against the specificities of internet voting and, instead of evaluating electronic voting systems using traditional standards for voters’ privacy and anonymity, evaluate how specific proposals aimed at ensuring voters' secrecy in internet voting comply with the very end that the principle of secret suffrage is aimed at protecting voting process.

Kashif Mehboob Khan et al., proposed the paper titled “**Secure Digital Voting System primarily based totally on Block chain Technology**” that turned into posted with inside the 12 months of 2019 via way of means of UWL in UK. Electronic vote casting or e-vote casting has been utilized in various bureaucracies due to the fact that Nineteen Seventies with essential advantages over paper primarily based totally structures inclusive of multiplied performance and decreased errors. [14] However, there stay demanding situations to attain huge unfold adoption of such structures in particular with admire to enhancing their resilience in opposition to ability faults. [15]Block chain is a disruptive era of present day generation and guarantees to enhance the general resilience of e-vote casting structures. This paper provides an attempt to leverage advantages of block chain inclusive of cryptographic foundations and transparency to attain an powerful scheme for e-vote casting. The proposed scheme conforms to the essential necessities for e-vote casting schemes and achieves quit-to-quit verifiability. [16]The paper provides information of the proposed e-vote casting scheme in conjunction with its implementation the usage of Multi chain platform. The paper provides in-intensity assessment of the scheme which correctly demonstrates its effectiveness to attain a quit-to-quit verifiable e-vote casting scheme. The number one goal of assessment turned into to evaluate the overall performance of the machine in view of the e-vote casting machine necessities provided and to discover any issues with reference to its software in an actual international scenario. [17-24]The experimentation consisted of a couple of steps i.e. carrying out a couple of transactions, verification of transactions, mining transactions into block chain, mirrored image of the modifications made with inside the public ledger to all of the nodes with inside the community and the usability of the machine.

III PROPOSED SYSTEM

In this proposed system, the voting system is improved with security features to avoid various security issues like illegal voting’s. The proposed system consists of various security authentications by various election officers followed by the implementation of aadhar with voters ID which is for the voter’s identification and the votes are casted by the voters using their fingerprints. The voters can get a notification of their casting as an alert SMS. This intimates the voters and they can crosscheck whether they have voted or not. This can be implemented and can provide safe and secure voting.

Figure 1 shows the block diagram of IoT. The first module is the authentication of the election officers by an IOT webpage which increases the security of the system. Through the webpage the election officer initiates the start of the election. The prototype provided is activated by the command from the IOT webpage which is given by the officer. The command from the webpage is received by the microcontroller (Arduino MEGA) and the voting process is initiated, this process is followed by the RFID authentication.

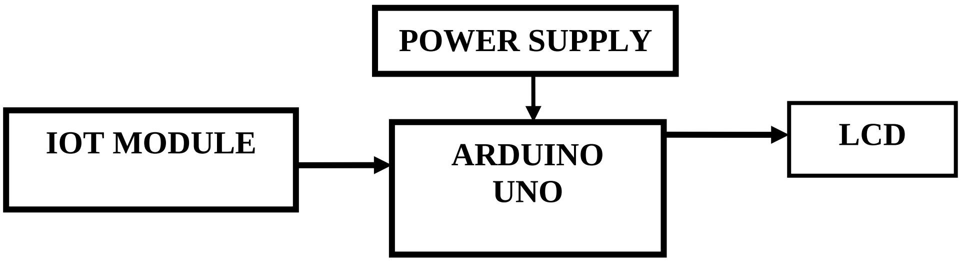


Figure 1: Block Diagram of IoT

The second module which is followed by the IoT authentication is the authentication by the polling officers who are incharge of the polling booth. The polling officers with their RFID tag ensures their identity and they are asked for their biometic for security reasons. The voter ID which is linked with the aadhar is a RFID tag by which the voters can ensure their identification in the polling booths. In figure 2 block diagram of RFID reader and tag is shown. The LCD attached shows the process of the model.

