International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Maintaining Security of Electronic Voting Data through Blockchains

Rohan Anil Patange, Sagar Rajkumar Rakshe, Vishal Maruti Jadhav, Prof. S. P. Jadhav

Computer Department, PVPIT, Pune, Maharashtra, India

ABSTRACT

Choosing a representative through the process of an election is one of the most important functions in a democracy. The Election Commission is responsible for all the proceedings of transparent and fair elections. The votes are cast through physical means with the help of a ballot. The voters in each constituency have several polling booths designed for this purpose. The physical casting and counting of votes through the ballot procedures is a lengthy task that uses a lot of resources and harms the environment. Therefore, the need for an efficient E-voting platform is the need of the hour which would also fulfill the capabilities for the Digital India campaign successfully. The migration to an E-voting paradigm must overcome the obstacle of security. The Blockchain is a perfect addition to this platform as it is one of the most secure and tamper-proof algorithms along with the AES or Advanced Encryption Standard that can guarantee the security of the citizen's votes. The security attained through Blockchain is also evaluated extensively through experimentation to achieve exceptional results dwarfing the conventional approaches.

KEYWORDS: *E-Voting, Blockchain, Hash Keys, Data Privacy, AES*

How to cite this paper: Rohan Anil Patange | Sagar Rajkumar Rakshe | Vishal Maruti Jadhav | Prof. S. P. Jadhav "Maintaining Security of Electronic voting data through Block-chains" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-4, June 2020, pp.245-250, URL: www.ijtsrd.com/papers/ijtsrd30931.pdf

IJTSRD30931

I. INTRODUCTION

Jeanne Kirkpatrick, scholar and former U.S. ambassador to the UN, has offered this definition: "Democratic elections don't seem to be simply symbolic. They are competitive, periodic, inclusive, definitive elections during which the chief decision-makers form a government area unit consisting of elite persons which are led by the voters. United Nations agency declares broad freedom to criticize the government, to publish their criticism, and to offer alternatives.

What do Kirkpatrick's criteria mean? Democratic elections are competitive. Opposition parties and candidates ought to relish the freedom of speech, assembly, and movement necessary to voice their criticisms of the govt openly and to bring numerous policies and candidates to the voters. The party in power might relish the benefits of incumbency. However, the foundations and conduction of the election contest should be honest.

Democratic elections are periodic. Democracies don't elect dictators or presidents-for-life. The electoral officer's team is accountable to the people, which they ought to return to the voters at prescribed intervals to hunt their mandate to continue in the geographic point. This means that officers in a very democracy ought to accept the danger of being voted out of geographic point or constituency. The one exception the judges in the UN agency, to insulate them against common pressure and facilitate a guarantee in their disposition, is additionally appointed forever and remove only for serious improprieties.

Democratic elections are comprehensive. The definition of subject and citizen should be massive enough to incorporate an outsized proportion of the adult population. A government chosen by a tiny low, exclusive cluster isn't a democracy--no matter how the election is conducted, however democratic its internal workings could seem. One in all the nice dramas of democracy throughout history has been the struggle of excluded groups--whether racial, ethnic, or spiritual minorities, or women, and with it the right to vote and hold the workplace. Within the U. S. For example, only white male property holders enjoyed the proper right to elect and be elective once the Constitution was signed in 1787.

The property qualification disappeared by the first nineteenth century, and ladies won the correct to pick out 1920. Black Americans, however, didn't fancy full choice rights within the southern u. s. till the civil rights movement of the Sixties. And at last, in 1971, younger voters got the right to vote once the U.S. reduce the age from twenty-one to eighteen.

Democratic election's area unit is definitive. They confirm the leadership of the government Subject to the laws and constitution of the country, popularly no appointive representatives hold the reins of power. They're not merely figureheads or symbolic leaders.

Finally, democratic elections aren't restricted to choosing candidates. Voters may be asked to make a decision policy problem directly through referendums and initiatives that constituency unit placed on the ballot. Within the U.S. for instance, state legislatures will attempt to "refer," or place, a difficulty directly before the voters. Within the case of the associate initiative, voters themselves will gather a prescribed variety of signatures (usually a proportion of the number of registered voters therein state) and need that difficulty to be placed on consequent ballot--even over the objections of the state general assembly or governor. During a state like Golden State, voters confront dozens of legislative initiatives when they vote.

