

QR BASED AADHAR ELECTRONIC VOTING SYSTEM WITH BLOCK CHAIN TECHNOLOGY USING INTERNET OF THINGS

K KAUSALYA, ANUSHA J R, GOKULADHARSHINI B, SUBHASHINI D
Easwari Engineering College, Department of Information Technology, Chennai, India
Easwari Engineering College, Department of Information Technology, Chennai, India
Easwari Engineering College, Department of Information Technology, Chennai, India
Easwari Engineering College Department of Information Technology Chennai, India

Abstract—*This system allows people to vote electronically in public elections with security system using Block chain technology. Progressively the application of scientific knowledge for the practical purpose within the idea helps many folks live. This methodology set out an Associate in legal organization for native election on blockchain knowledge dealing with applied sciences and Aadhar affirmation. The fact of being free from threat and dispositive may be a danger from extensive election with this prevailing methodology. A number of issues that may persist within the prevailing methodology are with a corporation, that has management over the information. It can be done to meddle with the information for a good time. The projected methodology is principally designed for our native supported Aadhar affirmation. To make sure a lot of security, fingerprint of elector is employed. A Single system will act as registering module and voting module. The system will act as registering module on activating switch by the super admin. For registering module, the QR code of Aadhar is scanned (which is brought by the use) followed by the fingerprint verification. The system permits the elector to vote through his fingerprint when they 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.*

Keywords—*Aadhar, Block chain, Fingerprint, Database, qr*

1. INTRODUCTION

The scientific knowledge which has been used for a practical purpose has become a daily routine at this time for fulfilling our needs. It has given a new obstacles within the method of practical principles of social equality as a general. public nowadays has no belief on their administration, creating election momentous in a very trendy social equality society. The election in current active needs a physical enrollment with a citizen identity. The citizen will initiate the formal decision of a choice only if they supply the citizen identity. The foremost downside of choosing formal decision is counterfeit poll. To overcome the difficulties our proposed system tends to use the several methods of approving unique standards. For each government process of performing it needs the identity card supplied with identification that gives no doubt that the citizen has all the rights to execute the specified activity. The projected information makes less the complete authorization within the small temporary tent and conjointly makes less the person employed in the investigation method. All the activity executed is automatic. These problematic area units are resolved by the Block chain. Block chain branch of dealing applied science is one answer that may be used to cut back the issues that persist in vote. In each democracy, the safety of an associate degree election may be a matter of national security. The main objective of this proposed system is that in public elections this would allow people to vote electronically with security aspect using Block chain technology.

A block chain may be a given a share of, unchanged over time, not able to denied, general record of important matters. This important technology enables into four important distinctive attribute:

(i) The collection of financial transaction in several alternative places: Not one of several extremity of incompetent within the continuation of the dispense collection of transaction.

(ii) The dispense management over who will attach the important dealings of the significant matter.

(iii) Any planned “new block” to the collections of the significant matters should refer the previous edition of the collection of the significant matters, making associate in the unchanged series of the linked material.

(iv) The internet should enlarge an agreement, before a new block adapts an important collections.

These applications of scientific knowledge options control the functions of move forward encryption, on condition that a level equals any previous familiar information.

2. LITERATURE SURVEY

Not long ago the application of statistical analysis to biological data has gained the importance of several persons who carried out academic research. During this subdivision, the associated exertion on a device with microchips with scientific analysis of biological data is talked about concisely. In a learning [S.M.Hasan et al.]2017, a representation of the device with microchips was talked about concisely where citizen affirmation was executed using identity module verification. In this series of action that took place, numerous pollings were cramped by an aspect of performance in this card after the citizen has stopped his ballot at phase. Using diverse scientific analysis of biological data in voting and their state of being free from danger were examined in another research led by Hof [S.Hof]2016.

He discussed a number of the self-indulgent liking for scientific analysis methodology such as the trick played by something, not true take on and dismisses quantity etc and so, connected to controversial scientific analysis vote with contraception. In a learning [D.A.Kumar et al.]2016, a metaphysical representation of electoral methodology with impression or mark substantiation and particular go with activity in impression specifics were established.

