iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** V **Month of publication:** May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5401

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: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

BlockChain Enabled Secure E-Voting System

Sumana C[1], Prof. G. Anitha[2]
[1, 2]*Department of computer science and engineering, UBTCE*

Abstract: ***E-VOTING is among the key public sectors that can be disrupted by blockchain technology. The idea in blockchain-enabled e-voting (BEV) is simple. To utilise a digital-currency analogy, BEV issues each voter a "wallet" containing a user credential. A manual voting process is excessively time-consuming and takes a lot of steps to finish the vote. With rapid development of information technology, an electronic voting system (E-voting system) is more convenient to vote for someone from a list of candidates shown on a computer screen. However, security is a big concern for electronic voting. In this paper, we build a secure voting system using Paillier homomorphic encryption. Paillier homomorphic encryption is a kind of public key cryptography that has the homomorphic property that can be exploited to calculate the sum of votes without revealing to the system which vote is voted for which candidate. The voting system design has a simple interface that clients can use easily. Here, we contend that blockchain may address two of the most predominant worries in casting a ballot today: voter access and voter extortion. The thought is as per the following. Qualified voters cast a vote namelessly utilizing a PC or cell phone.BEV employs an encrypted key and tamperproof personal IDs. For instance, the mobile e-voting platform of the Boston-based startup Voatz employs smart biometrics and real-time ID verification. In this paper, we highlight some BEV implementations and the challenges.***

Keywords: Block chain, E-voting, Homomorphic Encryption.

I. INTRODUCTION

"E-voting" is a term that is portrayed in various information and communication technologies (ICT) stages: Internet frameworks, surveying corner machines, and phone casting a ballot framework. Every stage has both negative and positive highlights. Be that as it may, the Internet voting frameworks are most prevalent and effective today. Every voter can vote in favour of competitors remotely through the Internet. Voters can undoubtedly open sites, programming, or applications on their PCs or cell phones to cast a ballot whenever, anyplace. In any case, their casting a vote framework can be assaulted on the off chance that it doesn't have any algorithm or convention to ensure it. Assailants can get parcels that voters exchange on the Internet effectively; they change data and send to the casting a vote server. Moreover, they can intrude on votes which voters send over the Internet. As needs be, scientists are contemplating techniques to guard against such assaults utilizing cryptography calculations to encode information a vote before sending it to the server. Here we utilized the homomorphic properties of Paillier Encryption to ensure a vote sent over the Internet.

In each majority rules system, the security of a decision involves national security. The PC security field has for 10 years concentrated the potential outcomes of electronic voting frameworks [1], with the objective of limiting the expense of having a national election, while satisfying and expanding the security states of a race. From the beginning of equitably choosing hopefuls, the vote casting framework has been founded on pen and paper. Supplanting the customary pen and paper conspire with another race framework is basic to restrict misrepresentation and having the voting procedure recognizable and obvious [2]. Electronic voting machines have been seen as imperfect, by the security network, fundamentally dependent on physical security concerns. Anybody with physical access to such machine can undermine the machine, in this way influencing all votes cast on the previously mentioned machine. Enter square chain innovation.

A blockchain is an appropriated, changeless, undeniable, open record.

The blockchain innovation may address numerous issues with respect to e-voting plans and make e-voting less expensive, simpler, and significantly more secure to execute. It is an impressively new worldview that can frame decentralized frameworks, which guarantee the information respectability, accessibility, and adaptation to non-critical failure. Some express that "the blockchain innovation is presenting to us the Internet of significant worth: new, disseminated stages that can enable us to reshape the universe of business and change the old request of human issues to improve things." This innovation plans to upset the frameworks. The blockchain frameworks are shaped as decentralized arranged frameworks of PCs, which are utilized for approving and recording the unadulterated online exchanges.

They additionally establish records, where computerized information is attached to one another, called the blockchain. The records on the blockchains are basically permanent.