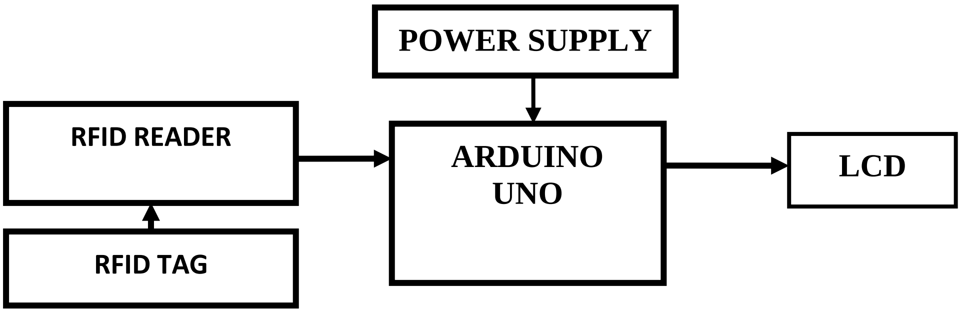


Figure 2: Block diagram of RFID Reader and Tag

The biometric authentication is one of the feature where the security is enhanched.The figure 3 shows block diagram of fingerprint sensor. The polling officer in the booth ensures their identity by RFID followed by their biometric when again activates the prototype after the IOT authentication by the election officer. The voters also ensures their identity by the RFID and followed by their biometric to cast their votes.

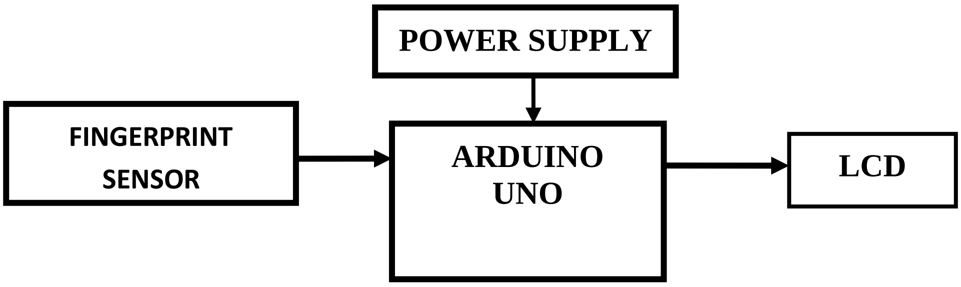


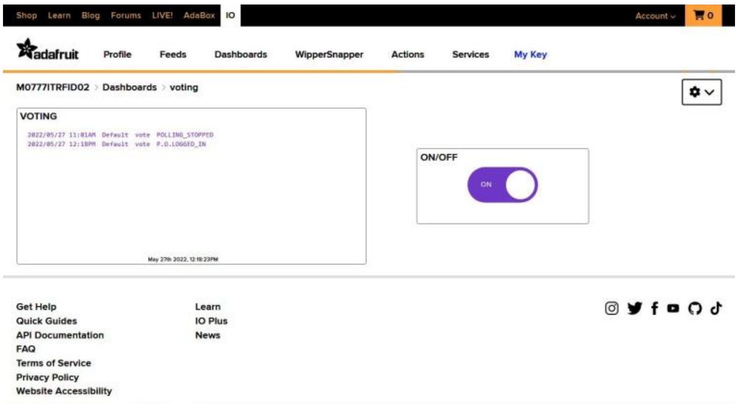
Figure 3: Block diagram of fingerprint sensor

After the verification of the biometric and votes are casted by the voters using the Keypad and a SMS is sent to the voters. All these process are displayed in the LCD.

IV RESULTS AND DISCUSSION

As per the proposed solution, the security of voting system is divided into 3 levels. The first level of security is given in IOT to switch on the voting process. The second level of security is given by the Polling booth officer, who can start, stop, and check the vote count by verifying their identity with RFID Tag and Biometric. The third level of security is given to the voters, they have to verify their identity with RFID Tag and Biometric then they can caste for their favourite parties.

