AN ENHANCED MULTIFACTOR AUTHENTICATION SCHEME FOR DYNAMIC ONLINE VOTING SYSTEM

[1]Hammed M., [2]Ibharalu F.T., [3]Folorunso O., [4]Dawodu G.A. and [5]Ojesanmi O.A

[1]Department of Computer Science, School of Applied Science, Federal Polytechnic, Ilaro, Ogun State
[2,3,5]Department of Computer Science, Federal University of Agriculture Abeokuta, Ogun, State
[4]Department of Statistics, Federal University of Agriculture Abeokuta, Ogun State

(tundemuhammedy2k@yahoo.com; tomibharalu@yahoo.com; folorunsolusegun@yahoo.com; abayomidawodu@yahoo.co.uk; dejioje@yahoo.com)

ABSTRACT

The increasing use of the internet introduces a lot of 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 authentication process used by most of these efforts are very weak to validate legitimate voter which determine the faith of whole electoral process. This work proposed a multifactor authentication scheme for e-voting system. The multifactor authentication scheme provides security efficiency through what the voter knows (PIN), what the voters have (phone and email) and what the voter is (photograph). The multifactor authentication scheme is more secured in authenticating voters during e-voting process.

KEYWORDS *- E-voting System, Luhn's algorithm. Association Rule Mining Algorithm, Convolution algorithm, Puzzles, Mobile Phone and E-mail.*

1.0 Introduction

Election is a fundamental instrument of a democratic process that enables the electorate to determine fairly and freely who should lead them at every level of government periodically [14]. Voting is a process that takes an important position in a democratic society. Recently, its adoption in institutions of higher learning among students for electing their leaders is gaining popularity as electronic voting (e-voting) brings to the polling station [1]. The basic idea behind this system is to overcome the limitations of the traditional voting system as there is complexity and huge time period required. This system has capability of reducing human errors and will provide better scalability for large elections [2]. Online Voting are simple, attractive and ease to use. It reduces manual efforts and bulk of information can be handled easily [3]. Properly implemented, e-voting solutions can eliminate certain common avenues of fraud, speed up the processing of results, increases accessibility and make voting more convenient for citizens, in some cases, when used over a series of electoral events, possibly even reducing the cost of elections or referendums in the long term. Unfortunately not all e-voting projects succeed in delivering on such high promises (International [7]. In a voting system, whether electronic or using traditional paper ballots, the system should meet the certain important criteria such eligibility and authentication, uniqueness, accuracy, integrity, verifiability, reliability, secrecy, flexibility, convenience, transparency, and cost effectiveness. Among these, authentication can be viewed as the most critical issue. As online voting is risky, it is difficult to come up with a system which is perfect in all senses [11]. A system is said to be democratic in nature if, it permits only eligible voters to vote and ensures that each eligible voter can vote only once [16]. Different authentication schemes have been proposed by different authors, among these are Two Way Mobile Authentication System

service [6], Fingerprint Biometrics and Personal Identification Number (PIN) [18], Multifactor Authentication and Cryptographic Hash Functions, Authentication for Online Voting Using Steganography and Biometrics [11], [10] proposed dynamic ID based remote user authentication scheme for multi-server environments,[9] A New Remote User Authentication Scheme based on Graphical Password using Smart Card and
[19], proposed Authentication Algorithm for Portable Embedded Systems using PUFs. An enhanced multifactor authentication scheme for dynamic online voting system
uses combination of what the user knows (Personal Identification Number), what the user has (Phone or E-mail address) and what the user is (Photograph) to provides a strong security mechanism for dynamic e-voting system as it is shown in figure 1.Online voting system depicted in figure 2 forms the basis of the proposed system.

