iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VII **Month of publication:** July 2022

DOI: https://doi.org/10.22214/ijraset.2022.45677

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

E-Voting System Using Homomorphic Encryption

Dr. Jyoti Neeli[1], Basavaraj P[2], Nandish P[3], Shrinidhi.G. Atgur[4], SurajM[5]
[1]*Associate Professor,* [2,3,4,5]*UG Students, Department of Information Science and Engineering, Global Academy of Technology, Bengaluru*

Abstract: ***A protected e-voting system using Blockchain technology is proposed in this paper. It is using homomorphic encryption casting a vote electronically. It is represented that in spite of the fact that blend-based casting a ballot is an extremely straightforward answer for special e-casting a ballot it is helpless against an intimidation threat from politically contesting individuals. The intimidation assault particularly goes after special e-casting a ballot plot just results the political decision result and uncovers no vote, so is safe to the assault. Homomorphic encryption calculation is taken advantage of not just to count the votes without uncovering them yet in addition to change the votes when another round of counting is required. Additionally, it accomplishes all the security properties normally wanted in e-casting a ballot. Since Blockchain technology is used to store the votes any sign of tampering will be easily detected with the discrepancy of the time signatures and the hash values. The proposed will enable the citizen or a voter entity to vote from the confines of their home thereby negating their travel expenses which would otherwise be too extreme if the voter entity resided in a place where there is no adequate infrastructure to support traditional voting schemes. The voter entity can first verify their identity and receive an OTP which then enable them to cast a vote online in a dedicated web application.***

Keywords: E-voting, OTP, homomorphic encryption, Web Application

I. INTRODUCTION

Innovation has been utilized in different perspectives, both disconnected and also on the web. The increment of its use, particularly in on the web putting away information causes security to become one of the most significant prerequisites. One of the ways of safeguarding information is with encryption. Encryption is an interaction to change over message or data into a structure that can be perused exclusively by the beneficiary. The expected beneficiary should decode the encoded information previously it very well may be perused. The beneficiary ought to have a key to unscramble it. There are two cryptosystem classifications: symmetric and unbalanced. The symmetric cryptosystem utilizes a similar key to play out the course of scramble and unscramble a message. In anuneven cryptosystem or generally called as open key cryptosystem, the public key utilized for encode messages can gotten to by anybody. The message must be perused by the explicit beneficiary who has the matched key called private key.

Blockchain is a conveyed and decentralized public record oversaw by a shared network. When the information in one block goes through change, the correction cycle is recorded and shared by the wide range of various blocks in the blockchain framework. All in all, it is difficult to covertly alter the information. This is a clear benefit in an e-casting a ballot framework on the grounds that blockchain itself can screen whether the democratic outcomes are controlled by outside powers. Any constrained correction of information is recognized right away.

The straightforwardness of a blockchain network prompts believability of the complete e-casting a ballot framework. In addition, the primary normal for blockchain framework, particularly open blockchain, is that its network is decentralized. Decentralized networks stay away from dependence on any focal power; choices for the all-out framework are made by a larger part of the individuals in the organization. Decentralization of blockchain organizations can forestall any conceivable defilement of all out e-casting a ballot framework made by focal specialists.

Regardless of these shortcomings, there have been many investigations to empower functional execution of homomorphic encryption. Homomorphic encryption is particularly appropriate with e-casting a ballot framework since votes can beincluded in their "scrambled" state. Since homomorphic encryption utilizes a public key to scramble information into hash numbers, encoded information can be recorded what's more, put away in a blockchain network. Homomorphic encryption guarantees protection and security while the blockchain data set ensures information trustworthiness what's more, straightforwardness. In this manner, homomorphic encryption and a blockchain network complete one another to make a fair e-casting a ballot framework

Homomorphic Encryption: is a cryptographic plan that permits specific calculations to be completed straightforwardly on cipher text, without the requirement for introductory decoding. The outcomes got from such calculations is a cipher text which when unscrambled, produces indistinguishable outcomes as when the calculations are performed on the plaintext.