FIRST LEVEL SECURITY



M0777ITRFID02 › Dashboards › voting

VOTING

```
2022/05/27 11:01AM  Default  vote  POLLING_STOPPED
2022/05/27 12:18PM  Default  vote  P.O.LOGGED_IN
```

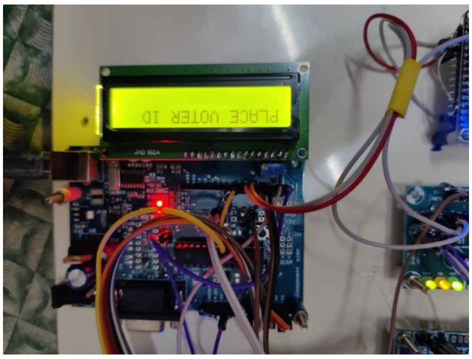
May 27th 2022, 12:18:23PM

ON/OFF

Figure 4: IOT webpage

The figure 4 shows the IOT webpage, in that we switch ON/OFF and monitor the Voting process.

SECOND LEVEL SECURITY



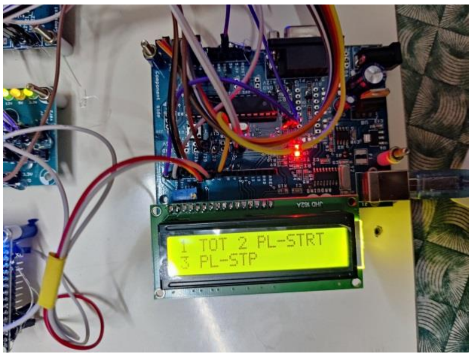


Figure 5: Main page

Figure 6: Polling officer access

The figure 6 shows three options for polling booth officer. They are

1. TOT- To check the vote count

2. PL-STRT- To start the voting process

3. PL-STP- To stop the voting process

THIRD LEVEL SECURITY

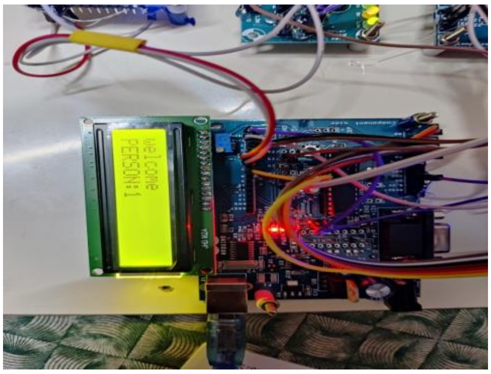


Figure 7: After RFID verification of Person 1

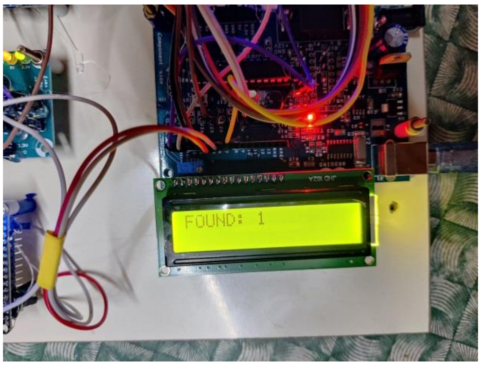


Figure 8: After Fingerprint Verification

Figure 4 shows the PERSON: 1 RFID Tag is tapped. After verifying Biometric of that person FOUND: 1 text is shown and list of parties is shown in figure 9.