Personal Identification Number (PIN) is obtained By individual voter
Encrypted PIN is sent to voter's phone while numerical value is sent to voter's e-mail
Photograph is uploaded during registration & each time voter wants to login

Figure 1: Three authentication factors

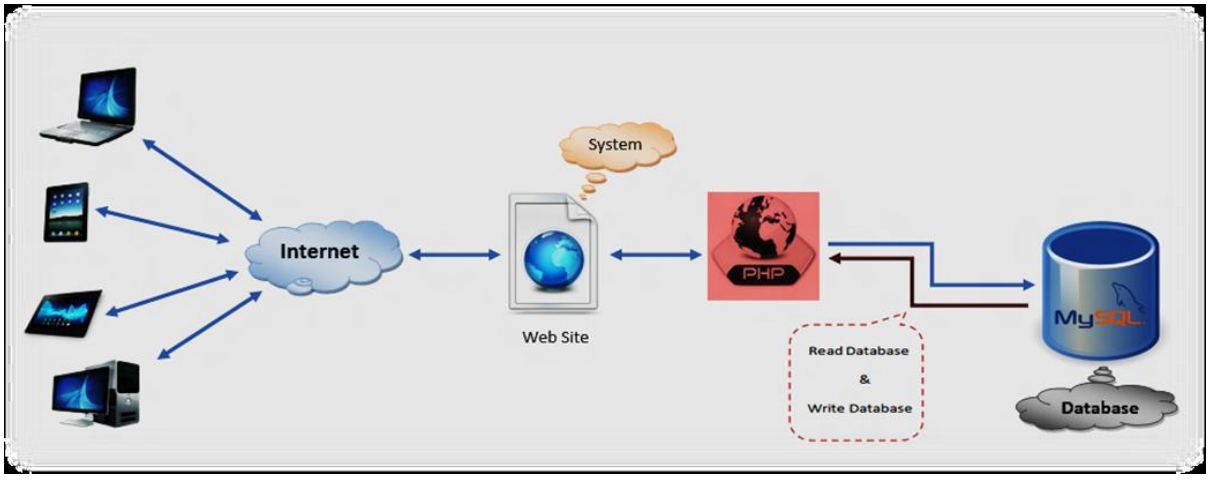

Figure 2: Internet e-voting system [4]

2.0 Literature Review

Many researchers have proposed different methods to deal with authentication in e-voting system. Although they differ in authorization of user based on the security problems. Among the researcher are:
[9], proposed a new remote user authentication scheme based on graphical password using smart card. In the scheme, the user's password is generated by using an image provided by

the user. One of the advantage of the scheme is that human can remember pictures easily than text. But, the weakness is that the adversary can intercept messages communication between the server and the registration center. Server should be the one performing registration and authentication. The scheme cannot also achieve two-factor authentication.

[15], proposed a robust secured stegano-cryptographic model and the model possessed capacity to guarantee and validate voter's for who they said they are, guarantees the integrity of elections, ensures privacy of the voters, guarantees the confidentiality of the vote and provide mechanism for fraud detection after the electioneering process. Using stegano-cryptographic technique to solve integrity and confidentiality issues of secured e-voting system. Though, the implemented steganography system showed low toughness to statistical steganalyst attack. The modification of cover image by an eavesdropper could destroy the hidden content before tallying by the administrator and the model cannot achieve multifactor authentication.

[10], proposed dynamic ID based remote user authentication scheme for multi-server environment, this scheme contains four phases which include registration phase, login phase, verification phase and password change phase. This scheme provides a strong security mechanism but the weakness is that the user's identity is related to the password by the value of $C=h(ID||h(y)||h(b\oplus PW))$ stored in the smart card. Therefore, the scheme cannot achieve two-factor authentication.

[18], developed a secure electronic voting system using fingerprint technique. This method count the counterfeit minutiae of the human thumb impression and separate out the authentic minutiae regions; which are subsequently extracted and used not only as user access control identity to the system but also the vote in the electoral process. This system nullifies multiple vote casting; provide a more accurate election results collation process, and a secured voter's authentication mechanism. However, the cost of providing the special hardware device to carry out biometrics enrolment was not considered and the system cannot achieve multifactor authentication.

[12] [11] , proposed online voting using steganography and biometrics. The voters use their fingerprint which has been pre-enrolled to access the voting machine. The usage of anatomical traits rather than behavioural attributes further create more secured and acceptable voters registration system, because the fingerprint is unique, distinct, universal, and not easily damaged for every individual. But, additional hardware is required to detect fingerprints. The steganography technique enables embedding of the vote into the high frequency band (high scale).The high frequency band was selected because the human visual system cannot perceive the tiny modifications of the band. The number of bits modified is directly proportional to the change in the statistical properties of any image. This technique does not give room to steganalytic detector to search for expected set of variations; thus increases casting of vote time for an individual voter. The method is limited to hashing speed of the underlying hash function and more time is needed to complete voting by a large populace. Also hardware for taking thumb impression is costly and Handicapped people cannot participate in voting in the system. The system cannot achieve multifactor authentication.