Critics indicate some major issues regarding DRE systems. The most important is the potential for citizen fraud. Proponents of DRE systems argue that it might take gifted people with terribly specialized data to compromise a system. Thanks to this level of experience, only a few individuals would be capable of committing fraud. DRE's systems are designed as self-contained units wherever the PC system is removed off from quick access. This suggests that the sole time anyone has access to the PC component would be once the system is during high securities space like a storage facility or among the assembly's space of the vendor's search. Critics argue that the likelihood of fraud on a monumental scale continues to be gifted below the proper circumstances (for example, a software engineer United Nations agency has accepted bribes) which fraud is probably tougher to find once mistreatment electronic ballots versus paper ballots.

Election officers and DRE system vendors have to be compelled to take into account several factors, together with citizen obscurity. A citizen's ballot can't be joined back to a particular voter while not compromising confidentiality. Paper-based ballots or a DRE system that generates a written record produce a physical record of every voter's decisions. While not producing this written record, the sole record created is electronic. Critics of paperless systems argue that a software engineer may alter the electronic record of ballots which are now forged and, as a result of votes can't be joined back to a selected citizen for verification, detection of vote change of state might be not possible.

More than a dozen vendors turn out the DRE systems currently in use. Every seller develops (or partners with another firm to develop) a distinctive software system to show, record and tabulate citizen ballots. States aren't absolute to one seller and will purchase systems from multiple sources. Critics argue that connecting completely different systems along may compromise the safety of the network of machines. Vendors don't style their systems to act seamlessly with different vendors' systems, thus connecting two terribly and completely different systems could create either or each behaves in causeless ways in which.

Another major concern is transparency. Transparency refers to a full and correct description of however, the system works. A technique of achieving transparency would be to share the ASCII text file utilized in displaying and capturing ballots with laptop scientists. ASCII text file is the programming language that's legible by the individuals. However, not by computers. By examining the ASCII text file, critics argue, laptop scientists may confirm that the program performs the supposed task while not returning an error. Vendors, however, consider their ASCII text file to be proprietary data. They're unwilling to share this info for worry competitors may use it.

Proponents of DRE systems are fast to indicate that by cathartic ASCII text file, vendors may expose vulnerabilities of their systems that others may exploit, creating such systems less safe. Critics argue that without a careful examination of the code, voters can't be sure that the system is doing what it's imagined to in a neutral form. Fraud, they say, may originate with the vendors either advisedly or through a software error, and votes might be misattributed while not the probability of detection decreases.

Building an associate degree electronic legal system that satisfies the legal necessities of legislators has been a challenge for a long time. Distributed ledger technologies are associated with a degree of exciting technological advancement within the information technology world. Blockchain technologies supply associate degree infinite variations of applications making the most of the sharing economies. This paper aims to judge the application of Blockchain as a service to implement distributed electronic vote systems. The paper felicitates the need for building electronic vote systems and identifies the legal and technological limitations of victimization of Blockchain as a service for realizing such systems. The paper evaluates a variety of the favored Blockchain frameworks that offer Blockchain as a service. We tend to then propose a unique electronic legal system supported Blockchain that addresses all limitations that are discovered. Additionally, this paper evaluates the potential of distributed ledger technologies through the definition of a case study, significantly the strategy of the election, and implementing a blockchain-based application that improves the protection and reduces the worth of hosting a nationwide election.

This research paper dedicates section 2 for analysis of past work as a literature survey and, section 3 describes the idea of the proposed model. Section 4 of this paper works on Evolution of the obtained results. And finally section 5 concludes this paper along with the traces of Future work.

II. LITERATURE SURVEY

This section of the literature survey eventually reveals some facts based on thoughtful analysis of many authors' work as follows.

Ashish Singh [1] proposed a university campus-based electronic voting system to find the best suitable candidate by using the concept of blockchain technology. There are four zones in the university east, west, north, and south zone. Each zone contains several colleges. The university administrator wants to elect one student leader from the contestants. Each college starts the voting process. Each vote under one college creates one block and each block joins together to make a blockchain. After completion of the voting process, the blockchain of each college under one zone join together to make a zone level blockchain. Now, each zone level blockchain joins together to make a university-level blockchain. Now, after getting complete blockchain the

committee will consider this single blockchain for the vote count. The voter has the facility to register only once into the system. The voter ID is used for unique verification and checking the eligibility of the user.