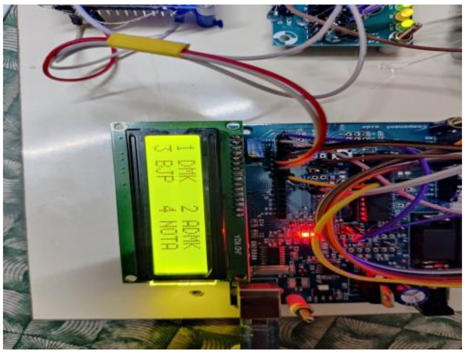


Figure 9: List of parties

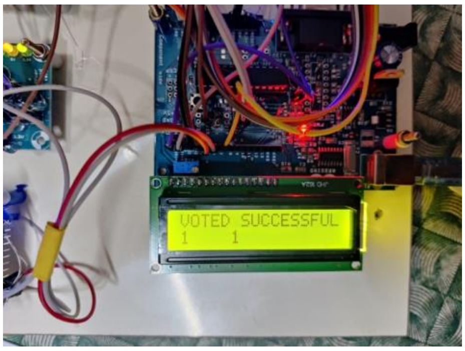
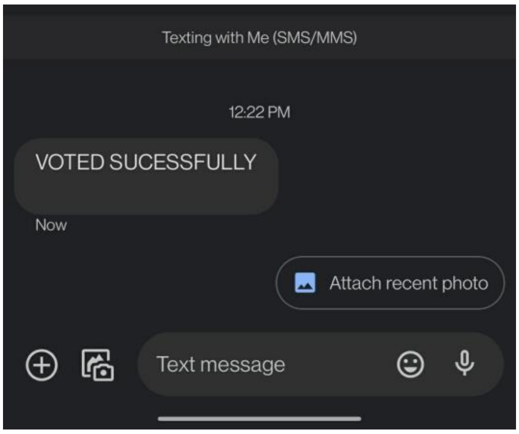


Figure 10: After voting

After selecting any parties VOTED SUCESSFUL is shown in figure 10 and same is updated in IoT page and also a confirmation message is sent to the Voter's mobile number which is shown in figure 11.



Texting with Me (SMS/MMS)

12:22 PM

VOTED SUCESSFULLY

Now

Figure 11: SMS received in voter's mobile number

V CONCLUSION

The main outcome of this project is to improve the security in the voting system. The security improvement is attained by the various authentication processes and finally polling by the biometric of the voters. As said the votes of the individual can only be casted by them and it can't be illegally casted by others as the biometric plays a vital role. The election officer and the polling officer are given separate authentication to start the polling process. By all the above processes the security has been increased in the voting system.

REFERENCES

1. Abbas Behrainwala., et.al (2022) "Smart Voting System Using Facial Recognition" published in International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC V

2. G. K. Kamalam, Shubham Joshi, Manish Maheshwari, K. Senthamil Selvan, Sajjad Shaukat Jamal, S. Vairaprakash, Musah Alhassan, "Augmented Reality-Centered Position Navigation for Wearable Devices with Machine Learning Techniques", Journal of Healthcare Engineering, vol. 2022, https://doi.org/10.1155/2022/1083978

3. Abadianto.D., et.al (2017) "Design of face detection and recognition system for smart home security application" in 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE) IEEE.

4. Alguliyev.R., et.al (2019) "Multi-criteria Evaluation+ Positional Ranking Approach for Candidate Selection in E-voting," Decision Making: Applications in Management and Engineering, vol. 2, no. 2, pp. 65–80, 2019.

5. Subburam, S., Selvakumar, S. & Geetha, S. High performance reversible data hiding scheme through multilevel histogram modification in lifting integer wavelet transform. *Multimed Tools Appl* **77,** 7071–7095 (2018). https://doi.org/10.1007/s11042-017-4622-0

6. Rajesh, G., Mercilin Raajini, X., Ashoka Rajan, R., Gokuldhev, M., Swetha, C. (2020). A Multi-objective Routing Optimization Using Swarm Intelligence in IoT Networks. In: Peng, SL., Son, L.H., Suseendran, G., Balaganesh, D. (eds) Intelligent Computing and Innovation on Data Science. Lecture Notes in Networks and Systems, vol 118. Springer, Singapore. https://doi.org/10.1007/978-981-15-3284-9_65
7. Kathiresan, S., & Mohan, B. (2020). Multi-Objective Optimization of Magneto Rheological Abrasive Flow Nano Finishing Process on AISI Stainless Steel 316L. Journal of Nano Research, 63, 98–111. https://doi.org/10.4028/www.scientific.net/jnanor.63.98

8. G. Indira, A. S. Valarmathy, P. Chandrakala, S. Hemalatha, and G. Kalapriyadarshini , "Development of an efficient inverter for self powered sand sieving machine", AIP Conference Proceedings 2393, 020144 (2022) https://doi.org/10.1063/5.0074347

9. AdiputraC.K., et.al (2018) "A proposal of block chain-based electronic voting system," in Proceedings of the 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), pp. 22–27, IEEE, London, UK, October 2018.