[6], proposed two way mobile authentication system that provides access to Web-based resources by using a two- way user authentication through the existing personal mobile

phones. It positively identify users and deliver services easily and in a most secured way to users, without having the need of an additional security system. End users can have the advantages of a very simple process that omits the need to remember multiple passwords. But, special software has to be installed on user's mobile device and if the mobile device is lost anybody can access the information on the device. The system cannot achieve multifactor authentication scheme.

3.0 Materials and Methods

The voter can vote anywhere and anytime once is able to connect to voting's website. Voting process consists of three phases which include: Registration phase and Authentication/vote casting phase and Tallying and counting phase. But, this research work focuses on Registration phase and Authentication/vote casting phase.

3.1 Registration Phase

All the voters must register first with their names, sex, age, phone number, e-mail address and photograph then obtain their Personal Identification Number (PIN) which are sent in encrypted form to the voter's phone number and the numerical values for the encrypted one are sent to voter's email. Subsequently, voters login to online voting system using generated PIN and upload his/her photograph. E-voting server confirm voter's illegibility using embedded Luhn's algorithm, Apriori algorithm and Convolution neural network. The online voting system contains voter's details to maintain its account. If there is any deviation from what is in voter's account the system will automatically deactivate the voter. But if the account is correct with the provided information the voter will be activated. The flowchart in figure 3 depicts e-voting registration process.

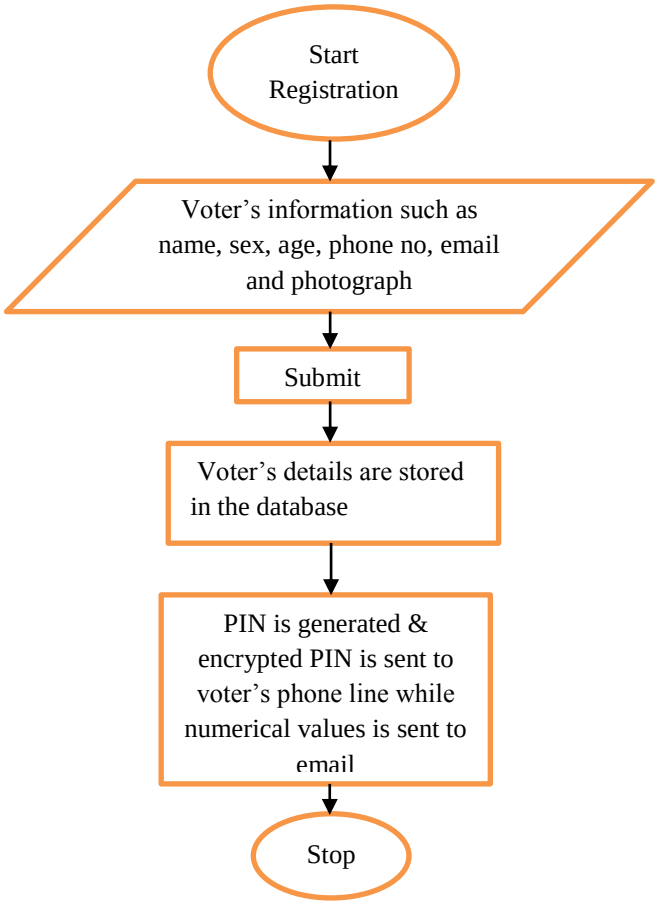

Figure 3: Flowchart for Registration Process

3.2 Authentication /vote casting phase

Each time a voter logs into the e-voting system with his/her PIN and photograph, the server's agent (administrator) collects the request and performs the Luhn's algorithm, Associative rule algorithm and Convolution neural network to determine activation and deactivation of the voter.

Luhn's algorithm verify whether the voter's number is authentic before deciding whether to activate or deactivate a particular voter. The algorithm [8] is shown in algorithm 1.

Algorithm 1: Luhn's 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.*

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 to 0, then subtract the remainder from 10. The resultant number is the check digit.*

The Associative rule mining algorithm is an IF/THEN statement to determine the relationship between the voter's PIN and information stored in the database each time the user tries to log in. In this work, we develop association rules 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. One of the associative rule mining algorithm that used for this purpose is Apriori algorithm described in [5]. It is depicted in algorithm 2 to compare the voter's PIN with the voter's information already stored in e-voting database for validation.