Homomorphic encryption plans can be grouped into two classifications, which are; Partially Homomorphic Encryption and Fully Homomorphic Encryption. Since the e-casting a ballot framework would require just the expansion of the voting forms, a to some degree homomorphic encryption conspire is reasonable for reception in this review, because of the presentation and security it offers instead of utility usefulness

Presentation of Figures and Tables: As stated above, Figures and Tables must be embedded within the main text. They cannot be set across two columns, and must be clearly readable when viewing the manuscript at 100% zoom, or when printed. Figures and Tables must also be separated from the main text with a blank line.

II. METHODOLOGY

The framework of political race surveying is complicated and expensive. Additionally, it offers a fresh take on security, insurance protection, and political choice analysis that makes use of the ideas of web development with GPRS accessibility, cloud data limits, and encryption utilising homomorphic algorithms. Two different types of clients are involved in managing the races under this system. The chief electoral officer comes in first, followed by the booth supervisor. A booth supervisor structure that is designed with the convenience of the elector is built where the residents will be surveyed. The chief election officer will likely resign as soon as it becomes necessary to evaluate the configuration and its context for political choice.

Stall managers are the local administrators who are mindful to include the resident's specifics into the system and have a recovery framework. Voters need to proceed to the corner where the stall supervisor will inspect them and let them cast their ballots on the stall's computer while the voting system is in motion. One advantage of this framework is

1) Decentralised engineering.
2) Simple vote projection interaction.
3) Vote manipulation is essentially unthinkable.
4) Votes are organised precisely and safely in the cloud in a transparent manner.

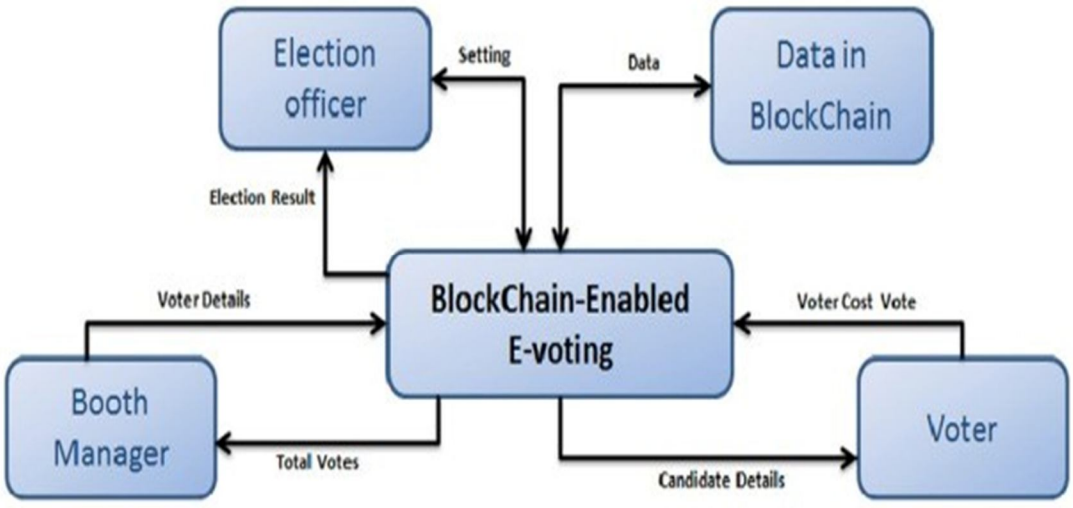


Figure 1: The roadmap of e-voting system

The chief electoral officer will be in a position to add to, remove from, or modify the political race area list. Details about a candidate, such as name, party, age, and location, may be checked, validated, altered, added, or removed. Additionally, it goes without saying that even the minute details of the slowdown, such as the reference number, location, and the slowdown in-charge, should be made clear or changed. The chief electoral officer has the authority and the secret code to decipher the specific votes of each candidate from various slow down and declare the winner of the political race in each region. The booth supervisor will have information on his stall, including the reference number, the size of the stall, the number of candidates running for office, and the total number of voters who are expected to cast a ballot in his area. He is in a position to see the complexities of local residents who interact with his corner. Any elector on the rundown may be added or removed by him.