10. Ahmed Ali., et.al (2020) “Fpga Based Real-Time Face Authorization System For Electronic Voting System” published in 3rd International Conference on Computing, Mathematics and Engineering Technologies (ICOMET).

11. Bhaskar., et.al (2021) "An Advanced Approach for Link-Based Spam Detection Using Machine Learning." Proceedings of the Second International Conference on Information Management and Machine Intelligence. Springer, Singapore.

12. Senthilkumar, K.K., Kunaraj, K. & Seshasayanan, R. “Implementation of computation-reduced DCT using a novel method. J Image Video Proc. 2015, 34 (2015). https://doi.org/10.1186/s13640-015-0088-z

13. Senthilkumar, K.K., Kumarasamy, K. & Dhandapani, V. Approximate Multipliers Using Bio-Inspired Algorithm. J. Electr. Eng. Technol. 16, 559–568 (2021). https://doi.org/10.1007/s42835-020-00564-w

14. V. S. Harshini and K. K. S. Kumar, "Design of Hybrid Sorting Unit," *2019 International Conference on Smart Structures and Systems (ICSSS)*, 2019, pp. 1-6, doi: 10.1109/ICSSS.2019.8882866

15. A.R. Aravind, K. K. Senthilkumar, G. Vijayalakshmi, J. Gayathri, and G. Kalanandhini , "Study on modified booth recoder with fused add-multiply operator", AIP Conference Proceedings 2393, 020139 (2022) https://doi.org/10.1063/5.0074212

16. G. Vijayalakshmi, J. Gayathri, K. K. Senthilkumar, G. Kalanandhini, and A. R. Aravind , "A smart rail track inspection system", AIP Conference Proceedings 2393, 020122 (2022) https://doi.ohrg/10.1063/5.0074206

17. G. Kalanandhini, A. R. Aravind, G. Vijayalakshmi, J. Gayathri, and K. K. Senthilkumar , "Bluetooth technology on IoT using the architecture of Piconet and Scatternet", AIP Conference Proceedings 2393, 020121 (2022) https://doi.org/10.1063/5.0074188

18. K. K. Senthilkumar, G. Kalanandhini, A. R. Aravind, G. Vijayalakshmi, and J. Gayathri , "Image fusion based on DTDWT to improve segmentation accuracy in tumour detection", AIP Conference Proceedings 2393, 020120 (2022) https://doi.org/10.1063/5.0074183

19. J. Gayathri, K. K. Senthilkumar, G. Vijayalakshmi, A. R. Aravind, and G. Kalanandhini , "Multi-purpose unmanned aerial vehicle for temperature sensing and carbon monoxide gas detection with live aerial video feeding", AIP Conference Proceedings 2393, 020124 (2022) https://doi.org/10.1063/5.0074193

20. CorryP.Mc., et.al (2017) “A smart contract for boardroom voting with maximum voter privacy,” in Proceedings of the International Conference on Financial Cryptography and Data Security, pp. 357–375, Springer, Sli- ema, Malta, January 2017.

21. Deepika Iswarya., et.al (2016) "A Survey on E-Voting System Using Arduino Software", International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization), vol. 5, no. 2, pp. 687-690, February 2016.

22. Girish Tere., et.al (2016) "An analysis of electronic voting machines for their effectiveness." International Journal of Computing Experiments (IJCE) Vol 1 (2016): 8-12.

23. T Sunder Selwyn, S Hemalatha, Condition monitoring and vibration analysis of asynchronous generator of the wind turbine at high uncertain windy regions in India, Materials Today: Proceedings, Vol. 46, pp3639-3643, 2021.

24. T Sunder Selwyn, S Hemalatha, Experimental analysis of mechanical vibration in 225 kW wind turbine gear box Materials Today: Proceedings, Vol. 46, pp 3292-3296, 2021.