Algorithm 2: Apriori Algorithm

Step 1: K=1

Step 2: $F_k = \{i \mid i \in I \wedge \mathrm{r}(\{i\}) \geq \mathrm{Nxminsup}\}$

{*Find all frequent 1-itemsets*}

Step 3: Repeat

Step 4: *K = k + 1*

Step 5: $C_k = apriori - gen\ (F_{k-1})$

{Generate Candidate itemsets}

Step 6: For each transaction $t \in T$ do

Step 7: $C_{t=}$ subset (C_k, t) .{Identity all candidates that belong to t}

Step 8: For each candidate *itemset* $c \in C_t$ do

Step 9: $\sigma(\mathrm{c}) = \sigma(\mathrm{c}) + 1.$ {Increment support count}

Step 10: *endfor*

Step 11: *endfor*

Step 12: $F_k = \{c \mid c \in c_k \wedge \sigma(\mathrm{c}) \geq Nx \min \mathrm{sup}\}$

{Extract the frequent k-itemsets}

Step 13: until $F_k = \phi$

Step 14: Result = $\bigcup F_k$

Step 5 of the Apriori algorithm in algorithm 1 performs the following operations:

(i) Candidate Generation: this operation generates new candidate k – itemsets based on the frequent (k-1) – itemsets found in the previous iteration.

(ii) Candidate pruning: This operation eliminates some of the candidate k – itemsets using the support- based pruning strategy.

This indicates that if voter should be authorized X (PIN) must satisfy Y (Voter's information)

i.e.

IF X satisfies Y THEN
    Authorize the voter
ELSE
    Don't authorize the voter
END IF
END

The Convolution neural network is to classify the voter's images whether is the original or fake within a short time. According to [13] the aim of the first convolutional layer is to extract patterns found within local regions of the input images that are common throughout the dataset. This could be achieved by convolving a template or filter over the input image pixels, and computing the inner product of the template at every location in the image and outputting a feature mapped **c**, for each filter in the layer. A linear rectification f(c) = max (0; c) then applies to each feature map **c**. This output is a measure of how well the template matches each portion of the image. The resulting activations f(c) are then passed to the pooling layer. This aggregates the information within a set of small local regions, R, producing a pooled feature map **s** as output, for each feature map, **c**, as given in equation (1).

$$S_j = pool(f(c_i)) \in \mathrm{R}_j \quad (1)$$

where R_j is pooling region j in feature map **c** and **i** is the index of each element within it. In convolution neural network, the weights of the convolutional layer being used for feature extraction as well as the fully connected layer being used for classification are determined during the training process [17].The proposed Convolution neural network is embedded on e-voting system to classify voter's image. The flowchart in figure 4 depicts authentication process

