International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

E-Voting Based Blockchain Mechanism Using Feature Selection Based Machine Learning

[1]Mr. T. Prabakar, [2]Dr. S. Kanchana

Submitted: 21/12/2023 **Revised**: 27/01/2024 **Accepted**: 09/02/2024

Abstract: The issue of scalability in e-voting system is typically circumvented by the utilization at majority of the time. These components are capable of operating without needing one another in order to function, and they are even able to keep their own records independently of one another. In this paper, we develop an intelligent E-voting system that uses machine learning algorithm for feature selection to generate the QR codes. The aim is to improve the security of the QR based on features by optimal selection of features. The QR code with other registered details is stored in database via proper blockchain authentication mechanism. The simulation is conducted in python to test the efficacy of the model against various other methods and the results of simulation shows that the proposed method has a reduced computational complexity and increased accuracy on feature selection than other existing E-voting mechanisms.

Keywords*: E-Voting, Blockchain, Machine Learning, Feature Selection*

1. Introduction

Every single citizen in a democracy is given the right to cast a ballot in democratic elections. It is imperative that the right to vote be protected, and the use of paper ballots is commonly regarded as the one and only technique that may credibly meet the requirements of this responsibility [1]. However, with this technique, there is possibility for both error and misuse. Neither of these outcomes is desirable. It is remarkable to contemplate how far technology has progressed to the point where current voters exercise their duty [2]. It is remarkable to consider how far technology has come, especially in light of the fact that voting is a fundamental democratic right and obligation. Voting is a basic democratic right as well as a democratic obligation.

In today society, illegitimate voting in the form of manipulating absentee ballots cast from a distance and other types of fraudulent electronic voting are commonplace. Previous research has shown that it is possible to influence the results of elections by taking advantage of the weaknesses that are inherent to the use of centralized ballot storage in electronic voting systems. This has been proved both experimentally and theoretically. There is a chance that the electorate will react with a level of dissatisfaction that is cataclysmic [3].

Similarly, utilizing blockchain technology in electronic voting systems makes it possible to trace and audit every vote in real time, which was difficult to achieve with prior voting techniques [4]. Electronic voting systems that make use of blockchain technology are starting to gain momentum, and this has led to the formation of a new line of inquiry [5–7]. These networks, in the opinion of a number of industry professionals, are able to be easily expanded, offer access to the general public, and can be independently checked. However, because there are no actual system structures to research, it is difficult to determine whether or not these systems in fact exhibit the features that have been asserted about them. This is because there are no actual system structures to study [8].

Decentralized voting systems with autonomous voting capabilities have the ability to eliminate as many human effects as is practically achievable, and many significant pieces of research have recommended the use of smart contracts as a means to achieve this goal. In a previous studies[9-11], we focused on a few recent developments that dealt with the privacy and safety difficulties of an electronic voting system that was based on blockchain technology. These innovations dealt with the problems in a way that was both innovative and practical. These advancements include things like:

A blockchain cannot be hacked in real time and cannot alter what has already occurred in the past. This makes

[1]M.Sc., M.Phil., Research Scholar,Department of Computer Science, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India - 603203
E-mail: patprabakar@gmail.com
ORCID ID: 0009-0009-7963-0243
[2]PhD, Assistant Professor, Department of Computer Science, Faculty of Science and Humanities, SRM Institute of Science and Technology,Kattankulathur, Tamil Nadu, India – 603203 Corresponding Author:
E-mail: kanchans@srmist.edu.in
ORCID ID: 0009-0003-5295-3903
**Correspondence of the manuscript addressed to: S. Kanchana, Assistant Professor, Department of Computer Science, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India-603203. Email:kanchans@srmist.edu.in*
E-Voting Based Blockchain Mechanism Using Feature Selection Based Machine Learning

blockchains extremely secure. In addition, the system does not let any changes to be made to the way it works in any way. During the voting process, all permitted devices and nodes display the same outcomes, and ballots may be tracked back to the point where they were first cast without the details of individual voters being disclosed. It is generally accepted that the creation of Bitcoin [12] was the turning point that started the revolution that is blockchain technology. Bitcoin was the very first digital currency ever established, and it is still the digital currency that the majority of people across the world want to use.

In addition, in order to solve a puzzle that needs a considerable amount of processing power in order to guarantee consistency each time a new block is formed and attached to the block that came before it [13], a specific method that is necessary that is known as Proof-of-Work (PoW). On the other hand, PoW is inefficient when it comes to the amount of energy that it consumes. Additionally, it has an effect on the throughput and the transaction delay, both of which, in turn, have an effect on scalability [14]. PoS, is an alternative to Proof of Work that has emerged as a viable option since it is able to circumvent the issues that PoW. To be more specific, the Proof-of-Stake (PoS) consensus process requires a group of validators to vote on the next block. The voting weight is determined by the value of the tokens that have been staked, so the more tokens that are staked, the more weight each vote receives. In addition to Proof of Work (PoW), Proof of Stake (PoS) gives the network a large financial boost, which enables it to operate effectively and minimizes the risk that it will be the target of a plot or an attack. In contrast to PoW, however, it does not call for a high level of computer complexity; hence, the issue of inefficient use of energy can be sidestepped. More recently, in an effort to solve the drawbacks of the PoW consensus technique, the hybrid consensus model has gained a lot of interest [15]-[18]. This is due to the fact that it takes the advantages of the PoW consensus technique as well as the classic consensus model and mixes them.

In addition, research has been done on the sharding technique because of the likelihood that it could improve the scalability and performance of blockchains. The aim of the paper is to improve the security of the QR based on features by optimal selection of features.

The main contribution of the paper involves the following:

- In this paper, we develop an intelligent E-voting system that uses machine learning algorithm for feature selection to generate the QR codes.
- The QR code with other registered details is stored in database via proper blockchain authentication mechanism.

2. Related Works

In the past, efforts that were made to design protocols for blockchain-based electronic voting systems resulted in the introduction of incentive structures for cryptocurrencies. These protocols were used to incentivize users to participate in blockchain-based electronic voting systems.

Cruz and Kaji [19] presented a system for electronic voting that would be based on the Bitcoin. In addition to this, they researched a wide variety of facets related to the safety of electronic voting.

Zhao and Chan [20] devised a system that, by leveraging Bitcointo the scalability of the blockchain-based electronic voting system, all three of the protocols that were outlined previously have their drawbacks. This is due to the fact that the process of reaching a consensus in Bitcoin requires a lot of time and is also expensive computationally.

End-to-End voting, also known as E2E voting, is a voting mechanism that is based on Bitcoin and was proposed by Bistarelli et al. [21]. In this approach, votes are tallied by adding up the tokens that have been recorded on the Bitcoin ledger for each candidate. These tokens represent votes for that candidate.

Other researchers [22-23] have developed a method for conducting electronic voting that is based on blockchain technology and makes use of the cryptocurrency referred to as ether. This method allows voters to cast their ballots anonymously and without the need for a central authority. The purpose of each of these pieces of study was to strengthen voter faith in the dependability of electronic voting systems by investigating potential uses for smart contracts established on the Ethereum blockchain. The studies are incorrect, however, because they did not take into account the speed and scalability of the blockchain technology. This is a significant limitation of the technology. There was an in-depth debate regarding the various potential solutions to the problems of slowness and lack of scalability that are present in blockchain-based electronic voting systems. These challenges are present in electronic voting systems.

The properties of blockchain-based electronic voting systems (BEVS) that make it impracticable to deploy them were discovered by Zhang et al. [24], who are credited with making this discovery. However, important components of ballot security, such as ballot receiving and ballot uniqueness, are not explored in depth in their work. These are two of the most important aspects of ballot security.

The number of voters, block size, the rate at which blocks are produced, and transaction speed were all factors that were considered in the research that Khan et al. [25] conducted on permissioned and permissionless blockchain configurations (PPBC).

Nevertheless, during contentious presidential elections, the results of any electoral procedure could seem to inspire suspicion. There is no longer any room for discussion regarding the legitimacy of the result as a consequence of the immutability of the bulletin board function provided by the blockchain. Blockchain-based electronic voting systems still face a number of significant challenges, despite the fact that there are many advantages associated with their use.

- *Election Integrity*: A significant worry raised by the use of electronic voting technologies is that these methods could compromise the honesty of elections.
- *Consensus*: Cryptography professionals are in agreement that the PoW methods need a significant investment of both time and resources.
- *Scalability*: When considerations such as network size, and latency are factored in, it can be seen that the network of an electronic voting system is expanding at a rapid pace. Because of this, the network needs to be able to expand while maintaining its high level of performance.

The hybrid consensus model that is discussed in this work is intended to solve these problems. The blockchain contract and the process of sharing constitute the backbone of the model, and the hybrid consensus model is aimed to rectify these flaws. Large-scale electronic voting systems may benefit from this technique in terms of improving their level of security as well as their level of performance and scalability. In addition, it has the potential to be utilized to lessen the likelihood of fraudulent electoral practices and manipulation.

3. Proposed Method

In this section, we develop an E-voting system that involves 1) voter registration phase, 2) Features selection, 3) QR code generation and 4) storage in database.

The first phase is used to register the voter details to perform secure voting and efficient user authentication via E-Voting. The user enters voter ID card details, Aadhaar card details, and user details. Secondly, based on the details entered, the optimized details or attributes will be selected. Using these optimized attributes, the QR code will be generated and from the entered details or attributes, the smart contract will be created. Finally, all the registered details along with the QR code and the smart contract will be stored in a database.

Blockchain based Voting

We will present a high-level overview of our electronic voting system that is based on distributed ledger technology in the next part (blockchain). The numerous organizations depicted in Figure 1 will be discussed in this review, along with the interactions that take place between them. It is not necessary for each voter to have a computer of their own; a smartphone will suffice. Every single voter that is registered has their very own, one-of-a-kind set of credentials that are stored in a wallet. These credentials are unique to the voter. In addition, each voter is given an amount of digital cash that is proportional to the number of votes that they have cast. We came to the conclusion that using the electronic voting system would be the best way to demonstrate how difficult it is to discover security, scalability, and performance in blockchain-based systems and to evaluate them.

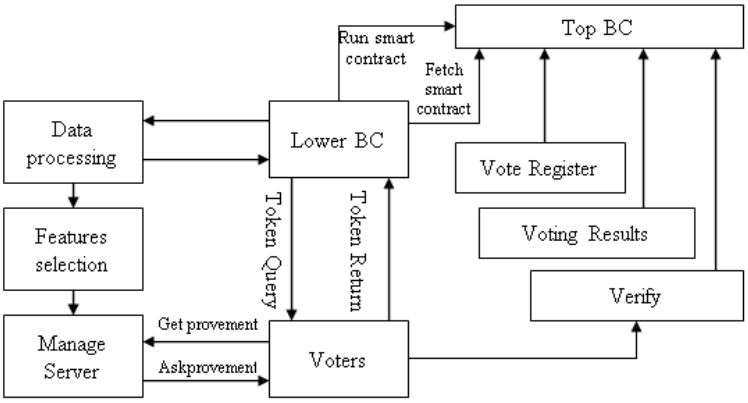

Fig 1: Proposed e-voting on blockchain

The architecture of a blockchain-powered electronic voting system is depicted in Figure 2, which may be accessed here. Blockchain technology is now being investigated as a prospective alternative for use in electronic voting systems because of its ability to facilitate decentralized architecture, increase transparency and integrity, and make it feasible for an independently verifiable voting process. In addition to this, we wanted to make certain that the election was conducted in a manner that was less risky, took place in a shorter amount of time, and was conducted at a lower cost.

3.1 Interacting entities

We are going to talk about the architecture of the system that has been suggested for electronic voting as well as the purposes of its many different sections in the first half of this section. Electronic voting is something that has been recommended.

Manage servers (MS):

Manage servers (MS) are in charge of storing node data in the lower blockchain network. This responsibility falls under their purview because they are part of both the lower and higher blockchain networks. They are also accountable for ensuring that the blockchain continues to retain its authenticity. The login credentials required to access the system and validate the nodes are included in this package.

Blockchain network:

The distributed ledger system that is now being created for use in electronic voting will likely consist of multiple blockchains, each of which will operate in parallel with the others. The capacity of the structure to support parallel execution makes a contribution to improvements in both the overall performance. Lower chains, also referred to as private chains, are employed for the purpose of storing data pertaining to nodes as well as the voter identity register. This is made feasible by the fact that every node on a private chain keeps a copy of the blockchain data locally, and it is on this blockchain that sensitive information is kept. On the upper-chain, which is a public blockchain similar to Ethereum, these transactions are stored and executed in parallel on the upper-chain. This occurs after a portion of the voters, using a mechanism known as proof-of-stake consensus, come to an agreement on the transactions. It is possible to rely on transactions that take place on an upper chain, which is sometimes referred to as a public blockchain, and these transactions cannot be altered. The information that was presented in a previous report regarding the management of routes between lower-chains and upper-chains has not been altered in any way.

Users (voters):

Users are members of the election committee as well as voters, and they utilize their identity IDs for both of these purposes. Users are referred to as Users. Users are required to employ their identity IDs in order to accomplish both of these goals. Every voter is given a digital token that they can use while casting their vote. This token can only be used once per voter. Therefore, the layer of the Ethereum blockchain that is closest to the surface is where the execution of smart contracts actually takes place.

Blockchain contract:

Contracts on the blockchain, also known as smart contractsof computer code that have the potential to carry out their terms independently within the context of the decentralized system that is currently being constructed. The execution of smart contracts results in the generation of contract agreement functions. These functions make it feasible for the top layers of blockchain networks to keep track of transactions. This is done in order to facilitate the construction of a flexible cryptosystem that is suitable for use in electronic voting systems and make it easier to do so.

3.2 e-voting Process

The act of voting is comprised of a series of distinct processes, which are carried out in the following order:

- **Setup**: To conclude the process of initialization, you must first supply the security parameter, then construct the key pairs, and then make use of those keys to encrypt (or decrypt) the operations that are associated with the process.
- **Register**: the votershave to sign up first by entering the identifiers as IDs before you can set up a private key. This is required before you can even set up a public key.
- **Vote**: It is up to the voters to come up with the vote value or parameter, and it is necessary to use this in order to obtain the encrypted text and signature.
- **Valid**: The fact that a vote has been marked as Valid will be taken into consideration by the ballot server when determining whether or not the marked ballot should be used as input for the counting process. The process of voting is carried out in a totally arbitrary manner.
- **Append**: It accomplishes this goal by generating a fresh version of the encryption at random on a regular basis and then periodically updating the cipher text that is stored in the polling box.
- **Publish**: If you choose this option and then click the Publish button, the final tally of votes for the polling box will be made available to the general public.
- Verify Vote: Following the voting phase, voters would then have the ability toput their votes. This would take place after the voting phase with

blockchain contract. The results that were returned either contain an error or do not contain an error.

- Once all of the votes have been cast and validated, the final tally is established by entering the associated private key as well as the parameters of the voting machine into a centralized computer. In the event that the calculation was carried out improperly, the computer will answer with an inaccurate value.
- When the public requirements are provided during the publicity phase, a vote is validated as a lawful and proper vote cast toward the ballot outcome. This ensures that the vote counts toward the outcome of the ballot. This verifies that the vote will be counted toward the total for the election.

Machine learning based feature selection

LSSVM is a technique for supervised machine learning that is useful in a wide variety of settings, including those dealing with data analysis and the detection of anomalies. LSSVM is a technique for supervised machine learning that finds utility in a wide variety of circumstances. A method for machine learning known as LSSVM is one that is fundamentally based on the solution of problems with two classes. Support vector machines are responsible for the discovery of an ideal hyperplane, which is then used in this method to partition the information. The boundary value of a training set can be determined by looking at the distribution of support vectors across both of the classes that make up the set. This investigation makes use of a model that is able to discern between applications that are safe and those that are hazardous. The model is constructed using an LSSVM that features kernels that operate on their own. The following is how we characterize the full scope of the functional capabilities offered by the LSSVM:

$$z\left(y\right)=a^{T}\phi\left(y\right)+b$$

here

z - output vector and

y - input vector,

$\phi(y)$ - non-linear function is used in order to translate the data input, which possesses a larger feature space, onto the desired output vector,

a - adapt weight vector and

b - threshold value.

The following equation stands to gain from the application of this method of enhancement:

$$\min 0.5w^{T}w+\frac{\gamma}{2}\sum_{x}IE_{x}^{2}$$

$$s.t.\,y\left(x\right)=w^{T}\phi\left(x\right)+c+E_{x}$$

here

E_x - input error sample a and

γ - cost function.

The equation can be used to assist in the process of calculating values for the detection of attacker:

$$Y'=\sum_{x}I\left(\alpha-\alpha^{*}\right)*K\left(b_{i},b\right)+c$$

here

$K(b_i,b)$ - kernel function is what permits us to carry out the operation of performing the product in the low-dimensional data space while at the same time operating in the high-dimensional feature space. The following kernel functions have to be taken into consideration in order for this research to accomplish what it set out to do:

$$K\left(x_{i},x_{j}\right)=x_{i}^{T}x_{j}$$

Subset Feature selection

The goal of these methodologies is to identify the most pertinent set of features that, when combined, offer the greatest probability for detection. These are dependent on the idea that the developed model improves upon the detection rate and minimizes the value of misclassification mistakes when employed in isolation or in conjunction with a limited number of additional features. One can choose from a number of different strategies to determine the optimal mix of traits that can be used to spot viruses. This can be done in a number of different ways. In this study, we compare and evaluate four different feature subset selection techniques in order to figure out how to determine how a feature score should be computed. The purpose of this study is to figure out how to determine how to determine how a feature score should be calculated. The photographs that follow illustrate some of the approaches that have been taken, which are as follows:

Correlation based feature selection

The correlational analysis, which is used to determine which traits are most closely associated to a certain class, uses this method as its foundation to determine which characteristics are most closely linked (i.e., benign or malware). Pearson correlation, which is also known as the coefficient of correlation, has been applied in this study in order to facilitate the analysis of the interdependence that exists between a variety of distinct components. If the correlation coefficient, denoted by r, increases while comparing two or more feature sets, this may indicate the presence of a significant link between the sets. This further lends credence to the idea that classes with low (or high) feature values tend to have similar low (or high) ranges in other highly connected characteristics. This provides us with a statistical reason to think about these classes since it shows that classes with low (or high) values for a feature tend to have comparable low (or high) ranges for other features that are heavily related. In other words, this gives us a reason to think about these classes.

Rough set analysis (RSA)

By combining several feature sets, this method generates an upper and lower estimate of the initial data set, precisely as the traditional way of set estimation that was covered in the prior section. This formal estimate presents the values in the source data set that are the most extreme and the values that are the least extreme. The use of this tactic is beneficial for data mining with inadequate information when it is available. This technique is applied to the extracted feature sets in order to pick the smallest feasible collection of features to put to use. The goal of this procedure is to maximize efficiency. The RSA algorithm uses three different types of notation: approximations, reduced features, and an information system. Below, we will describe and show the various methods in which RSA can be used to create a smaller subset. RSA can be used to obtain a subset that contains fewer elements.

Let us pretend that A equals C and Z, and that XZA equals C, Z, and YC. YC are all very close approximations of the value that is being sought after. It is necessary to first compute an approximation of X at both the top (XY) and the bottom (uline> X/uline> Y) in order to arrive at an approximation of Y. If there is even the tiniest potential that something might be included in both the biggest possible set and the lowest feasible approximation, then that item needs to be included in both of them. This is because the lowest feasible approximation is more precise than the largest possible set. In order to acquire the XY and the (uline> X/uline> Y), the following are various formulae that can be utilized:

$$X'Y=\{y_i\in U|[y_i]_{Ind(B)}\cap Y\neq 0\}$$

$$Y= \{y_i\in U|[y_i]_{Ind(B)}\cap Y\}$$

where

$$|[y_i]_{Ind(C)} - y_i \text{ class in } Ind(C).$$

Reduced attributes:

Following are the outcomes that the A⊆B correctness evaluation of group $Z(Acc(Z))$ produces, as revealed by the reduction of attributes:

$$\mu_B(A)=\mathrm{card}(BZ)/\mathrm{card}(B'Z)$$

The cardinality of a set is the number of individual elements that, when combined, produce the most comprehensive illustration of that set. In addition, we consider any and all feature sets so long as they possess the same degree of accuracy as the feature sets that were retrieved.

Information system:

In a computerized system, this is expressed as $Z = (C,B)$, where C refers to the universe and B refers to the sets of characteristics, each of which has a limited number of components. In other words, the universe is represented by C and the sets of characteristics are represented by B. There is a function that can be represented by the F_b:

For each b in B, calculate $F_b:C\rightarrow V_b$, where $V_b$is the value associated with the property b. There is an equivalence relation that can be represented using the notation B-indiscerbility relation (Ind(Z)), and this relation exists for every pair that consists of A and B. The explanation that follows is an example of a definition that could be used for Ind(Z):

$$IND_A(Z)=\{(x,y)\in C^2|\forall a\in Z,a(x)=a(y)\}.$$

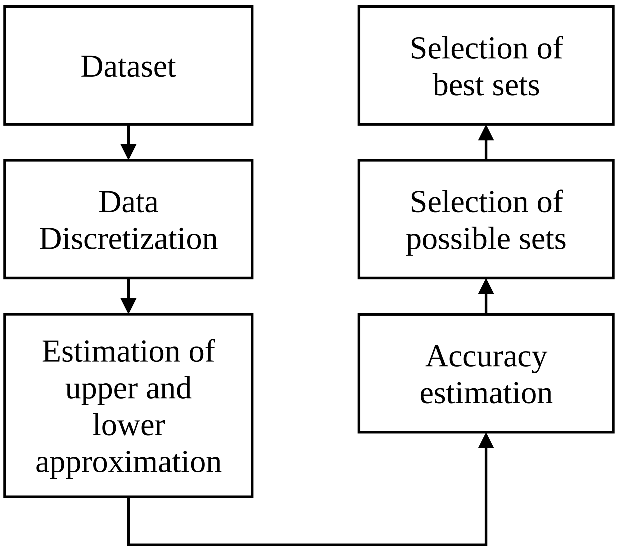
Dataset
Data Discretization
Estimation of upper and lower approximation
Accuracy estimation
Selection of possible sets
Selection of best sets

Fig 2: Feature Selection

When the training cases are applied to a subset of characteristics, the approach reveals the significance of those attributes based on the consistency with which they appear in class value predictions. This significance is determined by the degree of similarity between the training cases and the characteristics. The degree of similarity between the training instances and the features is the factor that decides how significant this finding is.

In the event that two data points have the same feature values but distinct class labels, the inconsistency rate is the variable that is utilized in the calculation of the consistency rate (for example, benign and malware). In the course of this inquiry, we are concentrating on programs that use a binary data type, which indicates that the programs either (i.e., 0 for benign apps and 1 for malware apps).

A group of features, often known as GF and abbreviated as such, is made up of Z separate features, with $Z = X_1 + X_2 + \dots + X_z$. Out of a total of A samples, we have found that the occurrence of Xi takes place in samples with a value of $A = A_0 + A_1$, where A0 represents the number of samples with a value of 0 and A1 represents the number of samples with a value of 1. The difference count, also known as Xi, is defined as $INC = A - A_0$ if and only if there is a difference between the values of A1 and A0. Xi is indicated by the symbol i. For the purpose of calculating the inconsistency rate (INCR) of the feature set, the following equation is utilized:

$$INCR = \frac{\sum_{i=1}^{z} INC_i}{Z}$$

Filtered subset evaluation

The objective behind filtered subset evaluation is to choose an evaluator at random from the data set that is produced by some kind of arbitrary filtering method. This is done in order to reduce bias in the evaluation process. This is the fundamental concept around which the approach is built. The filtering strategy does not utilize an induction method as one of its core components. The strategy of evaluating filtered subsets is both a time-efficient and scalable method of doing business. The process that must be followed, as depicted in Figure 6, in order to employ a filter effectively in order to identify the appropriate subset of characteristics.

4. Results and Discussions

In this study, we explain the essential performance measures that we discovered to be useful for evaluating the success of our proposed model for the detection of malware. We found them to be relevant based on the findings of our previous research. The confusion matrix is the component that must be utilized in order to ascertain each and every one of these values. It is a reference to the information that has been gathered by detection models and then utilized in the process of classifying items into categories.

Experiments were carried out in order to determine whether or not the proposed PSC-Bchain could be scaled. Additionally, experiments were carried out in order to evaluate the performance of the PSC-Bchain by comparing its throughput and latency to those of well-established consensus methods such as Proof-of-Stake and Proof-of-Work. We began by building a simulation network with 200 nodes in each cluster. Subsequently, we increased the total number of nodes in the network to 1000 over the course of our work. For each of the ten individual blocks, we monitored the throughput and investigated the delay. In order to move further, we used the PoW protocol and the PoS protocol in our experiments, but we ran them on the same virtual network. There was a wide range, anything from 200 to

1000, in the total number of nodes, which is a representation of the size of the network. In order to get an accurate measurement of the latency, we tested ten Proof-of-Work blocks as well as ten Proof-of-Stake blocks.

Figure 2 provides a comparison between the proposed BC consensus model under various probabilities *p*. The comparison is made with regard to the model for reaching consensus. According to Figure 2, the rate at which transactions were processed was unaffected by the total number of nodes, regardless of whether they were processed using Proof-of-Work or Proof-of-Stake.

The proposed BC model that was proposed handles an increasing number of transactions as the number of nodes expanded in the network with successful transactions. This demonstrates that the proposed BC is very scalable when utilized in conjunction with the sharding strategy over various mining power that varies between 0.1 – 0.5 in steps of 0.1.

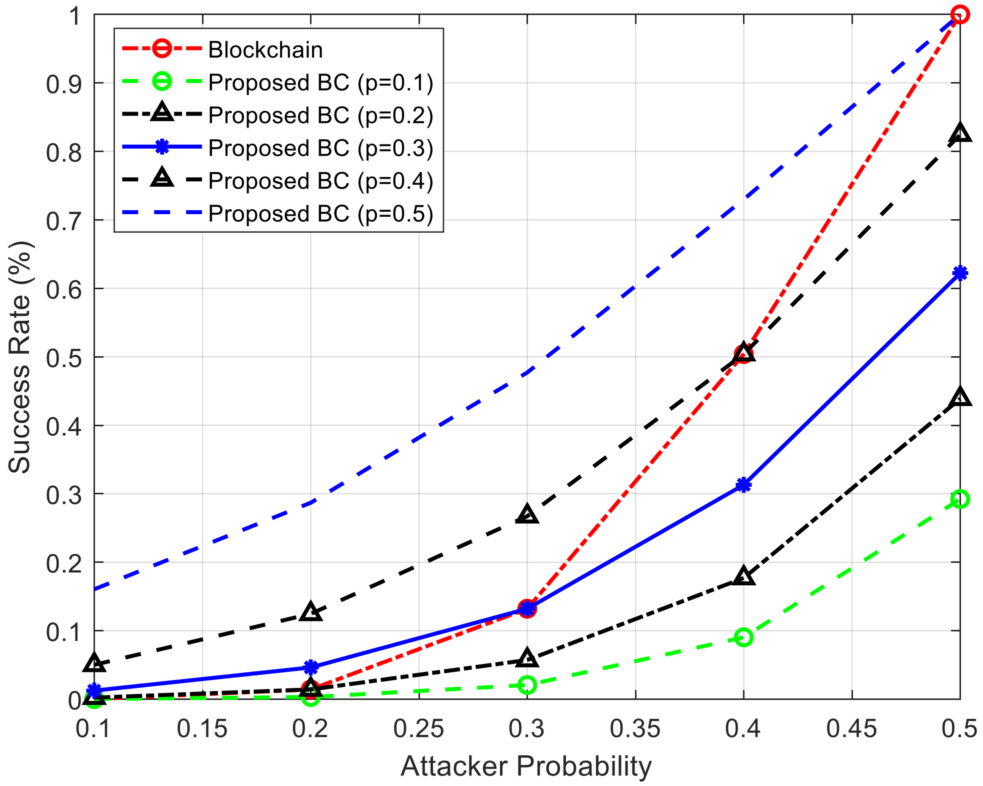

Fig 3: Successful probabilities of Attack in E-Voting system

The figure 3 shows the results of attacker probability in attacking the proposed model over various rate of mining power than the classical blockchain. There are two completely separate components that make up the overall assessment of the level of security. One of our primary concerns was whether or not the proposed model could be trusted once it had been deployed via the sharding method. Because nodes with more than half of the total CPU power can launch destructive attacks utilizing the proposed mechanism, a 49% attack poses a security risk to the blockchain. This is due to the fact that nodes that possess more than 50% of the total CPU power are able to manage the majority of the network.

The proposed mechanism, on the other hand, is seen as having a greater degree of trustworthiness in this regard. The cost of launching a 49% attack is higher in PoS than it is in PoW due to the bigger quantity of coins that are at stake. Despite the fact that the attacker payoff would be very small in the event that a 50% attack was successful, the cost of starting a 49% attack is higher. The reason for this is due to the fact that there are a greater number of coins at stake in PoS. Given that this is the situation, there is no justification for potentially hostile nodes to launch an attack on the network.

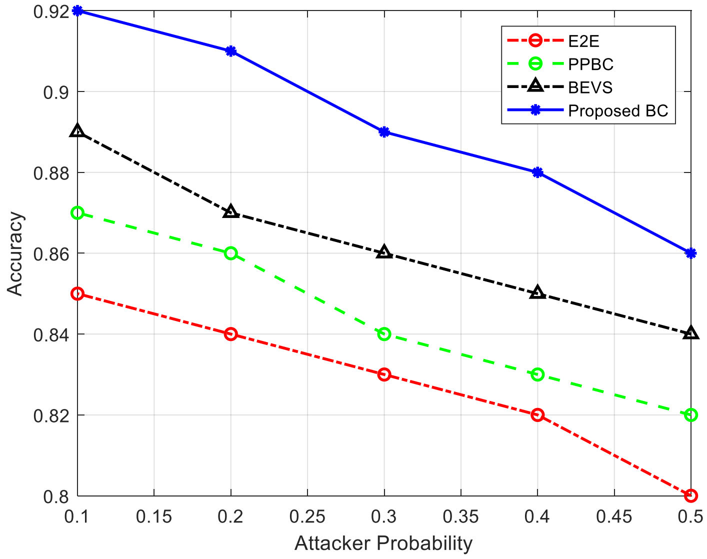

Fig 4: Accuracy

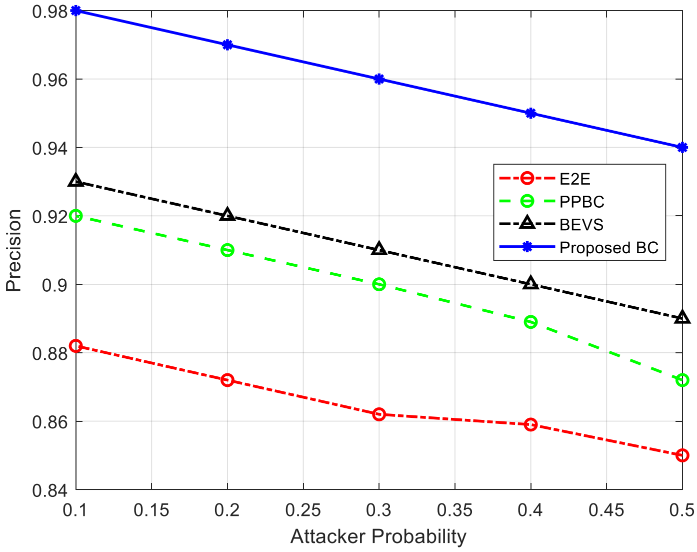

Fig 5: Precision

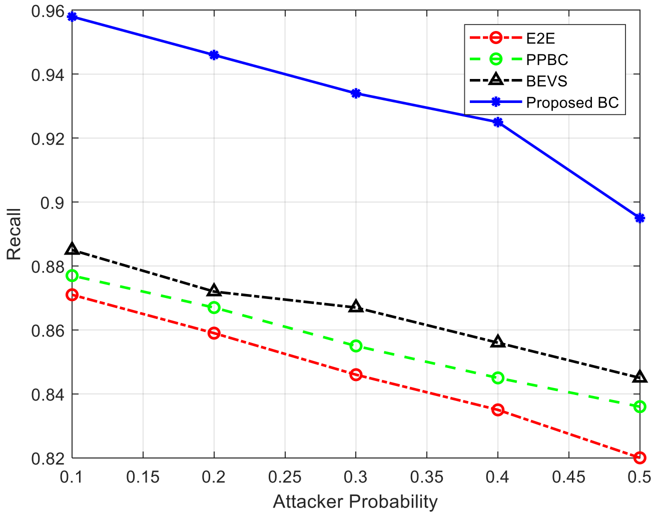

Fig 6: Recall

The Figure 4-6 presents the accuracy, precision and recall of features selected for generated the QR code and from the results, it is found that the present model achieves a higher rate of feature selection than the other methods. This helps the proposed method to achieve an accurate and attack-less E-Voting system than the other methods.

5. Conclusions

For the purpose of developing an intelligent electronic voting system, this project involves the creation of QR codes that use a method of machine learning to determine relevant attributes. It is hoped that the inherent security of the QR will be increased by picking the elements that will be included in the QR with great attention. By utilizing an authentication mechanism that is founded on blockchain technology, the database will record the QR code in addition to the other facts pertaining to the registration. Python models are used to run simulations in order to evaluate the effectiveness of the proposed strategy in relation to the various existing electronic voting procedures. The findings of these tests indicate that the method that was suggested is more accurate in the features that it selects and has a lower computational complexity than the one that was actually used.

References

[1] Al-Maaitah, S., Qatawneh, M., &Quzmar, A. (2021, July). E-Voting System Based on Blockchain Technology: A Survey. In *2021 International Conference on Information Technology (ICIT)* (pp. 200-205). IEEE.

[2] Abuidris, Y., Kumar, R., Yang, T., &Onginjo, J. (2021). Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. *Etri Journal*, *43*(2), 357-370.

[3] Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., &Badra, M. (2022). Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. *IEEE Access*.

[4] Baudier, P., Kondrateva, G., Ammi, C., &Seulliet, E. (2021). Peace engineering: The contribution of blockchain systems to the e-voting process. *Technological Forecasting and Social Change*, *162*, 120397.

[5] Rathee, G., Iqbal, R., Waqar, O., & Bashir, A. K. (2021). On the design and implementation of a blockchain enabled e-voting application within iot-oriented smart cities. *IEEE Access*, *9*, 34165-34176.

[6] Panja, S., & Roy, B. (2021). A secure end-to-end verifiable e-voting system using blockchain and cloud server. *Journal of Information Security and Applications*, *59*, 102815.

[7] Taş, R., &Tanrıöver, Ö. Ö. (2021). A manipulation prevention model for blockchain-based e-voting systems. *Security and Communication Networks*, *2021*.

[8] Ye, K., Zheng, D., Guo, R., He, J., Chen, Y., & Tao, X. (2021). A Coercion-Resistant E-Voting System Based on Blockchain Technology. *Int. J. Netw. Secur*, *23*, 791-806.

[9] Díaz-Santiso, J., & Fraga-Lamas, P. (2021). E-Voting System Using Hyperledger Fabric Blockchain and Smart Contracts. *Engineering Proceedings*, *7*(1), 11.

[10] Jumaa, M. H., & Shakir, A. C. (2022). Iraqi E-Voting System Based on Smart Contract Using Private Blockchain Technology. *Informatica*, *46*(6).

[11] Khan, K. M., Arshad, J., & Khan, M. M. (2021). Empirical analysis of transaction malleability within blockchain-based e-Voting. *Computers & Security*, *100*, 102081.

[12] Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A., & Mehta, K. (2021). End to end secure e-voting using blockchain & quantum key distribution. *Materials Today: Proceedings*.

[13] Widayanti, R., Aini, Q., Haryani, H., Lutfiani, N., &Apriliasari, D. (2021, September). Decentralized Electronic Vote Based on Blockchain P2P. In *2021 9th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-7). IEEE.

[14] Singh, S., Wable, S., &Kharose, P. (2021). A Review Of E-Voting System Based on Blockchain Technology. *International Journal of New Practices in Management and Engineering*, *10*(04), 09-13.

[15] Chaisawat, S., &Vorakulpipat, C. (2021). Towards achieving personal privacy protection and data security on integrated E-Voting model of blockchain and message queue. *Security and Communication Networks*, *2021*.

[16] Wahab, Y. M., Ghazi, A., Al-Dawoodi, A., Alisawi, M., Abdullah, S. S., Hammood, L., & Nawaf, A. Y. (2022). A Framework for Blockchain Based E-Voting System for Iraq. *International Journal of Interactive Mobile Technologies*, *16*(10).

[17] Kim, H., Kim, K. E., Park, S., & Sohn, J. (2021). E-voting System Using Homomorphic Encryption and Blockchain Technology to Encrypt Voter Data. *arXiv preprint arXiv:2111.05096*.

[18] Sharma, T., Krishna, C. R., &Bahga, A. (2021, March). A Cost-Efficient Proof-of-Stake-Voting Based Auditable Blockchain e-Voting System. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1099, No. 1, p. 012038). IOP Publishing.

[19] Cruz, J. P., &Kaji, Y. (2017). E-voting system based on the bitcoin protocol and blind signatures. *IPSJ Transactions on Mathematical Modeling and Its Applications*, *10*(1), 14-22.

[20] Zhao, W., Liu, D., & Li, Q. S. (2015). Proc. Int. Conf. on Renewable Power Generation.

[21] Yokoyama, T., Shiba, K., Nishizawa, A., Nagahara, S., Yamato, H., Usami, T., ... & Horiuchi, T. Proc. IEEE Int. Interconnect Technology Conf., Burlingame Proc. IEEE Int. Interconnect Technology Conf., Burlingame 19, 2002.

[22] Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., &Hjálmtýsson, G. (2018, July). Blockchain-based e-voting system. In *2018 IEEE 11th international conference on cloud computing (CLOUD)* (pp. 983-986). IEEE.

[23] Hanifatunnisa, R., &Rahardjo, B. (2017, October). Blockchain based e-voting recording system design. In *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)* (pp. 1-6). IEEE.

[24] Zhang, S., Wang, L., &Xiong, H. (2020). Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *International Journal of Information Security*, *19*(3), 323-341.

[25] Khan, K. M., Arshad, J., & Khan, M. M. (2020). Investigating performance constraints for blockchain based secure e-voting system. *Future Generation Computer Systems*, *105*, 13-26.