A learning management by Sarkar et al. lay out a short duration rundown on prevailing voting methodology and their frame work and dispute. They substantiated the prevailing expansion of methodology in state of affairs and proposed some plan of action to make better safety, exactness of the prevailing blueprint.

In yet curious learning, Sarkar et al. put forward a architecture of components such as microchip ballot with an impression that assisted to remove illegal of the non-automatic ballot methodology and foregoing renders of components of microchip balloting. They used 3 sheet criss-cross methodologies with 2 solicitation computer that responds and receipts to eject specifics from the user to stored resource.

In, Chakraborty et al. established a scientific analysis of ballot organization with impression conceding in the state of affairs. In their conceived representation, user’s statistics was retained in identity structured set of data was retrieved from this piece during ballot procedure. Piece of information comprises scientific analysis of particulars such as impression and aperture of every native. Some alternative of two schooling [N.S.Tilwani et al.]2017--[R.M.Prasad et a.]2016 a relating or based on composition to relatedness with a ballot arrangement was put forward.

A learning initiated by Khasawneh et al. put forward a thought of a multifaced computer connected through network methodology with joined or merged scientific analysis of biological data substantiated like impression, aperture foreseeing etc. In this build, vote printed form with several extent was injected and hardware imitation of the situation were moved at high speed to verify the precision .

In subsist system use of EVM were clearly substantiated and explained but the process of vote count was at its threat. Our system overcomes the problematic situation with the help of Block chain to increase the security and prevent vote theft.

3. PROPOSED SYSTEM

a. Overview

Initially, the election commission board set under registration process in server. In Under registration process, the new voter can register the ID for voting. In voting process, when election commission selects the voting progress in server. This is the time voter can poll their vote. Once the election commission deselected, the voting progress gets closed in server. The e-voting machine assigned as voting closed at this time voter cannot able to poll their vote. Finally, the election commission selects the Result announcement option in the server, at this time election commission will start to count the vote automatically and announce the result.

The proposed system is used for dual purposes:

- (I) Enrollment
- (II) Polling

In server application, our proposed system built four methods to improve the voting performance and reduce the manual process and man power. The four methods are:

1. Under registration
2. voting progress
3. Voting closed
4. The Result announcement

Given diagram (fig 1) describes the overall flow of the system and contains major components.

1. Overall Architecture Diagram

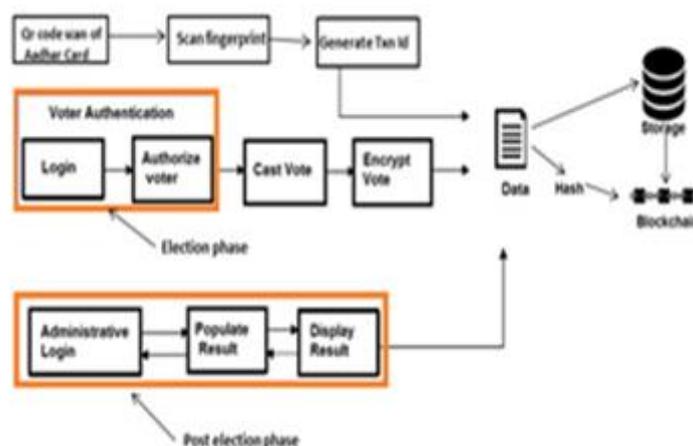


Fig 1: System Architecture Diagram

b. Workflow

i) Enrollment tier

- Super admin clicks the registration option provided on the screen.
- User enters the work space with his Aadhar card and the following steps are performed as shown in the figure (fig 2)
 - QR code is scanned from the card
 - Verification of fingerprint
 - Personal Details of the user displayed including the age of person
 - If age is above 18, request for voter ID is displayed on the screen
 - Transaction Number is sent to upthe mobile number requesting for voter ID.