A. Existing System

Electronic voting (also called e-voting) alludes to casting a ballot utilizing electronic intends to either help or deal with the errands tallying and casting votes. Contingent upon the specific usage, e-voting may utilize independent electronic voting machines (additionally called EVM) or PCs associated with the Internet. It might include a scope of Internet administrations, from fundamental transmission of classified outcomes to full-work web based voting through normal connectable family devices. The level of mechanization might be restricted to denoting a paper poll, or might be an exhaustive arrangement of vote input, vote recording, information encryption and transmission to servers, and union and organization of race results. A commendable e-casting a ballot framework must perform the majority of these undertakings while consenting to a lot of measures set up by administrative bodies, and should likewise be fit to manage solid necessities related with security, exactness, respectability, quickness, protection, review capacity, openness, cost-adequacy, versatility and natural supportability. The vast majority of the ongoing work discusses security, exactness, respectability, quickness, protection, and review capacity however existing frameworks are powerless for assaults at some degree.

B. Disadvantages of Existing System

1) Centralized architecture.
2) Attack prone.
3) Not trustable.
4) Non-transparent vote casting process.

C. Problem Statement

The current method needs an attacker to connect particularly with the voting procedure to aggravate it. On the other end, internet is more enthusiastically to control and manage the security as network and web related attacks are more diligently to pursue.

D. Proposed system

Election Polling is a complex system as well as costly system. Here we are presenting a novel Secure, Privacy Preserving and cost effective election polling concept which uses Web Technology with Homomorpic encryption. This system has two types of users one is Election Officer & another is Booth Manager, Booth Manager System developed with voter's functionality where voters are going to poll. Election officer will act as an admin user and he has to do the setting and configuration setting for election polling. Booth Managers are the area manages those who are responsible to add the voters details into the system and has retrieval system by which they can able to view the voted candidate details and sum of the votes. Voters have to go the Booth where the Booth manager verify the voter and allow him to poll on the Booth's Laptop where our voting system is running. This proposed system has a method to execute operations on encrypted data without decrypting them which will provide us with the same results after calculations as if we have worked directly on the raw data.

E. Advantage of Proposed System

1) Decentralized architecture.
2) Transparent vote casting process.
3) Manipulations of votes are nearly impossible.
4) Votes are recorded accurately, permanently, securely, and transparently.

F. Motivation for the electronic voting system

E-voting is the most helpful to cast vote. It is fantastic on uniformity, constructing a trust in constituent association, adding unwavering quality to decision results, and expanding the general effectiveness of the surveying procedure. In any case, to construct an E-voting framework that can work flawlessly over the Internet is a major test. Two noteworthy difficulties that can be considered are security and supporting an enormous number of voters. Most E-voting arrangements can't work with enormous number of voters. E-voting additionally faces security issues since voters vote and sends their votes over the Internet which is definitely not a controlled domain. What's more, casting a ballot under an electronic casting a ballot framework happens naturally with no human supervision. Positively, voters might want to cast a ballot by paper cast a ballot at a mail station or surveying station instead of through an E-voting framework since they don't confide in the E-voting as their tickets are exchanged over the Internet. For instance, in 2012, the national government permitted to utilize the E-voting in favour of Canton of Zurich voters. The 6 voters had

three alternatives to cast a ballot: tally voting, postal voting, and Internet casting a ballot. Be that as it may, just 20 percent of the votes were thrown through the Internet voting. To address a portion of these difficulties, in this undertaking, we have built up an E-voting framework that can permit an enormous number of voters. In particular, Paillier calculation is utilized to help countless voters and secure a vote when it is checked.

