AN E-VOTING AUTHENTICATION SCHEME USING LUHN'S ALGORITHM AND ASSOCIATION RULE

M. Hammed, F. T. Ibharalu and O. Folorunso

Department of Computer Science, Federal Polytechnic Ilaro, Nigeria.
Department of Computer Science, Federal University of Agriculture Abeokuta, Nigeria.

tundemuhammedy2k@yahoo.com, tomibharalu@yahoo.com, tundemuhammedy2k@yahoo.com

Abstract: The traditional voting system involves many flaws: inconveniences, time consuming delays and risks. All these threats brought about the existence of e-voting system. However, with increasing use of the internet causes, many e-crimes committed daily and this has led to challenges in the e-voting system. There are a number of researches on security issue on e-voting system, but most of these efforts did not take authentication into cognizance, whereas authentication is the most important phase that could determine the faith of the whole electoral process. This work proposed a secured authentication system for e-voting. The secured authentication system provides security efficiency through the luhn's algorithm augmented with association rule mining algorithm. The ideal of Luhn's algorithm is to detect errors in the identification number entered by the voters; this forms part of criteria to determine the activation and deactivation of voters. The ideal of using association rule mining algorithm is to uncovering the relationship between the identification number and voter's information already stored in the database. We also proposed a multi-server queue model to take care of performance problem in the case many voters intend to cast their votes at the same time. This proposed system efficiently secure authentication phase of e-voting system.

Keywords: E-voting System Luhn's algorithm. Association Rule Mining Algorithm, Multi-server Queue System.

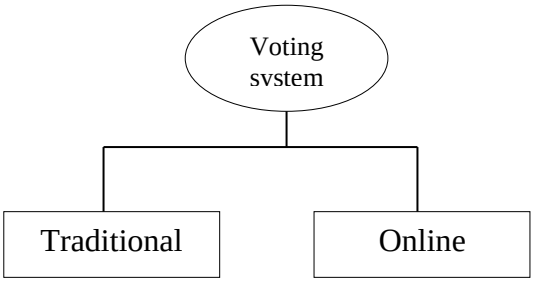
INTRODUCTION

Free and fair elections and voting are the essential ingredients for a democratic nation. Elections allow the populace to choose their representatives, express their preferences for how they will be governed. Thus, the integrity and accuracy of election process is fundamental to the integrity of the democracy itself. Today, many new technological innovations are changing the way we do things; such innovations include e-government, e-commerce, and e-voting etc. (Ciprian 2008). Despite the fact that traditional voting system involves a systematic process or procedure, frauds are still possible and the processes are cumbersome with inconveniences to the stakeholders, especially during the authentication phase, where long queues generated often lead to violent protest, loss of lives and destruction of public and private properties. It is therefore, imperative to evolve a reliable and generally acceptable electioneering mechanism that will boost the confidence of voters guarantee the legitimacy and wide acceptability of election results (Jegede *et al.*, 2012).

E-voting system is a system that allows the eligible voters to cast their votes via a computer normally connected to internet or intranet from anywhere like home or office. In contrary to the traditional way of voting, electronic voting is essential because it considers ways in which the polling task can be performed electronically without sacrificing voter privacy or introducing opportunities for fraud (Ajiboye et.al, 2013).

Electronic voting has many advantages over the traditional way of voting. Some of these advantages are lesser cost, faster tabulation of results, greater accuracy, and lower risk of human and mechanical errors, it offers improved accessibility for the people with disabilities, and it provides multiple-language support for the ballots. Electronic voting will increase voter convenience and voter confidence in the accuracy of election results (Shubhangi *et al.*, 2013).

Voting systems are in two forms as it shown in figure 1 below, offline voting system (i.e. voter uses ballot paper to cast his vote) and internet voting system (i.e. voter uses internet to cast his vote).