Basit Shahzad proposed a solution that is based on the electronic voting machines and biometric authentication of the voter before he can cast the vote. It presents a perspective in the electronic voting process. That includes but not limited to identifying the polling process, the selection of the suitable hash algorithm, the selection of adjustments in the blockchain, the process of voting data management, and the security and authentication of the voting process, in particular, are discussed [2]. The power of blockchain has been used adjustably to fit into the dynamics of the electronic voting process. The limitations of the proposed framework are that the voter is well educated and aware of his fundamental rights and the polling process, the data of all the voters is available and up for verification and It is also assumed that the polling staff is aware of the technology and they can guide the voters to effectively finish the process.

Freya Sheer Hardwick presented an e-voting scheme which depend on blockchain technology that meets the basic e-voting properties whilst, the protocol must permit for a voter to make one's mind and cancel one's vote, replacing it with another and at the same time, provides a degree of decentralization and places as much control of the process in the hands of the voters as was deemed possible [3]. The presented voting agreement utilizes the blockchain to reserve the cast ballots, therefore in these circumstances, the blockchain behaves as a transparent ballot box. The blockchain also has the additional benefit of being increasingly popular and well-trusted to function as intended, as evidenced by the sheer size of the cryptocurrency market.

Asraful Alam [4] proposed an IoT based e-voting model utilizing blockchain technology for a transparent, cost-effective and smooth election and an algorithm is also proposed that helps to protect voter's privacy and verifies the result in real-time. In the proposed system the voter needs to submit ID and thumbprint for verification. After verification, the system generates the private key for the voter. The voter cast a vote using the generated private key. The casted vote is stored as a hash that represents the voter in a blockchain ledger.

Kanika Garg presented a detailed study performed to understand issues faced by a voting system. There will always remain the concern of authentication of the user and will require some sort of biometric device or unique id. The Blockchain-based solution is a better alternative but the main goal is to making a secure and reliable system irrespective of platform and giving the voting system more transparency and error-free [5]. The authors stated that the E-Voting topic is still a hot debate both politically as well as individual level. It will require mutual understanding among people and strong foundation rules so that it will not be misused.

David Khoury proposed a decentralized voting platform which depends on Ethereum Blockchain. The main contribution of this platform is the restriction of multiple votes per mobile (MSISDN). The proposed system could be developed further to make it more eligible for national government elections, based on fingerprint or a special device located in the voting centers. The consumer interface and results visualization may be customized and adapted to the customer needs [6]. This platform ought to replace the existing centralized systems based totally on SMS polling and facilitate vote casting prepared through governments, competitions, expositions, etc. The proposed platform unlocked up a new business model for voting service providers where the players include: voting service providers, voting event organizers, and voters. The voting service provider enables the voting event organizers to deploy an event voting smart contract.

Rifa Hanifatunnisa [7] presented a database recording system on e-voting using blockchain technology. In the proposed system blockchain permission is utilized, for nodes to be made the opposite of the Bitcoin system and the Node in question is a place of a general election because the place of elections must be registered before the commencement of implementation, it must be clear the amount and the identity. This method aims to maintain data integrity, which is protected from manipulations that should not happen in the election process. This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Each node public key is sent to all nodes listed in the election process.

When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait for their turn to create the block. Upon the arrival of the block on each node, then executed verification to determine whether the block is legitimate. Once valid, then the database added with the data in the block. After the database update, the node will check whether the node ID that was brought as a token is his or not. If the node gets a turn, it will create and submit a block that has been filled in digital signature to broadcast to all nodes by using turn rules in blockchain creation to avoid collision and ensure that all nodes into the blockchain. The submitted block contains the id node, the next id node as used as the token, timestamp, voting result, hash of the previous node, and the digital signature of the node.

Haibo Yi presented strategies to take advantage of blockchain to enhance the security of e-vote casting. First, the author's layout a synchronized version of voting facts-based totally on DLT to avoid forgery of votes. Second, they design a consumer credential version depend on elliptic curve cryptography (ECC) to offer authentication and non-repudiation. Third a withdrawal layout version that lets in citizens to trade their vote earlier than a preset cut-off date. Integrating the above designs, they recommend a blockchain-primarily based e-voting scheme, which meets the essential requirements of the e-vote casting manner [8]. The implementation result suggests that it is a realistic and secure e-vote casting machine, which solves the trouble on forgery of votes.