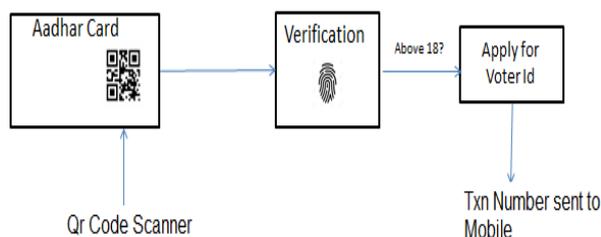


Fig 2: Registration Module Flow Diagram

ii) Polling tier

The activity point to supply a better state of being free from threat or danger in balloting the heavy instrument that get better of the counterfeit referendum. The components with microchips mechanical device is approached by corresponding in pattern the information with the identity info. To cut back the person authority and runoff utilization our proposed system tend to introduce block chain that produces a block for each vote and every vote is interlinked to every alternative.

- **Requesting to vote:** The user has to go the voter booth with his/her Transaction number, which is used for verification of the citizen. In this case, the user enters Txn number and the next step of verification flows inwards as shown in the figure (fig 3). The next step is biometric for verification. This may so eliminate the trail for fake vote, issues in uncertain credentials, use of fake identities, multiple times by the same person for voting at more than one center.
- **Casting a vote:** Voters can need to opt to either vote for one among the candidates or solid a vote. It ensures that the electoral fraud won't happen and therefore the transparency is going to be achieved. While casting, the system ensures that the person is not voted however. If the person has already voted, then the message is going to be displayed because the person is already voted. As an alternative, the person is going to be allowed to vote for his or her desired candidate.

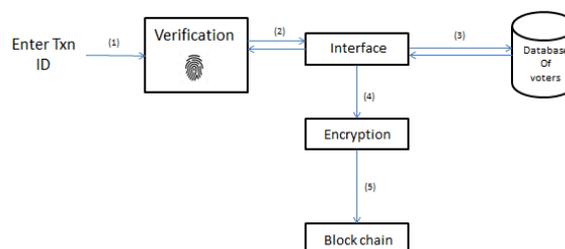


Fig 3: Voting Module Flow Diagram

- **Encrypting votes:** Once an individual vote, a block is instantiated and in real time hash code is calculated for the corresponding block, hash of the current vote in addition because the hash of the previous block are going to be hold on. This fashion every input is going to be unique and make sure that the encrypted outputs are going to be unique in addition. Block header records all the encrypted data of every vote solid. SHA-256 encrypts all the knowledge associated with each vote, and it's inconceivable to search out the encrypted hash function.
- **Adding the vote to the Block chain:** During this step, once an individual completed his vote, his/her vote will be incremented/add to the block chain as shown in the figure (fig 4). Every block gets linked to antecedently solid vote. Such a vote cannot be changed. If one block gets changed or tampered the additional blocks from the tampered block will be modified. Hence change of state is not possible in the block chain.

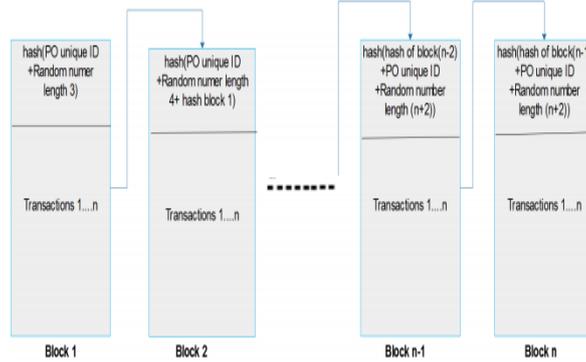


Fig 4: Blockchain network

Each vote is added into each block encrypted by 256-bit SHA hash codes as shown in the figure (fig5), the hashed block cannot be tampered by any individual as more security is added to the system. Information within the block chain is placed up in an organized manner and hold on in blocks. Each block has.:

1. The set of changes
2. Information created
3. A time stamp of the block
4. An allude to the block

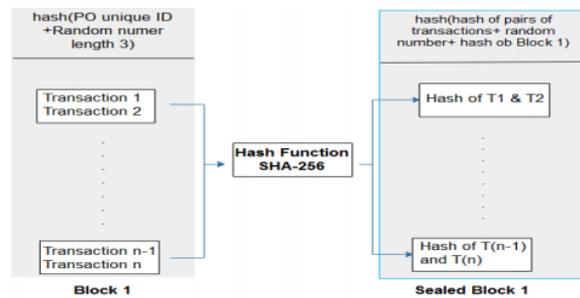


Fig 5: Ethereum stack exchange

The third purpose, each block contains an allude to the preceding block, that is that the main feature of Block chain. This reference helps to attach and build relations between each block. Block chain is the solution to solve the issues that occur within the choice system.