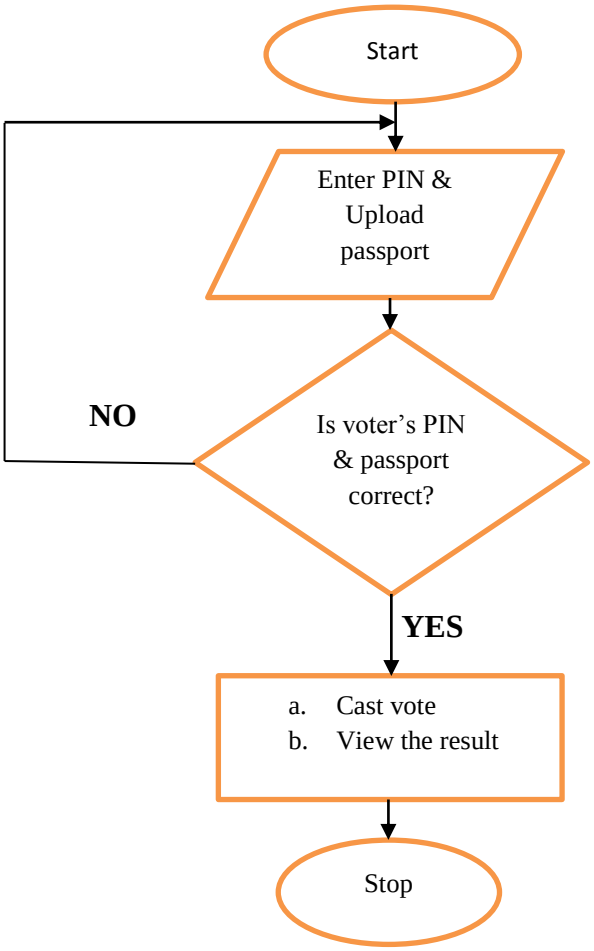

Figure 4: Flowchart showing Authentication Process

4.0 Discussion and Result

Every citizen (18-above) will register for voting, during the registration each voter submit his/her passport for security purpose by using webcam as it is shown in figure 5.

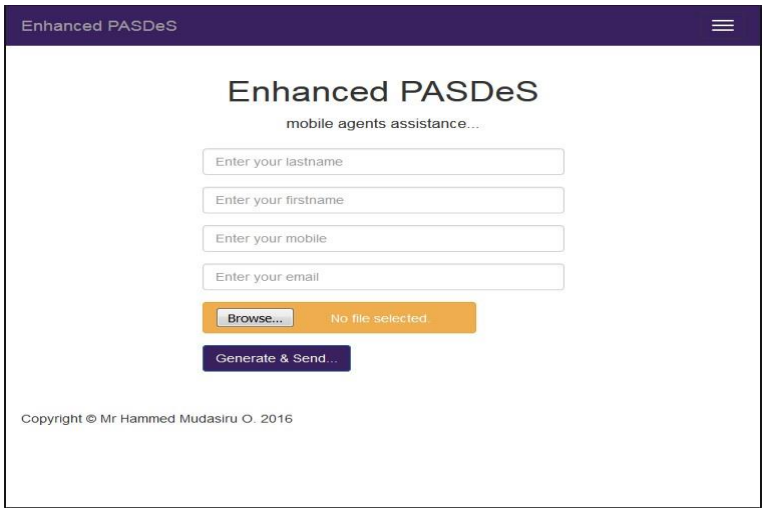

Figure 5: Voter's registration module

All information about the voters are stored in the e-voting database as it is shown in figure 6.

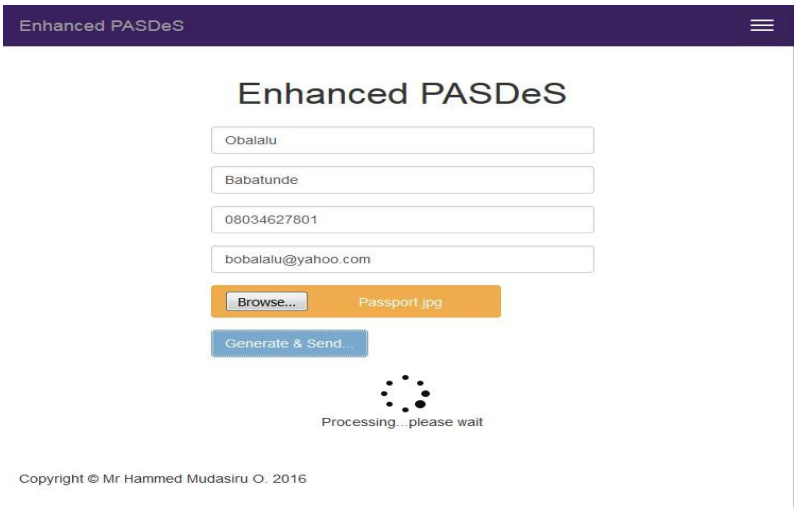

Figure 6: Voter's information processing module

PIN number which contains a group of letters is generated for every individual registered voter to maintain the voter's account. Numerical values for alphabets is sent to voter's email for security purpose as it is shown in figure 7