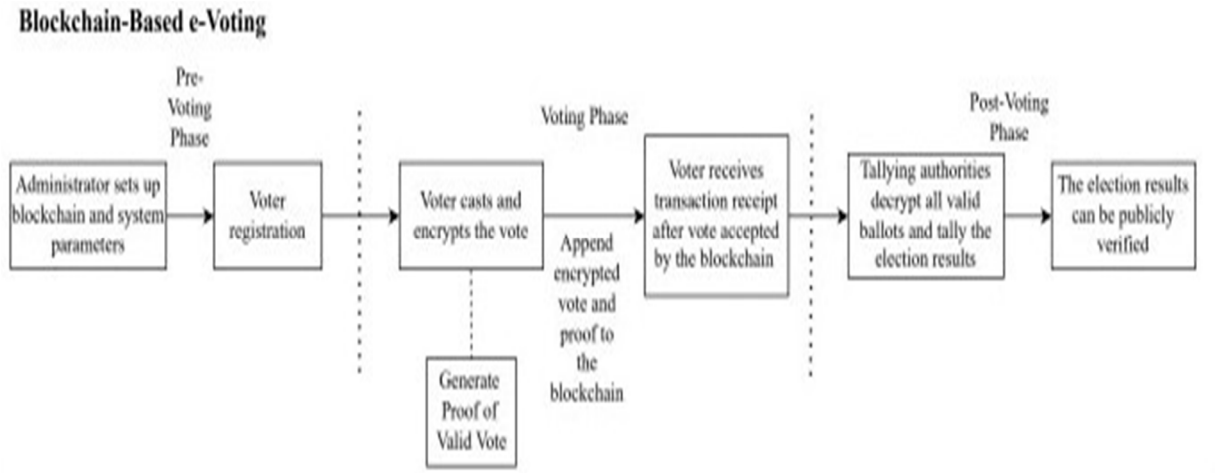


Figure 2: The pictorial representation of phases of voting system

If a citizen has chosen his decision and has a valid voter ID, he is allowed to cast a ballot. This happens when the stall administrator is assisting. After casting a vote, the booth supervisor can view the total votes, indirectly addressing the total number of respondents, but the individual votes for each candidate can be viewed in the scrambled configuration. making a vote Interaction: According to the stall, citizen nuances ought to be seen. No matter where the citizen is located or if a poll has been conducted, his character must be accepted. He can make his decision because he hasn't yet cast a ballot.

This vote will be mixed up, added to the particular candidate for whom he or she cast a ballot, and this information will be stored. A voting form projection pattern has been established. Once more, homomorphic encryption will be used to shuffle and mix all of the encoded votes. The votes first enter his qualifications and receive an OTP welcome to his registered email address, after which he continues to get checked to vote. Once the client has the right to vote, he is allowed to vote in secret while being observed by officials, and after that it will continue to count and display the desired results. Homomorphic Cryptography Security is crucial when using a homomorphic approach in web frameworks and apps.

The vast amount of information transmitted on the Web makes it susceptible to security threats and assaults. By using a shared key, cryptography enables secure exchange of mixed data. Data security is a major concern with this method since anybody with the key may access the data. When data is sent to the cloud, the client loses control over it in the expansion Any exercises should be played out using the client's key. The movement is then played out when the data has been downloaded and decrypted. These processes result in recurrent encryption translation and security problems. In this context, homomorphic encryption is the best choice. The ability to decipher ciphertext is granted to clients using homomorphic encryption.