id	Candidate Name	Voting Card_No	Party Name	Voting
1	jitu	23149879	BJP	<input checked="" type="checkbox"/>
2	om	231654	NCP	<input checked="" type="checkbox"/>
3	abc	WWA1520123	BJP	<input checked="" type="checkbox"/>

Fig 3.6: Result

5. EXPERIMENTAL RESULTS

A) Setup

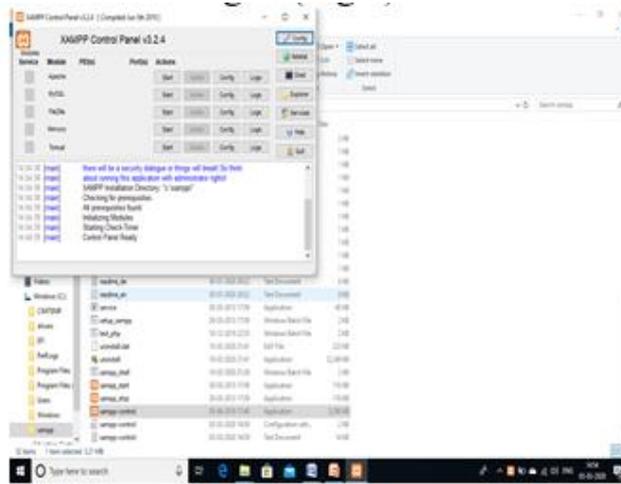


Fig 6: starting server

This figure(fig 6) shows how to start a server. Server is created in the XAMPP control panel.

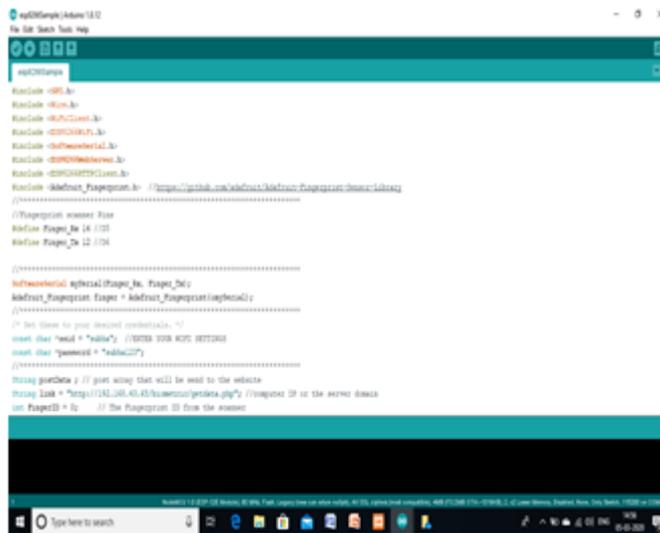


Fig 7: Opening esp8266sample

This figure (fig 7) shows how to open esp8266sample in Arduino 1.8.12 to generate Fingerprint.

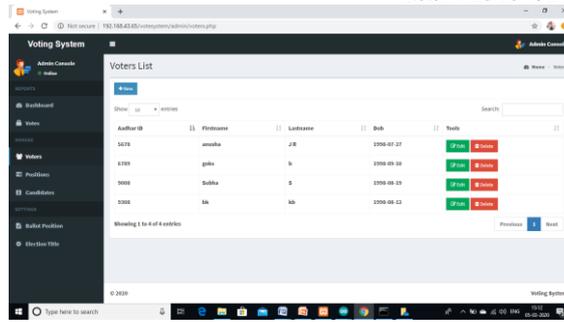


Fig 12: Voters List

This figure (fig 12) shows the number of candidates who registered their fingerprint and Aadhar card details.