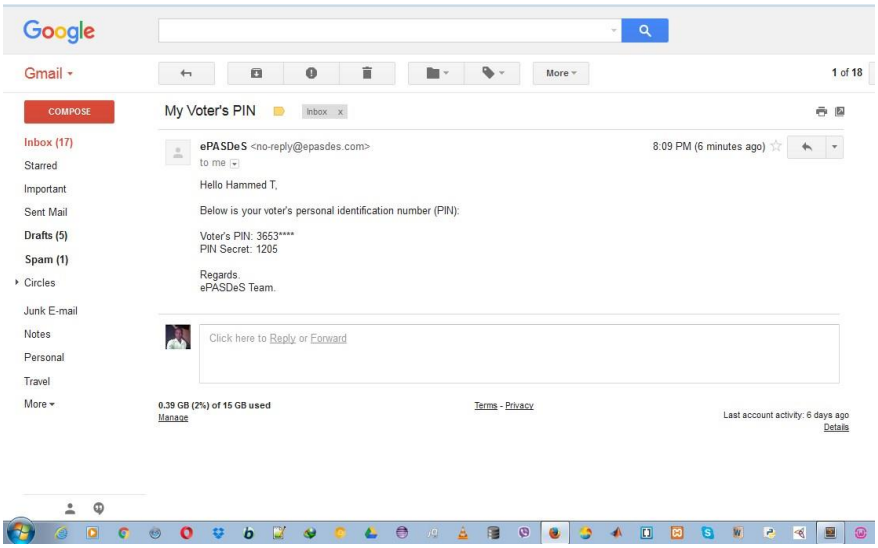

Figure 7: Voter's PIN generating module

This authentication system comprises of two module which include Call-back-Handler and Login module.

a. Call-back-Handler: allows the registered voter to login into the system for voting by entering PIN/photograph. The E-voting system is loaded from the D:\E-voting\Administrator directory as it is shown in figure 8.

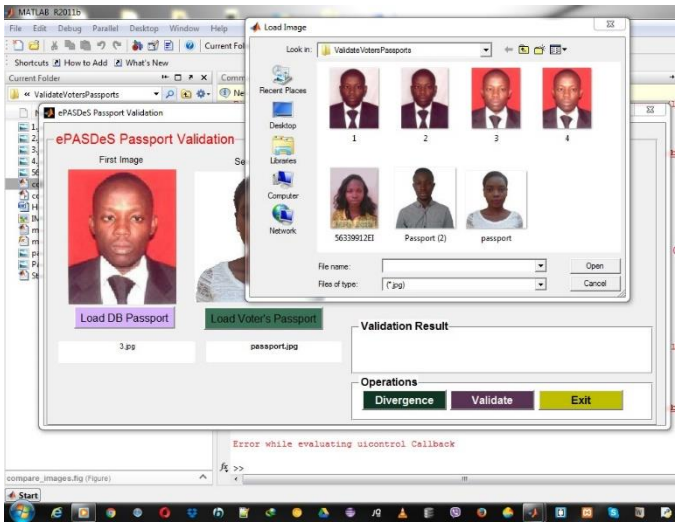

Figure 8: Call-back-handler for register voter to login

b. Login-Module: checks if these information are valid or not.

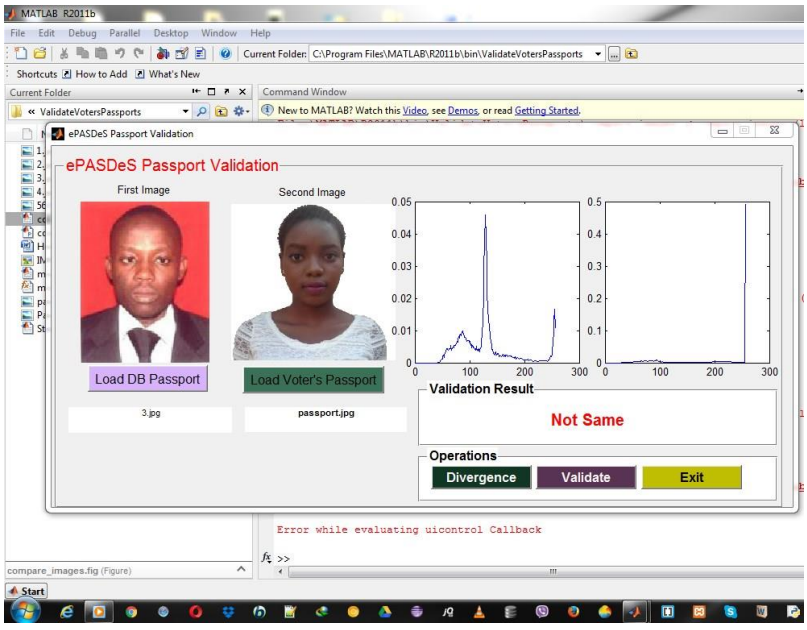

Figure 9: Login-module for validating voter

The graph in figure 9 shows that information provided during the authentication does not match the one provided during the registration which has been stored in e-voting database.

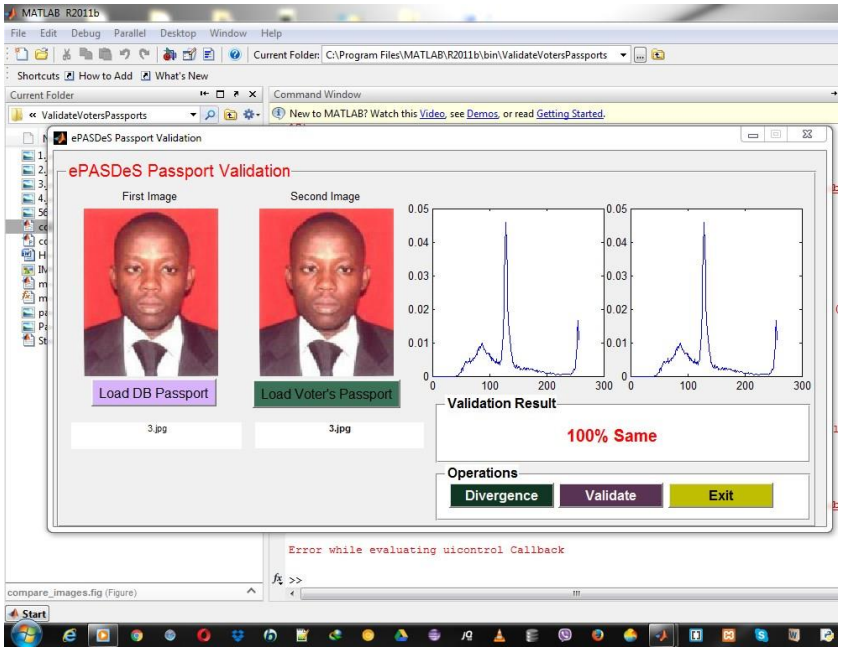

Figure 10: Login-module for validating voter

The result of the graph in figure 10 shows that information provided by the voter during the registration and authentication is 100% matches information stored in e-voting database during the registration.

4.1 Evaluation

When an evaluation is done on dynamic e-voting system, it is important to evaluate authentication issues because this phase determines the faith of whole electoral process. The main authentication issues are:

i. Unauthorized voters casting the votes.

ii. Eligible voters cast multiple votes.

iii. Casting vote on behalf of another person (impersonation).

Based on these authentication issues, the proposed authentication scheme has been tested for Student Union Government election at Federal Polytechnic Ilaro to evaluate the following dynamic e-voting issues:

i. Unregistered voters to cast votes

ii. Voters to cast votes repeatedly.

iii. Voters used incomplete PIN.

iv. Voters cast votes on behalf of another person.

In this work, authentication scheme is designed to validate voter's legitimate using Luhn's algorithm, Apriori algorithm and Convolution neural network, where input and output result is shown in figure 5 to figure 10.

Performance Evaluator calculate the various classification performance measure to judge the system accuracy. The confusion matrix is used for performance evaluator which was described in (Sofia *et al.,* 2011) as follows:

a is the number of correct negative prediction

b is the number of incorrect positive prediction

c is the number of incorrect negative prediction

d is the number of correct positive prediction

The classification and prediction accuracy for load balancing is obtained as it is shown in equation 32 and 33. The table 3 shown the confusion matrix evaluator for load balancing in dynamic e-voting system.

$$\text{Load balancing Accuracy} = \frac{a+d}{a+b+c+d} \quad (32)$$

$$\text{Load balancing Error} = \frac{b+c}{a+b+c+d} \quad (33)$$

Table 3: Confusion Matrix for Performance Evaluator

	Predicted Negative	Predicted Positive
Actual Negative	a	b
Actual Positive	c	d

Conclusion

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. A voter cannot register twice and cannot cast its vote more than once. This scheme gains a higher level of authenticity for secured systems with high degree of accuracy and reliability. The algorithms employed in the work enhanced the performance and security aspect of the system.

References

[1] Ajiboye, A.R., Jimoh, R.G., Oladipo, I.D. 2013. Modeling and Evaluation of E-Voting System for a Sustainable Credible Election. *International Journal of Applied Information*

Systems (IJAIS),ISSN: 2249-0868.Foundation of Computer Science FCS, New York, USA, Vol. 5, No. 3.

[2] Anisaara, N., Ashmita, K., Tushar, N., Rakhi, B., Durgesh, K.G. 2014. An Analysis of Secure Online Voting System. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST), ISSN: 2347-5552, Volume-2, Issue-5.*

[3] Ankit, A. and Pallavi, D. 2012. An Efficient Online Voting System. *International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.2, Issue.4, July-Aug. 2012 pp-2631-2634*

[4] Aree A.M. and Ramyar A.T. 2013. Efficient E-voting Android Based System. *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 11.

[5] Han, E.H., Karypis, G. and Kumar V., 1997. Min-Apriori: An Algorithm for Finding Association Rules in Data with Continuous attributes. *Retrieved 27th September, 2016 at www.cs.umn.edu/*han 1997*

[6] Harish, D. and Karthik, M., 2010, Two Way Mobile Authentication System, *Master Thesis Electrical Engineering Thesis no: MSE-2004-xx, June 2010. Department of Electrical Engineering, Blekinge Institute of Technology, Sweden.*

[7] International IDEA, 2011. *Introducing Electronic Voting:Essential Considerations*. International IDEA works worldwide. Sweden, Retrieved 4th September, 2016 at http://www.idea.int/publications/emd , pp. 1-35.

[8] Khalid, W. H., Nor Fazlida, M. S., Ramlan M., Mohammed Taufik, A. 2013, Enhance Luhn Algorithm for Validation of Credit Cards Numbers". International Journal of Computer Science and Mobile Computing,IJCSMC, Vol. 2, Issue. 7, pp.262 – 272.

[9] Khanjan, Ch. B., Subhasish B., Manash, P. D. and Chandan T. B. 2015. A New Remote User Authentication Scheme based on Graphical Password using Smart Card. *International Journal of Security and Its Applications Vol.9, No.12, pp.237-*244.

[10] Li, X., Ma, J., Wang, W., Xiong, Y. and Zhang, J. 2013. A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments. *Mathematical and Computer Modelling, vol. 58, no. 1-2, pp. 85-95.*

[11] Linu, P. and Anilkumar, M., 2012, Authentication for Online Voting Using Steganography and Biometrics, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Vol. 5, No. 10, pp. 26–32*

[12] Malwade, N., Patil, C., Chavan S. and Raut S.Y., 2013, Secure Online Voting System Proposed By Biometrics And Steganography, *International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 5*

[13] Nair, V. and Hinton, G. E., 2010, Rectified linear units improve restricted boltzmann machines, *Proceedings of the 27th International Conference on Machine Learning, Haifa, Israel.*

[14] Obakhedo, N. O. 2011. Curbing Electoral Violence in Nigeria: The Imperative of Political Education. *International Multidisciplinary Journal, Ethiopia Vol. 5 (5), Serial No. 22, pp. 99-110.*

[15] Olaniyi, O., Arulogun, O., Omidiora, E., and Okediran, O., 2014. Performance Evaluation of modified Stegano-Cryptographic model for Secured E-voting, *International Journal of Multidisciplinary in Cryptology and Information Security, vol. 3, no. 1, pp. 1–8.*

[16] Omolaye, P. O., Pius D. and Orifa, A. 2015. Systemic Evaluation of Semi-Electronic Voting System adopted in Nigeria 2015 General Elections. *American Journal of Information Systems* 3(1):15-21.

[17] Samer, H., Rishi, K. and Chris, R., 2015, Using Convolutional Neural Networks for Image Recognition, *IP Group, Cadence.*

[18] Sanjay, K. and Manpreet, S., 2013, Design A Secure Electronic Voting System Using Fingerprint Technique, *International Journal of Computer Science Issues, Vol. 10, Issue 4, No.1.*

[19] Sunil D. B. and Vijay R. M. 2015. Authentication Algorithm for Portable Embedded Systems using PUFs. *Global Journals Inc. (USA), Volume 15 Issue 1 Version 1.0.*