Lukas Hellebrandt [9] proposed to use the permissioned blockchains distributed among some Tor nodes, serving as blockchain peers. The blockchain holds and versions a list of its valid peers as well as the list of all Tor nodes. This allows

a Tor client to trust more in the validity of these lists and the information present in them. Thanks to the properties of blockchains, and decentralization, in particular, the presented approach provides a higher level of trust in Tor infrastructure in contrast to the current state.

Linh Vo-Cao-Thuy introduces the design and implementation of Votereum – an E-voting system that operates on the Ethereum platform which aims to minimize the trust needed in central authority and enhances fairness in the voting process. The proposed voting scheme is deployed to Rinkeby test net for implementation and analysis [10]. The system consists of a smart contract written in Solidity language, two functional NodeJS servers, and an interface developed with Angular framework.

III. PROPOSED SYSTEM

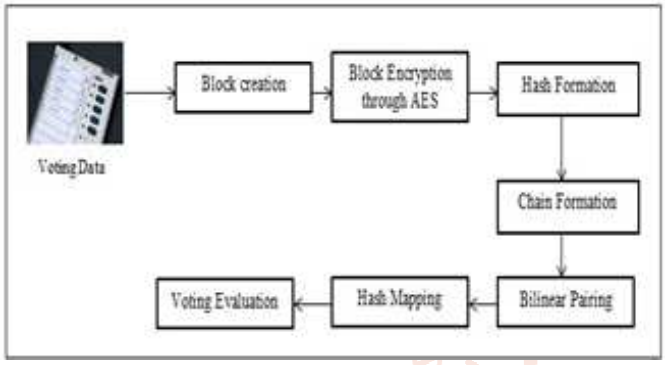

Figure 1: Securing E-Voting System Overview

The proposed system for providing security to the E-Voting data of an election process is established in figure 1 given above and the entire procedure that is executed to accomplish this system is detailed below.

Step 1: Simulation of Voting – The initial step of the proposed methodology which is utilized to generate the voting data, is being simulated in a java programming language-based environment. To generate the voting data N number of booths is created using the random function of the java platform. These N booths contain various attributes such as votes, booth no, symbol name, serial no, etc. The booths have authentication credentials are created using the booth officer names stored in a file. These booths along with the attributes are saved in the database in a separate table.

The candidates are created using a dedicated user interface with various attributes related to the candidate that is allotted manually. The candidates have attributes such as party name, party symbol, candidate name, age, sex, etc. The voting procedure is done on the various candidates that are created through this user interface. The voting for each candidate is done through the random function provided by the java library. The generated votes are encrypted before being stored in the respective database.

Step 2: Advanced Encryption Standard – The votes generated through the simulation in the previous step are subjected to the Advanced Encryption Standard or AES encryption before being stored in the database. The E-Voting data obtained in the previous step is in the string format which is subsequently converted into an array to perform the encryption. The encryption is performed using various transformations and a symmetric 128-bit key. The symmetric key can be used for both encryption and decryption purposes. The transformations include substitution through the substitution table, shifting of the substituted rows, and finally the combination of the rows which creates the ciphertext for storage in the database.

Step 3: Multi Linear Pairing – The encrypted voting data obtained from the previous step is divided into a selection of booths. These divisions are then utilized for parallel computation to achieve integrity evaluation. The divisions achieved through this process are provided to the blockchain for further processing and the integrity evaluation.

Step 4: Data Integrity through Blockchain – The booths and the divisions generated in the previous step through the use of the multilinear paring are utilized here for further process of integrity evaluation. The MD5 hashing function is utilized in this step to provide the hashing function for the generation of the hash key of the divisions. The long hash key generated is reduced in sizing using rotation and random selection.

The blockchain platform is then utilized by creating the block key and body for every booth generated from the previous step. This step is repeated until all the booths have been processed and the final divisional keys are generated for every one of the N booths. The head keys that are generated are stored in the database with respect to their booths. These keys are used for the integrity evaluation of the booth data.

The head keys are calculated during the counting process once again. This enables the previous and the current hash keys to be compared for the purpose of evaluating the integrity of the voting data. If there is any dissimilarity observed in the keys then that indicates that the E-Voting data has tampered and the data is compromised, which prompts the system to generate an Alert regarding the same.

The process of blockhead key generation is depicted in the algorithm 1.