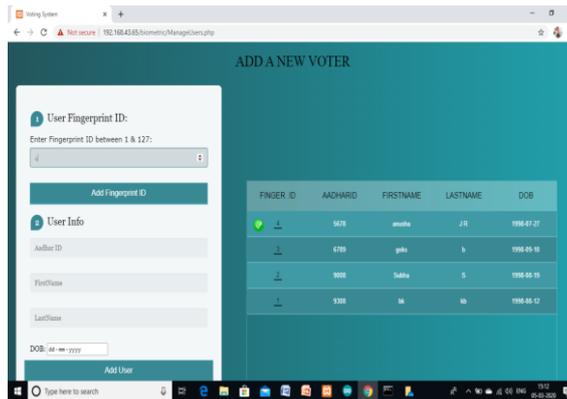


Fig 13 :Adding Fingerprint

This figure (fig 13) shows the details to be filled by the candidates for Registration.

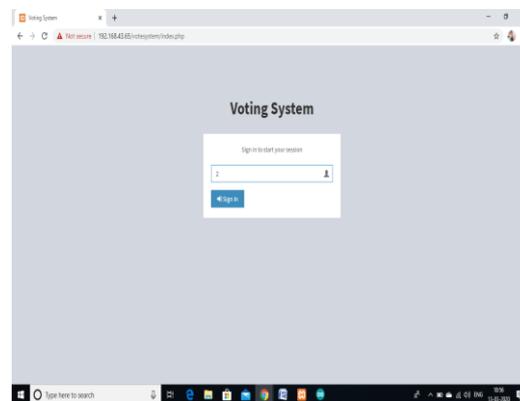


Fig 14 voter's login page

This figure (fig 14) shows the login page for the voting candidates to vote.

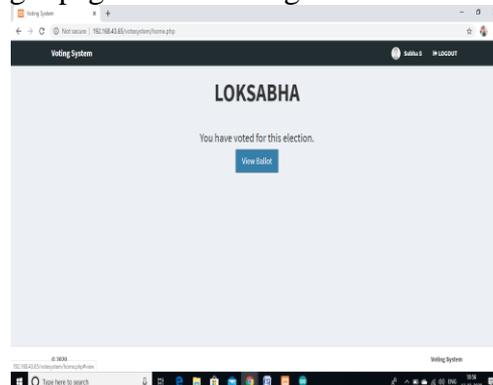


Fig 15: submission page

This figure (fig 15) shows that the voter has been successfully voted for their favourite candidates.

B) Hashing Algorithm

A hashing algorithm is a function which is mathematically used for converting string of characters into a fixed numerical value. It also creates a hash value from a set of strings. A hashing algorithm may create the same hash value with a different set of character data. This in turn causes collision among two sets of data having the same hash key.

Input: a set N Of the user in the network

Input: a block chain called B, is the last block on the block chain

Input: T, the deadline of voting

Step1: While Current Time less than T

Step2: Process the value of each N

Step3: Perform the Vote process

Step4: For each vote, count the candidate ID

Step5: Add vote to particular ID

Step6: Select Miner process (for loop that searches through blocks) for each ID

Step7: Add the block for each vote

C) Performance Measure

Table1: Results based on the proposed system

Network Size[nodes]	Block Period[s]	Runtime [s]	Throughput [tp]
1	3.8	26.9	37.2
2	2.3	15.8	63.5
3	1.6	11.3	88.7

Thus (Table1)and (Table 2) gives the accuracy result on verifying the finger print of each user at the time of voting. The module is generated on the idea of finger print scanner which provides Accurate results.

Table2: Comparison of the existing system with Proposed System related to Security Aspect

S.no	Paper ballot	Open Ballot	Secret ballot	Block chain
1	14%	12%	18%	56%

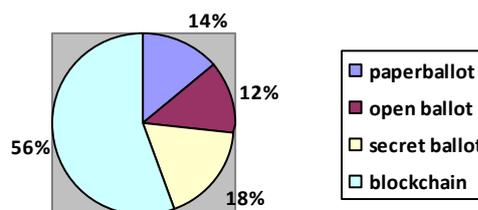


Fig 16: Comparison of the existing system with Proposed System related to Security Aspect

The result analysis is based on the comparison of the existing system with proposed system related to the security. Thus the figure (fig 16) shows the graphical representation of the existing system compared to proposed system where block chain is the only source for the security aspect.