G. Challenges

Governments and different partners should address a few noteworthy difficulties before blockchains see far reaching use for e-voting. Despite the fact that blockchains are great at giving security and exactness, open certainty and trust are fundamental elements for BEV's prosperity. Blockchains' multifaceted nature may prevent standard open agreeableness of BEV [3]. Broadband access and advanced client abilities are additionally concerns. In 2016, the non-benefit Democracy Earth Foundation utilized a blockchain to give Colombian exiles a voice in the 2016 harmony plebiscite that was directed to confirm the consent to end the contention between the Colombian government and FARC guerrillas [4]. As indicated by the establishment, a primary test in the arrangement blockchain is the innovation's youthfulness. We should now think about programming quality. Evaluations have recommended that, overall, there are from 15 to 50 absconds per 1,000 LOC.29 For Ethereum, the blockchain-based circulated registering stage utilized by Moscow's Active Citizen Program (which highlights shrewd contracts), the number may be twice that. This may be ascribed to Ethereum's adolescence. The Economist cited a blogger who said that Ethereum contracts are "treat for hackers."[5] Also, adequate perceptions haven't yet been amassed to decide blockchain-based stages' adaptability.

II. LITERATURE SURVEY

A. Anonymous voting by two-round public discussion projected an expansion of a self-counting capacity to the 2-Round Anonymous Veto Protocol (called AV-net). The AV-net gave remarkable proficiency contrasted with related procedures, it was centered on the feasting cryptographers arrange (DC-net) and its shortcomings and proposed the AV-net as another approach to handle that issue. The new convention, similar to the AV-net requires no confided in outsider or private channel. Members execute the convention by sending two-round open messages, however are fundamentally progressively proficient as far as the quantity of rounds, computational expense and data transfer capacity use [6].

B. A Smart Contract For Boardroom Voting with Maximum Voter Privacy, projected the primary execution of a decentralized and self-counting web casting a ballot convention with greatest voter security utilizing the Blockchain, called The Open Vote Network (OVN). The OVN is composed as a savvy contract for the Ethereum blockchain. In its general thought the OVN is a usage of the Anonymous casting a ballot by two-round open. The makers of the OVN arrived at the resolution subsequent to executing the framework, that the expense of running such framework on the Ethereum blockchain was 0.73$ per voter. The protected furthest point of confinement of voters was 50 voters, yet the expense could be viewed as sensible as it gave most extreme voter security and is freely unquestionable. The restriction of number of voters was prescribed as a result of as far as possible on the open Ethereum blockchain. [7].

C. A Secure and Optimally efficient Multi-Authority Election Scheme, projected a multi-specialist mystery ticket race conspire which would ensure protection, all inclusive unquestionable status and strength, where voters would take an interest utilizing a PC, where the principle thought is the exertion expected of Voter. In this model, voters make their choice by presenting polls on a release board. The release board fills in as a communicate channel with memory to the degree that any gathering can get to its substance however no gathering can eradicate anything from the announcement board. The ticket does not uncover any data on the vote itself but rather is guaranteed by a going with verification that the poll contains a substantial vote. The last count, the total everything being equal, which happens when the due date is come to, would then be able to be gotten and confirmed, by any eyewitness, against the result of all submitted tickets. This would guarantee general evidence, due to the homomorphic properties of the encryption technique utilized [8].

D. Netvote is a decentralized blockchain-put together casting votes coordinate with respect to the Ethereum blockchain. Netvote uses decentralized applications for the UI of the framework. The Admin dApp enables race managers to set decision strategies, make polls, build up enlistment guidelines and open and close casting a ballot. The Voter dApp is utilized by individual voters for enlistment, casting a ballot and can be coordinated with different gadgets, (for example, biometric perusers) for voter recognizable proof. The Tally dApp is then used to count and confirm decision results. Netvote bolsters three sorts of races:

1) Open Election: Anyone may vote

2) Token-Holder Elections: Only voters who operate accounts that have a balance of a designated compliant token may vote [9].

3) Private Election: Only authenticated and authorized individuals may vote.

