Computers, Materials & Continua
DOI: 10.32604/cmc.2022.023846
Article

Tech Science Press

A Framework for e-Voting System Based on Blockchain and Distributed Ledger Technologies

Shahid Hussain Danwar, Javed Ahmed Mahar* and Aneela Kiran

Institute of Computer Science, Shah Abdul Latif University, Khairpur, 66020, Sindh, Pakistan
*Corresponding Author: Javed Ahmed Mahar. Email: mahar.javed@salu.edu.pk
Received: 23 September 2021; Accepted: 16 December 2021

Abstract: Election allows the voter of a country to select the most suitable group of candidates to run the government. Election in Pakistan is simply paper-based method but some certain political and socio-economic issues turn that simple process in complicated and disputes once. Solutions of such problems are consisting of many methods including the e-voting system. The e-voting system facilitates the voters to cast their votes by electronic means with very easy and convenient way. This also allows maintaining the security and secrecy of the voter along with election process. Electronic voting reduces the human-involvement throughout the process from start to the end. Such system is not established yet in Pakistan. Hence, every election is disputed always. In this paper we proposed the framework of an e-voting system and simulation with the use of blockchain ledger technology. The proposed framework owns the capacity to deal with ballots in Pakistan. The novelty of the framework is that the e-voting system is linked to National Database and Registration Authority (NADRA) database which assures voter's validation. The fundamental requirements were kept in consideration during the performance evaluation of the system. The results are processed and depicted specially with reference to the number of voters and voting stations, real time of vote casting, network bandwidth and controlling principles. The results support the decision makers and guide them in the foundation and customization of an e-voting system in Pakistan.

Keywords: Simulation modeling; e-voting system; blockchain technology; distributed ledger

1 Introduction

Elections in any democratic country play a very important role for the development of the country. Any pre and post polling organized unfair means in the election can lead a sate towards political, economic and social instability [1]. In Pakistan, paper based voting system is used from the time of becoming separate and independent state to select the government for national assembly and provincial assembly. The allegation from one political group to other is a regular practice before and after the elections which sometimes caused the riot among the mob. The elections always remained

disputed due to manual process; presence of human involvement, uncertainty of inclusion of votes in final counting remained high for the voters.

Designing and developing the e-Voting system provides the solution to the problems exist in the paper based voting system. The e-Voting systems have already been adopted by the modern emerging information societies [2]. The voting process is affected positively with deployment of e-Voting systems; the systems that are used today are yet cannot be declared ideal as numerous issues of authentication, privacy and data integrity have been identified. Generally registration, authentication and authorization, vote casting, vote counting and vote verification is the key modules of any e-Voting system [3]. Furthermore, E-voting is a multidisciplinary study of software engineering, computer science, cryptography, social sciences, law and politics [4,5]. Researchers are very keen for developing a secure e-Voting system and focusing not only on cost reduction but also working on the security, privacy requirements to ensure the system's integrity. Traceability and verifiability of new election system can cut on fraud voting, which will help the replacement of paper based traditional system [6].

Blockchain (BC) has the state-of-art capability to allow transactions between the untrusted parties over the trustless computer networks [7]. It's a data structure of chained list of blocks where the peer-to-peer network is being used for distribution of chain of blocks, and every node maintain the latest version of the list with information about transaction stored inside the blocks. Distributed ledger of shared information replaces single database in BC technology which provides the higher security accessibility [8]. BC is distributed public ledger which is immutable and incontrovertible in its nature. Immutability feature of BC ensure the reference of previous block when the entry of "new block" to the ledger is made. As the ledger is decentralized, replicated and distributed over multiple locations, verifiability feature of BC ensure the high availability of ledger to all nodes with third party verification. Distributed Consensus is the third feature having a consensus mechanism or protocol which determines the node responsible to append the coming transaction on the ledger [6]. These high level features of BC have already attracted some countries and they have developed BC-based E-Voting systems [9]. Ledger can be verified and validated as it is always shared to every node in the network. The BC is always capable for recording and saving the transactions occurred over network and it also maintains irrevocable and auditable transaction history [10]. BC provide the platform for verification publicly which is helpful to design and develop an e-voting system, auditable at the voters level rather than only officials audit the system [11].

Six fundamental requirements i.e., accuracy, auditability, mobility, verifiability, privacy and democracy are considered and implemented in any traditional elections. The accuracy makes it difficult to alter any vote, to invalidate a valid vote or to consider invalid vote for counting. The democracy guarantees the right to cast the own and valid vote. The privacy makes it impossible to know the choice of any voter. The verifiability gives the possibility to recount the votes. A voter can vote to his choice regardless of the location with the implementation of mobility which also ensures the origin of voter for his vote. Finally the voting system must maintain auditability for validity by external observes. A framework for blockchain-based e-Voting system which is auditable and verifiable by the voter is presented in this paper. The proposed framework is simulated for free and fair elections in Pakistan. The simulation process was tested on eight selected areas of provincial assembly constituency number PS-26 Khairpur-1. The simulated e-Voting system is equally beneficial for both voters who used to vote by visiting polling station and for those eligible voters who want to vote from anywhere using digital device. The e-Voting system will reduce the number of disputes and make the voting environment pleasant which ensure the fairness in the election. The system is connected with NADRA database in order to increase the authenticity and reliability which shows the novelty of the work. After the certain

training to the voters, election commission can use the system effectively and voters can vote securely and freely.

2 Literature Review

Lot of work has been done in the context of e-voting system using blockchain and other technologies as well. An internet based voting system was proposed in [12] using BC technology in order to secure the voter's privacy which enabled voters to take control on their own vote only. The proposed system is a self-tallying e-voting system which doesn't require any trusted authority for computation and tallying process of votes. The proposed system was implemented on Ethereum's official network. Similarly, Pawlaka et al. [9] also proposed an auditable BC voting system and used multi-agent mechanism to integrate a supervised non-remote end-to-end verifiable approach in e-voting system. In the same way, reference [13] developed, tested and implemented an android based e-voting application on Ethereum platform using Ethereum wallets and solidity language. The developed system also enables such voters which even don't have an Ethereum wallet. All voting records stored in the Ethereum BC. Reference [14] proposed BC technology to design and implement a secure, reliable and anonymous electronic voting system which will help in the rise of number of votes.

The use of BC technology in current business and other fields enable researchers to focus on this modern and intensifying technique. Reference [15] described some challenges and opportunities of using BC in Business Process Management (BPM). Use of BC in the establishment of BPM life cycle and its relevancy in business ground was also described. Likewise, reference [16] reviewed some cases of BC technology used to improve government services specifically it enables to implement smart government services. In addition to this, authors also synthesis the security issues of BC and its solutions as well. Reference [6] evaluated the services of BC technology along with some popular e-Voting systems to design, construct and implemented an application based on distributed electronic voting systems whereas limitations in existing e-voting systems were also addressed. Hosting an e-voting system throughout the state is indeed costly and may face various security issues. Since to tackle this problem, authors evaluated the potential of distributed ledger technology to decrease major security issues as well as overall cost of the system. Hence to evaluate and to improve previously developed e-voting systems, an advanced technique immensely required. Reference [17] provided the concept of Delegated Proof of Stake consensus method, an election algorithm to improve the performance of ring-based coordinator election algorithm to fulfill the requirements of BC technology using multi-agents approach. Instead of using services from third-party, a decentralized e-voting system was designed and presented in [18]. The core purpose of the research is to work on combination of BC and homomorphic encryption to protect anonymity of voter and assure the privacy of data transmission.

Performance and scalability constraints of an e-voting system are discussed in [19]. A rough experimentation was conducted in this regards with BC settings to evaluate voting population, block size, block-generation rate and transaction speed. Various limitations in the developed e-voting systems were observed in the research study. To eliminate some of them limitations, Reference [19] proposed a BC based e-voting system which is suitable for small level elections. Smart contract of Ethereum platform were used and deployed by author using truffle framework. With the facility of internet based e-Voting system, also there are some risks besides this. Some risks and opportunities with respect to the existing e-Voting systems based on BC technology were discussed in [20]. Similarly, to overcome the security risk in BC based e-Voting system, reference [21] presented a P2P technique. The authors were used distributed ledger technology in order to avoid vote forgery. For user credentials

and authentication, elliptic curve cryptography was used. Based on e-Voting theory, cryptography and software engineering theory, Linux platform was used to design system. Reference [22] highlighted a major security issue; transaction malleability attack faced in the BC based e-Voting system. An experiment was done on a BC test bed hosting an e-Voting application to identify the significance of some parameters which may cause to lead the malleability attack. Network delay and block generation rate were the parameters used in the experimentation. To ensure the security in the e-Voting system, reference [23] proposed a hybrid consensus model which based on the mutual working of proof-of-credibility and proof-of-stake. Smart contracts were used by scholar to provide reliable bulletin board and increase the ballot accuracy.