6. CONCLUSION

Thus this system is a perfect solution to the current problem present in the voting process. The electronic voting, however has emerged as an alternative, but still not being practiced at a large scale. Most of the security has been added compared to the usual e-voting machine by adding the fingerprint feature and Block chain security so that there cannot be any kind of cheating. This system not only allows voter to vote but it also provides the registration button, where people who turned 18 can register for the voting process. This system will be more secure, faster and economical, by which the common people will elect their right representative in a secured way.

7. REFERENCES

- [1] X. Yang, X. Yi, S. Nepal, A. Kelarev and F. Han, "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption," in *IEEE Access*, vol. 6, pp. 20506-20519, 2018.
- [2] M. Kumar, S. Chand and C. P. Katti, "A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature," in *IEEE Systems Journal*, vol. 14, no. 2, pp. 2032-2041, June 2020.
- [3] AMNA qureshi ,David meglis,Helena Rifa-pous " seVEP: Secure and Verifiable Electronic Polling System "(Feb 22,2019).
- [4] Soma bhattacharrya,Dibyangana Roy,Esha Pramanik,Trishit Nath " Wireless Voting Machine "(2019)
- [5] N. S. Tilwani, N. Majumdar, and P. Bhargava, " Fair election system in india using uid data and biometric technolog " *International Journal of Scientific Engineering Research*, vol. 4,(2017).
- [6] Ashok Kumar D., Ummal Sariba Begum T., " " A Novel design of Electronic Voting System Using Finger print" " , *International Journal of Innovative Technology & Creative Engineering* (ISSN:2045-8711), Vol.1, No.1. pp: 12 19,(January 2011).
- [7] S. M. Hasan, A. M. Anis, H. Rahman, J. S. Alam, S. I. Nabil, and M. K. Rhaman, " Development of electronic voting machine with the inclusion of near field communication id cards and biometric fingerprint identifier " in *Computer and Information Technology (ICCIT)*, 2017 17th International Conference on. IEEE, (2017), pp. 383–387
- [8] S. Hof, "E-voting and biometric systems" *Electronic Voting in Europe Technology, Law, Politics and Society*, (2016)
- [9] Raja, S. Kanaga Suba, and T. Jebarajan. "Reliable and secured data transmission in wireless body area networks (WBAN)." *European Journal of Scientific Research* 82, no. 2 (2012): 173-184.
- [10] R. M. Prasad, P. Bojja, and M. Nakirekanti, " Aadhar based electronic voting machine using arduino " *International Journal of Computer Applications* (0975–8887) Volume (July 2016).
- [11] K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-4.
- [12] A. Pandey, M. Bhasi and K. Chandrasekaran, "VoteChain: A Blockchain Based E-Voting System," 2019 Global Conference for Advancement in Technology (GCAT), BANGALURU, India, 2019, pp. 1-4.
- [13] S. B, R. T. V, N. Krishna M P, B. R. J, S. Arvinth M and D. M. Alagappan, "Secured Electronic Voting System Using the Concepts of Blockchain," 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2019, pp. 0675-0681.
- [14] K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri and S. Gupta, "A Comparative Analysis on E-Voting System Using Blockchain," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-4.

- [15] S. Shukla, A. N. Thasmiya, D. O. Shashank and H. R. Mamatha, "Online Voting Application Using Ethereum Blockchain," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, 2018, pp. 873-880.
- [16] R. T M and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp. 71-75.
- [17] A. Singh and K. Chatterjee, "SecEVS : Secure Electronic Voting System Using Blockchain Technology," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, Uttar Pradesh, India, 2018, pp. 863-867.
- [18] A. Alam, S. M. Zia Ur Rashid, M. Abdus Salam and A. Islam, "Towards Blockchain-Based E-voting System," 2018 International Conference on Innovations in Science, Engineering and Technology (ICISSET), Chittagong, Bangladesh, 2018, pp. 351-354.
- [19] R. Rezwana, H. Ahmed, M. R. N. Biplob, S. M. Shuvo and M. A. Rahman, "Biometrically secured electronic voting machine," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, 2017, pp. 510-512.
- [20] J. Deepika, S. Kalaiselvi, S. Mahalakshmi and S. A. Shifani, "Smart electronic voting system based on biometric identification-survey," 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM), Chennai, 2017, pp. 939-942.