ALGORITHM 1: Block Head Key Generation

```
//Input : Booth List B_L
//Output: Head Key H_K
1: Start
2: H_K =" "
3: FOR i=0 to size of B_L
4:        KEY=" "
5:        B_D = getBoothData(B_L[i])
6:        B_D= B_D+ H_K
7:        MD5_HK=MD5(B_D)
8:        R= MD5_HK length MOD 7
9: FOR j=0 to KEY Length <7
10:       j=j+( R+1)
11:       IF ( j< MD5_HK length)
12:       KEY=KEY+ MD5_HK [j]
13:       MD5_HK = MD5_HK >> 1
14:       ELSE
15:       j=0
16:END FOR
17:H_K = KEY
18:END FOR
19:       return H_K
20: Stop
```

This is the procedure outlined for the simulation of the voting process. The real-time execution of the E-voting process is slightly different. In real-time execution, there would be the difference as the EVM or the Electronic Voting Machine is utilized for the objective of extracting the voting data which is different from the utilization of the device or a database for the simulation of the votes. This extrication process reduces any probability of voting data being compromised or contaminated while extracting the voting data as the stored data is encrypted. The obtained data will then be processed using the proposed system to generate a key through the blockchain process. This key will be shared with the respective bureaucrats of the Election commission for performing integrity evaluation. The execution of the E-Voting paradigm makes sure that any fault or corruption in the EVM will not have an influence on the E-Voting process. The E-Voting platform has also been made resistant to any form of corruption be it software or hardware in nature to the integrity evaluation paradigm. The voting data integrity of the collected data is evaluated through the hash keys that are generated and compared to the keys shared with the bureaucrats. Any tampering or corruption done in the data will be easily visible through the avalanche effect which would lead to a drastic difference in the keys. This is how the distributed Blockchain approach conserves the security of the E-Voting Data.

IV. RESULTS AND DISCUSSIONS

The presented technique for enabling the security of the E-voting data has been realized utilizing the Net Beans IDE and written in the Java programming language. The proposed methodology has been executed on a machine comprising of an average configuration such as the Intel Core i5 processor for the processing requirement supplemented by 500GB of storage and 4GB of RAM. The MySQL database server is utilized for the realization of the database responsibilities.

Extensive measurement of the performance of the presented technique was performed using in-depth analysis techniques. For the measurement of the accuracy of the presented technique, the Precision and Recall metric was utilized which can provide an assessment of the performance of the presented technique in detail. The performance metrics were measured extensively to illustrate that the technique for securing E-voting data. This is done through the AES encryption standard and the blockchain framework.

Performance Evaluation based on Precision and Recall

Precision and Recall can allow for the extraction of detailed information relating to the performance of the presented technique. The precision and recall metrics are highly thorough and insightful parameters that can measure the actual performance of the system. Precision in this assessment measures the relative accuracy of the proposed system by evaluating the accurate values of the degree of precision attained in the presented technique.

Precision in this approach is being measured as the ratio of the incorporated sum of all the correctly performed integrity evaluations to the number of incorrectly performed integrity evaluations. Therefore, the measurement of the values of precision attained is an in-depth evaluation of the accuracy of the proposed methodology.

The Recall metrics utilized for measurement of the absolute accuracy of the technique which is vastly different from the precision metrics. The Recall metrics are measured by the evaluation of the ratio of the number of correctly performed integrity evaluations versus the total number of incorrect integrity evaluations performed. This methodical evaluation provides judicious knowledge as it measures the absolute accuracy of the technique. Precision and recall are elaborated mathematically in the equations given below.

Precision can be mathematically explained as below

- A = The number of correctly performed integrity evaluations for N number of booths
- B= The number of incorrectly performed integrity evaluations for N number of booths
- C = The number of integrity evaluations not performed for N number of booths

So, precision can be defined as

$$\text{Precision} = (A / (A+ B)) *100$$

$$\text{Recall} = (A / (A+ C)) *100$$

Considerable experimentation has been performed on the proposed system through the application of the equations elaborated above. The readings of the experimentation are tabulated in Table 1, given below.