(Use of ballot paper) (Use of internet)

Figure 1: Types of voting system

The e-voting system has so many advantages over the traditional voting system: the electronic voting machine is intended both to reduce errors and to speed the authenticating, voting and counting processes. In e-voting system, either web-based or machine-based should meet the certain criteria or requirements such as eligibility and authentication, uniqueness, accuracy, integrity, verse, viability, reliability, secrecy, flexibility, convenience, transparency and cost effectiveness. Among these, Authentication can be viewed as the most artificial

issue. As online voting is risky, it is difficult to come up with a system, which is perfect in all senses (Linu and Anilkumar, 2012).Unfortunately, machine-based e-voting system is liable to the process of modification, which could lead to changes in the properties of Electronic Voting Machine (EVM) or total replacement of biometric template or card reader.

Least significant bit insertion is a common approach to embed information in a cover file (Sutaone and Khandare, 2008). An attacker could attacks machine-based e-voting system by inserting the information that will change the election records and the results. (Ciprian, 2008) talked about conventional security measures such as firewalls or SSL communications for machine-based e-voting system. He further said mechanisms that form the structure of security are:

- Personal identification numbers or passwords;
- Encryption;
- Digital signature;
- Smart cards biometric identifiers.

Attacks on the templates of biometric machine in machine-based e-voting system can come from two directions

(i) A third part could replace a member of biometric templates against other templates which would allow them manipulate the results of the vote.

(ii) Even if the risk of the above attack is seen as neglectable, there is one attacker that has a much more direct access to the biometric templates: the electoral authority.

No matter what methods are used to realize dynamic property of password for each authentication, the core is to ensure the randomness of factors added into the authentication. Many current OTP applications use mathematic methods like Hash function for dynamic passwords but still will suffer potential attacked risks Using static passwords for authentication, as it is commonly done, has quite a few security drawbacks: passwords can be guessed, forgotten, written down and stolen, eavesdropped or deliberately being told to other people. A better, more secure way of authentication is the so-called "two-factor" or "strong authentication" based on one time passwords, instead of authenticating with a simple password (Do van *et al.*, 2009). But, for the proposed e-voting system, a unique Personal Identification Numbers (PIN) or password will be given to individual voters. The election identification number is a “long number” which identifies the voters in specific election. Unique Personal Identification Number (PIN) allows voters an access to e-voting server, to be able to cast their votes and anybody with wrong PIN will not be authorized to cast his votes. In this work, we proposed a strong algorithm that detects errors in voter’s identification number and the algorithm that compares the voter’s PIN and voter’s information already stored in the database during the registration to see whether they match each other before the system could activate or deactivate the voter. This process will determine the legitimate voters and illegitimate voters.

RELATED WORK

Many researchers have proposed a number of techniques as a security mechanism for authentication system. Linu and Anilkumar (2012), proposed an authentication scheme for online voting using steganography and biometrics. In this scheme, each individual voter is provided with voter Identification Number or PIN (Personal Identification Number). This is needed for maintenance of voter accounts in the database. Secondly, we need facial images and fingerprints of all the individuals. Thirdly, during the account creation every individual will be provided with a system generated Secret key which he/she should not disclose to anybody. This will be needed to cast the vote. Voter can cast vote after login, which is done after authenticating the voter’s facial image, fingerprint, PIN number and secret key. The stego-image database is made by embedding secret key and PIN. Voter’s fingerprints and facial images are also stored in the database.

This system greatly reduces the risks, as the hackers have to find the secret key, pin number, fingerprint and facial image, which makes the election procedures to be secure against a variety of fraudulent behaviour. One of the shortcomings of this steganography is Fridrich’s set steg analysis that has a very large feature to achieve stego-image. Another shortcoming is the attacker (e.g. the state in political elections) who has much more direct access to the biometric template may replace a number of biometric templates against other templates, which would allow them to manipulate the results of the vote.

According to Kekre and Bharadi (2009), a biometric authentication is the advanced form of authentication. A biometric authentication is nothing but it scans the user’s characteristics such as finger print and eye retina and stores in the form of a string. When the user tries to authenticate it matches with the stored data and then gives access when a commonality is achieved and when the user has gained access he can enter the password to view the required information. The drawbacks of this approach are:

- Biometric authentication is convenient only for limited applications, since the system becomes very slow for a large number of users.
- Finger prints can be taken on a small tape and can be provided for the hardware
- Additional hardware is required to detect the fingerprints and eye retinas (Harish and Karthik,2010).