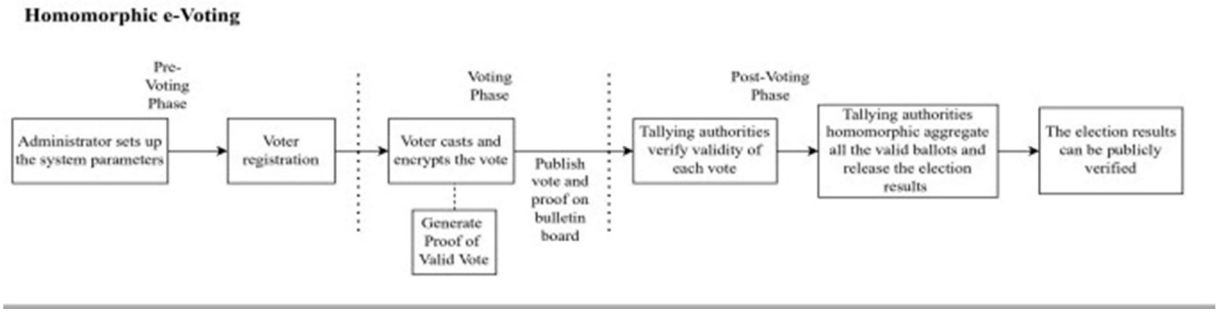


Figure 3: The pictorial representation of phases of Homomorphic Encryptiom

The greatest benefit of utilizing homomorphic encryption is that the counting methodology is extremely straight forward. Moreover, one more benefit over blend net-based casting a ballot plan is just the votes can becounted before every one of the votes have been projected without losing any security properties.

The plans in light of homomorphic encryption use homomorphic techniques to encode the votes. Then, at that point, the citizen sends his vote through open channel. To get the amount of the votes, specialists basically duplicate the votes

