The Nucleus ***56****, No. 4 (2019) 137-143*

www.thenucleuspak.org.pk

The Nucleus

ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

Formal Analysis of Improved and Secure Architecture of E-voting System using Hierarchical Coloured Petri Nets

Z. Ahmad[1], F. Ahmad[2*] and Z.A. Gondal[2]

[1]*Department of Computer Science, Govt. College of Commerce, Shahdara, Lahore, Pakistan*

[2]*Department of Computer Science, COMSATS University Islamabad, Lahore Campus, Pakistan*

ARTICLE INFO

Article history:
Received: *28 March, 2019*
Accepted: *16 June, 2020*
Published: *19 June, 2020*

Keywords:
E-voting,
Authentication,
Component based architecture,
Coloured Petri net

ABSTRACT

Casting a vote is the fundamental right of any citizen. Pakistan follows the traditional manual voting system and there are number of factors influencing in such a way that put a question as if the vote has been casted correctly and should be considered towards final count. Manual counting process of vote do not provide the security measures minimizing the attempts of frauds like increase or decrease in the vote count. Therefore, the idea of secure and improved E-voting system is proposed to overcome such flaws in current voting system in Pakistan. In this manuscript, an improved component-based architecture, security features and future recommendations are presented. Different techniques linked with voter's authentication, confidentiality and integrity are suggested to minimize the flaws and maximize the benefits of voting system. Further, the proposed architecture is formally modelled through 'coloured Petri nets' to validate it. Formal analysis is also performed based on the state space generated to simulate the hierarchical coloured Petri net based formal model of proposed E-voting system.

1. Introduction

Casting a vote is considered fundamental right of every citizen in modern and democratic countries including Pakistan. However, existing voting systems are vulnerable to different malpractices and deceptions. Further, compilation of results for vote balloting in existing systems are slow due to the collection of data from distributed and remote locations. Furthermore, tampering of ballot paper, inclusion of every vote in counting or avoidance of casting duplicate votes are some of the issues which cannot be guaranteed in the existing voting systems. Some of the major challenges that contemporary voting systems are facing include manpower, voters' inconvenience and security [1-3]. Motivation of alleviating such fundamental issues leads to the need of electronic voting systems. This suggested idea of E-voting system shall not only make the voting system efficient but saves time, cost and manpower involved [4]. Therefore, in this research article, we have introduced an improved architecture of E-voting system in Pakistan.

The proposed system is secure enough to maintain voter's secrecy by using security mechanisms. Further, the proposed system minimizes the chances of errors and fraud. It also provides user friendly interface for voters. In E-voting system, special emphasis is provided in order to keep a vote anonymous to other authorities in order to achieve its secrecy and security requirements [5, 6].

The proposed architecture of E-voting system is a design that stores and maintains secrecy and security of voter's casted vote by using security mechanisms. The proposed design is different from existing traditional voting systems. It discusses the authentication of voters, maintaining the confidentiality and integrity [5]. In addition to these benefits, anonymity of the voter along with the feature of time stamp has been introduced which further ensures the security, the concept of receipt generation to the voter has also been introduced. We have set our secrecy and security criteria under four main attributes namely: integrity, authentication, confidentiality and anonymity.

In order to validate the architecture, the system is modelled through hierarchical coloured Petri nets [7]. Further, component based architecture [8] is adopted, by developing the authentication and vote-casting modules, for formal modelling. Finally, formal analysis is performed by generating the state-space and occurrence graph. Formal analysis explains that formal model of the proposed architecture is deadlock free. In addition, boundedness property ensures the control of the system and fairness property guarantees the smooth execution of the system.

In the recent years E-voting has been attracting the attention of different researchers because the E-voting system has the capability to improve the existing manual system. The related work in the domain of E-voting has focused on different aspects such as requirements, architectural design and the security requirements of the E-voting system. Different authors have worked on these areas. Requirements for E-voting systems with enough precision were expressed, moreover evaluation and certification of existing catalogues were taken into account [1, 2, 9]. Previously different phases and main actors of E-voting systems were studied and the importance of security has been discussed comprehensively [3, 10, 11]. Chowdhury [12] and Sarajlic et al. [13] described different types of biometric practices, recent trend of using biometrics, biometric fusion and its uses in E-voting systems that protect user privacy using random password distribution.

*Corresponding author: farooqahmad@cuilahore.edu.pk

To deal with the significant issues like transparency and auditability in E-voting, recently developed Blockchain technology may be a solution to these issues. Blockchain-enabled E-voting (BEV) could reduce voter fraud and increase voter access [14-16]. But the significance of proposed E-voting system which makes it different from others is that we have included all the features (the requirements of the E-voting system, the architectural design and the security requirements that the system must provide as a complete solution). Block chain and cloud based technology has also been used to develop the electronic voting systems in recent times [17, 18]. The system proposed in this paper is specifically designed for NADRA Pakistan. These requirements include the functional and non-functional requirements of the E-voting system.

2. E-voting Requirements

The proposed E-voting system has not been designed to handle remote E-voting mechanism, but the voters can cast their votes at designated polling station only. We have divided these requirements into functional requirements and security requirements.

These categories have been discussed below:

2.1 Functional Requirements

Functional requirements focus on the fact that voting machines (in the present study kiosk machines) are working correctly. The E-voting system should not be allowed the unauthorized users to cast vote. The voters can express their choice freely (they can choose any candidate among the one who are contesting) through the E-voting system. Another important requirement of the E-voting system is that it should ensure that one voter is allowed to cast only one vote, i.e., no duplication.

2.2 Security Requirements

The security requirements include that the E-voting system is protected from the external and internal adversaries. Fig. 1 shows the important factors involved in security requirements which are discussed below:

Vote casting through designated user interface: Vote casting will be allowed only by the user interface of the designed system. There should be no other way that the voter can use to cast his vote.

No Data Loss: There should not be any loss of data during or after the voting process.

Confidentiality: One voter's data and casted vote should be completely protected from other voters.

Un-traceability: The voters cast their votes anonymously, which means that it is not possible to associate a vote with the corresponding voter.

Reliability: The E-voting system should be reliable which means that it should not give wrong results related to vote counting. In the case, if kiosk machine goes out of order it must be ensured that the voter's vote has been added to the system.

Integrity: There should be no change in the votes that have been casted, which means that the integrity should be ensured by the E-voting system.

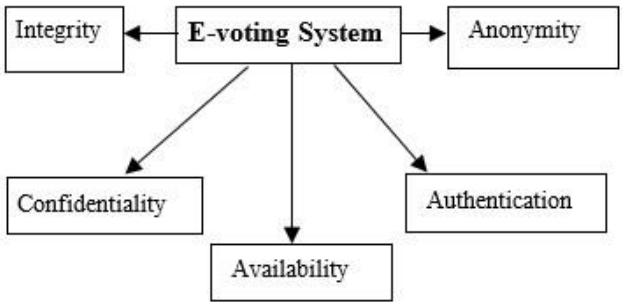

Fig. 1: E-voting security requirements.

3. Proposed Architecture of the System

E-voting system architecture consists of seven basic entities namely: voter, authenticator, validator, election commission (electoral database), voting manger, Ballot Distributor Counter (BDC) and tallying, as shown in Fig. 2. In E-voting, only registered voters can cast their votes. Registered voters lists are maintained in electoral database which is managed by election commission. Names of all eligible voters are stored in electoral database but only those citizens will be eligible to cast their votes who have registered themselves to get the right of casting vote. On being registered, election commission will give to that voter a unique login Id and password that is only known by the voter. When voter will come to cast the vote he/she has to pass from authentication criteria which is the very first step towards security.

Authenticator verifies the voter through biometrics device. On giving thumb impression, the details of a voter appear that include the CNIC of the voter, name and other details (see Fig. 2).

Then, validator will observe whether the voter is eligible to cast the vote. Validator uses three-way cryptographic policy and sends encrypted certificate to the voter. Voting console uses the three-way cryptographic strategy to encrypt the certificate with his/her key. The key is doubled by election commission and then from voter, afterwards it is sent to the validator from voter. Validator on receiving the encrypted certificate, decrypts it with the voter's own key and applies BDC key on the encrypted certificate and sends it back to the voter again. The voter receives certificate and uses his/her own key to decrypt the encrypted message. After this step, certificate can only be encrypted with BDC's key. The voter sends the encrypted certificate to BDC which is only encrypted with the BDC's key. BDC uses its private key to decrypt the certificate and then verifies that certificate from the election commission (EC). If the verification matches, then the voter is eligible to get ballot and can cast the vote. After the complete process of authentication and ensuring

confidentiality of voter, voting console is shown to the voter where he/she uses that unique login and password to cast his/her vote. The proposed system is efficient in every possible way and it adds a feature of trouble shooting voting console in the system. Suppose after authentication, when voter gets his/her voting screen to cast vote and he forgets his/her password that was provided to him by the EC. On entering the wrong ID and password a set of new ID and password is generated by the voting manager to the voter and he/she casts his/her vote. The second feature that has been included in this system is of timeliness that the voter has standard time of 5 minutes to cast his/her vote. After expiry of given time a troubleshooting occurs, voting console gets refresh and voter is ready again to cast his/her vote.

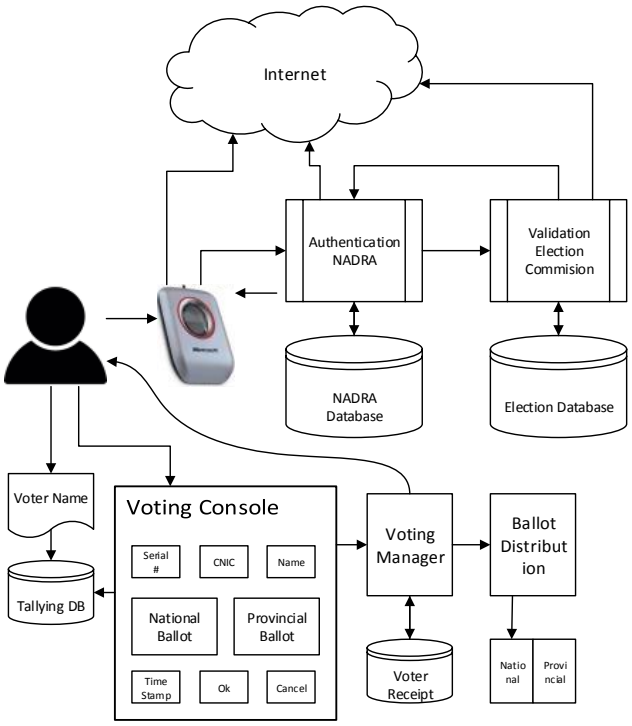

Fig. 2: E-voting system architecture.

As the voter casts the vote, voting manager generates the receipt to ensure the voter's satisfaction that vote has been casted and counted as well. Voting Manger sends that to BDC and BDC forwards it to the tallying which does the final counting and afterwards it is stored in the database of tallying while maintaining its integrity. The system stores final result that includes name along with the choice of the candidate.

3.1 E-voting Phase

We have split our system in three phases, pre-voting phase, during-voting phase and after-voting phase.

3.2 Pre-Voting Phase

The major objectives provided in this phase are: voter's authentication and validation process.

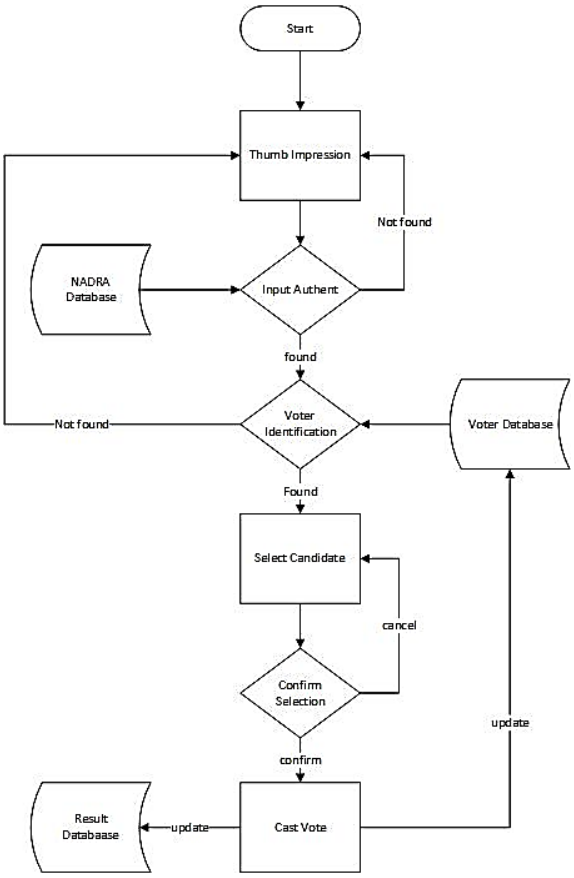

Fig. 3: Flow diagram for voter's identification and validation.