Harish and Karthik (2010), describes how effectively we can achieve the strong authentication using mobile phone without the need to carry the extra hardware for the one time password. Although, this system is robust and secured, but the scheme did not consider the performance problem that may occur since everybody has an access to the mobile phone.

Even though fewer than eighteen children will also terrorise the e-voting server with his/her mobile phone, which can cause congestion on server.

There is also a wide range of different security mechanism for e-voting systems. Most of these works did not cover the problem of securing the performance process, for example, Aneta and Zbigniew (2006) proposed An efficient e-voting system with distributed trust, the scheme is an example of the mix-net model where the trusted party randomly distributed messages to users so that any eavesdropper is unable to trace the sender or recipient of a given message. One of the shortcomings of the scheme is performance problem that may occur when many voters want to authenticate and cast their vote at the same time.

The proposed framework for authentication system, provides secured authentication process with Luhn's algorithm and associative rule mining algorithm as well as efficiency performance of server with multi server queuing model .The Luhn's algorithm and associative has been used in many ways to detect fraud in credit card e.g. Mahesh *et al.* (2015). So also multi server queuing model has been used to model the arrival and the departure of customer/or voter in a system in order to tackle performance issues e.g. Mohammed and Mohammed (2013).

METHODOLOGY

The authentication voting system using Luhn's algorithm augmented with Associative Rule Mining algorithm is to prevent hackers and unauthorized voters to login into the voting server, but authenticate all legitimate voters to cast their vote. The voting system consists of three phases and three parties. The phases are registration phase, vote casting phase and counting and tallying phase. The parties are voter, the server that will authenticate the voters and authority that would count and tallying the vote.

Registration Phase

In the registration phase the voter login to obtain Personal Identification Number (PIN) from the e-voting server as it is shown in figure 2,the voter provides his/her detail information, the server store the voter's information, generates and send a random number to the voter.

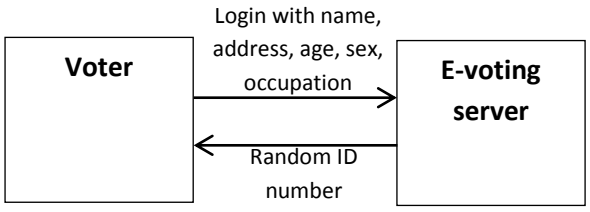


Figure 2: Identification number generating process.

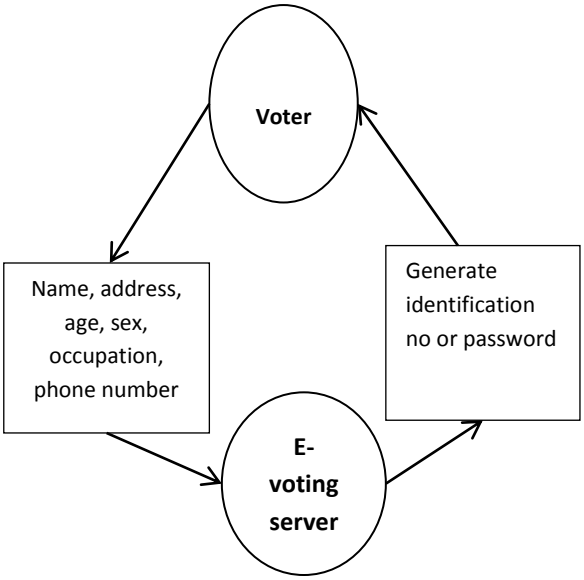


Figure 3: Stages in Identification number Generating Process.

We adopted a programming language that is linearly congruent, i.e. a language with a random number generating function that has these three properties suitable for e-voting: it generates evenly distributed numbers, the values are unpredictable, and it has a long and complete cycle. In other words, this programming language should be capable of generating large number of different values and all of the values in the cycle that can be generated are appropriate for computing identification number or password for this particular work. Figure 3 depicts this identification number and password process. Every voter is provided with an identification number and a password. This is needed to maintain voter's information in the database.

Vote Casting Phase

This is a critical phase, where authentication will take place. In election process, voter login with generated identification number obtained from e-voting server. The server performs adapted Luhn's algorithm as it shown in figure 4 below to verify whether the voter's number is authentic before decision could be made whether to activate or deactivate a particular voter.

Formula (Mod 10) Algorithm

Step 1: Starting with the second to the last digit and moving to the left, double the value of all alternating digits. If the product obtained from this step is greater than 9, then subtract 9 from the product.

Step 2: Add the digits of the products together with the digits from the original number. Exclude the check digit.

3. Step 3: Divide the sum by 10 and check on whether the remainder is 0. If so, then that is the check digit. However, if the number is not equal

Figure 4: Luhn's algorithm (Khalid *et al.*, 2013)

Adapted Luhn's algorithm in figure 3 is demonstrated using an example below. In the example, we want to validate the voter's PIN number 5342135411422512, for election.

Step 1: Starting with the second to the last digit and moving left, double the value of all alternating digits. If product of this doubling operation is greater than 9, then subtract 9 from the product, as it is previously described above (Figure 3).

Voter's PIN digits	5	3	4	2	1	3	5	4	1	1	4	2	2	5	1	2
Voter's PIN digits Doubled	10		8		2		10		2		8		4		2	
Result	1		8		2		1		2		8		4		2	

Table 1: First Step of Luhn's Algorithm

Step 2: Add the digits of the products together with the digits from the original number. Exclude the check digit (digits in brackets are the products from Step 1).

(2) + 5 + (4) + 2 + (8) + 1 + (2) + 4 + (1) + 3 + (2) + 2 + (8) + 3 + (1) = 48

Step 3: Divide the sum by 10 and verify whether the remainder is equal to 0. If the remainder is 0, then that is the check digit. If the number is not equal to 0, then subtract the remainder from 10. The resultant number is the check digit.

48 mod 10 = 8

10 – 8 = 2

Result (2) matches the check digit (2), which shows that the voter's PIN number is valid. Thereafter the administrator on the e-voting server subsequently validates the voters: compare ID number of each voter to the voter's information stored in the database using associative mining rule.

The ideal of associative rule is to determine the relationship between the voter's PIN and information stored in the database since it is an IF/THEN statement. In this work, association rules was develop for mining voters information from the database: If X as a voter's PIN and Y as a voter's information, X and Y are conjunctions of attribute value-pairs, and s (for support) is the probability that X and Y appear together in a database and c (for confidence) is the conditional probability that X appears in a database when Y is present. The association rule X→Y is interpreted as data set that satisfies the conditions in X and also likely to satisfy the conditions in Y. This indicates that if voter should be authorized X (PIN) must satisfies Y (Voter's information) i.e.

```
IF X satisfies Y THEN
    Authorize the voter
ELSE
    Unauthorized the voter
END IF
END
```

The flowchart in figure 4 depicts the entire operation involved in the detection of correct and incorrect PINs in the e-voting system, which determines voter's activation or deactivation.

The performance problems may occur when the e-voting server needs to authenticate many users who are login in to generate id number, generate ballot or to cast their vote and check the election result at the same time, delays could be guaranteed and it may be risky.

The remote internet voting systems need to have a quick response time. If voters become frustrated with request processing time, they will abandon the system, perhaps before they had a chance to vote. It is important to know where potential bottlenecks may reside whether with the servers, network, or applications and to be able to handle peak traffic loads without having to over-allocate resources, which can be costly and inefficient (Mohammed and Mohammed, 2013).

In this scheme, Queuing Modelling System was used to sensibly select number of voters per server to minimize the risk, delay and improve server's performance in the system. The queuing modelling system in this research work was implemented based on an adapted queue discipline and service mechanism used by Sharma (2009).

(1) Arrivals are described by Poisson probability distribution and come from an infinite population.
(2) Single waiting line and each arrival waits to be served regardless of the length of the queue (i.e. infinite capacity) and that there is no balking or reneging.
(3) Queue discipline is 'first-come, first-served'.
(4) Single voter's server and service times follow exponential distribution.
(5) Voters' arrival is independent but the arrival rate (average number of arrivals) does not change overtime.
(6) The average service rate is more than the average arrival rate.

Multi-Server Queuing Models

In our scheme, this queuing system, the arrivals follow a Poisson Probability distribution at an average rate of λ voters per unit of time. They are also served on a first-come, first-served basis by any of the servers. The service times are distributed exponentially with an average of voters unit of time. When there are n-voters in the queuing system at any point in time, then the following two cases arise:

i. If $n < s$, (number of voters in the system is less than the number of servers (**s**)), then there will be no queue. However, ($s-n$) number of servers will not be busy. The combined service rate will then be $\mu_n = n\mu$; $n<s$, where μ is the mean service rate
ii. If $n \geq s$ (number of voters in the system is more than or equal to the number of servers then all servers will be busy and the

maximum number of voters in the queue will be (n-s). The combined service rate will **be µn=sµ; n≥s** .

Terminology and Notation

S= number of servers (parallel service channel, in queuing system)

λ_n = Mean arrival rate (expected number of arrival per unit time) of new voters when n voters are in system

When λ_n is a constant for all n, this constant is denoted by λ

$1/\lambda$ is the expected inter arrival time

μ_n = Mean service rate for overall system (expected number of voters completing service per unit time) when voters are in system

μ_n Represents combined rate at which all busy servers achieve service completions

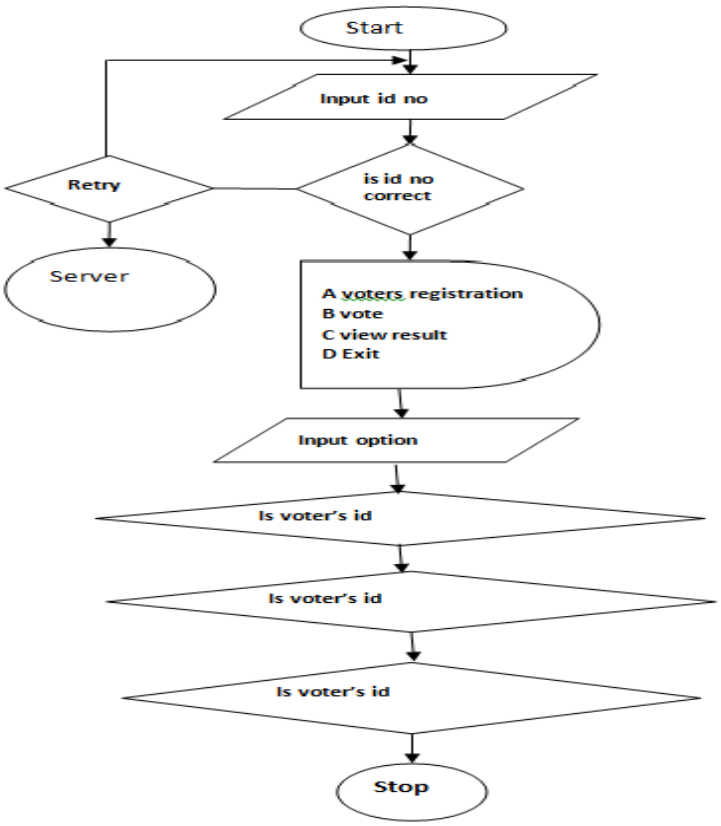


Figure 5: E-voting system Flowchart

When the mean service rate per busy server is a constant for all $n \geq 1$, this constant is denoted by μ

$\mu_n = s\mu$ When $n \geq s$ (all servers are busy $1/\lambda$ is the expected service time)

$p = \lambda(s\mu)$ is the utilization factor for the service facility, i.e, the expected fraction of time the individual servers are busy.

p_n = Probability of exact n voters in queuing system

L= expected number of voters in queuing system = $\sum_{n=0}^{\infty} n\,p_n$

Lq = Expected queue length (excludes voters being served) $= \sum_{n=0}^{\infty} (n-s)\,p_n$,

W=waiting time in system (include service time) for each voters

W= $E(w)$

W_q = Waiting time in queue (exclude service time) for each voters

$W_q = E(wq)$

Relationship between L,W, Lq and wq

Assume that λ_n is a constant for all n

In a steady –state queuing process, $L = \lambda W$ (Little's formula) and $L_q = \lambda W q$

If the λ_n are not equal, then λ can be replaced in these equation by λ, the average arrival rate over the long time. Assume that the mean service time $\left(\frac{1}{\mu}\right)$ is a constant. Thus $W = Wq + \frac{1}{\mu}$

These four fundamental quantities L, W, Lq and Wq could be immediately determine as soon as one is found analytically

M= exponential distribution (markovian), which is the most widely used
D= degenerate distribution (constant time)

Movement of voters among several states

Thus, to derive the results for this model, we have:

$\lambda_n = \lambda$ for all $n \geq 0$

$$\mu_n = \begin{cases} n\mu; n \leq s \\ s\mu; n \geq sn \geq s \end{cases}$$

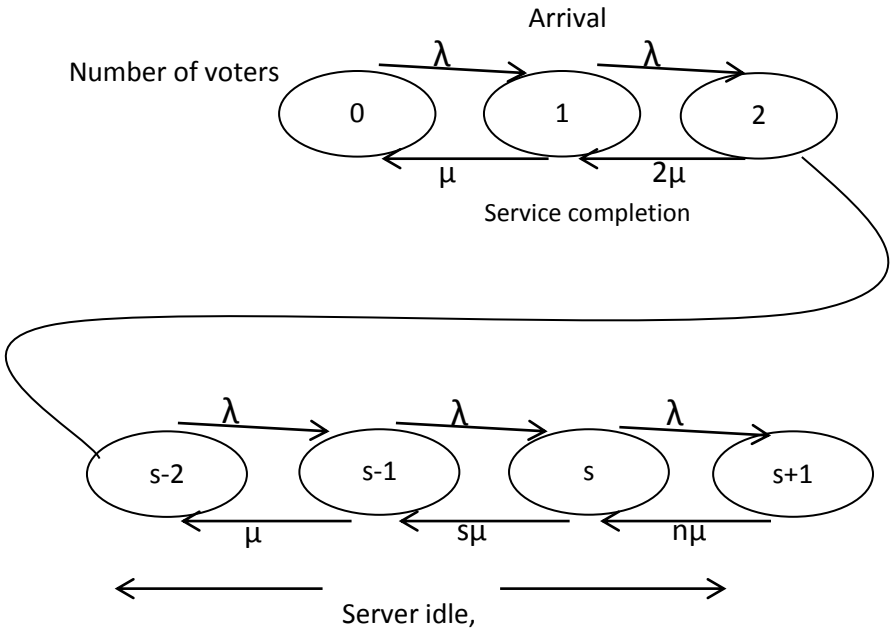


Figure 6 : The Transition Diagram for Movement of Voters (Sharma, 2009).

Performance measures for multi-server queuing model are:

i. The expected number of voters waiting in the queue (length of time):

$$L_q = \sum_{n=s}^{\infty} (\mathrm{n}-\mathrm{s})\, \mathrm{p}_n = \sum_{n=s}^{\infty} (\mathrm{n}-\mathrm{s}) \frac{p_n}{s^{n-s} s!} p_0$$

$$= \frac{p^s p_0}{s!} \sum_{n=s}^{\infty} (n-s) p^{n-s} = \frac{p^s p_0}{s!} \sum_{m=0}^{\infty} {}^{m} p^{m}; n-s = m, p = \frac{\lambda}{\mu} \quad \ldots \quad i$$

i. The expected number of voters in the system:

$$L_s = L_q + \frac{\lambda}{\mu} \qquad \ldots \quad ii$$

ii. The expected waiting time of a voter in the queue:

$$w_q = \left[\frac{1}{(\mathrm{s}-1)!} \left[\frac{\lambda}{\mu} \right]^s \frac{\mu}{(s\mu - \lambda)^2} \right] p_o = \frac{L_q}{\lambda}$$

iii. The expected waiting time that a voter spent in the system:

$$w_s = w_q + \frac{1}{\mu} = \frac{L_q}{\lambda} + \frac{1}{\mu} \qquad \ldots \qquad iv$$

v. The probability that all servers are simultaneously busy (utilization factors)

$$p(n \geq s) = \sum_{n=s}^{\infty} p_n \quad iii \quad \sum_{n=s}^{\infty} \frac{1}{s! s^{n-s}} \left[\frac{\lambda}{\mu} \right]^n p_o$$

$$\frac{1}{s!} \left[\frac{\lambda}{\mu} \right]^s \sum_{n=0}^{\infty} \left[\frac{\lambda}{\mu} \right] = \frac{1}{s!} \left[\frac{\lambda}{\mu} \right]^s \frac{s\mu}{s\mu - \lambda} p_o \quad \ldots \quad v$$

Counting phase

All votes are counted and tallied by the administrator in the system and election results are made available on the e-voting server to be accessed by legitimate voters.

IMPLEMENTATION

The implementation of this scheme is achieved by setting up a Local Area Network and computers that use windows .The program was designed using php and java script to develop front-end and back-end. MySQL was also used to handle voters' record in the database over a Secured Socket Connection.

RESULT

The validity of our approach was tested using the Student Union Government election of The Federal Polytechnic, Ilaro. A high degree of authentication security was achieved making it difficult for invalid voters to cast their votes. Also efficient performance of servers allowed the election to be conducted quickly (within one hour) even though only four system server was setup and used in the election of ten thousand voters.

CONCLUSION

E-voting system overcomes problem associated with traditional voting system. The present system provides a secured authentication system, which plays a vital role in any voting system, and it is also achieve a high degree performance of server, so that election is conducted very quickly without any delay.

Authentication framework provided in this work guarantees sufficient security mechanism for authenticating individuals for election processes which ensures that only the legitimate voters are allowed to have access to the e-voting system. This scheme gains a higher level of authenticity for security systems with high degree of accuracy and reliability. The algorithms employed in the work enhanced the performance and security aspect of the system. Our future work is going to be an E-voting Agent System to improve the security mechanism for e-voting system.

REFERENCE

Ajiboye et al., 2013, Modelling and Evaluation of E-Voting System for a Sustainable Credible Election, International Journal of Applied Information Systems (IJAIS), Foundation of Computer Science FCS, New York, USA, 5(3).

Aneta Z., Zbigniew K., 2006. An Efficient Agent e–Voting System with Distributed Trust",VODCA 2006.

Ciprian S. 2008. e-Voting Security, Buletinul Universităţii Petrol–Gaze din Ploieşti, LX (2):93-97 SeriaMatematică - Informatică–Fizică.

Do van Thanh Jorstad *et al.,* 2009. Strong Authentication with Mobile Phone as Security Token, Mobile Ad-hoc and Sensor Systems, 2009 IEEE 6th International Conference.

Harish D., Karthik M., 2010. Two Way Mobile Authentication System, Electrical Engineering Master Thesis, Thesis no: MSE-2004-xx June 2010.

Jegede *et al.*, 2012. Electronic Voting: A Panacea For electoral irregularities in developing countries, International Journal of Science and Knowledge, 1(1): 17-30.

Khalid *et al.*, 2013. Enhance Luhn Algorithm for Validation of Credit Cards Numbers. International Journal of Computer Science and Mobile Computing, 2(7) 262–272.

Kekre H. B., Bharadi V. A., 2009. Using Component Model for Interfacing Biometric Sensors to Capture Multidimensional Feature, International Journal of Intelligent Information Technology Application, 2(6):279-285

Linu P., Anilkumar M. N., 2012. Authentication for Online Voting Using Steganography and Biometrics, International Journal of Advance Research in Computer Engineering and Technology, 1(10).

Mahesh *et al.*, 2014. Credit Card Fraud Detection by Improving K-Means, International Journal of Engineering and Technical Research (IJETR), 2(5).

Mohammed I. A. and Mohammed Abo-Rizka, 2013. Internet Voting: Security and Performance Issues, Egyptian Computer Science Journal, ECS,37 (4).

Sharma J. K. 2009. Operations Research Theory and Applications, 4th Edition, Macmillan Publishers India Ltd.

Shubhangi *et al.*, 2013. Secure E-voting Using Homomorphic Technology, International Journal of Emerging Technology and Advanced Engineering, 3(8).

Sutaone, Khandare, 2008. Image based Steganography using LSB insertion technique, IEEE WMMN, pp.146-151.