III. RESULTS

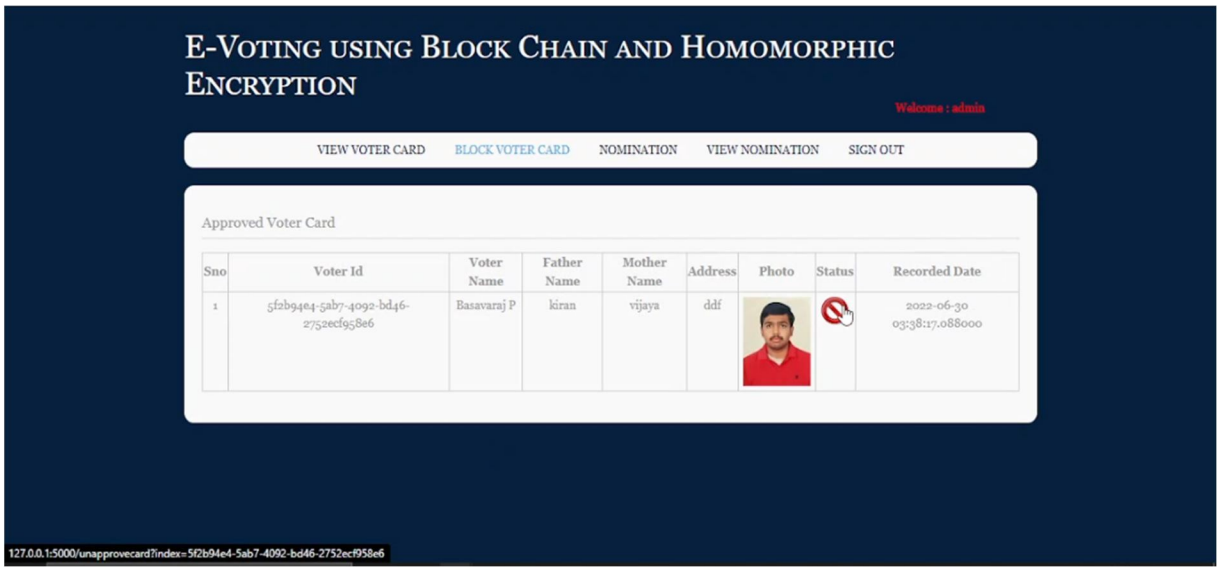


Figure 4: The pictorial representation of phases of blocking a voter

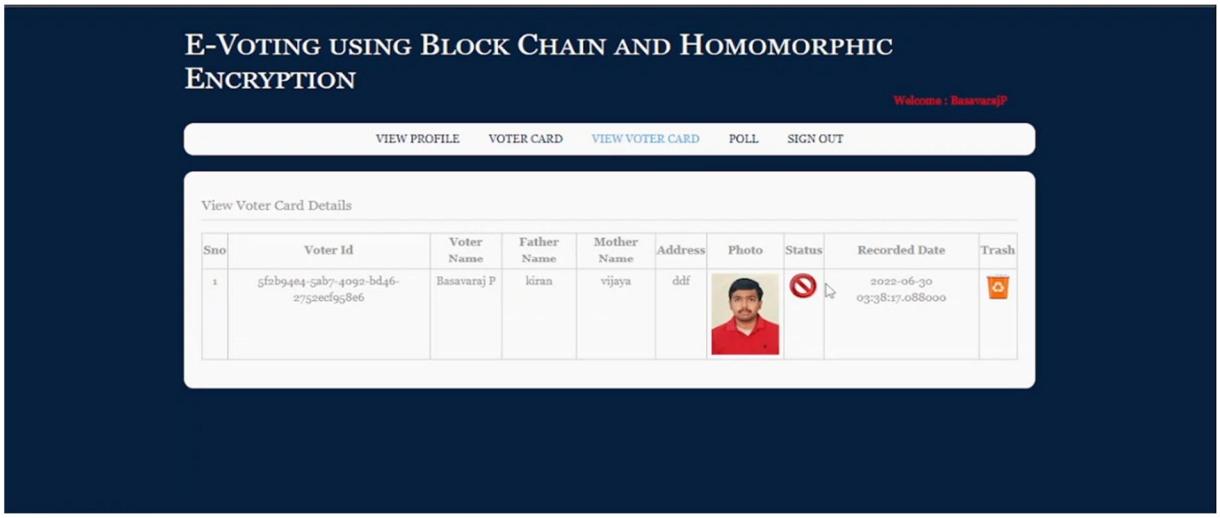


Figure 5: The pictorial representation of deleting a voter's Details

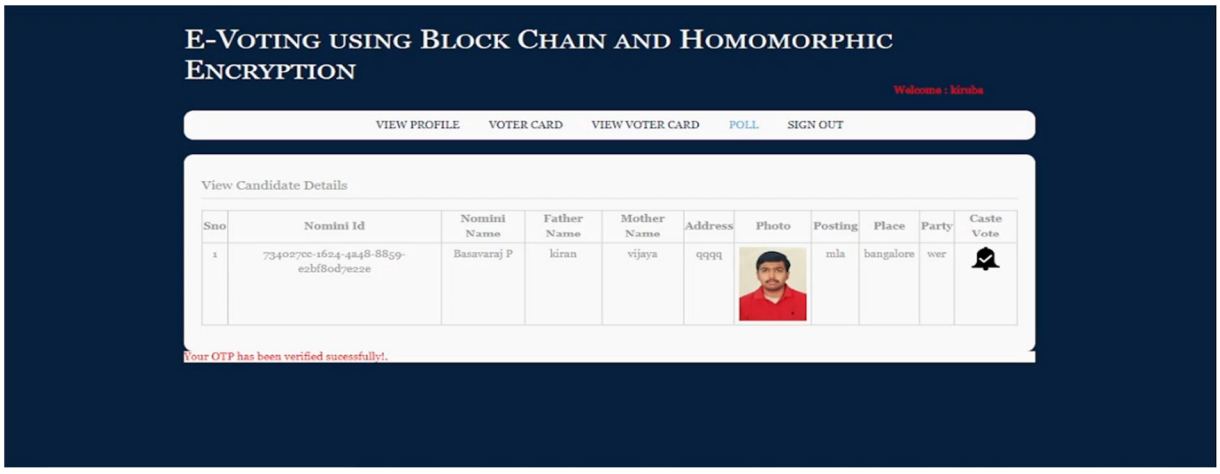


Figure 6: The pictorial representation of phases of casting a vote

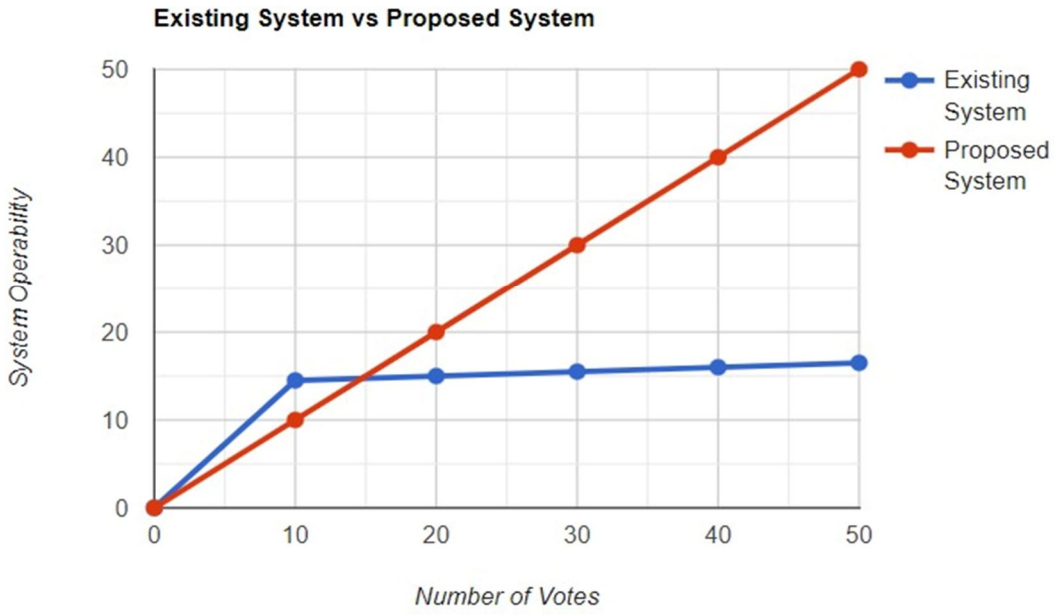


Figure 7: Graph

From Figure 4 we can see the process of blocking a voter from voting in an election. This process can be carried out the booth manager who is responsible for counting the number of votes and verifying the voter details of voter. Similarly we can see in Figure 5 the process of deleting a voter's details if they fail the verification process which is conducted by the booth manager. Figure 6 illustrates the process of a voter casting a vote through the Blockchain E-voting system.

As Shown in Figure 7 the traditional ballot system has a stagnant voters growth with low system operability which made the whole process more time consuming but with the proposed system as shown in the above paper provides a higher voter growth as the system is easily deployable and user friendly and allows maximum voter to cast the votes from the comfort of there home and also the proposed system is highly secure which increases the voter trust in the election process.

IV. CHALLENGES

Security in online election is a challenging task. Authenticating the voter is a major challenge along with the privacy of the vote. We have considered manual authentication and proposed a modification to the existing voting scheme which uses electronic voting machine. The voting machines are not reliable and also in certain situations where the number of candidates is more, more than one voting machine needs to be connected. The proposed scheme is cost effective and also reliable.

Building a framework according to the plan detail isn't in many cases straight-forward. As the security necessities are complicated, the cryptographic convention configuration is additionally intricate. The intricacy is then moved to the advancement stage, and the complexity made it challenging to impeccably execute a framework as indicated by its plan. Besides, there are trust issues to casting a ballot. Inept developer can present programming bugs in their program, or even make a broken one. Degenerate designer/seller can intentionally put a secondary passage to casting a ballot programming to later control casting a ballot result. A conspicuous arrangement is to utilize a confided in designer/seller to construct a protected democratic framework as per the safe plan. In any case, even a decent software engineer can coincidentally present programming bugs in the program. Likewise, it is powerless to gauge security of a framework by the reliability of the designer/seller. A superior technique to guarantee the security of a framework is by following best practice in the advancement cycle.

Electronic frameworks possibly permit enormous scope imperceptible fraud. In reality, fraud in manual frameworks restricted by necessity to create or discard paper, which is very difficult to do imperceptibly in presence of TV cameras

Protocol complexity an obstacle to public confidence – Public confidence is the most important part of an election system.

V. CONCLUSION

Here we are implementing a unique blockchain-based electronic voting system that uses homomorphic encryption to enable secure and cost-effective elections while maintaining voter privacy. Compared to previous work, we have shown that blockchain technology offers democratic countries a new way to move from the paper-and-pencil voting system to a more cost- and time-efficient voting system, while increasing the security of the current system and offering new opportunities of transparency. Electronic voting is still a controversial topic in politics and science. Despite the existence of some very good examples, most of which are still in use; Many other attempts failed to provide the security and privacy features of a traditional solution, or had serious usability and scalability issues. In contrast, blockchain-based electronic voting solutions, including the homomorphic encryption and Cassandra database we've implemented, address (or can address with relevant modifications) almost all security concerns, such as rejection of votes and transparency of counting. However, there are also some properties that cannot be addressed with blockchain alone, for example, voter authentication (at the personal level, not at the account level) requires additional integration mechanisms , such as the use of biometric factors.Blockchain technology shows great promise, but in its current state requires much more research and may not be reaching its full potential at this time. A concerted effort is needed in the core blockchain technology to improve its support for more complex applications and make it more user-friendly and efficient.

REFERENCES

[1] H. S. Govinda, Y. Chandrakant, D. S. Girish, S. Lokesh, Ravikiran and B. S. Jayasri, "Implementation of Election System Using Blockchain Technology," 2021 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), 2021, pp. 1-9, doi: 10.1109/ICSES52305.2021.9633828.

[2] Lahane, Anita & Patel, Junaid & Pathan, Talif & Potdar, Prathmesh. “Blockchain technology based e-voting system”. ITM Web of Conferences, 2020 Doi: 32. 03001. 10.1051/itmconf/20203203001.

[3] S. K. Vivek, R. S. Yashank, Y. Prashanth, N. Yashas and M. Namratha, "E-Voting Systems using Blockchain: An Exploratory Literature Survey," 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), 2020, pp. 890-895, doi: 10.1109/ICIRCA48905.2020.9183185.

[4] Kaudare, M. Hazra, A. Shelar and M. Sabnis, "Implementing Electronic Voting System With Blockchain Technology," 2020 International Conference for Emerging Technology (INCET), 2020, pp. 1-9, doi: 10.1109/INCET49848.2020.9154116.

[5] C. Sravani, G Murali, “Secure Electronic Voting using BlockChain and Homomorphic Encryption” International Journal of Recent Technology and Engineering (IJRTE), September 2019, ISSN: 2277-3878,Volume-8, Issue-2S11

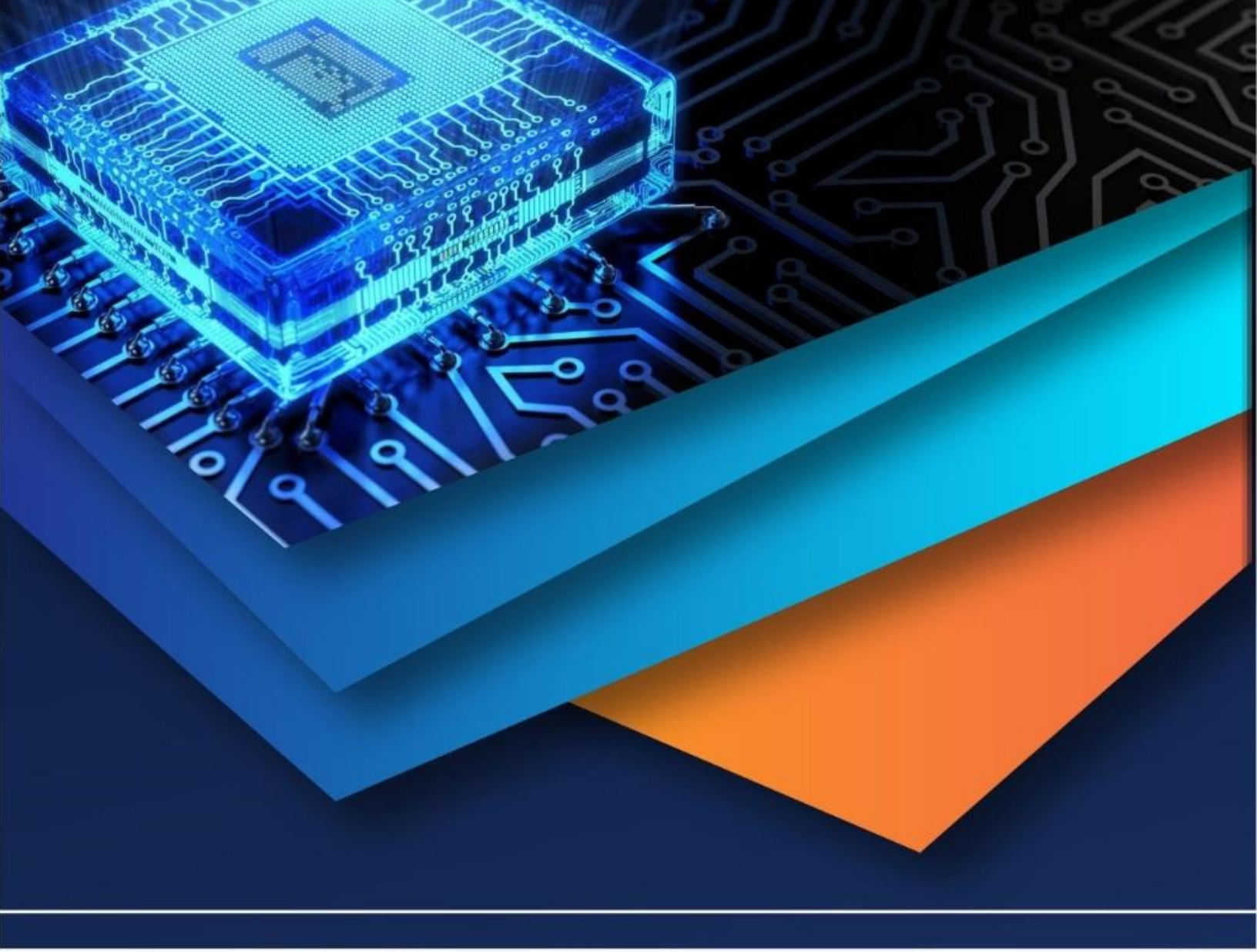
[6] Pandey, M. Bhasi and K. Chandrasekaran, "VoteChain: A Blockchain Based E-Voting System," 2019 Global Conference for Advancement in Technology (GCAT), 2019, pp. 1-4, doi: 10.1109/GCAT47503.2019.8978295.

[7] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," in IEEE Access, vol. 7, pp. 24477-24488, 2019, doi: 10.1109/ACCESS.2019.2895670.

[8] K. Teja, M. Shravani, C. Y. Simha and M. R. Kounte, "Secured voting through Blockchain technology," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1416-1419, doi: 10.1109/ICOEI.2019.8862743.

[9] K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944820.

[10] E. Bellini, P. Ceravolo and E. Damiani, "Blockchain-Based E-Vote-as-a-Service," 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), 2019, pp. 484-486, doi: 10.1109/CLOUD.2019.00085.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY