*[1]Vinayachandra,

[2]Dr. Krishna Prasad K.

Cryptogrphy and Blockchain Based E-Voting System for Secured Voting Process

Abstract: - In recent years, development of technology has brought various advancements across domains. Due to the advancement of technology, various traditional methods have been replaced by the computational methods. One such technical advancement is e-voting system. Traditional voting techniques such as paper ballot has its own disadvantages, which includes prone to human errors, duplication of votes. Hence, different computational methods have been used by various existing studies for e-voting process. However, these existing techniques lacked in providing a secured and efficient model for e-voting process due to usage of ineffective algorithms. Therefore, proposed model employs AES-3DES (Advanced Encryption Standard-Triple Data Encryption Standard) algorithm for e-voting process. Proposed AES-3DES model is considered as a quick and secure algorithm as it is employs symmetric encryption algorithm which uses the data encryption standard three times. Further, AES-3DES algorithm possess the potential to encrypt the huge amount of data safely and securely. Besides, data of the voters are stored in the Blockchain (BC) technology as BC secured, transparent and tamper-proof, which makes the attackers difficult to fetch the data of the voters. Moreover, BC aids in creating a secure and transparent voting system and assist in reducing the fraud which can happen during e-voting. Finally, performance of the proposed system is assessed by evaluating encryption and decryption time, size of the input and length of the key, moreover, the performance of the proposed model is compared with the existing model in order to estimate the efficiency of the proposed model.

Keywords: E-voting, Cryptography, Advanced Encryption Standard, 3 -Data Encryption Standard Encryption, Blockchain, Decryption, Data protection, Secured Voting System.

I.INTRODUCTION

Immense and mammoth amount of sensitive as well as complex information are managed and stored in online. Further information can be attacked by various unauthorized parties to hack information [1]. Therefore, it is important to protect the information against these attacks. These data security comprises deploying tools and technologies which enhances and improves the visibility of the organization into where its critical and crucial data resides. It has been revealed that, cryptography offers huge number of benefits and assistances to e-voting and counting solutions. Cryptography is one of the fields of information security technology which applies the technique of sending the personal information via open network communication [2]. Services provided by cryptography are - Confidentiality, Integrity and Accessibility. Cryptographic techniques consist of 2 process which are namely encryption process and decryption process [3]. Cryptographic methods are employed in several fields and even in day to day life. Likewise, cryptography is also employed in e-voting system [4]. As voting is considered as a rudimentary democratic activity. In voting different conventional methods are used for casting the votes like paper balloting. However, these traditional approaches are prone to errors and confusions and other such issues like involvement of fraudulent activities like modifying the outcome of vote calculations for particular contenders, repetition of votes or human error techniques are some of the conundrums which are faced during the conventional voting process.

Therefore, e-voting approach is utilized for overcoming these issues by delivering different tactics such as casting votes and securing the votes from the anonymous threats, saves the cost of the printing ballot, storage of data for longer period of time without any tampering of the votes. Further, e-voting is considered as one of the developing applications of block chain (BC) technology with the aim to leverage different benefits such as non-repudiation, anonymity and integrity as these are critical for voting application. Further, usage of BC technology in e-voting application has facilitated in achieving securable and verifiable voting systems [5] as BC employs decentralized

[1] *[1]Research scholar, Institute of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India.

[2]Professor & HOD, Cyber security and Cyber Forensics in the Institute of Engineering and Technology, Srinivas University, Mangalore, Karnataka, India.

*[1]Corresponding author mail ID: veeciashu@gmail.com

[2]Co author mail ID: karanikrishna@gmail.com

nodes for e-voting due to the advantages end to end verification, further wholly distributed voting infrastructure is delivered by the BC technology. Some of the e-voting requirements includes privacy of the voter, convenience and verifiability of the voter are confined by the using BC technology. BC technology deliver additional security to the e-voting platform and peer to peer transaction ledger which allows each and every vote that is casted will be deliberated as a transaction of the individuals as this process creates a secured and transparent environment for elections. BC has the ability to prevents modifications and altercations of the data stored in blocks using different cryptographic techniques. Hence it has been revealed that BC technology aids in providing security, fairness and transparency in terms of voting [6].

