International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 3, June 2016, pp. 1197 ~ 1204
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i3.9449

FPF: Fraud Proof Framework for Electronic Voting System

Innocent Kabandana[1], A.N. Nanda Kumar[2]
[1]Departmenr of CS&E, School of Engineering and Technology, Jain University Global Campus, India
[2]R.L. Jalappa Institute of Technology, Doddaballapur, India

Article Info

Article history:

Received Nov 17, 2015
Revised Dec 26, 2015
Accepted Jan 10, 2016

Keyword:

Authentication
Cloud computing
Electronic voting
Encryption
Multi-level authentication

ABSTRACT

In a democratic process voting plays a vital role in selection of policy as well as candidates. Voting though gives the freedom to voter to cast his opinion it is not free fraudulent. In order to have secure voting and convey the opinion of authorized voter in this paper we have presented a java based framework for fraud proof electronic voting system. In this framework we ensure that only the authorized voter is permitted to cast his vote and mitigate illegal voters cast votes on faking or pretending to be someone else. Proposed FPF provides a multi-level of authentication mechanism to validate the voter. The proposed system is tested for efficiency and robustness in comparing it with the existing system and is found to be efficient through comparative analysis. At present FPF is successful in mitigating the unauthorized voting further enhancement in the electronic voting system is being carried out as future work.

Corresponding Author:

Innocent Kabandana,
Departmenr of CS&E,
School of Engineering and Technology,
Jain University Global Campus, India.
Email: innocentkabandana123@gmail.com

1. INTRODUCTION

Elections have a long history, different part of the world followed different methods for electing representatives. In a Democratic nation elections are considered as the key factors for the growth of the nation as it provides the voter with opportunity be a part of the policy making and nation building. The process of election involves co-ordination of different mechanisms involving the registration of the voter, registration of the candidates and scrutinizing the information provided by the voter as well as candidates. Collaborating these information, maintaining confidentiality of these information and conducting a free and fair election turns to be a tedious process. In order to have a free and fair election no loopholes in any of the mechanism should be allowed, in failing to do so will fail the moto of the democracy. In order to overcome these challenges and with the advancement of technology also the need to reduce cost, improve security, efficiency and reduce human interface gave rise to the idea of Electronic voting. With the more and more countries opting for democratic way of electing representatives has also resulted in emerging of new techniques in voting. From the predated technique of publiclyacclaiming the vote to recent mechanism of ballot paper voting there has been tremendous enhancement in voting system [1]. With the growth in information technology and internet new techniques like electronic voting is introduced in many different countries. Earlier electronic voting was just referred to the use of electronic voting machine in the process of voting. With times different approaches were experimented to establish a secured electoral system and increase the involvement of the citizen in nation building.

E-voting can be consider as a voting system wherein the data related to election are stored and processed as digital information. The main objective of e-voting is, it should be compliant with election rules and law and must provide voting opportunity to all authorized voter whereby mitigating illegal voters or fake voters'voting follows the same traditional way of voting which uses the authentication of voter, maintaining

privacy of the vote and so on which are achieved in more sophisticated as well advance way. Electronic voting offers many advantages such as it allows having fast and accurate result. It reduces the use of manpower. It helps in increasing the involvement of more and more citizen in the electoralsystem [2]. It also helps in reducing the time cost conducting the election. It allows in building trust among the citizen about free and fair election. It plays a vital role in reducing malpractice and corruption in the electoralprocess. Though electronic voting system offers certain advantages it is also prone to different kind of disadvantages. In spite of the advantages offered by the electronic voting system, many critics believe that the problem of inequality and security prevail in large in electronic voting system. They also argue that people with low wage might not be able the afford the system as they might have less access to the system and lose their privilege of voting. In some developing countries where the accessibility of the system is uneven it might also result in low turnout in the overall voting process causing the people to stay out of the voting [3]. The main drawback critics have identified in electronic system is the security system, as technology is advancing it is also posing more and more threats to electronic system failing to address these issues might result in failure of the total system.

The following section is organized as follows in section II we discuss about the existing work carried out by different authors in the electronic voting domain. In section III we discuss about problem description prevailing in the existing system emphasizing more on security aspect. Section IV illustrates about architecture of proposed FPF.Section V provides the details about the implementation of the proposed system. Section VI discusses about the performance analysis of the proposed system. Section VII discusses about the conclusion to proposed system.

1.1. Background

In this section we discuss about various techniques and mechanisms used by different authors in implementing the existing electronic voting system. The ambiguity in deciding whether to use or not use electronic voting still persists in certain part of the world. Many researchers have put forward their views in this regard one such work is carried MatejTravnicek [4] performed analysis considering various aspects of voting and has suggested that it can reduce few issues as well as give rise to some new challenges as well.

The author has concluded that there is no universal answer for justify the use of electronic voting or opposing it.It completely depends on the nature of its deployment based on the respective electoraldesign. Different countries use different methods of electronic voting one such work is being carried out by Chaeikar et al [5] performed the analysis of electronic voting systems in different parts of Europeanunion's such Estonia, Germany,Ireland, UK, Switzerland and Belgium.

The authors have performed an analysis of their weakness, technical characteristic in order to assist researchers to develop a better understanding the system and to provide solution to current drawbacks prevailing in the system. Another such work was carried out by Achieng and Ruhode [6] performed a survey on the adoption and challenges that are prevailing in electronic voting techniques in context to South Africa, the survey was carried out in Cape Town where people had access to internet. The survey was carried in the form of on-line questionnaire. The analysis was based on thematic analysis as well as diffusion of innovation theories that is adopted for theoretical analysis.Various authors have used different techniques to implement electronic voting system one such work is carried out by Lai et al [7] have designed and implemented a electronic voting system using contactless IC card. This can be used to successfully identify the voter and also ensure validity of the IC card.

1.2. The Problem

This section provides a description related to various problems prevailing in the existing system. Work carried by MatejTravnicek suggests that the success of E-voting system depends on the proper deployment of system as per the electoral need. Though election process is a similar in nature, it differs from nation to nation in terms of complexity, implementation and cost. Different approaches have been followed by different authors to implement electronic voting system. Lai [7] has implemented anelectronic voting using contactless IC to enhance the security. Since ICC is vulnerable physical damage, and communication card and reader can be hacked.

1.3. The Proposed Solution

This section provides the details about the proposed system. It discusses about the various module present in the design and also their functionalities.

Registration: Here the Administrator can be an individual entity or a Government Agency, which can be mathematically denoted as F(R). Administrator is responsible for performing the initial function such as registering the voters and candidates. It is similar to the process followed in the conventional election process. Entire registration process is controlled by the Administrator. On successful registration the voters

and Candidate is allowed tologin, througha secret code which is sent to concern individual through SMS,Email and QRCode so that the voter will receive the code in one or the other way even if there exists a problem in system. Which there can perform latter operations such as enrolling and voting? Another crucial operation performed by the Administrator is the verification of Documents. This is performed to eliminate fake voters or unauthorized voters. The verification process is entirely dependent on the Administration /Govt Agency which performs verification as per their rules and regulation.
Where F(R) =Administrator Controlling function
V(R) =Voter registration function
C(R) =Candidate registration function and
D (V) =Document verification function. Mathematically Administrator Controller is represented as:
F(R) ← V(R) +C(R) +D (V).

1.3.1. Enrollment

On Successful registration, the voter and the candidate can enroll to Election system through the login they have been given by the administrator. Here the voter and candidates has to furnish supporting documents in the form of Text file and images in order to justify that the concerned individual is the authorized voter or candidate. In case of the documents are not valid or authenticate one the administrator can reject the voter or candidate as per the rules and regulation. Here there is two ways of enrolling one is for the voter and the other is for the candidate. A perquisite for a candidate is that he should be a registered voter.And a major difference between the voter enrollment and the candidate enrollment is that the candidate needs to register to a party and obtain a symbol in order to contest the election. On the completion of the enrollment process by the candidate and voter, all the details including their personal details along with the supportive documents furnished by them is forwarded to the Administrator Controller or Govt Agency for validation. Only on the success of this validation the voter and candidate is facilitated to take part in next process of Election. Candidate enrollment can be mathematically expressed as:
C(R) ←P (D) +D(R) +S(R).
Where P (D) =Personal detail of Candidate or Voter
D(R) =Supportive Documents to Justify the Authorization.
S(R) =Denotes the Party the candidate has enrolled to contest election.

1.3.2. Architecture of the System

The Architecture of E-voting system is depicted in the Figure 1. The entire operation of the election is controlled by Administrator /Govt Agency. It performs various operations such as scheduling the election as per the requirement such as local election, assembly election or parliament election. Registration of voters and candidates and result announcement are crucial for free and fair election.

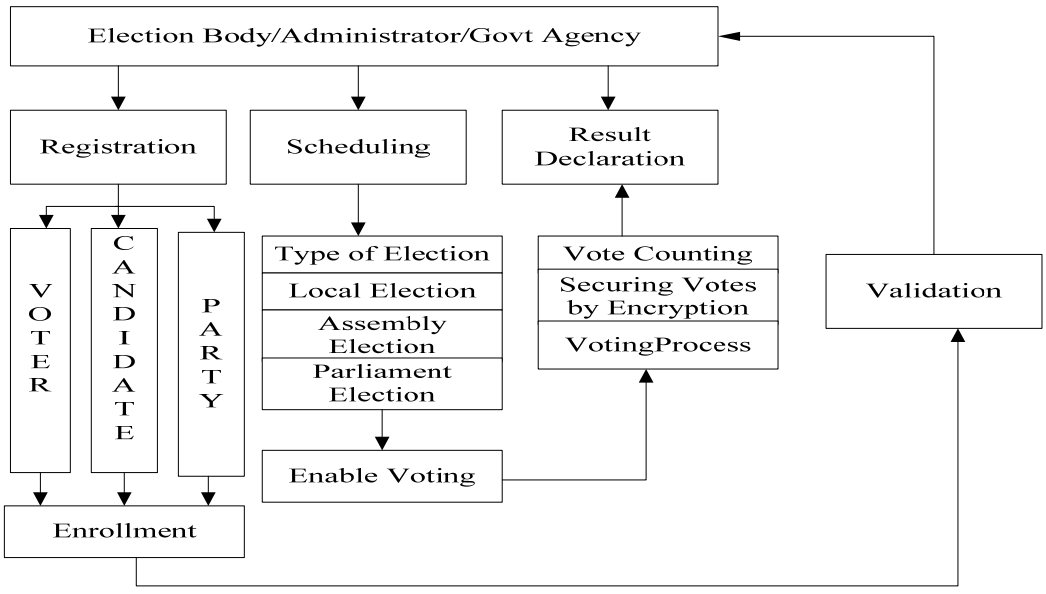

Figure 1. System Architecture

The architecture illustrates the modern electoral system. The electoral process is same as the traditional ballot paper based election. Major difference here is the use of modern technology to minimize the human interface and enhance security to make it fool proof system in achieving the intended objective of free and fair election. As depicted in the Architecture the entire process of the election is governed by the Administrator or a GovtAgency. The rules and guidelines to carry election is framed and monitored by the administrator. In case of any violation the administrator as the right to terminate or reschedule the election process. Administrator is responsible to register new voters, candidates and parties which take part in the election. As and when needed the administrator will also schedule the election. Wherein the election can be different kind, such as: local body election, assembly election or Parliamentary election. It is the responsible of Administrator to ensure free and fair election is held. The administrator is also responsible for scruting the documents furnished by the voters and candidates during the enrollment processes in order to verify if they are valid voters or imposters or illegal voters. On successful verification of the documents and details of the voter, he/she will be provided with a unique Identification number known as VoterID which is needed to cast vote.It is the responsibility of the Administrator to ensure that no VoterID is provided to the illegal or unauthorized voter. In case of Candidate is found to produce invalid or fake documents the Administrator has the right to terminate him from contesting the election. After the scheduling the Administrator will release a link through which the voting is carried out. This link is valid only for a particular election on particular schedule, only the authorized or valid voter is allowed to cast his vote in this link, no imposter or illegal voter will be able to cast his vote.In order to cast the vote the voter needs provides certain credentials like his user name, password and voterID.On entering into voter page the voter is provided with certain information such as kind of voting, list of candidates and their symbols. Figure 2 depicts the voting link enabled for the prime ministerial election wherein it is shown that the particular schedule for which the link is active. The voting is allowed only on that schedule.

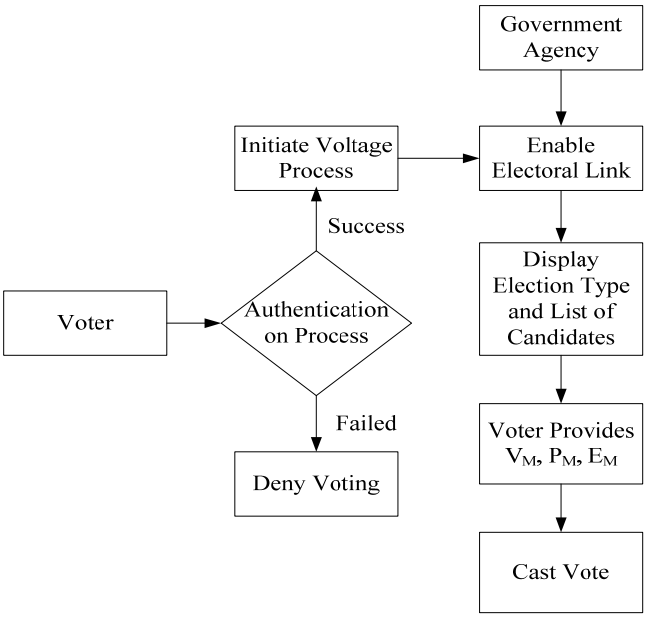

Figure 2. Voting Link Enabled

Another crucial function performed by the administrator is the result declaration. On completion of the voting process and counting of the votes, theadministrator will declare the result. The entire process of vote counting is decided and monitored by administrator or Govtagency. The administrator declares the result to general public using different Medias like print media; electronic media and currently social Medias are also used to announce the result. The candidates are also allowed to check through their account login in which they will be provided with the details of votes received by him and his opponent and total vote polled.

1.3.3. Assumption Used

Some assumptions used in this work are:

1. It is used that the list of eligible voters, candidates are performed fairly by the administrator.
2. The Govt agency has declared the schedule and guidelines for conducting elections.

3. The list of eligible voter's isprovided for the polling station.
4. Administrator has provided the voters their polling station.
5. The voters are provided with Voter Id required to participate in the election.

2. OUR CONTRIBUTION

Authentication is an important in any operation. The main objective of authentication is improving the integrity of the system thereby resisting invalid voters or illegal voters affecting the system. In order to achieve this we have introduced a unique authentication mechanism in E-voting system. This helps us to ensure that only the authenticated voter is casting the vote. In order to authenticate a voter we generate a secret key which is sent to the voter in three different ways i.e. email, sms and as QRcode.The intension of this is to ensure that voter will not miss the voting process due to some situational hazards like, congested mobile network, internet server down and in order to make sure even people without smart phone to be part of the electoral. The process of generating the secret key is illustrated in the Algorithm 1.

2.1. Secret key Generation for Authentication

Algorithm for Secret key Generation for Authentication:-

Step 1: Voter credentials like username (V_n) secret code (S_c) and Voter's Device ID (D_{im}) is sent to Administrator.

$$\Gamma = V_n + S_c$$

Step 2: Random secret key (R_K) is generated by the virtual Machine.

Set (α, β)

Di+1= (Z*Di+1) mod S

O=Ω

R_K=ASCII (Ω).

Step 3: Secret Key input (S_{KIN}) generated using U_p plus R_K.

Step 4: Secret Key (S_K) is generated using encryption.

$$S_{KIN} \rightarrow H\ (S_{KIN}) = S_K$$

Step5: Generation of 128 bit C_{Key}

$$H\ (D_{im}, S_{KIN}) \xrightarrow{P(x)} C_{Key}$$

Step 6: Encryption using C_{Key}

$$H\ (S_K, CKey) \xrightarrow{Q(x)} \mu$$

Step 7:μ embedded in Barcode.

The secret code generation to authenticate the voter is carried out in two levels.Initially the secret code generation is started by consider the γ which contains user credentials such as username and secret code. Along with device ID of the voter, which in this case is the IMEI code represented as D_{im}. The virtual machine generates the Random number required in order to generate the final secret code. The process of random number generation is illustrated in the algorithm; the generation Random number is based on the principle of linear congruential formula. Here two levels are predefined each to limit the value in between two levels; High level represented by 'α' and lowers level represented 'β'. The output of this operation 'O' is a Random generated which is represented by 'Ω'.In order to generate the final secret code we need to have a character, so as to obtain a character the 'Ω' is subjected to binary to ascii conversion. The output of this operation is our required Random key which is denoted by 'R_K'.Using this R_K and U_p secret Key input S_{Kin} is generated. Using this input final secret key is produced. In order to have the final secret key, S_{Kin} is subjected to two level of encryption, where in the first level the encryption is performed using the MD5 which results in a result of 128 bit (16 byte) value which is expressed a hexadecimal code of 32 digit which is denoted as the C_{key}. This encryption operation is represented by a function denoted by P(x). The second level of encryption is carried out on this result i.e C_{Key} and S_K. This operation is performed using AES encryption which is denoted by Q(x) and produces results which is also a 128 bit. This result which is representing in μ

is the final secret code. In order to enhance the security feature we have embedded this code within the QRcode. So that it will not be decrypted by others, this code is decrptable only using the voter's device since it needs the IMEI of the voter's device. Taking in consideration technical limitations that are caused accidentally we have ensure that the final secret key is sent to the user in three different ways i.e. SMS, Email and QRCode. It should be noted that all three are sent to voter through his personal email, mobile number and so on so that it is not accessed by others.

2.2. Result Securing using Digital Signature

Once the Election is completed the polled votes must be secured from miscreants so that the result should not be manipulated or cheated. In order to achieve this we have used encryption, so that the polled votes are secured.This achieved using three parameters such as VoterID (V_{ID}), PartyID (P_{ID}), Election ID (E_{ID}) where,

V_{ID}= is the vote casted by the voter.

$P_{ID=}$is the party ID to which the vote as been casted.

$E_{ID=}$is the election ID representing the type of election.

In order to safeguard the casted votes these three parameters are subjected to encryption operation. The process of securing the votes through encryption is illustrated in algorithm 2. After the encryption the resulting digital signature is stored in the database.So that even if anyone accidentally access the data base will not be able to identify the result since they would not get the details of person voted or whom he has voted or which party as secured how much vote.

Algorithm 2.

Vote polling and result counting

Step 1: Voter (V) $\rightarrow P_{ID}$.

Voter will select the party he wants to vote. After the casting of vote, encryption is performed on three attributes V_{ID}, E_{ID} andP_{ID}

Step 2: H (V_{ID}) +H (E_{ID}) +H (P_{ID}) = $S_{DB.}$

Encryption used is MD5, after the encryption using the digital signatures we store all the attributes as result in the Database. No raw result is stored.

Step 3:$P_{VD} \rightarrow S_{DB}$

Polled votes are selected from the stored database.

Step 4:$R_E \rightarrow (DE_{ID} \&\& DP_{ID})$.

The above algorithm illustrates the process of vote polling, initially depending on the type of election the candidates are listed on the voting site. The voter selects the candidates whom he wants toelect. The candidate selection is done on the basis of party ID.Once the voting is done the program automatically performs the encryption of $P_{ID;}$ EID and $V_{ID.}$The encryption is performed to achieve secrecy. The type of encryption used is the MD5. Here it should be noted that only the Hashed value of the polled votes is stored in the database, no raw data is stored. So that even in the case of the database is hacked, the hackers or the rogue entity does not get the information about who was voted for whom. There by helping to mitigate the malicious act of manipulating votes. During the counting of the votes the polled votes in the form of hashed values or digital signature of the Party ID and Election ID in order to announce the winner. The voter ID gives information about whom as voted whom is neglected in counting process. In the following section we discuss about the performance and result analysis of our proposed system.

3. RESULT ANALYSIS AND PERFORMANCE PARAMETERS

The experiments are carried on Test bed Designed on the Java environment. The experiment is performed using Intel processor operating at 1.6GHz, RAM of 2GB, and storage of 500GB. The key observation observed from the experimental result is that, the authentication method offers, Efficiency, Robustness and Speed.

3.1. Execution speed and Lightweight

In compared to the algorithms used in conventional electronic voting system, FPF algorithms consume less time and resources such as memory in order to perform various tasks like encryption, decryption and generation of the secret key required for the authentication process.

3.2. Defendable Algorithm

The algorithm uses multiple encryption and decryption and external attributes such as IMEI to generate the secret key .Which makes it difficult for the attacker to guess, retrieve and generate duplicate secret key.

3.3. Secret Key Hiding

The generated secret key is sent to the concerned voter through three different means ensuring he does not lose the voting opportunity. These three means are sms, email, and QRCode. It should be noted that all these are send to voters personally through his personal email, and phone number. The secret key to the voter is encrypted and is not visible in order to visualize the code it needs to be decrypted which requires the voter's device.

3.4. Result Encryption and Hiding

Another key factor is the encryption of the polled results in order to avoid manipulation. The encrypted result is stored rather than storing the original data. By doing so we achieve higher degree of secrecy such that even when accidentally achieves the access to database it will be impossible for him to relieve the details since it is stored using digital signatures of the original result.

3.5. Multiple voter Accessibility

FPF supports multiple users' login and authentication simultaneous there by allowing large number of voters to vote without any program generated error. Therefore FPF can be considered as scalable and robust.

3.6. Result analysis and Performance Parameter

The experiment is conducted using Test bed developed on the basis of Java. The experiment is performed on a system using Intel core i3 processor running at speed of 3.20GHz and having a memory of 4GB, and 64 bit windows 7 operating system. By a time function the total of time taken for authentication is summation of the all above performance parameter which is illustrated as follows in the graph.

$T_{tot}=KT$

Where $T_{tot}$is the overall time for the complete cycle.

Where K is the Performance Ratio

$K=\eta N$

Where the $\eta=A/B$

Where N is the number of simultaneous user.

η is the ratio of user credential, Where A is Username and B is Password or secret code. Where in the username is a maximum of 90 characters whereas password length is infinity.

The processing time capability of the FPF is analyzed using the time required in processing various operation in order to perform the authentication task. In Figure 3 it is graphical depicted the behavior of the FPF for the multiple voters with fixed length of user credential parameters.

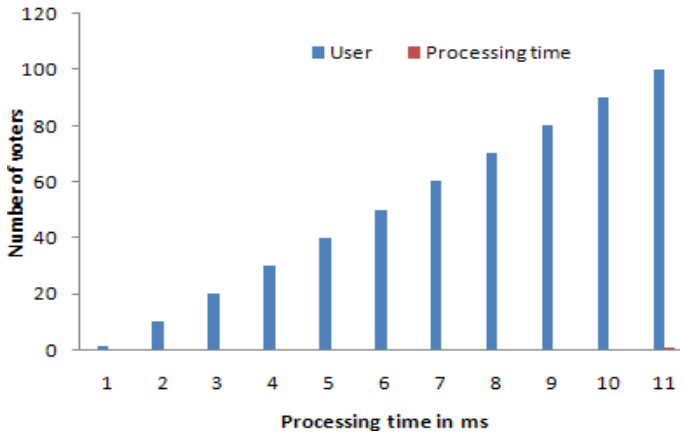

Figure 3. Processing Time Analysis using Fixed Length User Credential

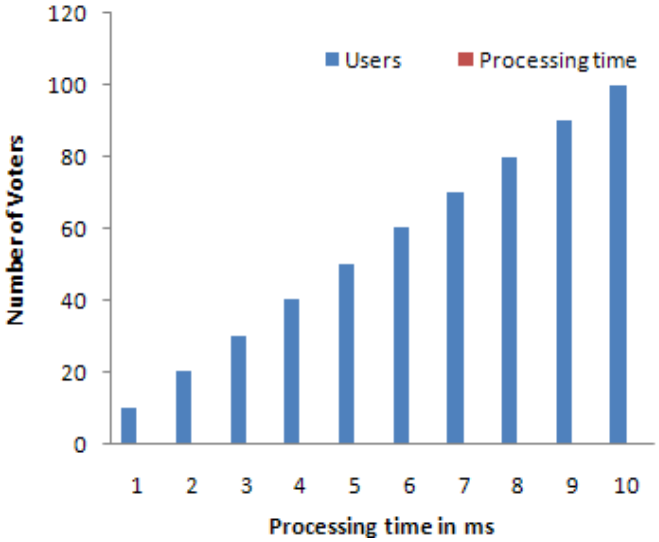

Figure 4. Processing Time's Analysis for Variable Length User Credential

Figure 4 depicts the graphof processing time obtained for the proposed system using variable length user credential for multiple voter login simultaneously. It is seen from the graph the frame work successfully achieves the intended lower processing speed irrespective of the various parameters such as number of simultaneously, the length of user credential and so on. The processing time for the framework is considered in milliseconds.

4. CONCLUSION

In this paper an efficient Fool proof Framework for electronic voting is developed wherein the security in voting system is enhanced by using the proposed system. Proposed system as designed a new authentication mechanism making use of the user device as well as user credential and also a secured encryption of the final result is performed in order to avoid the manipulation of result.In compared to the existing system the proposed system as achieved reduced processing time to authenticate the voter and the use of digital signature to save result mitigates the problem of manipulating the polled results.

REFERENCES

[1] M. Volkamer, "Evaluation of Electronic Voting: Requirements and Evaluation Procedures to Support Responsible Election Authorities," *Springer Science & Business Media, Law*, pp. 248, 2009.
[2] P. Ryan and B. Schoenmakers, "E-Voting and Identity: Second International Conference," *VOTE-ID 2009, Luxembourg, Proceedings Springer, Computers*, pp. 191, 2009.
[3] S. Caarls, "E-voting Handbook: Key Steps in the Implementation of E-enabled Elections," *Council of Europe, Political Science*, pp. 60, 2010.
[4] M. Travnicek, "Electronic Voting to have or not to have?" *European Scientific Journal*, vol. 3, 2014.
[5] Chaeikar, "Electronic voting systems for European Union Countries," *Journal of Next Generation Information Technology*, vol/issue: 4(5), 2013.
[6] Achieng and Ruhode, "The Adoption and Challenges of Electronic voting Technologies within the south African Context," *International Journal of Managing Information Technology*, vol/issue: 5(4), 2013.
[7] J. Y. Lai and C. F. Lin, "Design and Implementation of an Electronic Voting System with Contactless IC Cards," Graduate Institute of Information and Computer Education, National Kaohsiung Normal University, Retrived, 12th Nov, 2015.