Another investigation was done in [24] on the account of contribution and influence of BC technology towards electronic voting system. An observation came after interviewing election and BC experts that due to the complex structure of this advanced technology, various conflicts generated among election candidates. The BC technology allow every user to visualize whole data (election updates) but at the same it restrict users to access or modify data. In the same perspective in [25] proposed a double-layer model BC based e-Voting system to prevent administrator as well as miners from manipulation and previewing of results. In the proposed model, the counting process started after the completion of voting process which led to prevent the manipulation, no need of central authority, privacy of voter and a distributed structure for storing of votes. In the comparison of current election system, an internet based or BC based election system examined more secure, authentic and verifiable [26]. Voting through computer or smart phones increases the turnout of votes [27]. The scalability and maximum use of resources (hardware/software) are the main shortcomings of e-voting systems. Summary of BC based e-voting systems is given in Tab. 1. In this research, techniques and approaches were chosen from the literature. We have composed and simulated a framework by focusing the actual election environment of Pakistan.

Table 1: Summary of BC based e-voting system

Reference	Type of e-Voting	Techniques	Purpose
[6]	Distributed electronic voting system	BC and Distributed Ledger Technologies	Evaluated BC services, famous e-Voting systems, potential of distributed ledger and security issues
[9]	Auditable and verifiable voting	BC and multi-agent mechanism	Integrate a supervised non-remote end-to-end verifiable approach
[12]	Internet based voting system	BC	To secure the voter's privacy
[13]	Android based e-voting application	BC, Ethereum wallets and solidity language	Developed system enables voters which even don't have an Ethereum wallet and stored voting records

(Continued)

Table 1: Continued

Reference	Type of e-Voting	Techniques	Purpose
[14]	BC based e-voting	BC	Design and implement a secure, reliable and anonymous electronic voting system
[17]	Delegated Proof of Stake consensus method based e-voting	BC, election algorithm and multi-agents approach	Improve the performance of ring-based election algorithm and e-voting system
[18]	Decentralized e-voting system	BC and homomorphic encryption	To protect anonymity of voter and assure the privacy of data transmission
[19]	BC based e-voting system	BC	Evaluate voting population, block size, block-generation rate and transaction speed
[21]	BC based e-voting system	BC, P2P, elliptic curve cryptography and distributed ledger	To avoid vote forgery.
[22]	BC based e-voting system	BC	Highlighted major security issue; transaction malleability attacks.
[23]	Hybrid consensus model based e-voting	Bulletin board	To ensure the security and mutually working of proof-of-credibility and proof-of-stake.
[24]	BC based e-voting system	BC	Investigated influence of BC towards electronic voting system.
[25]	BC based e-voting system	BC and double-layer model	Prevent administrator and miners from manipulation and previewing of election results

3 Proposed Framework for e-Voting

The study of this paper is instigated the design and development of practical, efficient and secure e-voting system based on BC and distributed ledger technologies. The developed e-Voting system based on our proposed framework is basically consisting of three main phases such as: voter registration,

vote casting and creating and adding of voting in to the BC. Where voter login to the system with the provided credentials and cast the vote against the respective candidate. When the vote is casted, a block is generated based on voter's detail. Blocks with same hash number are considered as the duplicate entry and discarded by the system with the error message. The successful casting of vote resulting in generation of new block containing hash number of the last block in the BC which help in the addition of the newly generated block in the existing BC. Moreover, all these phases are described in detail in this section while Fig. 1 is the complete depiction of our proposed framework of e-Voting system where the three colors such as the phase in purple color represents the voter registration process, the blue color represents the voter log-in process and the green color represents the vote casting and validation process.

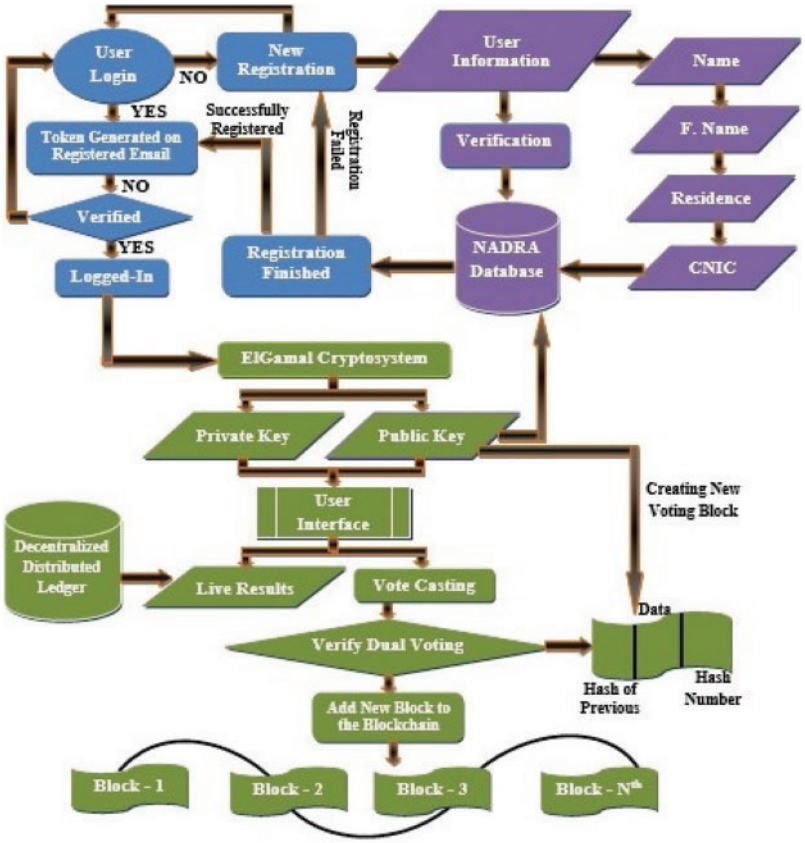

Figure 1: Proposed framework for e-voting

The proposed framework is designed by focusing the general elections in Pakistan which has never been done before, elections in Pakistan are being conducted through manual process using paper ballot and other paper based tools. In this framework the real election environment of Pakistan has been depicted and simulated using state-of-art Blockchain-Distributed Ledger technology. Government agencies like Election Commission and NADRA have been taken onboard. All the phases of the framework have been used to test the system in collaboration with the government agencies. Hash function and encrypted techniques are very carefully selected to simulate the real time process of elections in Pakistan. The algorithm for vote casting process using the public and private keys is really helpful in the voting process of Pakistan. Poison process model and queuing model help to support

the system in rush time when the arrival of voters highly increased. We believed that by applying the proposed framework in the general elections can result the fairness and transparency in elections which help the government to save the precious life of the people of Pakistan as it was observed in past that every election took the human life in riots between different political groups in absence of any trusted election system.

3.1 Registration Phase

The first phase of the proposed framework is registration process which should be done before election-day. However, proposed framework allows user to get registered even at the day of election. To ensure the security of system, voter's verification is essentially required. Especially when it came to the case of voting it is hardly required to assured someone's identity secure in order to reduce fraudulent vote casting. Hence our developed system in this concern is connected with the NADRA database through which basic information like user's authenticity and user's voting eligibility is cross checked and confirmed either user has a record in NADRA database and current status of his/her record [28].

There are some essential steps required for the process of voter's registration. At the first step, all the candidates should bring their necessary documents like CNIC for verification by the officials. The automated system is conformed the status of the registration when the provided documents are successfully verified and grant consent for advance process of registration. After that the mandatory information is inputted to the database, system automatically verifies the age status of the particular candidate. If candidate is eligible in all perspectives then he is allowed to provide his fingerprint along with photo which is appended into the database. It is correct time to send all the information in an encrypted form. The administrator server receives the information and maintains separate candidate record into the database. After that voter ID number is generated by the system for a specific candidate. Following these mentioned steps the registration process is completed. Once the voter registration confirmed, user assigned a hash address based on his/her NADRA record and Voter ID assigned during registration. The assigned hash address is supplied with the digital token which is provided with user log-in credentials and also ensures one-time voting with particular hash address (particular voter can vote only single time after log-in to the system). Work flow of registration phase is shown in Fig. 2.

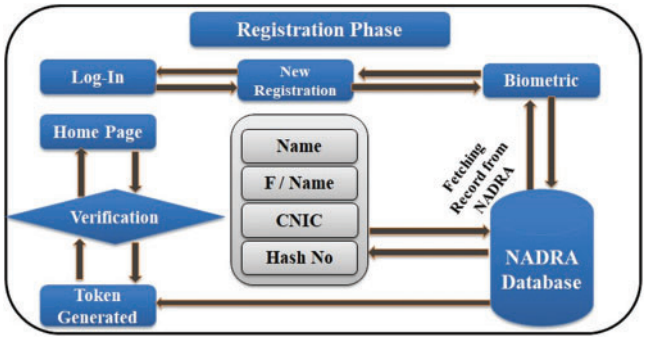

Figure 2: Processing steps of registration phase

Polling booths will be deployed for voters which have no any access to the digital devices (mostly peoples of remote areas). An electronic machine will be available there including a biometric device which will facilitate voters with registration and vote casting. The biometric device will fetch the data

for NADRA database and assigned with hash address as if voter's information verified and redirect voter to the home page of e-voting portal using hash address as a log-in credentials.

3.2 Voter's Validation Phase

Alike [15], Elliptic curve cryptography technique is used in this e-Voting system which will validate and provided with non-repudiation properties to reduce voting forgery ratio. Once the user performs the registration process, he/she will be assigned a digital token, sent to their respective email ID provided at the time of registration phase. The digital token will be used as log-in credentials in future to get access to the e-voting system. This digital token contains hash number which was completely generated on the basis of user's information stored in NADRA database. Using biometric log-in will auto fetch data from the NADAR and using respective information made registration and log-in for voter at the time of voting.

Provided user credentials will be verified from the NADRA database to ensure the authentication of user. In case of failure in log-in and authentication, e-Voting system will redirect user to the registration form to start from the beginning. Once the voter authenticated and successfully logged-in to the e-Voting system from his/her digital device (Mobile/Computer), voter will be redirected to the Home page of the portal and a Digital Voting Ballot (DVB) will be created for voter. This creation of DVB happens only once and at the time of election only. Hence, it assures that voter has only single chance to cast a vote. Creating a voting ballot will confirm the voter's privacy i.e., voter's personal information and to whom voter vote. Voter will use this DVB to cast a vote marked it with signature. The assigned digital token which has a unique hash number will be used by the voter to sign the ballot for casting a vote following Elliptic curve digital signature algorithm. At the initial stage, system will compute (C′) the hash number (c) generated on the basis of NADRA details.

$$Compute\ C' = HASH\ c \tag{1}$$

Consider 'I' as the identity element and 'E' denote elliptic curve base point where 'q' is the integer order in 'q × E = 0. The bit length of 'q' is denoted by 'L_q'. Let, z be the L_q left most bit of compute C′.

A pair of keys i.e., public key and private key will be generated by the system using ElGamal Cryptosystem along with the creation of digital ballot. Where the public key 'PK_i' will hold voter's personal information like name, f/name, CNIC etc. and private key is an integer denoted by 'PK_j' contain confidential information such as candidate to whom voter cast a vote. The public key PK_i is a curve point. The flow of signing process is depicted in Fig. 3 and can be calculated using pseudo code given below.

Pseudo code: Vote Casting Process

Step 1. Set $PK_i = PK_j \times E$ (where '×' denotes elliptic curve point multiplication)
Step 2. Select a random integer k from [1, q − 1]
Step 3. Compute, PK_i, $PK_j = k \times E$
Step 4. $r = PK_i \pmod n$
Step 5. If r == 0 then return to (step 2)
Else Compute, $s = k^{-1}(C + r(PK_j)) \bmod q$
Step 6. If, s = = 0 then return to (step 2)
Else the signature of the vote is (r,s)

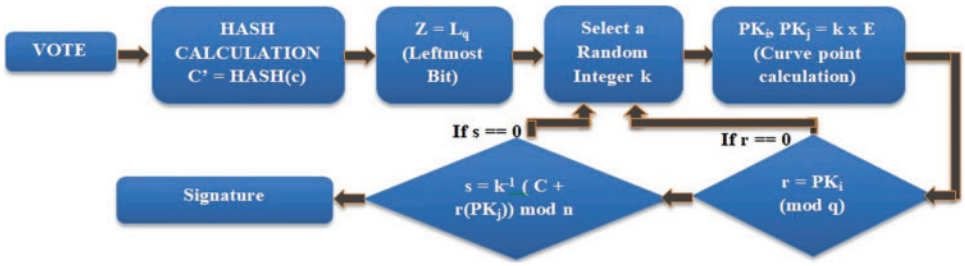

Figure 3: Voter authentication and ballot signing process

3.3 Vote Casting Phase

After the completion of voters validation phase, the process of vote casting is started. First of all, voter display the CNIC card in front of officials. The e-Voting system automatically detains the identification number and conforms either it is registered or not. If the voter is already registered then system ensures its status. If the status is not verified by the system then voter is inquire to give his fingerprint. The e-Voting system will recognized the voter after successful matching of fingerprint and provide vote ballot. Now the voter is able to cast his/her vote to his/her preferred candidate. After this process, the necessary information pertaining to the vote along with identification number will send in an encrypted form to the local as well as main servers. Furthermore, the voting stage will be enabled to the voter as soon as election takes place. Voter will be assigned with the Public key (PK_i), Private key (PK_j) and DVB. The voting ballot will be created and encrypted by the central authority (using ElGamal encryption algorithm) as this voting ballot is full of confidential information when signed and passed by the voter. Hence, voter needs to decrypt the ballot by using his/her PK_j.

3.3.1 Keys Management

Focusing on the security issues and system's credibility, we use asymmetric key structure in this system. Keys will be generated based on the ElGamal Cryptosystem, RSA 1024-bitand Hash functions using MD5 [29]. The generated PK_i will be uploaded which will later be used for updating voting blocks and PK_j will be kept secret by the voter used for signing and casting a ballot. This pair of PK_i and PK_j will be generated only at the time of election and will be valid till the validation of DVB. As soon as the session of the DVB will destroy, these pair of keys will no longer be useful. A common encrypted key will be used by the system through which public keys of all the voters will be computed and update voting blockchain accordingly.

3.3.2 ElGamal Cryptosystem

ElGamal Cryptosystem is popular and efficient in performing encryption and decryption tasks. Consider 'C' be the cyclic group, 'P' group of prime order numbers and 'g' as a key generator where 'n' denotes the total number of voters. PK_i and PK_j will be generated for each i^{th} voter (individually), and then the distributed ElGamal algorithm for key generation is defined as follows:

$$CK = \prod_{i=1}^{n} yi = g^{x1+\ldots xn}(CommonPublicKey = CK) \tag{2}$$

Common Public Key = CK

3.3.3 Encryption

The encryption process for PK_i and PK_j will be done by the system by keeping in view increasing the security and authenticity of the system. Encrypt the plaintext for CK: $m \in C$. Choose an Integer '*i*'(randomly) from 'P' i.e., $\int_P^*$, compute c1 and c2 respectively;

$c_1 = C^i$ and $c_{2=C}{}^m.PK^r$

Encrypted Keys generated for the voters $E(n) = (c_1, c_2)$.

3.3.4 Decryption

CK will not be computed during decryption. Partially, decrypted values for Pk_j will be computed and decrypted by the system. Combining all the decrypted values of keys, plaintext will be revealed to the voters. The decryption process of keys will be performed as follows; broadcast $c_1{}^{xi}$ will be calculated for n^{th} voter. Whereas, system will be allowed to calculate $H(c_1{}^{xi})$ values and compare and matches it with respective voter's $c_1{}^{xi}$

$$\frac{c2}{\prod_{i=1}^{n}} = \frac{c2}{c1^{x1+\ldots+xn}} = C^n \tag{3}$$

Discrete logarithm will be computed and revealed *n.* To perform the multiplication and exponentiation operations on a cipher text at their encrypted format, ElGamal encryption method allows with homomorphism property.

$$\begin{aligned} E(n_1) \times E(n_2) &= (g^{r1}, g^{n1}.CK^{r1}) \times (g^{r2}, g^{n2}.CK^{r2}) \\ &= (g^{r1+r2}, g^{n1+n2}.CK^{r1+r2}) \\ &= E(n_1 + n_2) \end{aligned} \tag{4}$$

$$\begin{aligned} E(n_1)^{n2} &= (g^{r1}, g^{n1}.CK^{r1})^{n2} \\ &= (g^{r1.n2}, g^{n1.n2}.CK^{r1.n2}) \\ &= E(n_1.n_2) \end{aligned} \tag{5}$$

3.3.5 Ballot Signing and Ballot Casting

A Digital voting ballot will be created by the system when the voter will be ready for casting a vote. ElGamal encryption algorithm is used for the encryption of DVB as this ballot is full of confidential information i.e., voters secrete data and to whom voter cast a vote [30]. Each ballot will be displayed with all the candidates who took part in the election. Voter needs his/her PK_j in order to decrypt the ballot to sign DVB and cast a vote. Voter will put his/her signing mark on its considerable candidate supporting with Digital Signature Algorithm at the back-end. The casting ballot will be in the encrypted format so that voter's information will be concealable. After signing the ballot, whole information of the ballot will be converted in to the binary number and ballot will be considered as matrix of the size of $N_c \times B_c$. Where, N_c is considered as the total number of candidates while B_c defines number of bits to voter's selected candidate. After binary conversion, the signed ballot will be encrypted before submission. A block encryption instead of bit-by-bit encryption process may decrease somehow computational cost of the system. But from the security point of view it seems quite efficient method. Hence, making the system more complicated in order to make it more secure, each bit of the ballot will be encrypted individually by the e-Voting system where, $B^i_{x,y}$, represents the selected candidate by the voter with respect to the total number of candidates as a binary bit (0,1) with (x, y)

position while $E^{i}_{1,1}$, denotes encrypted value of binary number where $x \in [1, N_c]$ and $y \in [1, B_c]$. The equally conversion of binary matrix and encrypted version of the DVB is shown in Fig. 4.

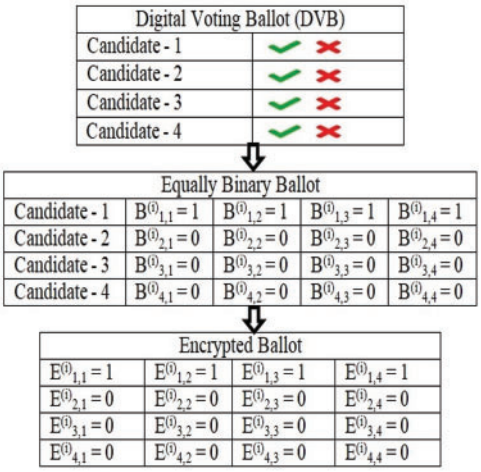

Figure 4: Conversion of digital voting ballot

The encryption and decryption process of digital ballots performed using distributed ElGamal encryption algorithm [30]. The respective ballot after the completion of encryption task will be computed using Proof of Partial Algorithm (PPK) given below and will be casted (sent) to the system. PPK is used to generate each encrypted element consist of variables $T0 = g^{t}$, $T1 = PK_i^{t}$, $T2 = (g^{m2.v2}.PK_i^{s2})/c2^{v2}$, $v = \text{hash}(c1||c2||T0||T1||T2$, $v1 = v \oplus v2$ (where $\oplus$ denotes XOR), $s1 = r.v1 + t$. The variables v2 and s2 are used for random values and variable k is used for repetition of group of statements, while T0, T1, T2, v1 and s1 are computed by using random values t, v2 and s2. Based on voter's signature against the selected candidate, the encrypted ballot $E(B_i) = (E^{(i)}{}_{1,1}, \cdots, E^{(i)}\ N_c, B_c)$ represents either $E_{(1)}$ or $E_{(0)}$.

Algorithm: Proofs generated process for casted ballot

Input: V_i, $E(B_i)$, PK
Output: $PPKs^{(i)}$
1 set PPKs = { }
2 for $j \leftarrow 1$ to n_c do
3 for $k \leftarrow 1$ to L_P do
4 PPK of $C^{(i)}{}_{j,k}$: prove $C^{(i)}{}_{j,k} = (c_1, c_2)$ is either E(0) or E(1)
PPK{($C^{(i)}{}_{j,k}$, *T0, T1, T2, v1, v2, s1, s2*):
$v1 \oplus v2 = H(C^{(i)}{}_{j,k} ||T_0||T1||T_2)$, $g^{s1} = T_0 \cdot c_1{}^{v1}$,
$PK^{s1} = T_1 \cdot (c_2/g^1)^{v1}$, $PK^{s2} = T_2 \cdot (c_2/g^0)^{v2}$}
$PPKs^{(i)} = PPKs^{(i)} \cup PPK$
5 end
6 end
7 return $PPKs^{(i)}$

3.4 Block Generating Phase

As soon as voter cast a vote and DVB sent to the system and our system will generate a block with the data of voter name, voter CNIC, voter PK_i & PK_j, DVB ID & Number, DVB data (vote casted against the selected candidate), DVB Hash Number, Hash of current block (unique), Hash of last block added in to the voting blockchain. The newly generated block is illustrated in Fig. 5.

Figure 5: Illustration of a newly generated block

System will verify the dual voting against the same voter using the hash identity of the block. If same hash number found in the distributed ledger, system will generate a message regarding rejection of vote and redirect user to the dashboard or else cast the vote as valid. Furthermore, the system will compute the hash number of new generated block using SHA-256 algorithm and compare with the hash number generated for the DVB to determine the data integrity. SHA-256 algorithm is mostly preferable by the scholars for the computation process of hash number. In our developed system, the binary encrypted DVB is considered as the message to the SHA-256 algorithm. Pad E with n^{th} time of iterations in a sequential manner. The length 'l' of the ballot will be considered 64 bit. Such as:

$$E' = Pad(E) \tag{6}$$

The system will then broke E′ in to the multiple chunks i.e., 512-bit chunks. Such that:

$$E' = E^{(1)}, E^{(2)}, \ldots, E^{(n)} \tag{7}$$

We use 64 constants i.e., $Z_0, Z_1, \ldots Z_{63}$ and select eight working variables as an initial hash values such as: $A = 0 \times 6A09E667$, $B = 0 \times BB67AE85$, $C = 0 \times 3C6EF372$, $D = 0 \times A54FF53A$, $E = 0 \times 510E527F$, $F = 0 \times 9B05688C$, $G = 0 \times 1F83D9AB$, and $H = 0 \times 5BE0CD19$. Based on these given values system will start iterative process of computation of computing 64-Cryptographic cycles. The output of the 1^{st} iteration will be used as an input for second iteration and so on. At the end of the last iteration, the generated result will be considered as the final hash number of the block. The hash value computation process is depicted in Fig. 6.

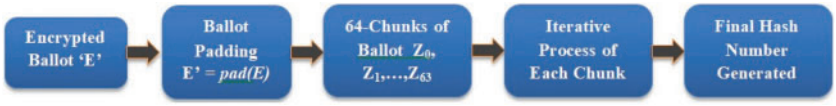

Figure 6: Computing process of hash value

3.5 Adding New Block to Blockchain

The concept of Blockchain is structured in such a way that every block in the chain is cryptographically connected with the previous block. Every new block added in to the chain has the hash value of the previous block. Successful computation of hash value for the block indicates a valid block

formation. Block with the same hash value indicates dual-voting and it will lead system towards the discarding of dual-voting block. A P2P network concept is used for adding new block in to the chain. Number of block chains is depending on the number of candidates participated in the election. When a new block is generated, system use PoW algorithm to link the block with the respective blockchain by using voter's PKi. Newly created block, when added in to the chain, linked to the previously casted vote/block (using Hash of previous ID/Block). The block chain will be updated every time when new block will be added to it. Each block is composed of three parts i.e., Hash of the block, Data part and Hash of the previous block. Fig. 7 shows the structure of the blockchain and blocks added in to it.

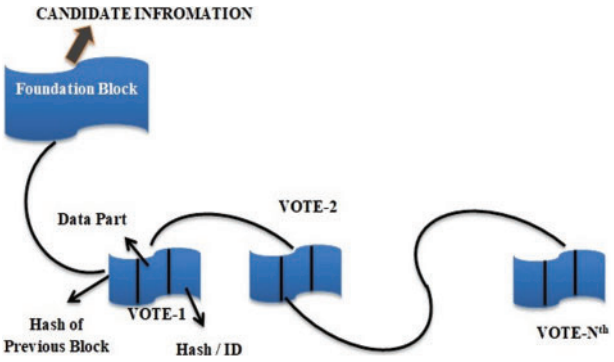

Figure 7: Structure of blockchain

3.6 Votes Counting

We have used some main steps for the process of votes counting using the simulated e-Voting system. The counting process is started by the counter module after receiving the particular vote; e-Voting system decrypts the given information of voter using the ID number and private key. After that overall voting information along with casted vote is automatically updated and using the all votes obtained from the counter module system will confirmed and announced the winning candidate of specific area of district. At the end of the election period, system will display election results solely on user's dashboard. System will display real time results to the voter i.e., total votes cast to that particular candidate and total votes cast against other candidates.

4 Simulation Study of E-Voting System

State diagram in Fig. 8 shows the voting process and the complete process of simulation modeling present in [31] has been adopted and 28 voting stations were selected for simulation average. Voting process and arrival of voters were emulated and include as simulator modules. Vote casting by the voter irrespective of voter's voting origin was allowed by the simulator and that is the main advantage of an online e-Voting system. A fairy large number of simulation for the proposed framework of e-Voting was conducted by selecting the sample range of 10220 voters. It was realized that the simulated voter's number is much lesser the actual number of voters in the constituency but the results after simulation seems fairly scalable as the simulation model is capable to model fairly large number of voters. The number of voters at the given polling stations was fixed during the simulation process though in reality this number may be varied by a small fraction due to the fact that people will be allowed to vote from anywhere for the voting convenience. A simulation software application is required hence; Flexsim 3D modeling software is used for development and execution of simulation model for E-Voting System. The simulation model is illustrated in Fig. 9.

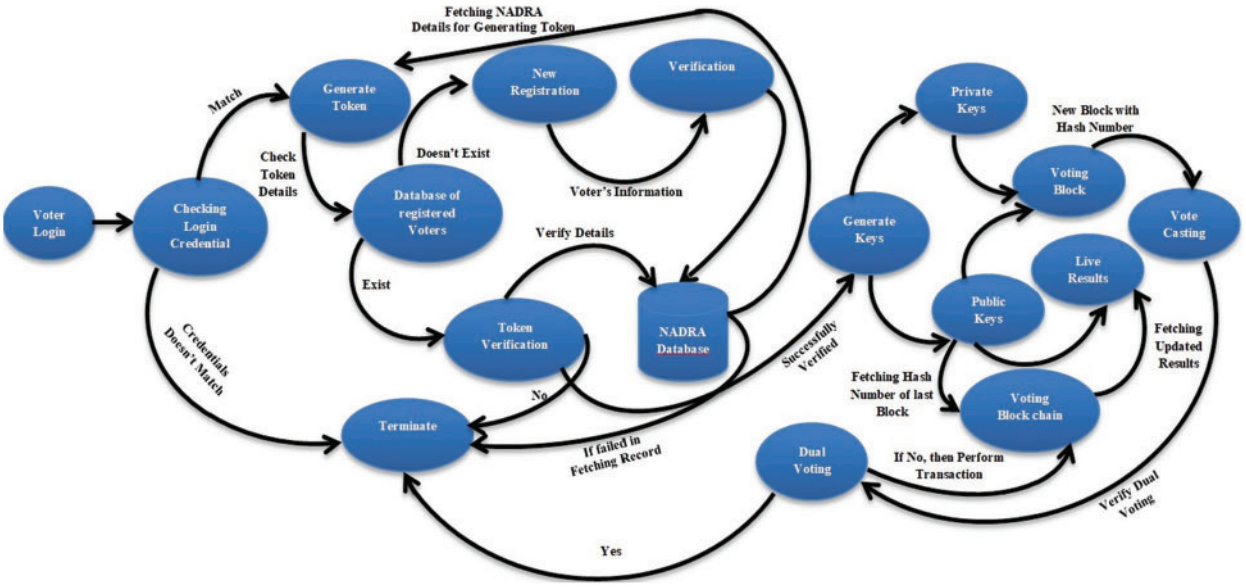

Figure 8: State diagram of simulated model

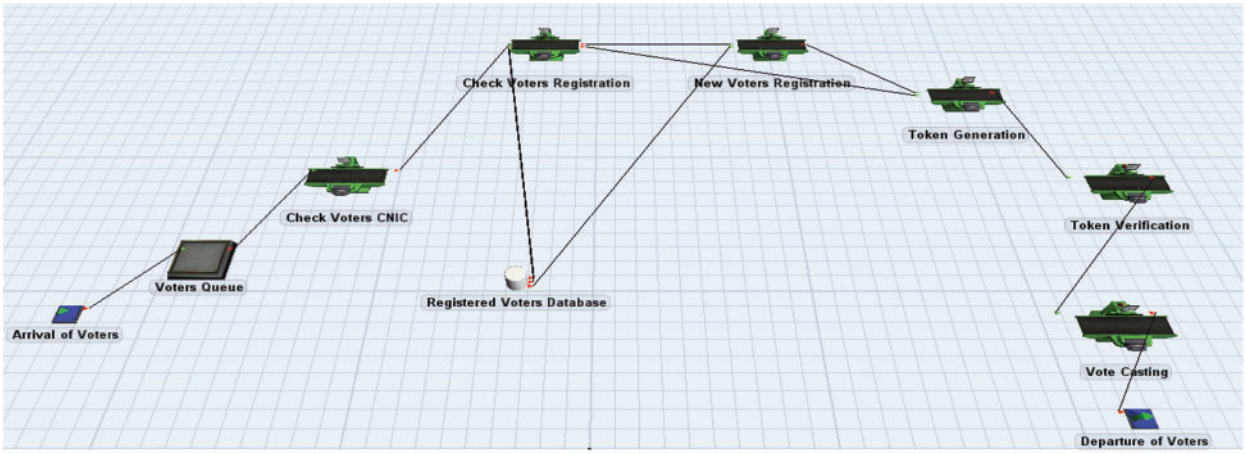

Figure 9: Simulation model for e-voting system

Voters are randomly arriving at polling station according to Poison random process in simulation model based on the (M/M/S) queuing model because we have multiple servers and single queue for voters. Mean time method is used to control the inter arrival rate between two successive arrivals (mean inter arrival time, μ) and is governed by an exponential distribution. The number of voting station can be increased as desired. The arrival of voters varies over time; near to election closing time and in mid-morning time rate of arrival is characterize as heavy, and in early hours the rate is characterized as low. Values of $\mu = 2$, 5 and 10 chosen for low, moderate and large inter-arrival rates respectively during the simulation [31].

Usually voters arrive in clustered manners i.e., in groups compared to individual arrival; variable λ represents Poison random variable for an average size cluster. In the simulation $\lambda = 2$ and $\lambda = 5$ represents the low and high voter densities respectively as discussed in [31]. For example large clusters

of voters arrival are represented using the values $\lambda = 5$ and $\mu = 10$ with dispersed time intervals. On every polling station the number of voters expected to vote is always predefined. Our model simulates the stations with as few as 365 voters and as many as 10220 voters. In general the random number of voters per polling station will be selected for the simulation which will be executed until all the registered voters cast their votes. Simulator can be tuned for any required simulation time period but in the model it is set to 8 h.

Voters are required to be in queue at every voting both in each voting station and there will be N voting both in a voting station hence the N queues formed in every voting station. On arrival of group of voters, the simulator shifts the voters to the proper appropriate queue using round robin method like one voter per queue at a time. The round robin scheduling policy is used in the simulator. Moreover, service time (the time taken by one complete voting transaction) is blend as real time execution and random delay time due to several factors. The combination of average time required verifying voter using CNIC and time voter takes from de-queued to vote cast used to measure the random delay time. The mean vote casting time is also calculated and presented in the paper. The average time is empirically determined using typical scanners and tough screen. The database transactions undertaken in the simulator include setting the voter flag.

In our simulation model, the central database server and the local voting station servers are placed within the same local network segment, so the random delay is introduced to compensate for transfer time over inter-network. The transfer time is a function consists of available network bandwidth and the message size, several bandwidth sizes are used in this study. The simulation model entails a blockchain-based distributed ledger technology to enhance the security for voters and candidates as well. Authentication and locality of voter is also recorded beside the personal information of voter. The simulation consist of modules emulate the arrival of voters at the polling station and voting process itself.

5 Results

Pakistan is divided in 4 units called provinces and Sindh is one of them. Province Sindh is consisting of 29 districts with 22.391 Million registered voters and Khairpur is among the one of largest districts of Sindh having 1.075 Million registered voters. The district consist of 7 seats for provincial assembly i.e., PS-26, PS-27, PS-28, PS-29, PS-30, PS-31 and PS-32. To experiment the e-Voting System polling stations of PS-26 constituency are selected for the simulation study. The total 166068 number of voters in the constituency are divided in 456 polling stations where the elections are being organized by Election Commission of Pakistan. Tab. 2 show the detailed information about the registered voters of selected polling stations collected from district office of Election Commission Khairpur and that information was generated to conduct the General Elections, 2018. A voter is an individual who is not only the eligible to vote but also he/she can authenticate himself/herself, load ballot, cast the vote and verify the vote also after the election. NADRA is the central agency to keep record of information of every individual in Pakistan and the voter's information can be fetched from NADRA as this agency has the complete developed information system. It is mentioned in our proposed framework, that database from NADRA will be used in our developed system but at current level a local database is created with the same schema as the NADRA's database for the experiments due to official restrictions and permissions from the government of Pakistan.

Table 2: Selected polling stations and number of voters

Name of selected polling station	No. of voters assigned to polling station		
	Male	Female	Total
GPS Saleem Abad	976	772	1748
District Council Office, Khairpur-1	540	0	540
District Council Office, Khairpur-2 (M)	1358	0	1358
GPS Sultanul Madaras-1 (M)	966	0	966
GPS Saida Goth-1 (M)	1015	0	1015
GPS Girls Katchary Road, Khairpur-1	728	643	1371
GPS JilaniMuhallah (M)	1604	0	1604
Govt. Elementary College, Khairpur (M)	1618	0	1618
Total			**10220**

A vote can be casted using a ballot having the name of all the candidates with different electoral symbol against the name of each candidate. Voters can cast their votes according to the candidates their polling stations. In our proposed e-voting system, a described procedure in [30,32] is adopted for the voter's registration, in which the CNIC ($i = 1, 2, \ldots, N$, where N is equal to maximum voters allowed in polling) must be presented by the each voter (V_i). After the verification of a voter a Signature Key Pair consist of a Public Key (pkv_i) and a Private Key (pkv_j) is generated for the voter. The (pkv_i) is publically available to the public bulletin board by uploading the key while (pkv_j) is the secret key for the voter (V_i) which must be kept secret by the voter. Once the registration of the voter is completed the voter's identity and the correspondence public key will be available on public bulletin board. Digital Signature Algorithm will be used for each voter's required signature to sign the ballot. The pkv_j of voter is used to sign the voters submission and published pkv_i can be used to verify their signature $Sigv_i$.

Scope of our project is limited to small-scale polling stations and election but a larger voting system for thousands of voters may have different issues to address. Scalability of P2P network is still unknown and required more research to address the issue so these contracts for nation-wide elections cannot be suggested. Providing anonymity for voters is fundamental problem in BC based e-Voting system with making compromise on the transparency of the general voting procedure. All the transactions are necessarily being written to the blocks of the BC as plain text and it is not possible that such system can be useful in official/critical elections. Guaranteeing the anonymity is also an important challenge in the current state-of-art networks.

5.1 Number of Voters and Voting Stations

It is always recommended to add more voting stations when the arrival of voters and number of voters rise in any particular constituency. Increment in polling stations may not the guarantee of improvement in the results significantly using centralized approach rather more voting stations simply shift the workload from local station to the central server. Distributed approach will be more useful in this context as the addition of local stations will distribute the execution load locally without affecting the central server.

Number of voting stations required to complete all electoral transactions in the time duration of 8 h for different voting populations are shown in Fig. 10. For example to allow all the 10220 voters to vote in 8 h (8:00 am to 5:00 pm) 28 voting stations are required to be setup With the assumption of 1 Mb/s bandwidth and a clustered policy in a distributed architecture. It is reiterated that the list of polling stations and voters in PS-26, Khairpur are selected for the experiments and the list of selected polling stations and the number of voters assigned to each polling stations are represented in Tab. 2. Fig. 10 shows the 10220 voters and 28 polling booths where 1 booth is fixed for 365 voters.

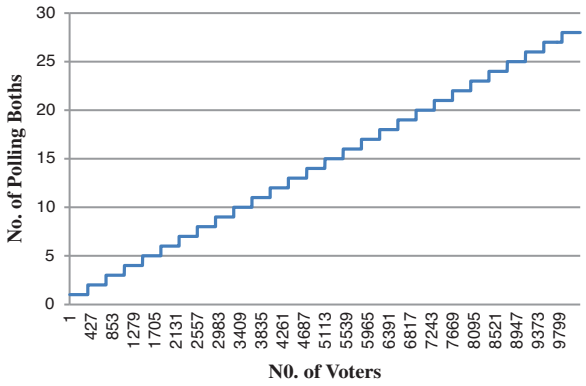

Figure 10: Configurations of polling booths and voters

Office of the Election Commission is responsible to properly size a given voting station with the certain number of voting population and the bandwidth availability. Time required to complete all voting transactions is shown in Fig. 11 with a certain number of voting stations and the voting population. The trade-off between the voting time and the number of voting stations is illustrated in this figure. Voting time period can be extended as per the availability of voting stations in the countries, where the cost of voting stations is a real burden. In Pakistan the voting time is usually limited to 8 h for the voters to cast their votes i.e., 8:00 am to 5:00 pm. The voting times and contract creation is presented in Tab. 3. As above discussed the 28 polling stations are estimated for 10220 voters to cast their votes and 166068 voters are registered in the selected constituency of the PS-26, Khairpur. It is difficult task for election commission to arrange such large number of polling stations and one of the solutions to this problem is to increase the voting time by decreasing the number of polling stations. The tradeoff of voting time distribution over the number of polling stations is shown in Fig. 11. From this figure decrease of 3 polling stations can be observed with increase of 1 h of poling time and 5 polling stations can be decreased with increase of 2 h of voting time.

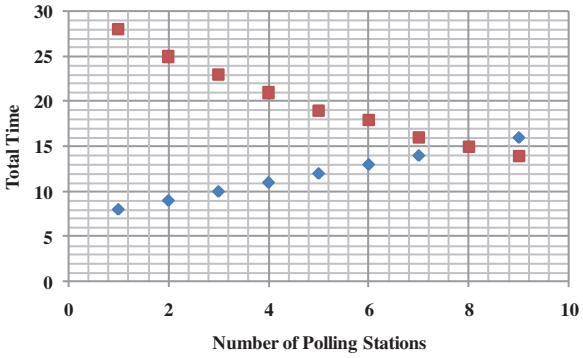

Figure 11: Distribution of voting time over no. of polling stations

Table 3: Voting times and contract creation

	Contract creating	Voter-1 trans.	Voter-2 trans.	Voter-3 trans.	Voter-4 trans.	Voter-5 trans.
V-1	58 s	56 s	1 m 2 s	1 m 3 s	1 m 25 s	1 m 17 s
V-2	55 s	55 s	1 m 21 s	59 s	1 m 27 s	1 m 28 s
V-3	1 m 5 s	1 m 2 s	1 m 9 s	1 m 9 s	1 m 33 s	1 m 9 s
V-4	1 m 9 s	1 m 9 s	1 m 8 s	1 m 8 s	54 s	1 m 38 s
V-5	1 m 14 s	1 m 15 s	56 s	42 s	1 m 1 s	1 m 23 s
V-6	58 s	1 m 29 s	1 m 38 s	57 s	1 m 37 s	59 s
V-7	1 m 18 s	1 m 12 s	1 m 29 s	1 m 23 s	1 m 41 s	1 m 16 s
V-8	1 m 17 s	1 m 25 s	1 m 43 s	1 m 28 s	1 m 51 s	1 m 44 s
V-9	1 m 28 s	1 m 3 s	1 m 17 s	1 m 41 s	1 m 24 s	1 m 22 s
V-10	1 m 39 s	59 s	1 m 4 s	1 m 52 s	1 m 29 s	1 m 9 s

Each voter should submit the vote to the server by casting ballot which required to be encrypted for each voter to prevent the order of votes to be revealed after the submission of vote and to achieve this target every element in the ballot must be encrypted. The performance of the system with respect to the voter is calculated in [30,32]. The well-known Digital Signature Algorithm is used for signing purpose of each ballot before the submission. Furthermore the time for processing the sign is approximately equal to the time of one exponentiation. In the experiment, the total time spent for encrypting one ballot is tested in five rounds on the laptop, for the different number of candidates i.e., 3, 5, 10, 15 and 20. In Fig. 12, the computation time is presented which does not include the decision time taken by the voters. Only the algorithm's computation time is represented which converts all plaintext ballots casted by the voters to cipher text ballots and tallying them. The results of Fig. 12 shows the time cost for casting a ballot is approximately 0.18 s even in the case of 20 candidates in the election.

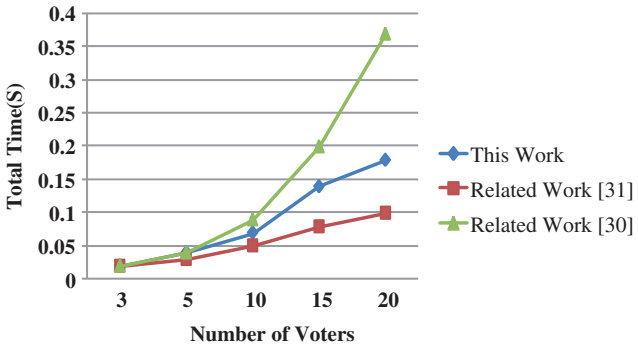

Figure 12: Estimated time spend casting a ballot with 20 voters

5.2 Network Bandwidths

Models performance can be varied depend on the bandwidth of wide area network as the performance is directly proportional with the network's bandwidth. Fig. 13 shows the average service time for three different bandwidth values (3, 12 and 20 Mb/s). The results are shown for different voting stations; and it is shown that network affect at the various voting stations i.e., 28 voting stations have been incubated at a particular voting center. The time taken to process a vote once the voter is admitted into system is described as the service time. This time is consisting of identity verification, authentication, flag checks, update time to the central database and the statistics update. Bandwidth over 12 Mb/s, any pronounced improvements start to weaken. In the figure x-axis represents the number voting stations used to process the voter population. The results are averaged over an 8-h simulation time frame for 10220 voters which are shown in the Fig. 13.

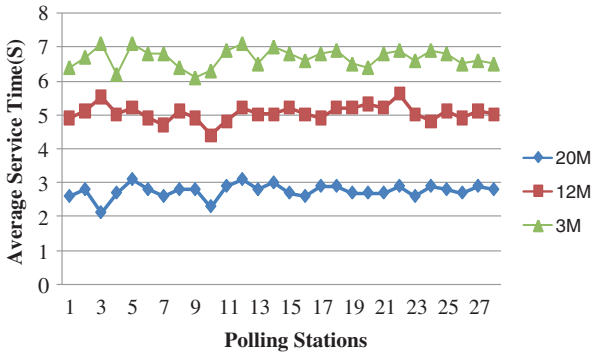

Figure 13: Impact of network bandwidth

Furthermore, the simulator was setup to simulate and accommodate all voters within a time frame of 8 h. The average queue length for different bandwidths and polling stations is also calculated during the simulation. The shorter the queue is lesser the time for a voter to expect waiting time before sating a vote inside the voting station. The average queue lengths can get 3 times bigger length with low speed network connections (3 Mb/s). Fig. 14 also confirms improvement of performance beyond the 3 Mb/s is rather insignificant.

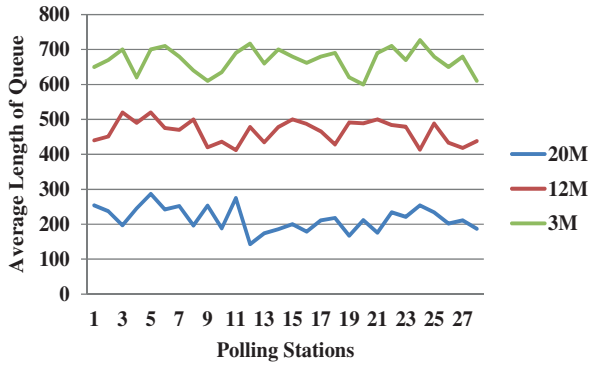

Figure 14: Average length of queue at polling stations with network bandwidth

5.3 Scheduling Policy

Another performance measure of the voting process is scheduling policy of the voters to the available voting stations which impact directly on the overall performance. The appropriate selection of scheduling algorithm is important for e-Voting system. In this paper, we have experimented clustered scheduling mechanism because people usually arrive in groups. Furthermore, at the polling stations, voters are arrived at an average rate of $(1/\mu)$. It is observed that the voters are usually reached at polling stations in groups with a mean (λ) as per Poisson random process. Hence; clustered based scheduling policy is used while the simulation of e-Voting system and assigns all (λ) voters with the smallest length of queue even it is fact that few polling stations may become busy with large number of voters and some are free. The average queue length at 8 voting stations is depicted in Fig. 15 using clustered scheduling technique that demonstrates extensive variation among the selected polling stations. The vote completion time and the lengths of queue are focused in experiments. The voting process in some polling stations is completed within 6 h while at some stations voting process is continuing up to 5 pm. Furthermore, this scheduling scheme is adopted due to the simple implementation while distribution of voters is not required among the polling stations.

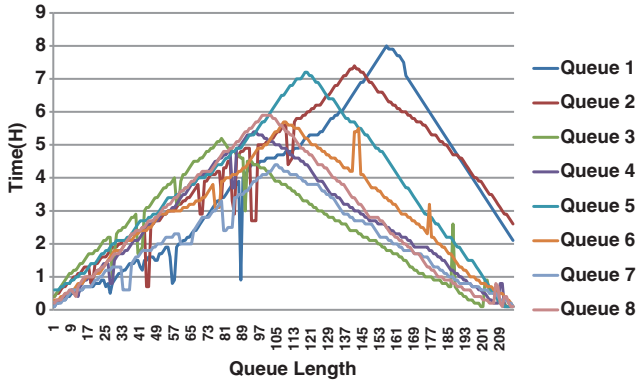

Figure 15: Clustered scheduling

The developed e-voting featured with blockchain technology was evaluated with fundamental variables of any robust and reliable e-voting system and it is purely based on our proposed framework. Different software practitioners conducted the testing involving the political intellectuals considering the 28 polling stations. A questionnaire with the questions related to accuracy of the developed e-voting

system was distributed among them. System behavior for intelligent democracy was also asked in the questionnaire. Various questions related to privacy, accuracy, verifiability, mobility and auditability of the e-voting system were also part of the questionnaire. 100% response ratio was received from the selected observers as shown in Fig. 16.

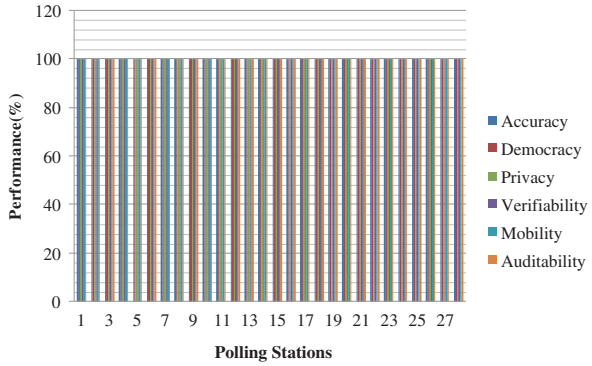

Figure 16: Performance evaluation at selected polling stations

5.4 Latency Measurement

Moreover, we also performed analysis on obtained results by measuring the latency of our proposed system. However, instead of measuring the latency of individual block we compare latency of overall system. A cumulative density graph is depicted in Fig. 17 which shows the latency distribution against the predicted and simulated measurement. In practice we measure roundtrip-time which is composed of block processing latency (transmission, propagation and queuing delay time). For latency scale the transaction process is defined as follows. When a voter finalized the submission process, a script generated which trigger the transaction (the voting block). An adequate number of authenticated blocks confirmed by the trigger against the blockchain included the transaction block and returned results to the script. After which script for the next transaction is generated.

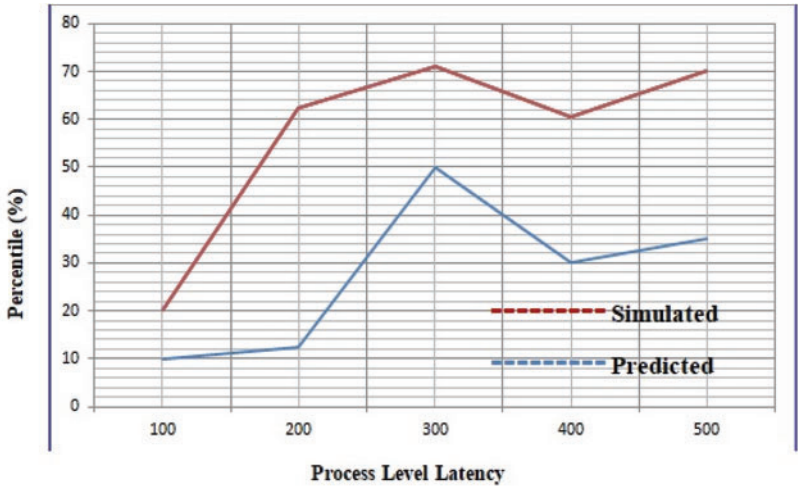

Figure 17: Cumulative distribution of latency

6 Conclusion

The purpose of this research is to design a framework that helps to develop reliable e-voting system with the use of latest state-of-the-art technologies for fair and free elections in Pakistan. Flexsim 3D simulation software is used for simulation of proposed framework. The system keeps up to date with the voting calculations in real-time along with the observance of integrity of voting process from very minute steps of casting vote. Highest priority is focused upon the transparency and auditability, on the part of voter, the candidate, election office and the system levels. The system is smart in order to deny any illegal voter/s interrupting the system by attempting multiple times for the same vote. The system block all forms of malice producing adverse effects on the voting process simultaneously. The simulated results can also raise the confidence of voters, candidates and the election commission as the BC based distributed ledger are used effectively. The simulated results show the frequency of the important factors to be examined prudently by the election commission of Pakistan. The contesting parties may also prioritize the e-voting in order to keep from the malignant factors affecting the election process every time. These factors work to realize the number of booths at any voting stations that is required according to the voting needs of the voting district and the network bandwidth to be given to a polling station. The system through these simulations has proved to be effective and useful having rigid and sustained reliability. This is because of the capacity of the system for denial of the same voter and internal audit maintenance. The encryption and decryption processes are performed focusing fundamental requirements of e-voting. The experimental simulation modeling is performed on the eight selected polling stations of district Khairpur. This will also be experimented on the platforms of urban and rural areas of Pakistan.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] W. Wojtasik, "Functions of elections in democratic systems," *Political Preferences*, vol. 4, pp. 25–38, 2013.
[2] K. Mahender, C. P. Katti and P. C. Saxena, "A secure anonymous e-voting system using identity-based blind signature scheme," in *Proc. Int. Conf. on Information Systems Security. Lecture Notes in Computer Science 10717*, Mumbai, India, pp. 29–49, 2017.
[3] P. S. Naidu, R. Kharat, R. Tekade, P. Mendhe and V. Magade, "E-Voting system using visual cryptography & secure multi-party computation," in *Proc. Int. Conf. on Computing Communication Control and Automation*, Pune, India, pp. 1–4, 2016.
[4] M. Prandini, L. Sartori and A. Oostveen, "Why electronic voting?," in *Proc. Int. Conf. for e-Democracy and Open Government*, Hong Kong, pp. 1–7, 2014.
[5] N. Zafar and A. Pilkjaer, "E-voting in Pakistan," Master Thesis, Department of Business Administration and Social Sciences, Lulea University of Technology, 2007.
[6] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa and G. Hjalmtysson, "Blockchain-based e-voting system," in *Proc. IEEE 11th Int. Conf. on Cloud Computing*, San Francisco, CA, USA, pp. 983–986, 2018.
[7] J. Mendling, I. Weber, W. V. Aalst, J. Brocke, C. Cabanillas *et al.,* "Blockchain for business process management-challenges and opportunities," *ACM Transaction on Management Information System*, vol. 9, no. 1, pp. 4:1–4:16. 2018.
[8] S. Olnes, J. Ubacht and M. Jansseen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Government Information Quarterly*, vol. 34, pp. 355–364, 2017.

[9] M. Pawlaka, A. Poniszewska-Maranda and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," *Procedia Computer Science*, vol. 141, pp. 239–246, 2018.
[10] J. MyungSan, "Blockchain government-a new form of infrastructure for the twenty-first century," *Journal of Open Innovation Technology Market and Complexity*, vol. 4, no. 7, pp. 1–12, 2018.
[11] A. Ojo and S. Adebayo, "Blockchain as a next generation government information infrastructure: A review of initiatives in D5 countries," in *Government 3.0-Next Generation Government Technology Infrastructure and Services*, Cham: Springer International Publishing, vol. 32, pp. 283–298, 2017.
[12] P. McCorry, S. F. Shahandashti and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *Proc. Int. Conf. on Financial Cryptography and Data Security*, Malta, pp. 357–375, 2017.
[13] E. Yavuz, A. K. Koç and U. C. Dalkılıç, "Towards secure e-voting using ethereum blockchain," in *Proc. ISDFS*, Antalya, Turkey, pp. 1–7, 2018.
[14] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," *International Journal of Network Security & Its Applications*, vol. 9, no. 3, pp. 1–10, 2017.
[15] J. Mendling, I. Weber, W. V. D. Aalst, J. V. Brocke, C. Cabanillas *et al.,* "Blockchains for business process management- challenges and opportunities," *ACM Transactions on Management Information System*, vol. 9, no. 1, pp. 1–16, 2018.
[16] A. Ahmed, N. Qassim and M. Abu Talib, "Blockchain for government services-use cases, security benefits and challenges," in *Proc. 15th Learning and Technology Conf.*, Jeddah, Saudi Arabia, pp. 112–119, 2018.
[17] Y. Luo, Y. Chen, Q. Chen and Q. Liang, "A new election algorithm for DPos consensus mechanism in blockchain," in *Proc. 17th Int. Conf. on Digital Home*, Guilin, China, pp. 116–120, 2018.
[18] J. Hsiao, R. Tso, C. M. Chen and M. E. Wu, "Decentralized e-voting systems based on the blockchain technology," *Advances in Computer Science and Ubiquitous Computing*, vol. 474, pp. 305–309, 2018.
[19] 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.
[20] K. Patidar and S. Jain, "Decentralized e-voting portal using blockchain," in *Proc. 10th Int. Conf. on Computing, Communication and Networking Technologies*, Kanpur, India, pp. 1–4, 2019.
[21] H. Yi, "Securing e-voting based on blockchain in P2P network," *Journal on Wireless Communication and Networking*, vol. 2019, no. 137, pp. 1–9, 2019.
[22] K. M. Khan, J. Arshad and M. M. Khan, "Empirical analysis of transaction malleability within blockchain-based e voting," *Computers & Security*, vol. 100, pp. 102081-1-22, 2021.
[23] Y. Abuidris, R. Kumar, T. Yang and J. Onginjo, "Secure large-scale e-voting system based on blockchain contract using a hybrid consensus model combined with sharding," *ETRI Journal*, vol. 43, no. 2, pp. 357–370, 2020.
[24] P. Baudier, G. Kondrateva, C. Ammi and E. Seulliet, "Peace engineering: The contribution of blockchain systems to the e-voting process," *Technological Forecasting and Social Change*, vol. 162, pp. 120397-1-11, 2021.
[25] R. Taş and O. O. Tanrıover, "A manipulation prevention model for blockchain-based e-voting systems," *Journal of Security and Communication Networks*, vol. 2021, no. 6673691, pp. 1–16, 2021.
[26] S. Prk, M. Specter, N. Narula and N. L. Rivest, "Going from bad to worse: From internet voting to blockchain voting," *Journal of Cyber Security*, vol. 7, no. 1, pp. 1–15, 2021.
[27] B. A. Campbell, C. C. Tossell, M. D. Byrne and P. Kortum, "Voting on a smartphone: Evaluating the usability of an optimized voting system for handheld mobile devices," in *Proc. of the Human Factors and Ergonomics Society Annual Meeting*, vol. 55, no. 1, pp. 1100–1104, 2013.
[28] C. Padmaja and N. S. Reddy, "Aadhar based electronic voting machine (AVM) using IOT," *International Journal of Research*, vol. 7, no. 11, pp. 1096–1103, 2018.
[29] I. M. Rodiana, B. Rahardjo and I. W. Aciek, "Design of a public key infrastructure-based single ballot e-voting system," in *Proc. Int. Conf. on Information Technology Systems and Innovation*, Bandung, Indonesia, pp. 6–9, 2018.
[30] X. Yang, X. Yi, S. Nepal, A. Kelarev and F. Han, "A secure verifiable ranked choice online voting system based on homomorphic encryption," *IEEE Access*, vol. 6, pp. 20506–20519, 2018.

[31] M. Malkawi, M. Khasawneh and O. Al-Jarrah, "Modeling and simulation of a robust e-voting system," *Comm. of IBIMA*, vol. 8, pp. 198–206, 2009.
[32] A. Qureshi, D. Megias and H. Rifa-Pous, "SeVEP: Secure and verifiable electronic polling system," *IEEE Access*, vol. 6, pp. 19266–19290, 2019.