However prevailing e-voting systems possess different issues such as the employing e-voting systems as reliability, integrity and vulnerability to hacking the data by attackers. Hence, in order to overcome the issues proposed system employed AES- 3DES model for encryption and decryption. AES algorithm aids in supplying vote, securing the information of the voters, integrity of the confirmation of the pool and verification of the voters by using multi-factor authentication. Though, the existing works delivered decent outcome, it still lacked in enhancing the security of e-voting system and confidentiality of the voter's data. Besides, the existing models were slower and less secure than the proposed model as the proposed AES-3DES model is faster to encrypt large amount of data securely along with faster encryption of data than the prevailing methods.

Main contribution of the research includes,

- To create secured E-Voting system by employing AES-3DES (Advanced Encryption Standard-Triple Data Encryption Standard) model as AES-3DES model works faster and possess the potential to encrypt huge data.
- To apply a secure and tamper-proof ledger for storing voter's data using block chain technology
- To analyse the performance of the proposed model using size of the block, verification time, encryption and decryption.

1.1 Paper organization

Section II discusses the review of conventional works with the problems identified. Following this, section III elaborates on the proposed techniques with suitable flow, algorithms, and mathematical derivations. Subsequently, section IV presents the results attained after simulating the proposed work. The overall study is concluded in section V with future suggestions.

II. LITERATUIRE REVIEW

Different traditional employed in e-voting systems for secured voting process are emphasized in this section.

E-voting is measured as an alternative method for different existing voting mechanism. Though e-voting mechanism are evaluated as one of the highly promising technologies in recent times, still it is not completely free form defects. Hence, the suggested study employs hybrid AES-RSA algorithm along with the LSB technique with the aim to secure the information present in the ballot. The encrypted ballots were concealed by employing LSB algorithm, which aided in augmenting the integrity of the system. Finally, the performance of the recommended paper was assessed using different metrics such as PSNR, co-relation and MSE metrics [7]. Similarly, e-voting system aids in minimizing the percentage of the nonparticipation and assurances security against various fraudulent activities such as tampering and duplication of votes. Hence, recommended study aids in employing Blockchain technology as it is considered to be an effective and efficient technology in e-voting system. BC technology plays a crucial role in e-voting system as it stores the data of the voters safely and securely. Therefore, recommended paper employed an aadhar card verification in e-voting scheme in order to overcome the duplication of votes. V-ID and the details of the voters in form of biometrics are attained form the database of aadhar with the aim to cats the vote and digital key is employed for both encryption of votes which exist inside in the block [8]. Likewise, existing paper utilized block chain technology on analyzing the likelihoods and inevitabilities of the distributed ledger technology in e-voting system. Hence, the existing paper utilized AES-256m algorithm along with SHA-hashing function. Further, SHA-256 employed in the existing paper is considered a s one of the powerful ad consistent has functions for securing the e-voting system [9].

Similarly, suggested study focused on employing effective hashing approaches in order to ensure the security and credibility of the data. Therefore, block sealing technique was used in BC technology in order to meet the requirements of the polling process,. The use of the existing technique aids in not allowing the unauthorized access which could be made from the external world. Therefore, the existing paper focused on efficacy of the polling process, then the helpfulness of the hashing algorithms along with the security management in e-voting process [10]. Though, e-voting model delivers convenience and other such advantages, it is still a concern for people to vote through online due to various reasonable aspects safety and security. Further, rise of various attacks can cause huge conundrums in future. Therefore, existing paper focused on employing VC (visual cryptography) and BC technology for protecting the e-voting system from innumerable dangerous attacks [11].

As security is considered to be one of the most critical and momentous concerns in terms of e-voting system, it is important to build a reliable – e voting system using effective algorithms and technique. Therefore the suggested study employed BC technology to secure the process of e-voting along with the double layer encryption model with the aim to avoid the influences of votes, which would have occurred with the outcome of the election. Further, performance of the recommended model aided in providing privacy of the voters [12]. Processing of voters information and the storage ascended instant worries regarding the privacy of the data and security, due to this, existing study addressed the issues associated to securing the information of the voters and post-election issues and confidentiality of the users using different cryptographic techniques. The model implemented in the recommended study was E-AES model for overcoming the issues related to privacy and security. Further, it has been revealed that E-AES model delivered better and satisfactory outcome for secured e-voting mechanism [13].

In recent days, traditional voting systems are considered as a hassle for voting as they are prone to errors, be it human or computational errors. Further, they can cause different problems like duplication of votes and stealing the information of voters. Hence in order to these issues caused by the traditional approaches, e-voting has become one of the significant applications in the technology world. However, these e-voting system can also cause create hassles related to security due to intervention of third party entities. Hence in order to overcome these issues, suggested study emphasized on Blockchain technology along with various cryptographic techniques for overcoming issues related to security and constraints in the number of voters [14]. Likewise, existing paper focused on utilizing BC technology for e-voting as they possess greater transparency due to distributed and open ledgers, inherent anonymity, reliability and immutability [15].

2.1 Problem identification

From the assessment of the above-existing works, core concerns are emphasized as explored below,

- Existing studies lack in delivering reliability, confidentiality and privacy of the voters data [12].
- Duplication as well as tampering of the votes are considered as one of the significant concerns in the existing paper [8].
- Model employed in the recommended paper is considered to be slower and incapable of handling huge data for e-voting [9].

III. PROPOSED METHODOLOGY

E-voting system is considered as one of the important applications in the recent times due to rise of fraudulent activities in the traditional voting system. E-voting is used for ensuring the verification of the identity as it employs the usage of computer, which makes the e-voting system safe, secured and provide high level of efficiency and transparency for election process. However, the traditional e-voting systems are considered to be slower and lack in securing huge amount of data, which can be overcome by employing proposed AES-3DES method for e-voting process as the proposed AES-3DES encrypt huge amount of data securely and works faster than the existing models, which makes it efficient and reliable for e-voting process.

In initial phase, the study has employed AES-RSA algorithm to secure voters data by using encryption and decryption. Further Blockchain technology has been used to verify the login details of the voters and validate the mismatching of data. However, there is a scope of improvement which can make the model efficient and capable than the existing ones. Therefore, current study utilizes AES-3DES algorithm for securing the voters data securely. Figure 1 shows the overall flow of the proposed model.

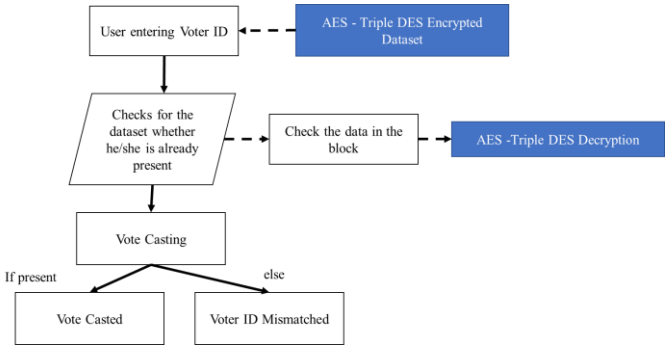

Figure.1. Overall Flow of the Proposed Work

Figure 1 shows the overall process of the proposed work. Initially, the data of the voters is encrypted by using AES-3DES encryption process, since the proposed AES-3DES model aids in faster and secured voting process in the e-voting system as AES-3DES model uses symmetric algorithm. Once the data is encrypted, it checks if the person is present or not in the dataset, which is stored using Blockchain technology. Blockchain is a technology which stores the data in blocks and makes proposed model effective for voting. Further, the data is again decrypted using AES-3DES algorithm. If the person is present in the dataset, voting will be casted, if not, voter ID is turned to be mismatched.

3.1 AES-3DES Algorithm

The data of the voters is encrypted by employing AES-3DES algorithm for e-voting system. It possess symmetric block size of 128 bits. AES algorithm has the capability to perform effectively for both encryption and decryption. AES algorithm is considered to be extra secure against brute force attacks and much inexpensive than the other algorithms. Likewise, 3DES algorithm employs three stage encryption process in order to make it more difficult for attackers to decrypt the data. Further, 3DES algorithm is considered to be more secure due to the small key length of DES. However, these algorithms are not fast and capable enough to encrypt or decrypt huge amount of data securely. Hence proposed model combined AES-3DES algorithm for e-voting system as AES-3DES performs faster than the existing algorithms and can be utilized to encrypt over insecure networks efficiently. Moreover, AES-3DES model can encrypt and decrypt large amount of data safely and securely for voting via network. Figure shows the mechanism of the proposed work. Initially the admin and the voter is the window, in which the details of the voter is stored in the local dataset. Further, the data will be encrypted, once the voter enter the data by employing proposed AES-3DES algorithm. Then the encrypted data will be pass via block chain, once the data is verified. Then the data, which has been verified is decrypted and passed to the voting process. If the data gets matched with the already existing data, vote will be casted, if not, vote will not be casted. The encryption and decryption process aids in process of e-voting enhances the safety and security of the voting system.

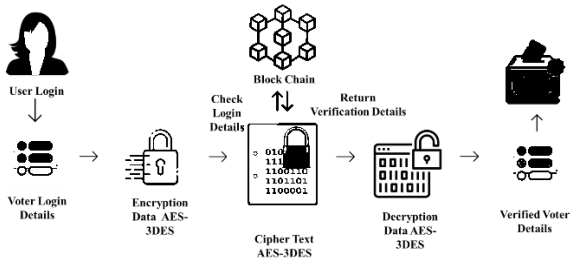

Figure.2. Process of E-voting Mechanism

AES is combined with other security protocol in order to acquire an additional layer for security. The data, which has been encrypted from the AES algorithm is encrypted and decrypted using 3DES algorithm. The 3DES algorithm employs 3 instance of DES on same plain text. It employs 3 different types of keys, first all used keys are different and in second two keys are same and one is different and in third all keys are similar. Both Public key and private key are utilized. In which, keys are utilized for encrypting the data. After encryption, the data is performs process for e-voting then the data is decrypted once the details of the voters are verified. Then the data

is sent to cast the vote. This mechanism aids in securing the e-voting systems against several harmful attacks in order to prevent fraudulent activities and steal of data. AES-3DES algorithm is depicted in algorithm I.

Algorithm I: AES-3DES

Initialization
input (text)
input keys
op1 = Mutually indepentant keys(Key1 ≠ Key2 ≠ Key3 ≠ Key1). key space of $3 \times 56 = 168$ bits
op2 = Two mutually independent keys, 3^{rd} key as same as 1^{st} key
Key1 = Key2 & Key3 = Key1. key space $2 \times 56 = 112$ bits.
op3 = Identical keys(key1 = key2 = key3).
$Num_{block} = 4$ block_size of 128 bits
Encryption
CipherText ($byte_{in}[4 * Num_{block}], byte_{out}[4 * N_{block}]$, word $w[Num_{block} * (N_{row} + 1)]$)
begin
byte st $[4, Num_{block}]$
state = in
AddRoundKey(st , $w[0, Num_{block} - 1]$)
for round 1 step 1 to $Num_{row} - 1$
Sub_{Bytes}(st)
$Shift_{Rows}$ (st)
$Mix_{Columns}$(st)
AddRoundKey(st , $w[round * Num_{block}, (round + 1) * Num_{block} - 1]$)
end for
SubBytes (st)
ShiftRows (st)
ID_{val} = AddRoundKey (st , $w[Num_{row} Num_{block}, (Num_{row} + 1) * Num_{block} - 1]$)
cipertext = ct = $h(ID_{val} \oplus h(PW \oplus x))$
out st cipertext
Decryption
plaintext → decrypt (cipertext, key)
begin
Decryption: $ct' = h(ID_{val} \oplus h(PW \oplus x))$
If $ct' = ct$
Proceed to next Alg.
Else
Abort
byte st $[4, Num_{block}]$
$st = ct'$
AddRoundKey(st , $w[0, Num_{block} - 1]$)
for round 1 step 1 to $Num_{row} - 1$
$InvMix_{Columns}$(st)
$InvShift_{Rows}$(st)
$InvSub_{Bytes}$(st)
AddRoundKey(st , $w[round * N_{block}, (round + 1) * N_{block} - 1]$)end for
end for
Sub_{Bytes}(st)
$Shift_{Rows}$(st)
output(plaintext)
end

3.2 Block Chain

Blockchain is employed in the proposed study for storing the data of the voters securely and tamper-proof. The Blockchain mechanism employed in the proposed model to store the encrypted and decrypted data which aids in comprehending the data for e-voting mechanism. A Blockchain is a distributed ledger and a type of database which stores the data in the block which are linked together using AES-3DES algorithm. Blockchain is employed to create a secure and transparent voting system. This results in reducing the fraudulent activities which takes place while voting and aids in ensuring that every vote is counted. Though, BC is considered as a complex technology, it is a secure technology which helps in storing the data safely and securely.

IV. RESULTS AND DISCUSSION

The proposed design has been executed with Python. The obtained results are discussed in this section, along with a comparative analysis to determine the efficacy of the proposed approach over conventional methods.

4.1 Performance Analysis

Performance of the proposed method is analyzed in the subsequent section, which consist of size of the input and its encryption time and decryption time. Then the time taken by the proposed AES-3DES model for different lengths of the keys.

Table-1. Encryption and Decryption Time

Input Size	Encryption Time (ms)	Decryption Time (ms)
512	0.019	0.018
1536	0.028	0.03
3345	0.048	0.05
4096	0.072	0.058

Table 1 shows the encryption and decryption time of the input, in which different input sizes exhibits different encryption and decryption time. When the size of the input is 512, encryption time exhibits 0.019 and 0.018, likewise when the size of the input is 1536 the encryption and decryption time obtained is 0.028 and 0.03. Similarly, when the size of the input is 3345, time taken for encryption is 0.048 and time taken for decryption is 0.05. Finally, when the size of the input is 4096 is encryption and decryption time obtained is 0.072 and 0.058. Figure 3 shows the graphical representation of the table.

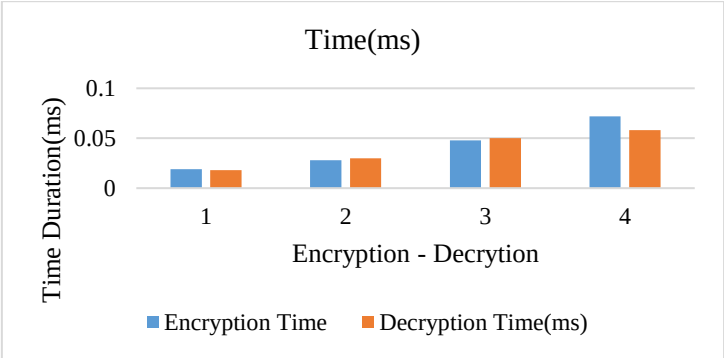

Figure.3. Encryption and Decryption Time

Table 2 shows the time taken by the AES-3DES model with respect to length of the keys in terms of byte. Time taken by the AES-3DES when the length of the key is 1024 is 0.369 ms, whereas the time taken by the proposed model when the length of the key (4096) is 30.08 ms. The graphical representation of the table is depicted in the Figure 4.

Table-2. Length of the keys by AES-3DES

Key Length(bytes)	Time by AES - 3DES
1024	0.369
2048	3.52
3072	19.52
4096	30.08

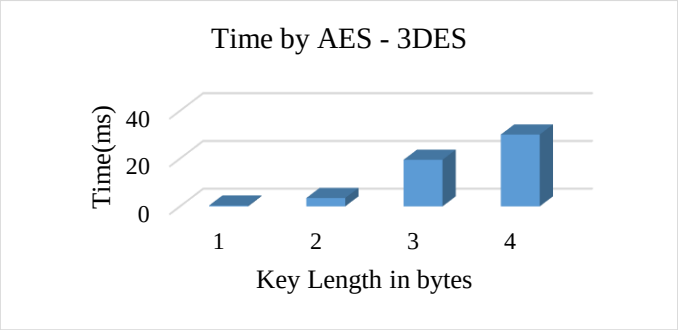

Figure.4. Length of the keys by AES-3DES

Table 3 shows the encoded and decoded values of the details entered. Information like register ID, name, gender, city, state, ward number has been tabulated in the table along with the decoded data.

Table-3. Encoded and Decoded data

Encoded	Decoded
10032	cbe8ae
Ana	3e751ff7d227
Female	ad8a
TN	505e0d6c1fd406
Madurai	e02777
147	ef
1	6325
32	6a80d5f3a4

From the performance analysis, it has been identified that, proposed model delivered better outcome than the existing models. Encryption and decryption time of the input size has been calculated along with the encryption time of the length of the key has been calculated.

4.2 Comparative Analysis of the Proposed Model with Existing Model

Comparative analysis involves comparing various existing models with the proposed model in order to illustrate the effectiveness of the proposed model. Table 4 shows the existing and proposed model with different aspects such as generation of public and private keys, verifying the f(i,j) other voters, Computation of public keys, reconstruction of subsecret of reconstruction and finally time taken by the proposed and existing model.

Table-4. Analysis of the existing and proposed model [16]

Number:Operation	Existing Model (ms)	**AES-3DES model**
A.Generate Public / Private Keys	36.19	30.14
B.Verify f(i,j) other voters	0.23	0.18
C.Compute Public key	4.01	3.2
D.SubSecret Reconstruct	0.08	0.04
Total Time Taken	40.51	**35.26**

From the table 4 it can be examined that, proposed model delivered better performance than the existing models by taking less time than the existing models for key generation (30.14 ms), verification of voters (0.18 ms), computing the public key (3.2 ms), reconstructing the subsecret (0.04 ms) and time taken (35.26) by the model.

Table-5. Comparative Analysis of the Encryption time [12]

	Encryption Time Duration (ms)	
Voters	Existing Model	**Proposed Model**
Voter 1	94	84
Voter 2	89	82
Voter 3	91	84
Voter 4	87	81.3
Voter 5	90	83

Table 5 shows the encryption time taken by the voters in both existing and proposed model. When compared to the existing model, proposed model took less time for encryption, which makes the model efficient than the existing models. In Proposed model, voter 1 took 84 ms for encryption, voter 2 took 82 seconds for encryption, voter 3 took 34 ms for encryption, similarly, voter 4 and voter 5 took 81.3 and 83 ms for encryption. Graphical representation of the table is depicted in Figure 5.

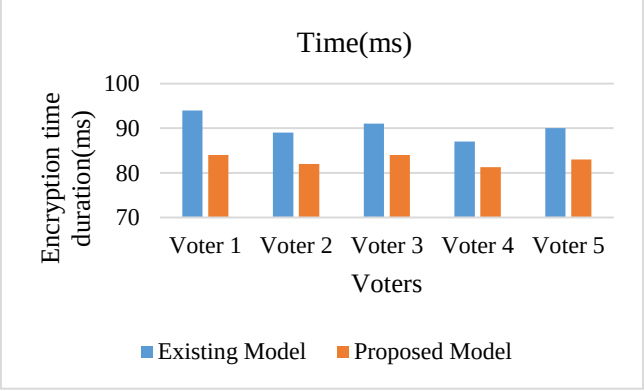

Figure.5. Comparative Analysis of the Proposed and Existing Model

From the experimental outcome, it can be revealed that, proposed model delivered better outcome than the existing models in terms of encryption, decryption time, length of the key and other aspects related to due to the incorporation of proposed AES-3DES model as the proposed model which is faster than the existing model and can encrypt the data over insecure networks. Further, it also possess the capability to encrypt huge amount of data securely when compared to the prevailing models, which makes the voting process safe and secure over the existing models. In addition, usage of Blockchain technology deliver the added advantage to the e-voting process as the Blockchain technology is protected, tamper-proof and secure at the same time. Hence, implementation of BC makes the proposed model reduce the voter fraud and ensure that every vote is counted.

V. Conclusion

E-voting has become one of the significant technological developments in recent years. Further, traditional voting system such as paper ballot and other such conventional techniques have been replaced by e-voting system. E-voting system aids in reducing the duplication of votes and other innumerable fraudulent activities. However, privacy and security of the e-voting system is still a debate. Hence, various studies have introduced different techniques for creating an effective e-voting mechanism, however, these prevailing methods lacked in delivering faster and secured e-voting data which possess the ability to encrypt large amount of data. Therefore, proposed study employed AES-3DES model for faster working process as AES-3DES model employs symmetric encryption algorithm. Further, AES-3DES algorithm performed encryption on huge amount of data safely and securely. Besides, the data was stored using Block chain technology as helped in reducing the voter fraud and ensured the count of the voters. Moreover, the performance of the proposed model is analyzed using the encryptions and decryption time of the input size. Further, the proposed model is compared with the existing models with different aspects such as duration of the encryption time and other operations like generation of public and private keys, verifying the f(i,j) other voters, Computation of public keys, reconstruction of subsecret of reconstruction and finally time taken by the proposed. The time taken by proposed model is 35.26ms which is less than the existing model, this makes the model effective than the other existing models. In future, it can be used by the different security analysts for secure voting process.

REFERENCES

[1] S. Sharma and U. India, "The Effectiveness of Different Cyber Security Measures in Protecting Organization for Cyber Threats."

[2] R. Prasad and V. Rohokale, *Cyber security: the lifeline of information and communication technology*: Springer, 2020.

[3] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: a survey," *Wireless Networks*, vol. 27, pp. 1515-1555, 2021.

[4] R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for E-voting," *Symmetry*, vol. 12, p. 1328, 2020.

[5] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems*, vol. 105, pp. 13-26, 2020.

[6] A. A. Kumar, P. Neelima, and T. Mahalekshmi, "Online Voting System Using Secure Blockchain," *Journal homepage: www. ijrpr. com ISSN*, vol. 2582, p. 7421.

[7] O. O Okediran, A. A Sijuade, and W. B Wahab, "Secure electronic voting using a hybrid cryptosystem and steganography," *Journal of Advances in Mathematics and Computer Science*, vol. 34, pp. 1-26, 2019.

[8] T. Roopak and R. Sumathi, "Electronic voting based on virtual id of aadhar using blockchain technology," 2020, pp. 71-75.

[9] M. Nagar, P. Kumar, P. Anand, S. Shukla, and P. Gera, "Implementation of Blockchain for Fair Polling System," *Pranav and Anand, Praveen and Shukla, Shubh and Gera, Paras, Implementation of Blockchain for Fair Polling System (July 14, 2022)*, 2022.

[10] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24477-24488, 2019.

[11] A. S. Rajawat, S. Goyal, P. Bedi, S. Malik, B. C. Neagu, M. S. Raboaca, *et al.*, "Visual Cryptography and Blockchain for Protecting Against Phishing Attacks on Electronic Voting Systems," 2022, pp. 663-666.

[12] R. Taş and Ö. Ö. Tanrıöver, "A manipulation prevention model for blockchain-based e-voting systems," *Security and communication networks*, vol. 2021, pp. 1-16, 2021.

[13] B. A. Oke, O. M. Olaniyi, A. Aboaba, and O. T. Arulogun, "Securing electronic voting system using crystographic technique," 2019.

[14] K. V. Rao and S. K. Panda, "Secure Electronic Voting (E-voting) System Based on Blockchain on Various Platforms."

[15] A. Indapwar, M. Chandak, and A. Jain, "E-voting system using Blockchain technology," *Int. J. of Advanced Trends in Computer Science and Engineering*, vol. 9, 2020.

[16] J. Lyu, Z. L. Jiang, X. Wang, Z. Nong, M. H. Au, and J. Fang, "A secure decentralized trustless E-voting system based on smart contract," 2019.