E. Agora is a start to finish undeniable blockchain based casting a ballot arrangement intended for governments and foundations. Public square uses their very own Token on the blockchain for races, where governments and establishments buy these tokens for every individual qualified voter. This casting a ballot framework is a multi-layer engineering which incorporates the blockchain, called the Bulletin Board, which depends on the Skipchain design. The information on the Bulletin Board is cryptographically attached to the Bitcoin blockchain through the Cotena layer, which gives an abnormal state of unchanging nature and decentralization of the information. The Bulletin Board uses permissioned aggregate expert hubs, which affirm exchanges, where every hub in the system keeps up a duplicate all things considered and favors them into squares as a feature of the systems agreement component [10].

III.METHODOLOGY

The Module Distrciptions of the methodology is as follows:

1) *Electoral dist. Maintenance:* Election officer has the authority to add, delete or edit the election district list. Candidate details like name, age, party, district can checked, edited, added or deleted. Likewise even the booth details like the reference number, district and the booth manager in-charge can be seen or edited. Mainly the election officer has the authority and the secret key to decrypt the individual votes of each candidate from different booth and announce the winner of election district wise.
2) *Booth Maintenance:* Booth manager will have information about his booth regarding booth reference number, booth location, number of candidates contesting for election and total number of voters destined to vote in his booth. He has the authority to see the voter details who belong to his booth. He can add or delete any voter from the list. Voter is allowed to vote provided his voter-id is valid and cast his vote. This happens under the booth manager assistance. After voting, Booth manager can view the total number of votes, indirectly representing the total number of voters polled but individual votes per candidate can be viewed in the encrypted format.
3) *Voter Details:* Voter details have to display as per the booth.
4) *Voting Process:* In this module the process of voting is carried out. The voter's identity is to be validated, whether he belongs to his assigned booth and whether is has polled or not. Provided he hasn't already voted, he can cast his vote. This vote will be encrypted and added to the particular candidate to whom he/she has voted and this data is stored.
5) *Homomorphic Encryption:* Homomorphic encryption on data, a pailier hash function algorithm is used. It is easier and robust and also more efficient compared to other algorithms.
6) Block chain Storage: *A block chain, originally block chain, is a growing list of records, called blocks, which are linked* using cryptography.

The system Architecture is shown below in the Fig 1.

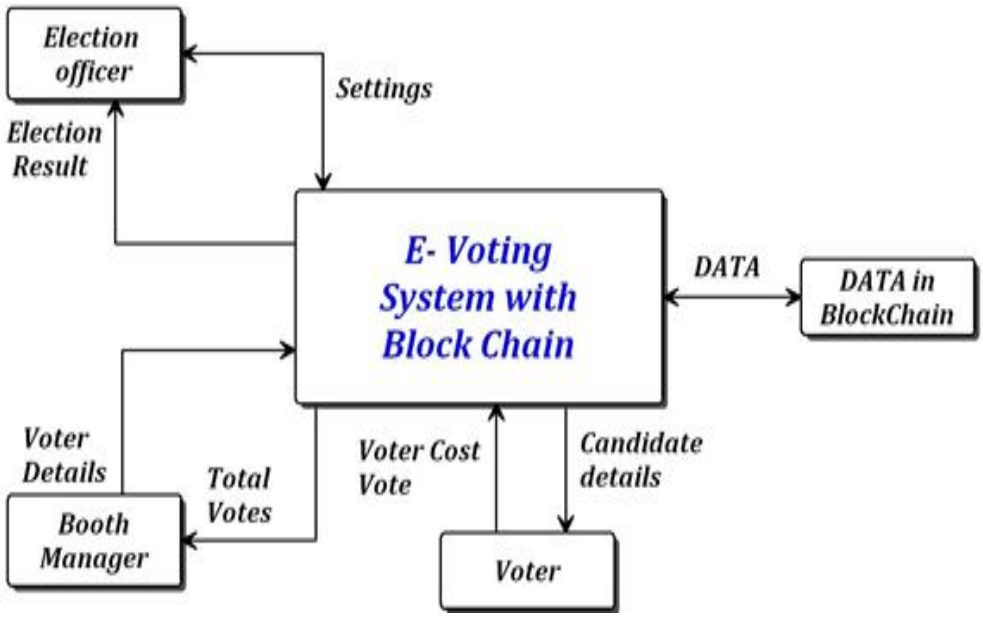


Fig .1: System Architecture

A. Algorithm

Paillier encryption is the most well-known cryptography scheme. Pascal Paillier invented it in 1999. It is more advantageous than previous schemes. Thus, it is very handy in E-voting applications. Paillier encryption also is an algorithm for public key cryptography similar to other public key cryptography schemes. Here is a detail about how Paillier algorithm works:

Key Generation Algorithm

Input: Two large primes p and q.

- Compute $n = pq$ and $\lambda = lcm\ (p\text{-}1, q\text{-}1)$
- Select a random integer g, where $g \in \mathbb{Z}^*_{n^2}$ and $gcd\ (L(g^\lambda \bmod n^2), n) = 1$

Output: (ek, pk)

The evaluation key is $\boldsymbol{ek} = (n)$ and the private key is $\boldsymbol{pk} = (n, g, \lambda)$.

Encryption Algorithm

Input: plaintext $m < n$

- Select a random integer r, where $r \in \mathbb{Z}^*_{n^2}$ and $gcd\ (r, n) = 1$
- Compute $c = g^m \times r^n \bmod n^2$

Output: $c = E\ (pk, m)$

Decryption Algorithm

Input: ciphertext $c < n^2$

- Compute $m = \dfrac{L\ (c^\lambda \bmod n^2)}{L\ (g^\lambda \bmod n^2)} \bmod n$ where, $L(u) = \dfrac{u-1}{n}$

Output: plaintext $m = D\ (pk, c)$

IV. EXPERIMENTAL RESULTS

The results of the E-voting system are shown below.

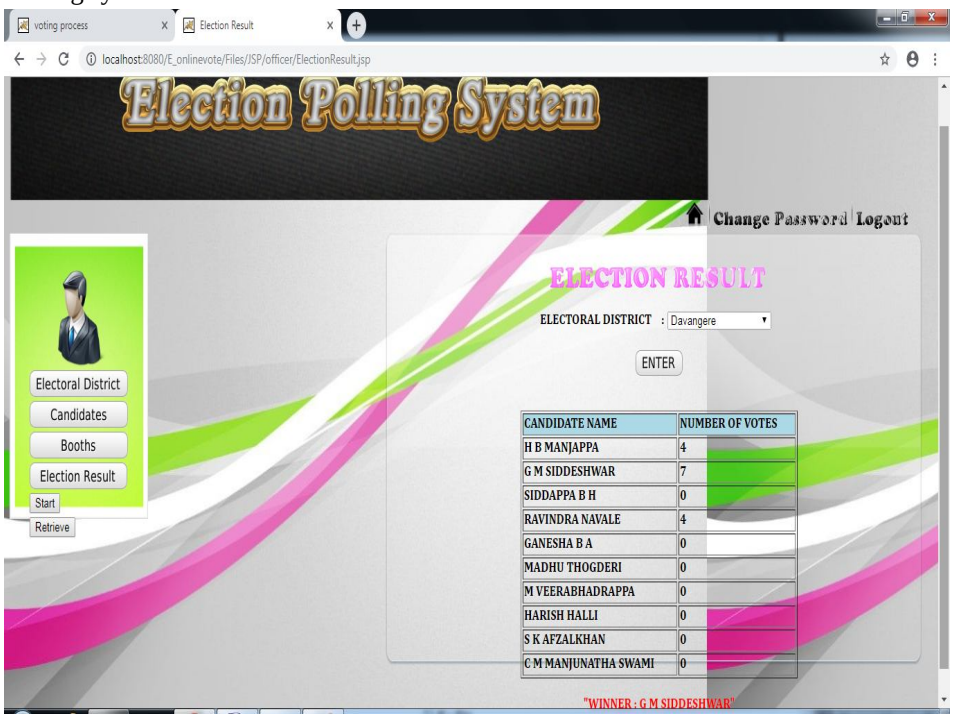


Fig 2: The Results of Election Polling Process

In Fig 2, the Election result among various candidates is displayed.