No of Booths	Correctly Performed Integrity Evaluations (A)	Incorrectly Performed Integrity Evaluations (B)	Integrity Evaluations not Performed (C)	Precision	Recall
35	35	0	0	100	100
59	58	0	1	100	98.30508475
88	86	1	1	98.85057471	98.85057471
121	120	1	0	99.17355372	100
138	135	1	2	99.26470588	98.54014599

Table 1: Precision and Recall Measurement Table

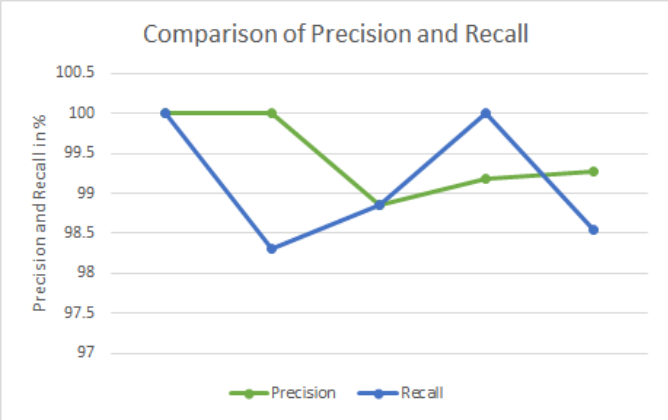

Figure 2: Comparison of Precision and Recall

Figure 2 above illustrates the graphical presentation of the experimental readings. The execution of the proposed methodology for securing E-voting data attains unparalleled accuracy which is evident through the precision and recall evaluation. The proposed methodology attained the precision of 99.45% and Recall of 99.13% which is considerably surpassing the conventional techniques for securing E-voting data utilizing the Advanced Encryption Standard and the distributed Blockchain framework.

V. CONCLUSION AND FUTURE SCOPE

India is the largest democracy in the world, with such a large population, it is imperative to take into consideration the votes of every single eligible voter in the country which is a herculean task. The physical process of Ballot voting is an

archaic process that is due for an uplift. The physical method is prone to be degrading to the environment as it creates a lot of wastage and utilizes a lot of paper. The casting of the votes is also a physically laborious process that takes a lot of effort from the voter to travel to the polling booths, wait in a lengthy line to cast their vote. This is something undesirable and is also the reason why there has been a very poor voter turnout in the country. The addition of Blockchain to the E-Voting paradigm along with the AES encryption allows for highly secure, fair, and transparent elections that are also tamper-proof. The methodology proposed in this paper has been experimented in detail to achieve significant improvements in accuracy over other E-voting approaches as evident from the precision and recall performance metrics obtained.

For Future research applications, the proposed methodology can be implemented on a real-time election process, or on a large and multi-structured voting data that is obtained for reaping the benefits of the improved accuracy.

REFERENCES

[1] Ashish Singh and Kakali Chatterjee, "SecEVS: Secure Electronic Voting System Using Blockchain Technology", 2018 International Conference on Computing, Power and Communication Technologies (GUCON), 28 March 2019.

[2] Basit Shahzad and Jon Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology", IEEE Access, Vol: 7, 25 February 2019.

[3] Freya Sheer Hardwick ; Apostolos Gioulis ; Raja Naeem Akram ; Konstantinos Markantonakis, " E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy ", 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 03 June 2019.

[4] Asraful Alam, S. M. Zia Ur Rashid, Md. Abdus Salam and Ariful Islam, "Towards Blockchain-Based E-voting System", 2018 International Conference on Innovations in Science, Engineering and Technology (ICISET), 27 June 2019.

[5] Kanika Garg, Pavi Saraswat, Sachin Bisht, Sahil Kr. Aggarwal, Sai Krishna Kothuri and Sahil Gupta, "A Comparative Analysis on E-Voting System Using Blockchain", 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 29 July 2019.

[6] David Khoury, Elie F. Kfoury, Ali Kassem and Hamza Harb, "Decentralized Voting Platform Based on Ethereum Blockchain", 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), 07 January 2019.

[7] Rifa Hanifatunnisa and Budi Rahardjo, "Blockchain-based e-voting Recording System Design", 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), 01 February 2018.

[8] Haibo Yi, "Securing e-voting based on blockchain in P2P network", Yi EURASIP Journal on Wireless Communications and Networking, Springer, 2019.

[9] Lukas Hellebrandt, Ivan Homoliak, Kamil Malinka, and Petr Hanacek, "Increasing Trust in Tor Node List Using Blockchain", 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 01 July 2019.

[10] Linh Vo-Cao- Thuy, Khoi Cao-Minh, Chuong Dang-Le-Bao, and Tuan A. Nguyen, "Votereum: An Ethereum-Based E-Voting System", 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF), 16 May 2019.