3.3 Voter's Identification

Voter's identification must be verified at two distinct phases: through login and biometrics. Registered voters request for verification or voting privilege from the authorities. Registration authorities then check the eligibility of that voter and only allow those who are eligible and registered before.

3.4 Voter's Validation

Voter is validated by validator authority. Only registered voter is eligible to cast vote. Fig. 3 shows the flow of the data for identification and validation of a voter.

3.5 During-Voting Phase

On the basis of the results of 'pre-voting phase' and 'during voting phase' the system allows the eligible voters to make their decisions and cast their votes through console window. Moreover, the console window is managed by the voting manager and the results are saved in e-database.

3.6 Post-Voting Phase

The final phase of the system is post-voting phase that deals with counting and finalizing the result reporting.

3.7 Votes Counting

Counting is one of the most crucial step in completing E-voting system and in our system this important task is performed by the vote collector.

4. Security Requirements

4.1 Authentication

In authentication phase, system determines that whether a user is authorized to use a voting system that includes few steps of identification and authentication. Identification is a process in which user provides a unique identity so a system can distinguish the entity from all others. Authentication is the process of establishing confidence in user identities. Proper voter authentication is done to ensure that only eligible voters can cast their votes. The authentication of the voter is done in the following way.

When a voter puts his finger on the biometric device the voter's NIC is generated against his finger print. The voter ends his request to get nonce from the authentication server. The authentication server sends a randomly generated value to the voter. The voter calculates the hash value of NIC number and nonce, sends it to the authentication server, i.e., NADRA which checks that whether this user exists in the database. The authentication server calculates the hash of the NIC Number stored in it. If both the hash values match, then the user is authenticated. In the next step, the NIC Number of the voter is validated from the election commission of Pakistan's database that this particular voter's name is present in the electoral rolls and he is eligible to cast the vote.

4.2 Integrity

Integrity in E-voting system refers to the genuineness of data in the system. To maintain factor of integrity it involves precautionary measures to ensure that unauthorized person cannot modify the data on a system.

Integrity ensures that final tally should be genuine and no compromise has been done on it. It also ensures that the final vote counting is exact and voter's uniqueness remains as it is. It has been ensured by installing efficient antivirus in the system to make it protected against virus attacks and software bugs. An integrity violation can be overcome by using mirroring mechanism to maintain the integrity of the system. This technique works in a way that by maintaining two or more copies of the same data in the storage device, integrity checks can be made by comparing the copies [1]. When a suspected user will attempt to change the data, it would seem to get successful at first instance. However, upon matching with the copies which are maintained in a confidential manner, all the malicious alterations introduced by the intruder will be caught and roll backed.

4.3 Confidentiality

The vote should be kept confidential. E-voting systems must protect all the sensitive information from being used illegitimately. Any such information related to voter or about the casted vote should be kept confidentially in the system. The proposed idea of E-voting system must identify and authenticate voters in order to verify their eligibility and provide them right to cast their votes. Confidentiality is necessary to protect the privacy as well as secrecy of the vote.

Voter's confidentiality is supposed to be one of the main focus in elections and so many scholars and researchers have done work on it regarding this issue [5, 19, 20]. In this system it has been made sure that the adversary should not know about the casted vote. Further, validator uses three-fold cryptographic protocol and sends encrypted certificate to the voter. Voter uses the three-way cryptographic protocol to encrypt the certificate with his/her key. By this process the key is doubled now from election commission and then from voter, it is sent again from the voter to the validator. The validator, on receiving the encrypted certificate, decrypt it with the voters own key and applies BDC's key on the encrypted certificate and send it back to voter again. The voter receives certificate and uses his/her own key to decrypt the encrypted message. After this step certificate can only be encrypted with BDC's key. The voter sends the encrypted certificate which is only encrypted with the BDC's key. BDC uses its private key to decrypt the certificate and then verifies that certificate from election commission. If it is verified, then voter is eligible to get ballot and cast vote. In addition, BDC applies RSA algorithm to encrypt the data. RSA is an efficient Public Key encryption and secure cryptographic algorithm and cannot be repudiated that ensure the confidentiality [19].

4.4 Anonymity

Once the voter is authenticated from the election commission of Pakistan there comes the role of another entity called Module for Password Distribution (MPD) which randomly generates a set of passwords for every eligible voter. The user picks up one password at random from that set and then uses this password for using the voting console. This password is only known to the voter and it is hidden from the E-voting system. It basically hides the identity of the voter which ensures to conceal the voter's choice of a candidate.

5. Formal Modelling and Analysis of Proposed System

For the purpose of formal modelling and verification of proposed secure E-voting system, a component based architecture [8] has been adopted. Further, coloured Petri net (CPN) based formalism is adopted for modelling of the proposed system because CPN modelling language [7] supports the component based architecture to model a system. A high level view showing the two components are given in Fig. 4. The authentication module is responsible to authenticate the voter on the basis of biometric security feature, which may be thumb impression image. Further, a voter is authenticated based on his ID in a national database. For the definition, notation and terminology about coloured Petri nets, readers are referred to [7].

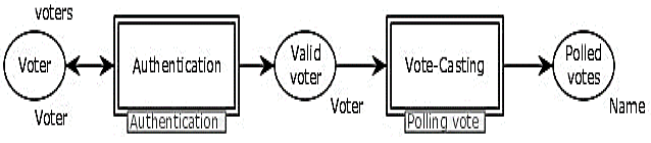

Fig. 4: High level view of the colored Petri net model.

5.1 Authentication Module

Authentication module has four places and two transitions. The transition "Biometric Recognition" is responsible for the recognition of voter on the basis of his biometric input. Further, this transition takes the input from the place Voter. Each voter contains the information viz. id, name and a party name to which he wants to cast the vote (see Table 1). Furthermore, the transition "Biometric Recognition" uses a function to recognize a voter, which is given on the arc to and from the transition (see Fig. 5). Thereafter, the transition "Check_NDRA-DB" confirms whether a voter's ID is in the NADRA database. This transition produces the authenticated voter in the output place "Valid_voter".

Table 1: Definition of color sets.

Color set (Type)	Definition
Colset Party = with AA|BB|CC;	Specifies the name of political parties participating in an election.
Colset Name = string;	Specifies the name of a voter.
Colset ID = int;	Specifies the id of a voter.
Colset Count = int;	Specifies the count of votes casted.
Colset PxC = product Party*Count;	Product of color type Party and Count. This color set is used to generate the vote count for each party.
colset Voter = product ID*Name*Party;	Product of color type ID, Name and Party. This productcolor type is used to carry the information of a voter.
Closet Authenticate = with rcgnz|notRcgz;	Enumeration data type used for recognizing or not recognizing the voter on the basis of biometric information.

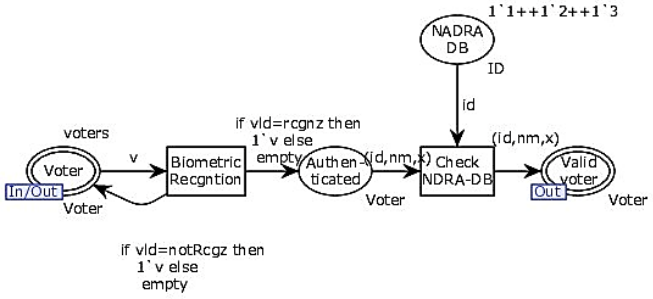

Fig. 5: Authentication module of the colored Petri net model.

5.2 Vote Casting Module

Vote-casting module has two transitions which are used to poll a vote as shown in Fig. 6. The transition "Check_list" confirms the valid voter in the voter list. This transition takes a valid voter as input and produces the confirmed voter in the voter list. Thereafter, the transition "Cast_vote" is used to cast a vote. The transition adds a vote against the political party to which a voter wants to cast a vote. The count of the vote is depicted in the place "Count_votes". This place shows the casted votes for each participating parties in the election. Finally, the transition "Cast_Vote" populated the list of voters who casted the votes.

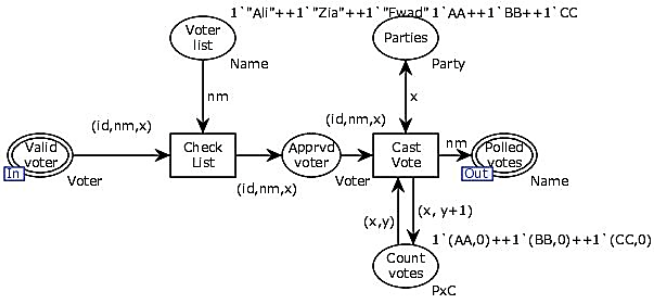

Fig. 6: Vote-casting module of the proposed colored Petri net model.

5.3 Simulation

For the purpose of simulation and to validate the smooth execution of the developed CPN model, three voters have been added as tokens (data values) in the place Voter. It is important to mention that any number of voters can be added in the system. Further, the place "Voter" is also an input place of the Authentication module (see Fig. 5). The tokens 1`(1,"Ali", AA)++1`(2, "Zia", BB)++1`(3, "Fwad", CC) represent the members of multi-set "Voter". Furthermore, each voter (token) is three-tuple which has ID, name and a name of party to which he wants to cast a vote. The transition "Biometric Recognition" uses two functions which use Boolean variable "vld" to recognize the voter on the basis of biometric input. Thereafter, authenticated voters are verified in the NADRA database through the transition "Check_NADRA-DB" which uses the variable "id". Moreover, verified voters on the bases of their ID are added in the place "Valid_voter", which is the input place of the Vote-casting module. The voter's name is further verified in the voters' list to confirm whether a voter is eligible to poll a vote. For such purpose, a variable "nm" is used by the transition "Check_List". Thereafter, verified voter casts vote to a political party of his/her choice by using the transition "Cast_Vote", which uses the variable x for a party. In order to count the votes polled to each contesting party, an integer variable y is incremented by one on a poll of single vote. At the end of the polling, variable y returns the total votes casted to the party in the given in the order pair (x, y). Finally, a list of polled votes in generated in the place "Polled_votes".

5.4 Analysis

For each possible values of declared variables (known as binding values), all possible executions of the transitions in the proposed CPN model generate the state space. Table 2 presents the information about the state space which can be represented in the form of occurrence graph (O-graph) [7]. Further, Table 2 provides the statistics and behavioural properties of proposed CPN model for E-voting system. There are 125 nodes (states) in the state-space generated by the developed CPN model. Further, upper bound for the number of tokens in each place is three viz. actually number of voters added in the model. Therefore, proposed CPN model is bounded which verifies that there is not over flow of token and the systems is under control.

Table 2: Statistics of O-graph and behavioural properties of the CPN model.

State Space:
Nodes: 125
Arcs: 375
Secs: 0
Status: Full
Scc Graph
Nodes: 125
Arcs: 300
Secs: 0

Boundedness Properties:
Best Integer Bounds

	Upper	Lower
Authentication'Authen 1	3	0
Authentication'NADRA_DB 1	3	0
Main'Polled_votes 1	3	0
Main'Valid_voter 1	3	0
Main'Voter 1	3	0
Polling_vote'Apprvd_voter 1	3	0
Polling_vote'Count_votes 1	3	3
Polling_vote'Parties 1	3	3
Polling_vote'Voter_list 1	3	0

Liveness Properties:
Dead Markings
[125]
Dead Transition Instances
None
Live Transition Instances
None

Fairness Properties:
Impartial Transition Instances
Authentication'Biometric_Recgntion 1
Fair Transition Instances
None
Just Transition Instances
None

Table 2 further shows that state number 125 is dead marking, which is actually the last state generated by the CPN model, given in Fig 4. Therefore, marking number 125 is terminal state which shows total votes casted to each party and a list of casted votes. Further, liveness property given in Table 2 explains that there is no dead transition instance in the O-graph which validate the smooth execution of the proposed architecture for E-voting system. Furthermore, non-existence of dead transition instance ensures the smooth execution of the proposed model for any number of voters to cast a vote.

The transition "Biometric Recognition" is impartial fair transition as it occurs infinitely often in every infinite run of the CPN model. Therefore, this property of the transition ensures the biometric based recognition of every voter.

6. Conclusions

In this research article, a component based architecture for E-voting system is presented which improves the authenticity and strengthen the vote-casting process. Further, data sharing features in a distributed environment and future recommendations are also presented. Different techniques linked with voter's authentication, confidentiality and integrity are suggested to minimize the flaws and maximize the benefits of the E-voting system. Moreover, security requirement for secure and efficient E-voting system are also discussed. Confidentiality, integrity, availability and authentication are incorporated in the proposed system architecture. Functionality of voting receipt generation has also been introduced in the proposed system to ensure the satisfaction of the voter.

Furthermore, the proposed architecture is formally modelled through hierarchical coloured Petri nets to validate it. Authentication module and vote-casting modules have been developed in the coloured Petri net based formal model. Thereafter, formal analysis is performed by generating the state-space and occurrence graph. Occurrence graph based analysis explains that formal model of the proposed architecture is deadlock free. Further, existence of boundedness property in the formal model ensures the control of the system and fairness property guarantees the smooth execution of the system.

References

[1] M. Volkamer and M. McGaley, "Requirements and evaluation procedures for eVoting", The Second International Conference on Availability, Reliability and Security, pp. 895-902, 2007.

[2] N. Paul and A.S. Tanenbaum, "The design of a trustworthy voting system", Annual Computer Security Applications Conference, pp. 507-517, 2009.

[3] A. Al-ameen and S.A. Talab, "E-voting systems vulnerabilities", IEEE 8th International Conference on Information Science and Digital Content Technology, vol. 1, pp. 67-73, 2012.

[4] R. Cooke and R. Anane, "A service-oriented architecture for robust e-voting," Serv. Oriented Comput. Appl., vol. 6, no. 3, pp. 249-266, 2012.

[5] H. Pan, E. Hou and N. Ansari, "E-NOTE: An e-voting system that ensures voter confidentiality and voting accuracy", IEEE International Conference on Communications, pp. 825-829, 2012.

[6] K.M. Abosamra, A.A. Abdelhafez, G.M.R. Assassa and M.F.M. Mursi, "A practical, secure and auditable e-voting system", J. Inf. Secur. Appl., vol. 36, pp. 69-89, 2017.

[7] K. Jensen and L.M. Kristensen, "Coloured Petri nets : Modelling and validation of concurrent systems", Springer Science & Business Media, 2009.

[8] F. Ahmad, A. Sadiq, A.M. Martinez-Enriquez, A. Muhammad, M.W. Anwar, U. Bajwa, M. Naseer and S.A. Khan, "Component based architecture for the control of crossing regions in railway networks", 16th IEEE International Conference on Machine Learning and Applications, pp. 540-545, 2017.

[9] H.D. Tho and N.T.H. Ha, "A protocol for securing e-voting system", International Conference on Advanced Engineering Theory and Applications, Springer, Cham, pp. 38-48, 2017.

[10] P. Realpe-Muñoz, C.A. Collazos, J. Hurtado, T. Granollers, J. Muñoz-Arteaga, and J. Velasco-Medina, "Eye tracking-based behavioural study of users using e-voting systems," Comput. Stand. Interfaces, vol. 55, pp. 182–195, 2018.

[11] Y. Zhou, H. Gao and J. Cheng, "An extension of QSL for E-voting systems", Advances in Computer Science and Ubiquitous Computing, Singapore: Springer, pp. 87-96, 2016.

[12] A. Chowdhury, "Revolution in authentication process by using biometrics", IEEE International Conference on Recent Trends in Information Systems, pp. 36-41, 2011.

[13] A. Sarajlic, N. Behlilovi and I. Sokolovi, "A modular concept of E-voting system that protects user privacy using random password distribution", 18th IEEE International Conference on Systems, Signals and Image Processing, pp. 1-5, 2011.

[14] N. Kshetri and J. Voas, "Blockchain-enabled e-voting", IEEE Software, vol. 35, no. 4, pp. 95-99, 2018.

[15] M. Pawlak, A. Poniszewska-Marańda and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system", Procedia Comput. Sci., vol. 141, pp. 239-246, 2018.

[16] J.-H. 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, Singapore: Springer, pp. 305-309, 2018.

[17] L. Jing, X. Wang, Z. Huang, L. Wang and Y. Xiang, "Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing", J. Parallel Distr. Com., vol. 130, pp. 91-97, 2019.

[18] K.M. Khan, J. Arshad and M.M. Khan, "Simulation of transaction malleability attack for blockchain-based e-voting", Comput. Electr. Eng., vol. 83, p. 106583, 2020.

[19] H.C. Chen and R. Deviani, "A secure e-voting system based on RSA time-lock puzzle mechanism", IEEE 7th International Conference on Broadband, Wireless Computing, Communication and Applications, pp. 596-601, 2012.

[20] S. Djanali, B.A. Pratomo, K.P.N. Cipto, A. Koesriputranto and H. Studiawan, "Design and development of voting data security for electronic voting (E-Voting)", 4th International Conference on Information and Communication Technology, pp. 1-4, 2016.