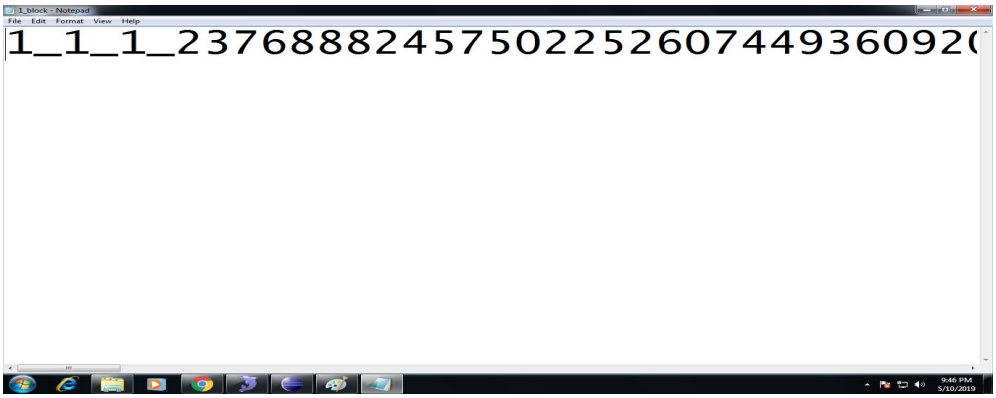


Fig 3: Votes are stored as Block Chain

In Fig 3, the votes are stored as blocks in the block chain server.

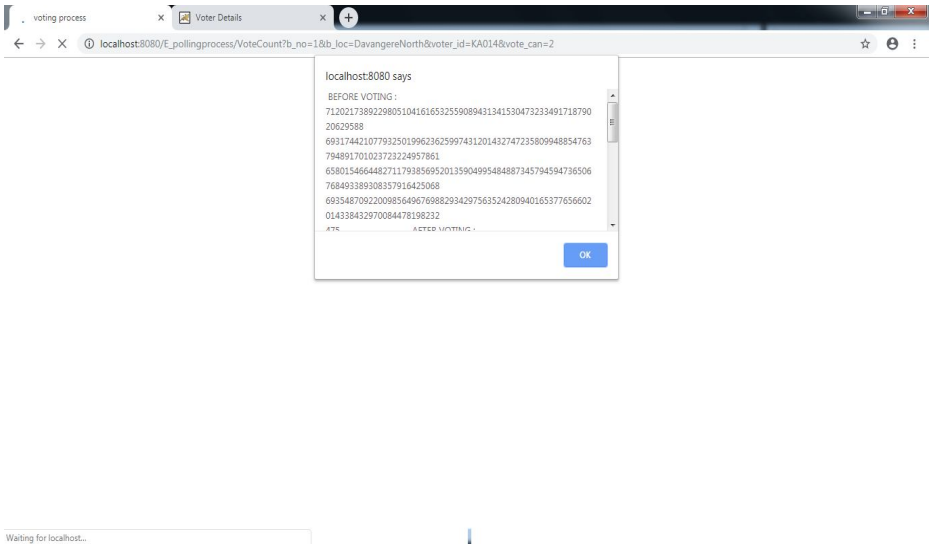


Fig 4: Voters details and votes are encrypting using Homomorphic Encryption

In Fig 4, Voter details such as voter ID, name and their casted votes are encrypted using Homomorphic Encryption Scheme.

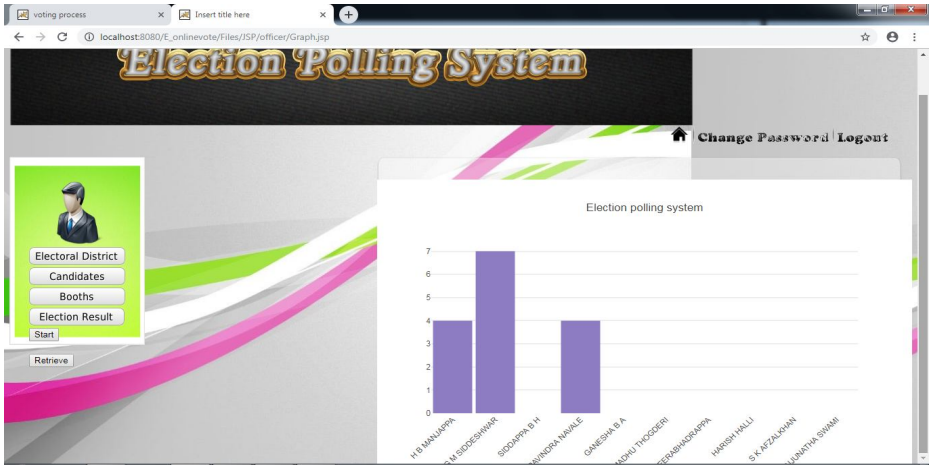


Fig 5: Graph of Election polling system

In Fig 5, the graph of the Election process is displayed.

IV. CONCLUSION

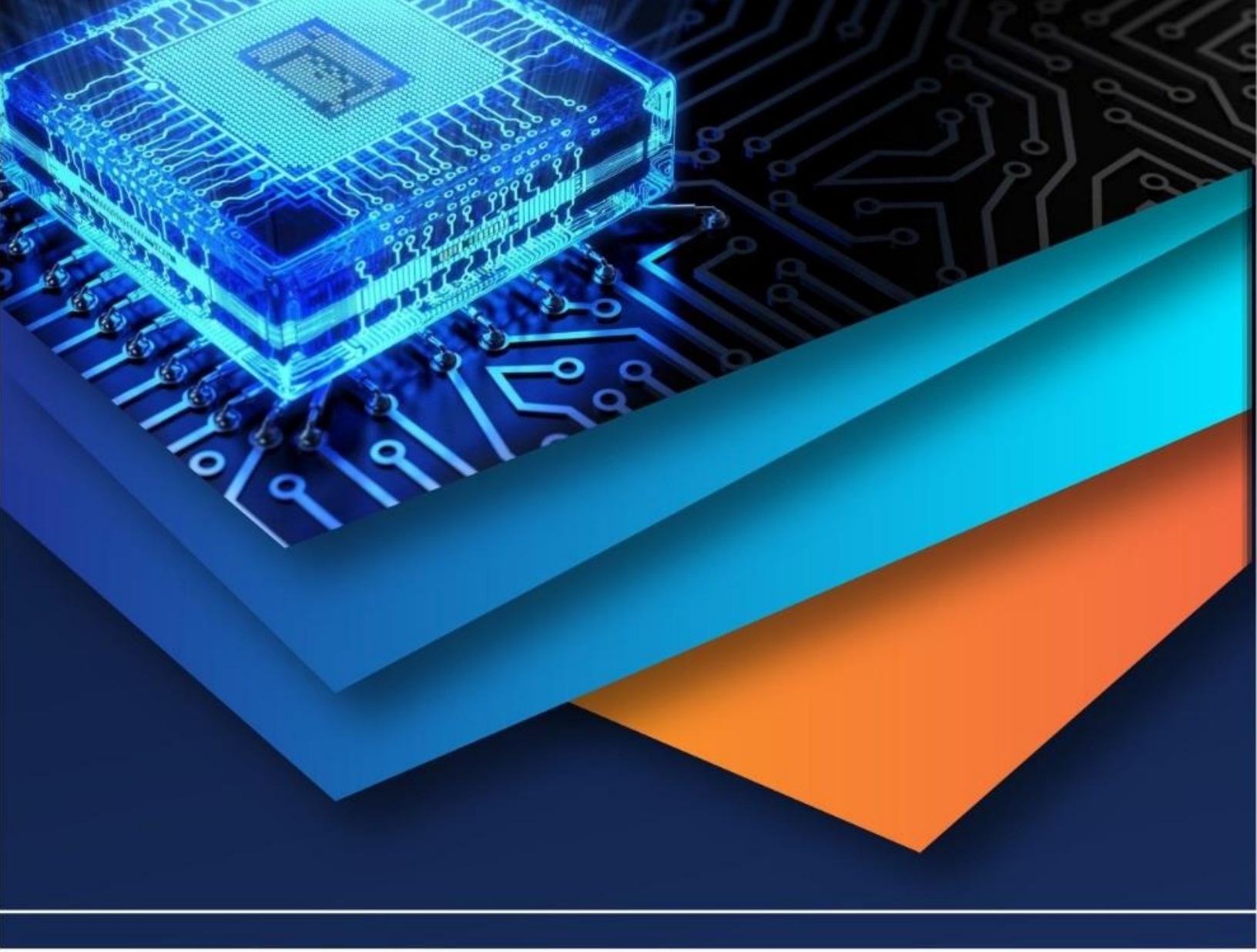
The idea of adapting computerized voting frameworks to make the open appointive procedure less expensive, quicker and simpler, is a convincing one in current society. Making the appointive procedure cheap and snappy, standardizes it according to the voters, evacuates a specific power obstruction between the voter and the chosen authority and puts a specific measure of weight on the chosen authority. It additionally opens the entryway for a more straightforward type of majority rule government, enabling voters to express their will on individual bills and suggestions.

V. FUTURE ENHANCEMENT

Applications to cast a ballot from cell phones can be assembled. There are two stages should have been considered to create them: Android and iOS. Appropriately, voters should download the casting a ballot application and introduce to their cell phones, at that point they will most likely vote. It is substantially more helpful in light of the fact that at the present, the vast majority use cell phones. All techniques ought to be bolstered to build up an expert E-voting framework for such stages.

REFERENCES

[1] Sos.ca.gov. (2007). Top-to-Bottom Review | California Secretary of State. Available at: http://www.sos.ca.gov/ elections/ voting-systems/oversight/ top-bottom-review/.
[2] Nicholas Weaver. (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/secure-vote-today.
[3] P. Boucher, *What If Blockchain Technology Revolutionised Voting?*, European Parliamentary Research Service, 2016; http://www.europarl .europa.eu/thinktank/en/document .html?reference5EPRS_ATA (2016)581918.
[4] C. van Ooijen, "How Blockchain Can Change Voting: The Colombian Peace Plebiscite," Forum Network, 20 Dec. 2017; https://www.oecd -forum.org/users/76644-charlotte -van-ooijen/posts/28703-how -blockchain-can-change-voting-the -colombian-peace plebiscite.
[5] "Not-So-Clever Contracts," *Economist*, 28 July 2016; https://www .economist.com/news/business /21702758-time-being-least-human -judgment-still-better-bet-cold-hearted.
[6] Feng Hao, P.Y.A. Ryan and Piotr Zielinski. Anonymous voting by two-round public discussion. 2018.
[7] Patrick McCorry, Siamak F. Shahandashti and Feng Hao. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. Available at: https://eprint.iacr.org/2017/110.pdf.
[8] Ronald Cramer, Rosario Gennaro and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme
[9] Agora: Bringing our voting systems into the 21st century.2017
[10] Ethereum Blog.On Public and Private Blockchains-Ethereum Blog. Available at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/2018



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY