Proceedings AICTTRA 2018 Proceedings AICTTRA 2018 Proceedings AICTTRA 2018

Proceedings

Of the

12th International Multi-Conference on ICT Applications

Theme:

APPLICATION OF INFORMATION AND COMMUNICATIONS TECHNOLOGY TO TEACHING, RESEARCH AND ADMINISTRATION

AICTTRA 2018

Venue

MAIN AUDITORIUM
AFRICAN CENTRE OF EXCELLENCE
(OAK-Park)
OBAFEMI AWOLOWO UNIVERSITY
ILE-IFE, NIGERIA.

FOR LEARNING AND CULTURE

OBAFEMI AWOLOWO UNIVERSITY, ILE-IFE.
Department of Computer Science and Engineering
In collaboration with
Africa Centre of Excellence:
OAUICT Driven Knowledge Park

OAK-PARK

ISSN 2141 - 0240

The 12th International Multi-Conference on ICT Applications

With the Theme

Application of
Information and Communications Technology
To Teaching, Research and Administration

AICTTRA 2018

November 11th – 14th, 2018

@

Main Auditorium
African Centre of Excellence *(OAK-Park)*
Obafemi Awolowo University, Ile-Ife, Nigeria

PROCEEDINGS

Volume XII

Edited by

Professor E.R. Adagunodo
Professor G.A. Aderounmu
Dr. A. I Oluwaranti
Dr. E.A. Olajubu
Dr. B.I. Akhigbe
Dr. I.P. Gambo

Organized by
Department of Computer Science & Engineering
In Collaboration with
African Centre of Excellence: OAUICT Driven Knowledge Park
Obafemi Awolowo University

FOREWARD

It is my great pleasure and delight to welcome all of us to the 12th International Conference on Application of Information and Communication Technology to Teaching, Research and Administration tagged AICTTRA 2018, which is holding at the African Centre of Excellence (OAK-Park), Obafemi Awolowo University, Ile-Ife, Nigeria between November 11th and 14th, 2018. I understand that conferees came from different places and beyond to attend this great event. I usually refer to the conference as a pilgrimage for ICT professionals and enthusiast. A total of 45 well written and reviewed papers have been selected for presentation at different times in the conference.

The Programme of the conference is a varied one that reveals the wide range of application to which ICT is being put and exposes the impossibility of placing any specific bounds or limits on the field. The field of ICT has continued to grow with mind blowing evidences in its area of application. To be able to compare note and learn from each other through the exploration of techniques remain the motivation to hold this conference year in year out. Thus, this quest has been on as a matter of strict business as was in the previous eleven versions of the conference. This twelfth edition seeks a multi-conference approach to the forgoing, and promises to extend the frontiers of the exploration of the deployment of ICT in various spheres of human activities.

The programme of the conference has been threaded into parallel sessions. The sessions promised to stimulate fruitful debate on emerging areas of research in the use of ICT. We are sure that cutting edge issues have been included in organized syndicate and informal discussion sessions that will take place during the conference. This promises to be useful and informative.

The President, Nigeria computing Society (NCS), Professor G.A. Aderounmu, and the current Dean of the Faculty of Technology, Obafemi Awolowo University happens to be one of the initiators of the conference will be on hand to share his wealth of experiences in teaching, research and administration. There will be lead paper presentations by eminent researchers and practitioners in ICT. The organizers of the event owe special thanks to the Vice-Chancellor of Obafemi Awolowo University, IIe-Ife, Nigeria, Professor E.O. Ogunbodede for his continuous support in the organization of the conference.

We are also very grateful to one of the fathers of this conference - Professor L.O. Kehinde, for his support. To the Chairman LOC - Dr. A.I. Oluwaranti and his technical team and members such as Dr. E.A. Olajubu (Vice Chair LOC), Dr. B.O. Akinyemi, Dr. B.I. Akhigbe, Dr. I.P. Gambo, Dr. S.A. Bello, Dr. R.N. Ikono, Dr. S. Aina, Dr. H.O. Odukoya, Engr. Tope Ajayi, Ms. A.R. Lawal who had all worked tirelessly to ensure the success of this conference; I say a big thank you and congratulations for a job well done. I also appreciate the members of staff - academic, non-academic, and technical - for their immense support towards the conference. This conference could not have been successful without the support of individuals and several corporate entities, which time will not permit to mention. All the same, our thanks go to all of them for their continuous belief in the conference and continual support. You are all wonderful people and great as well, and most especially all the attendees in this year’s Conference.

Professor E. R. Adagunodo
Department of Computer Science & Engineering,
Obafemi Awolowo University, Ile-Ife, Nigeria.

LIST OF REVIEWERS

S/No	Name of Reviewers	Contact Address
1.	Prof. E.R. Adagunodo	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
2.	Prof. G.A. Aderounmu	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
3.	Prof. K. Gbolagade	Kwara State University, Ilorin, Kwara State
4.	Dr. A.O. Oluwatope	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
5.	Dr. B.S. Afolabi	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
6.	Dr. (Mrs.) R.N. Ikono	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
7.	Dr. K.I. Ogundoyin	Department of Computer Science, Osun State University, Osogbo
8.	Dr. S.A. Akinboro	Department of Computer Science, Bells University, Otta, Ogun State
9.	Dr. C.O. Akanbi	Department of Computer Science, Osun State University, Osogbo
10.	Dr. L.A. Akanbi	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
11.	Dr. A.O. Ajayi	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
12.	Dr. A.A. Adeyelu	Department of Mathematics & Computer Science, Benue State University, Makurdi
13.	Dr. P.A. Idowu	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
14.	Dr. (Mrs.) A.R. Iyanda	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
15.	Dr. (Mrs.) B.O. Akinyemi	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
16.	Dr. A.I. Oluwaranti	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
17.	Dr. (Mrs.) G.O. Binuyo	African Institute for Science Policy and Innovation, Obafemi Awolowo University, Ile-Ife.
18.	Dr. F.O. Asahiah	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
19.	Dr. (Mrs.) S.A. Bello	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
21.	Dr. S. Aina	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
22.	Dr. O. Osunade	Director, Information Technology and Media Services, University of Ibadan, Ibadan

S/No.	Name of Reviewers	Contact Address
23.	Dr. O.F.W. Onifade	Department of Computer Science, University of Ibadan, Ibadan
24.	Dr. (Mrs.) M.L. Sanni	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
25.	Dr. H.O. Odukoya	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
26.	Dr. O.A. Ojesanmi	Department of Computer Science, Federal University of Agriculture, Abeokuta
27.	Dr. A.O. Akinwumi	Department of Computer Science & Information Technology, Bowen University, Iwo
28.	Dr. A.S. Sodiya	Department of Computer Science, Federal University of Agriculture, Abeokuta
29.	Dr. S.A. Onashoga	Department of Computer Science, Federal University of Agriculture, Abeokuta
30.	Prof. S. Tanko	University of Jos, Nigeria & Scarborough, North Yorkshire, United Kingdom
31.	Dr. O.O. Abiona	Department of Computer Information Systems, Indiana University, North West U.S.
32.	Dr. Jimoh	Department of Computer Science, University of Ilorin, Ilorin
33.	Dr. (Mrs.) I.O. Awoyelu	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
34.	Dr. (Mrs.) O.D. Ninan	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife
35.	Dr. R.G. Jimoh	Department of Computer Science, University of Ilorin, Kwara State.
36.	Dr. S.I. Eludiora	Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife

TOWARDS THE USE OF BPANN TECHNIQUE FOR MITIGATING LAYER 4 DDOS ATTACK IN ELECTRONIC VOTING

[*]Almustapha A. J., [1]Olaniyi O. M., [1]Abdullahi I. M. and [1]Abdulsalam,Y. S
*Department of Computer Science, Federal University of Technology, Minna, Niger-State, Nigeria
*Department of Computer Science, Federal Polytechnic, Bida, Niger-State, Nigeria
[1]Department of Computer Engineering, Federal University of Technology, Minna, Niger-State, Nigeria
*E-mail: almustapha@st.futminna.edu.ng
*Phone: +2348063636347

ABSTRACT

System availability is a criterion that e-voting systems are required to satisfy. This involves ensuring that an e-voting system is secure whenever a Distributed Denial-of-Service attack occurs and that voters could always have access to the system during election. System availability can be a serious security challenge faced by e-voting system, since publishing results after the conclusion of elections is a major function of the e-voting system, and this process cannot be delayed if the system's security is under DDoS attack. In the proposed model, the problem of system availability was addressed using an efficient detection sub-system based on Back Propagation Artificial Neural Network (BPANN) to mitigate Transmission Control Protocol Synchronous (TCP SYN) flood attacks. This technique developed would classify TCP SYN Flood packets captured on a workstation that serves as the Internet Voting kiosk and parameters were extracted to analyze and classify the attack. The developed technique would classify TCP SYN Flood packets captured on a workstation that serves as the Internet Voting Kiosk thereby improving the network performance and availability of the e-voting server.

Keywords: E-voting System, Distributed Denial-of-Service, Artificial Neural Network, Transmission Control Protocol Synchronous Flood.

1.0 INTRODUCTION

An Electronic voting (E-voting) system is a socio-technical selection system in which the election data is recorded, stored and processed primarily as digital information. E-Voting system helps common man to opt for their representatives more firmly and articulate their preferences for how they want to be governed [1]. Numerous Electronic Voting devices exist to aid the election process, such as using the Internet and telephone as well as android phones or wireless devices.

The election system is bedevilled with challenges around administration at all levels of decision-making, and as such requires great level of security [2]. The present voting authority must ensure that electronic elections are conducted in a transparent manner so as to encourage the building of patriotic citizens as well as good relationship amongst the next governing administration. Recently, there is a huge increase of people using the Internet and e-voting technologies are offering the opportunity to improve ease and accessibility of the voting process.

Denial-of-Service attacks disrupts e-voting systems leading to security breach and system unavailability, include Ping of death, Distributed Denial-of-Service (DDoS) attacks, packet flooding, viruses, worms, Trojan horses and physical attacks.

Overcoming the security challenges in e-voting systems is an ongoing research. Advanced cryptography and its study on security technology applied to e-voting have been documented by reputable researchers in the field of Computer Science. These technologies allow voters' anonymity and that there votes are secured, and they include Homomorphic Technology Based Protocol [3], Stegano-cryptography [4] and Identity-Based Encryption Technique [6].

Therefore, the aim of the paper is to develop a DDoS detection technique for e-voting systems using an efficient detection sub-system based on Black Propagation Artificial Neural Networks (BPANN). This paper is organized into sections with Section I providing an introduction to e-voting as it relates to DDoS environment. Section II represents the literature review and review of related works on e-voting around DDoS scenarios. Section III presents the proposed methodology to be adopted, Section IV presents result, and Section V concludes our research endeavors.

2.0 LITERATURE REVIEW

2.1 Overview of DDoS Attack

According to [3], a typical DDoS attack contains two stages with the first stage involving an attacker who performs unauthorized actions within a vulnerable system using one or more applicable tools that can connect to the system's weakness. The researchers argued that with the second stage, resources exhaustion attack can take place. This attack could either involve successfully overloading a web server with enough traffic to use up all of the available bandwidth or other resources, such as sockets, CPU, memory, disk/data-base bandwidth, and I/O bandwidth. These essentially include application-level flooding attacks.

During a DDoS attack, the attacker initiates the attack by sending a command to the zombie computers (infected computers) then these zombies send a connection request to a genuine server as if it was sent by the victim's computer as shown in Figure 1. "Thus, the genuine server sends the requested information to the victim where the victim's computer gets flooded with unsolicited responses from several computers at once to reduce the performance or cause computer to shut down". The diagram in Figure1 shows the various entities involved in a DDoS attack.

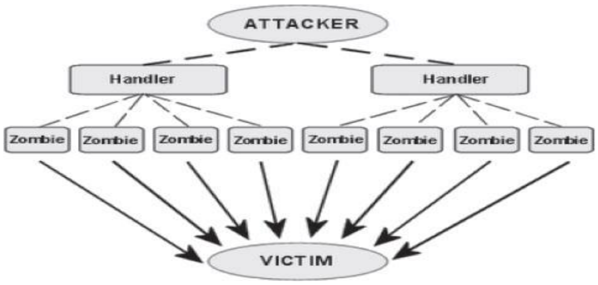

Figure 1: Architecture of DDoS Attack
Source: (Aamir. & Zaidi 2013)

A DDoS attack is successful when an attacker creates a network of infected computers by spreading malicious software to vulnerable computers called zombies. The attacker can then instruct and control these zombies by making them to flood the victim, which could be a server, with traffic. The victim is unable to provide its users with the necessary service and the network performance is also affected. In the early creation of DDoS attacks, the attacker had to identify ports, vulnerable computers manually before launching an attack [8]. DDoS attack has evolved over time becoming more sophisticated and these attacks can now be carried out using sophisticated systems that cover a wide range of access points. Also, Figure 2 shows the various classifications of DDoS attacks.

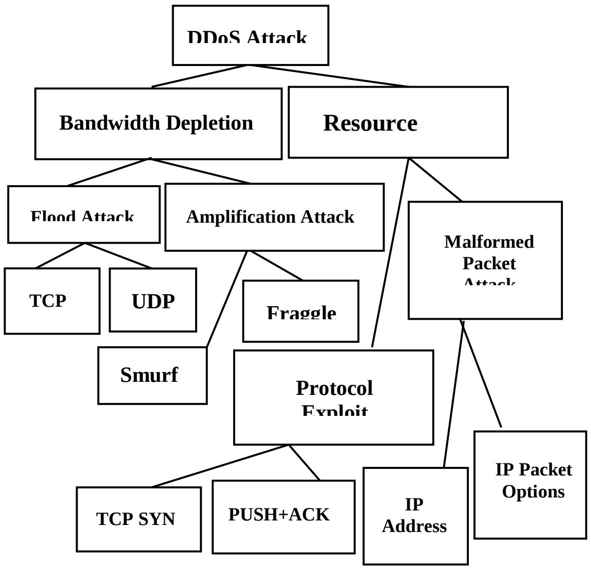

Figure 2: DDoS Attack Classification
Source: (Prasad *et al.,* 2014)

In every design of an e-voting system, voters must remain anonymous during the entire voting process [4]. Although, the TCP protocol establishes a reliable channel between the client and server, it is susceptible to flood attacks. Flood attacks use the expected behaviour of TCP protocol to the attacker's advantage [7]. Figure 2 shows TCP SYN as a protocol exploit attack. This flood attack consumes most of the network's resources, meaning that they are not readily available to other users. It takes advantage of the standard TCP three-way handshake by sending a request for connection with an invalid return address.

2.2 Electronic Voting as a Modern Channel of Franchising

"E-voting can be conducted either in controlled or in uncontrolled environments" [9]. In the former, a voter enters a polling booth to cast his/her vote while under the supervision of the officer in charge. E-voting is physically supervised by representatives of independent electoral authorities. This process is distinguished from traditional voting methods as votes are recorded through electronic technologies placed at specific locations, such as a polling kiosk. While the latter, also referred to as Remote Internet voting, is a voting mechanism that allows access to the election process for voters who need not go to their polling location on Election Day. Remote e-voting via the Internet is where the voter submits votes electronically to e-voting server from any location unsupervised by election official [9].

According to [9], Electronic Voting Machines (EVMs), Optical Mark Reading (OMR), Electronic Ballot Printers (EBP) and Internet voting (I-voting) are the various technologies available for e-voting, and they briefly explained as follows.

- *Direct Recording Electronic (DRE) systems* use a keyboard, touch-screen, pen to allow a voter to record vote electronically. They are used in polling kiosks. Different countries have implemented a paper record called Voter-Verified Paper Audit Trail (VVPAT), which is produced by DRE shows evidence of votes cast.
- E-voting machines having an optical scan that examine paper ballots and uses the OMR technology to determine which box the voter marked. Marked ballots are either scanned by precinct count system in polling kiosk or scanned by central count systems situated at a central location.
- *Electronic Ballot Printers (EBPs)* are similar to DREs, in that the voter uses a DRE-type interface for voting choices. Although, it does not store vote data, it prints out a paper receipt containing the voting choices. The voter then takes the receipt and places it into electronic ballot box for automatic counting of the votes.
- *I-Voting* is a system that allows voters to cast their votes from any computer or electronic devices, such as smart phones connected to the Internet. These devices used for i-voting can be placed in a polling kiosk or voters can vote right form their homes. According to [10], typically Internet Voting is divided into two categories: "*internet voting at the polling place* and *remote internet voting*." Internet voting kiosk is identified as e-voting in a controlled environment and this is where ballots are cast from voting kiosk connected to the Internet and placed at a particular location. The latter may involve the use of computers connected to the Internet situated in places not directly controlled by election officials.

E-Voting Scenarios include onsite e-voting with supervised authentication, such as DRE, OMR, EBP and Internet Voting at the polling place (internet voting kiosk), remote computer voting based on password authentication and remote mobile telephone voting based on password authentication.

The diagram in Figure 3 below identifies the distinction between Onsite E-voting and Remote E-voting.

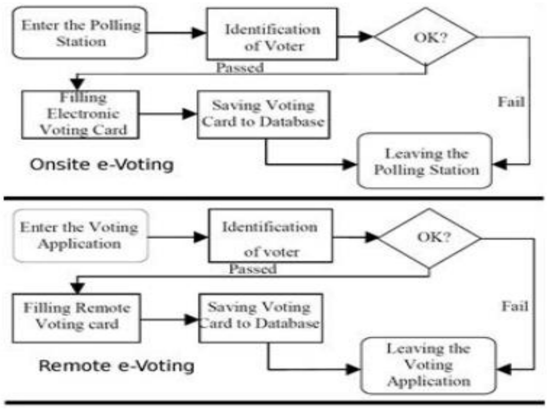
Enter the Polling Station
Identification of Voter
OK?
Passed
Fail
Filling Electronic Voting Card
Saving Voting Card to Database
Leaving the Polling Station
Onsite e-Voting
Enter the Voting Application
Identification of voter
OK?
Passed
Fail
Filling Remote Voting card
Saving Voting Card to Database
Leaving the Voting Application
Remote e-Voting

Figure 3: Onsite E-voting versus Remote E-voting
Source: (Abdulla and Samani, 2013).

Figure 3 illustrates the difference between onsite e-voting from remote e-voting. In onsite e-voting, a voter is identified by entering an access key electronically before filling out the provided ballot. The casting of votes is done inside a polling station controlled by electoral officials. In remote e-voting, voters can cast their ballots using voting credentials and electronic device connected to the Internet. The casting of votes is done any place outside a polling station.

2.3 Security Vulnerability in e-voting

In May 2015, David Jefferson examined the possibility of Internet voting in a paper called 'Intractable Security Risks of Internet voting.' The professor explained that DoS attacks launched from any part of the world on e-voting systems can be carried out by teenage pranksters or a government, and these attacks can compromise the integrity of votes.

According to [10], providing security to systems imposes three mandatory characteristics; confidentiality, reliability and availability. An e-voting system's server is available when there is no delay while voters are accessing the voting website during the voting process.

2.4 Categories of DDoS Attacks Affecting E-voting System

There exist numerous variant forms of threats to e-voting systems. These threats explained below can breach the security of e-voting systems making them unreliable during election process.

Volumetric Attacks: The volumetric flooding-based DDoS attack is a specific type of DDoS. It acts by increasing the number of requests or packet size. Increasing the number of requests aims at exhausting server processing, whereas increasing the packet size has the goal of overloading network resources, such as bandwidth. In general, attackers increase the number of requests and packet size simultaneously. Given its simplicity, this type of DDoS attack is becoming increasingly more significant [11]. Examples include UDP Floods and Ping Floods.

Protocol Attacks: These attacks exploit weaknesses in the TCP three-way handshake connection. They focuse on exploiting server resources. The victim of a protocol attack cannot accept legitimate traffic [12]. Example of a protocol attack is the TCP SYN flood that establishes a half open connection with the victim's server causing service to shut down. This flood attack is made up of SYN packets originating from spoofed addreseses.

Application Attacks: These attacks focuse on web applications. They exploit vulnerabilities in applications. Botnets that carryout the attack are either IRC-based or Web-base and the latter hides within legitimate HTTP traffic making them difficult to detect. According to [6], "Advanced web developments languages (PHP, ASP, JSP, etc.) through encrypted communication over HTTP or HTTPS protocol are used to configured and control the bots."

Malicious Computer Programs: These computer programs harm computer networks by disrupting their performances. A common example is Trojan malware that often disguises as a legitimate software and can conduct DoS attacks on e-voting servers by sending confidential voters' information on the attacker. Trojan horse represents an immense threat to systems confidentially and integrity of information of e-voting systems [13].

Man–in-the-Middle (MITM) Attack: An attacker that can smuggle information about how a voter voted can compromise every voter's secret ballot [14]. MITM attack is a modern-day version of bugging a computer system.

Physical Attacks: These attacks could come in the form of removal of hard drives of e-voting computers and replacing them with modified malicious data as well as stealing e-voting machines containing voters' information in order to sabotage an election process [13].

2.4 Review of Related Works

Reputable researchers have proposed or developed techniques, such as biometrics, watermarking, crypto-graphy, Steganography and their hybrids using protocols, models and algorithms to promote e-government credibility [15]. A comprehensive survey of existing cryptographic and Steganographic models were carried out and a Stegano-Cryptographic in and multimedia e-voting model was proposed for secure e-voting systems in [16]. The developed model in [16] did not solve the security issue of system availability in e-voting system.

In [17], a remote e-voting prototype using blind signature was proposed. This system was able to address security characteristics, such as privacy, integrity amongst others by using digital signature to protect the privacy of how a voter voted during election. Although, the proposed model met some major security require-ments of e-voting, there is still the need to address the problem of e-voting server being vulnerable to attacks that can cause unavailability of service and resources during the voting process.

Furthermore, the paillier cryptosystem, which is an additive homomorphic cryptosystem, can be used to calculate the total votes while protecting how a voter voted [18], and this scheme has been proposed and implemented on cloud computing to provide security for e-voting system [19]. The main objectives of cryptographic techniques and protocols are authentication, non-repudiation and integrity [20]. E-voting systems using Internet platform and based on cryptography could be vulnerable to flood attacks.

In [21], the proposed model was designed using six step algorithm and used chaos theory to detect DDoS attacks effectively. The learning process involved the use of a variety of DDoS attacks to compromise a network environment. Supervised and unsupervised methods of artificial neural networks were used to differentiate DDoS attacks from genuine traffic. Lyapunav coefficient was used to get the best result in differentiating the legitimate traffic and DDoS attack. The advantage of the proposed detection technique using artificial neural network resulted in greater than 95% accuracy in DDoS attacks detection. Unfortunately, this research was not implemented in an e-voting system.

According to literatures, recent researchers revealed that various e-voting systems, such as those based on Enhanced Stegano-Cryptographic Model [4], Cryptographic Voting Verifiable Scheme for E-Voting Based on Bit Commitment and Blind Signature [22], and Biometrics Authentication Methods [23] addressed security issues on Integrity and/or confidentiality and not system availability.

Furthermore, various techniques are being developed and some implemented in e-voting systems to mitigate DDoS attacks, which are constantly evolving and becoming bigger and more destructive to systems connected to the Internet. These DDoS defence technologies will have to also evolve to keep up with the attacks in order to ensure that the election process is conducted in a safe environment. This paper intends to address the major problem caused by TCP SYN flood attack, which is unavailability of an e-voting server. This problem in turn leads to voters not being able to cast their ballots and unusually slow network performance. The proposed system will be successful as long as the attack is detected early enough in Internet voting Kiosk System.

2.5 Comparison of some Related Works with Proposed System

According to [24], remote poll station voting scheme needs a secure and private network for connecting Internet kiosk stations. As such, systems connected in networks have similar feature in that they are most at times connected to the Internet. In [21], a DDoS mitigation technique using packet sampling threshold (PST) was developed on a university campus network and OPNET modeler 14.5 was used to simulate the network. The steps in the system develop-ment are shown in the flowchart in Figure 4.

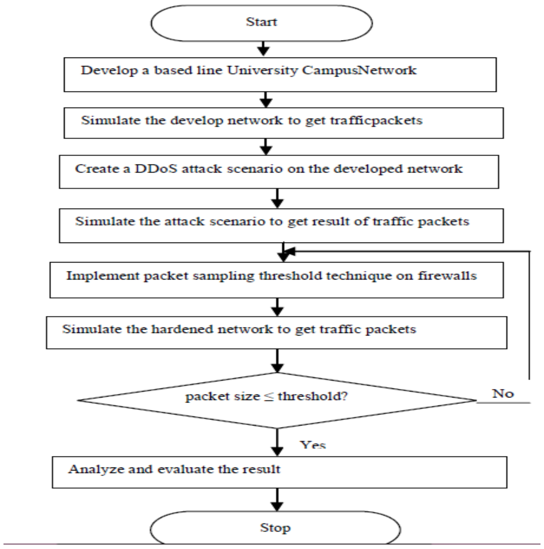
Start
Develop a based line University CampusNetwork
Simulate the develop network to get trafficpackets
Create a DDoS attack scenario on the developed network
Simulate the attack scenario to get result of traffic packets
Implement packet sampling threshold technique on firewalls
Simulate the hardened network to get traffic packets
packet size ≤ threshold?
No
Yes
Analyze and evaluate the result
Stop

Figure 4: DDoS Mitigating Technique on University Campus Network
Source: (Dominic, *et al.*, 2013).

Figure 4 shows that the system can detect DDoS attack and prevents such an attack using a threshold, but the system could be made intelligent, such that it can not only classify all incoming packets as either normal traffic or attack traffic but also learn from the environment.

Machine learning is part of Artificial Intelligence (AI) and its goal is to make computer networks to learn on their own. Artificial Neural Network (ANN), which is a machine learning technique, can be used for network security threat detection. ANN is one of the commonly applied machine learning algorithm and can be applied to systems for monitoring and detecting DDoS attacks.

Internet voting channel is a public channel that provides security for data transactions, storage and process auditing in e-voting. According to [25], in an article published by Forbes.com, there was the mention of Dan Wallace, who is a Professor in the Departments of Computer Science and Electrical and Computer Engineering, expressed concern in Internet voting registration systems as they could be compromised by DDoS attack.

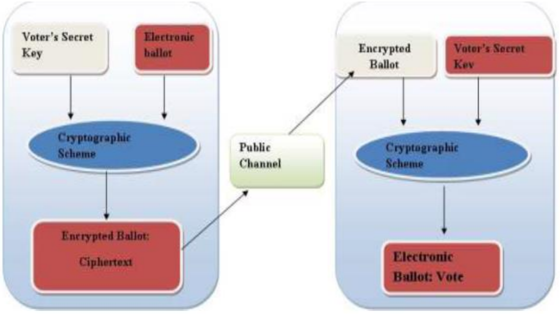

Figure 5: Cryptographic Model to Secure E-voting System
Source: (Olaniyi, *et al.*, 2013).

In Figure 5, a framework for securing e-voting system is shown and the model provides security requirements that include confidentiality and integrity. The use of a public channel in this model puts the e-voting system at risk of being compromised by DDoS attack.

Information security measures try to address the issue of information confidentiality, protecting information integrity or providing availability of data for use by security officials. The confidentiality, integrity availability (AIC) goals are the basis of all security systems [28].

Table 1 provides a meta-analysis of some current researches in e-voting in terms of addressing the security goals.

Table 1: Literature Survey

AIC (Availability, Integrity and Confidentiality) Triad **Adopted Methodology**	**A**	**I**	**C**
Steganocryptograhic Techniques [5, 17]	False	True	True
Blind Signature Scheme [17, 24]	False	True	True
Homomorphic Encryption Scheme [4, 19]	False	True	True
Biometric Authentication Method [16]	False	True	True
DDoS Mitigation Technique [22]	True	False	False

3.0 METHODOLOGY

3.1 Proposed System Architecture

This section defines the various modules that make up the proposed system architecture and the various elements that will be used to accomplish the implementtation and evaluation objectives of the first phase of the proposed model, which is the detection sub-system.

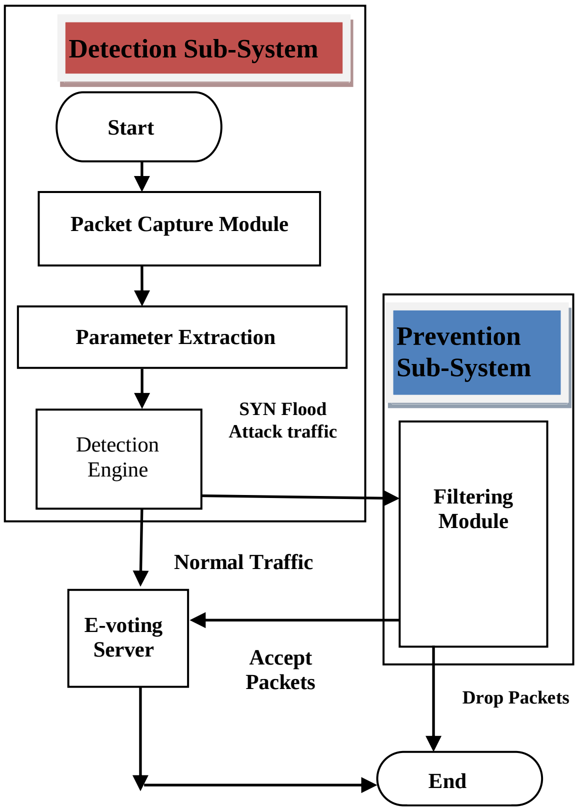

Figure 6: The Proposed Model for Mitigating TCP SYN Flood Attack in an E-voting System

Figure 6 shows an illustration of the various modules that are present in the proposed model and they are explained below.

Capturing Module: This module also called a Packet Sniffer is a software tool that can intercept and log traffic on an Ethernet network. The captured packets are then transferred to the detection module for classification.

Parameter Extraction Module: The proposed detection sub-system makes use of the following packet characteristics to classify TCP SYN flood packets from the legitimate traffic. This module calculates these characteristics of captured packets shown with their respective formulas below.

(i) Total Packet Count (TPC): This is the total number of incoming packets. During an attack, the attacker sends a large number of TCP SYN packets to the e-voting server.

$$\text{TPC} = \sum_{x=1}^{n} P_x \qquad (1)$$

where P_x: packet with x = 1 to n

(ii) Average Packet Size (APS): During TCP SYN flood, the value of APS increases.

$$\text{APS} = {}^{1}\!/_{n} \sum_{x=1}^{n} PS_x \qquad (2)$$

where PS_x: Packet Size with x = 1 to n

(iii) Packet Rate: This is the rate of incoming packets per second and it is calculated as:

$$(PR/s) = P_i\,/PT_e - PT_s \qquad (3)$$

PT_e: sent packet termination by unit of time

PT_s: start sent packet by unit of time

(iv) Time-interval Variance: Attack packets are sent to e-voting server repeatedly within a small time slot and the result is closer to zero. According to [26], timing variance is calculated by performing mean and then squaring it.

$$\bar{t} = \frac{\sum t_x}{x} \qquad \text{where: x = 1 to n (4)}$$

$$t_k^2 = \frac{\sum (t_x - \bar{t})^2}{x} \qquad \text{where: k = 1 to n (5)}$$

$$t_k = \sqrt{\ } \frac{\sum (t_x - \bar{t})^2}{x} \qquad (6)$$

(v) Packet-size Variance: Attack packet sizes are large and the same compared to legitimate packets, which are of different sizes. Variance will be closer to zero. According to [26], packet-size variance can be calculated using three equations shown below.

$$\bar{p} = \frac{\sum p_x}{x} \qquad \text{where: x = 1 to n} \quad (7)$$

$$p_k^2 = \frac{\sum (p_x - \bar{p})^2}{x} \qquad \text{where: k = 1 to n (8)}$$

$$p_k = \sqrt{\ } \frac{\sum (p_x - \bar{p})^2}{x} \qquad (9)$$

3.2 The Proposed Packet Classification Algorithm (Back-Propagation Algorithm)

(1) Detection Engine Module: This module is used for error detection and correction in Neural Networks (NN). The basic idea of back propagation is to guess what the hidden units should look like based on what the inputs look like and what the outputs should like.

It is an algorithm that receives data points one at a time where we get our observation ***x*** with ***d*** different attributes. Each edge has a weight on it and the weights are used to compute the values of each of the hidden units. As inputs and weights are fixed, we can compute the values of the hidden units (running the Sigmoid).

In neural network, the network performance can be computed using the Mean Square Error (MSE). If there are *n* projections of feature *f'* and perceived vectors of *f* values that correspond to the input function which produced the projections, then the MSE of the projector is calculated as:

$$\mathrm{MSE} = {}^{1}\!/_{n} \sum_{x=1}^{n} \overline{(f_x} - f_x) \qquad (10)$$

Sigmoid Activation Function is a function that takes some number and squashes it into a range between 0 and 1. It is a nonlinear activation function that makes it easy for a model to adapt with variety of data and to differentiate between the outputs. The Sigmoid Function curve looks like a S-shape. This can be given by:

$$\mathrm{f}(n) = \frac{1+e^{-n}}{1} \qquad (11)$$

In Figure 5 below, the bias goes to all neurons and the training pair comprises of the input and output.

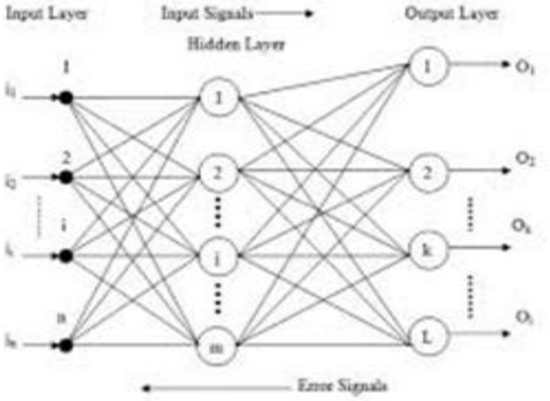

Figure 7: Schematic Diagram of Detection Engine using Back-Propagation Artificial Neural Network (BPANN)

Source: (BrainKart.com, 2018)

In Back-Propagation Neural Network the following procedures are applied.

1. Set of random weights to input data is applied and output is calculated using the Feed Forward approach.
2. The weights between the hidden layer and output layer are adjusted so that the margin of errors is reduced.
3. Calculate the incremental change to these weights.
4. The necessary change in the output sum is calculated by taking the derivative of the active-tion function and applying it to the output sum.
5. The process is repeated from Steps 1- 4, until the final output is equal to the expected output.

In the proposed study, the IP addresses, Protocol (TCP) and Port Number will be used as input neurons. Three hidden neurons will be selected and two output neurons would have actions, such as ACCEPT and DROP. The expected output will indicate 0 for accepting packets and 1 for SYN Flood attack packets.

(4) Filtering Module: The Filtering Module would be the prevention sub-system, which lists the attack packets based on IP addresses and protocol in order to either accept or reject these packets using Evenly-Based Dynamic Algorithm (EBDA).

4.0 RESULT

Using the kdd cup dataset split to 66% for training and 34% for testing, the Back Propagation Artificial Neural Network algorithm indicated a higher accuracy of 98.65% in detecting flood attacks.

5.0 CONCLUSION

The findings of this technique will provide the election process with a secure e-voting system that voters can rely on and have trust. The developed technique will successfully detect and prevent TCP SYN flood attack in Internet voting kiosk system. Furthermore, this technique will expectedly heighten the awareness of voting officials and voters to equip a counterattack to possible DDoS threats. In future researches, this research can provide baseline information on the recent status of efficient techniques against DDoS attacks. At this stage, the proposed technique is open for further review and criticism.

REFERENCES

[1] H. Patil, B. TarteBabita, S. Wadekar, S. Zurunge & R. Phursule. A Secure E-Voting System Using Face Recognition and Dactylogram. International Engineering Research Journal (IERJ) Volume 2, Issue 2, Page 758-762, 2016, ISSN 2395-1621.

[2] R. Banerjee. Internet Voting System: How Secure is your Vote? Authored by TCS Enterprise Security and Risk Management, 2017.

[3] S. Shinde, S. Shukla & D. Chitre. Secure E-voting using Homomorphic Technology. International Journal of Emerging Technology and Advanced Engineering. www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 8, August 2013).

[4] O. M. Olaniyi, O. T. Arulogun, E. O. Omidiora & O. O. Okediran. Enhanced Stegano-Cryptographic Model for Secure Electronic Voting. *Journal of Information Engineering and Applications* ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol.5, No.4, 2015. Available Online at www.iiste.org.

[5] G. Gallegos-Garcia & H. Tapia-ecillas. Electronic Voting Protocol using Identity-Based Cryp-

tography. The Scientific World Journal, Volume 2015, Article ID 741031, 6 pages. http://dx.doi.org/10.1155/2015/741031.

[6] K. M. Prasad, A. R. Reddy & K. V. Rao. DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms - A Survey. *Global Journal of Computer Science and Technology: E Network, Web & Security*, Volume 14 , Issue 7, Version 1.0, 2014, Double Blind Peer Reviewed International Research, Global Journals Inc. (USA),Online ISSN: 0975-4172 & Print ISSN: 0975-4350.

[7] C. Chen, Y. Chen, J. Jan & C. Chen. A Secure Anonymous E-Voting System based on Discrete Logarithm Problem. *International Journal in Applied Mathematics & Information Sciences* 8, No. 5, 2571-2578 (2014). http://dx.doi.org/10.12785/amis/080556.

[8] M. Aamir & M. Zaidi. A Survey on DDoS Attack and Defense Strategies: From Traditional Schemes to Current Techniques. Interdisciplinary Information Sciences Vol. 19, No. 2 (2013) 173–200**,** Graduate School of Information Sciences, Tohoku University**,** ISSN 1340-9050 print/1347-6157 online**.** DOI 10.4036/iis.2013.173

[9] International Institute for Democracy and Electoral Assistance (International IDEA). Introducing Electronic Voting: Essential Considerations, 2011. ISBN 978-91-86565-21-3.

[10] M. Musial-Karg. implementation of Electronic Voting and the Matter of Security. DOI:10.1515/ curie-2015-0022.

[11] Y. S. Abdulsalam, O. M. Olaniyi, A. Ahmed & O. M. Olaniyan. Developing a Secure Distributed ElectronicHealth System Using Information Hiding Techniques. Proceedings of the iSTEAMS Multidisciplinary Research Nexus Conference May, 2017, Caleb University, Lagos, Nigeria.

[12] S. Mansfield-Devine. The Growth of Evolution of DDoS. *Network Security Journal*, Vol. 2015, Issue 10, October, 2015, pp. 13-20.

[13] D. Zacharopoulos. Electronic Voting. Analysis of the Status & Functionality and Components of Electronic Voting. Development of Methods on how creating trust relationship between E-voting System & Voter/Client. University of Piraeus, Department of Digital Systems Security in Digital Systems Thesis, 2015, Athens.

[14] D. Springall, T. Finkenauer, Z. Durumeric, I. Kitcat, H. Hursti, M. MacAlpine & A. I. Halderman. Security Analysis of the Estonian Internet Voting System. CCS'14, November 3-7, Scottsdale, Arizona, USA. ACM 978-1-4503-2957-6/14/11. http://dx.doi.org/10.1145/2660267.2660315. https://doi.org/10.1016/S1353-4858(15)30092-1.

[15] O. M. Olaniyi, A. F. Taliha, A. Aliyu & J. Olugbenga. Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking Approach. *International Journal Information Engineering and Electronic Business*, 2016, 5, 9-17. Published Online September 2016 in MECS (http://www.mecs-press.org/). DOI: 10.5815/ijieeb.2016.05.02.

[16] O. M. Olaniyi, O. T. Arulogun, E. O. Omidiora & O. O. Okediran. A Survey of Cryptographic and Stegano-Cryptographic Models for Secure Electronic Voting System. *Covenant Journal of Informatics and Communication Technology* (CJICT) Vol. 1, No. 2, December, 2013.

[17] M. R. Kouta, F. E.Elfakharany & B. W. Mohamed. Proposed Secured E-Voting Model based on Blind Signature. *Global Journal of Computer Science and Technology Network Web & Security*, Volume 13, Issue 13, Version 1. 0, 2013. Online ISSN: 0975-4172 & Print ISSN: 0975-4350.

[18] N. Cuong. Secure Voting System using Paillier Homomorphic Encryption. Graduate Project submitted to the Faculty of the Department of Computing Sciences, Texas A&M University – Corpus Cristi, Texas, 2014.

[19] R. Jain, S. Madan, B. Garg, Y. Kapila & A. Gupta. E-Voting System using Homomorphic Encryption in a Cloud Based Environment. International Journal of Security and its Applications, Vol. 11, No. 5(2017), pp. 59-68.

[20] S. Roy, P. S. Ahuja, D. P. Harish & R. S. Talluri. Energy Optimization in Cryptographic Protocols for the Cloud. DOI: 10.4018/978-1-5225-4044-1.ch002. IGI Global, 2018.

[21] B. Dominic, H. Inyiama, A. Ahmed, M. Abdullahi & O. M. Olaniyi. A Packet Sampling Thersholding Technique for Mitigating Distributed Denial of Service (DDoS) Attacks in a University Campus Network. Internation Engineering Conference Paper, 2015. Available Online at https://www.reserachgate.net/publication/283120300.

[22] A. Aljumah & T. Ahamad. A Novel Approach for Detecting DDoS using Artificial Neural Networks. *International Journal of Computer Scinec and Network Security*, Vol. 16, No. 12, December 2016.

[23] A. Darwish & M. El-Gendy. A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature. *International Journal of Swarm Intelligence and Evolutionary Computation*, 2017. DOI: 10.4172/2090-4908.1000158.

[24] G. Vinodu & M. P. Sebastian. Remote Internet Voting: Developing a Secure and Efficient Frontend. CSI Transactions on ICT, September 2013, Volume 1, Issue 3, pp 231-241.

[25] A. Weinreich. The Future of Online Voting: Hacking Elections and the First U.S Online Voting Trial. Available Online at https://www.google.com.ng/amp/s/www.forbes.com/sites/andrewwienreich/2017/06/14/the-future--of-online-voting-hacking-elections-and-the-first-u-s-online-voting-trial/amp/. Retrieved on 13th July, 2018.

[26] T. Zin, J. Pan & M. Yokota. Genetic and Evolutionary Computing. Proceedings of the Ninth International Conference and Genetic and Evolutionary Computing, August 26-28, 2015, Yangon Myanmar – Volume 1. DOI 10.1007/978-3-319-23204-1.

[27] A. Abdalla & T. Samani. The Technical Feasibility and Security of E-Voting. *The Inter-*

national Arab Journal of Information Technology, Vol. 10, No. 4, July 2013.

[28] J. Breithaupt & S. M. Merkow. Information Security pricniples of Success. 2018 Pearson Education, Pearson IT Certification. www.pearsonitcertification.com/article/article.asp?p=2218577&seqNum=3.

[29] 2017-2018 BrainKart, LLC. Back Propagation Neural Network. www.brainkart.com/article/Back-propagation-neural-network_8923/.

BIOGRAPHY OF AUTHORS

Almustapha Aphia Jiro obtained a Bachelor of Technology (B.Tech.) Degree in Computer Science from Abubakar Tafawa Balewa University, Bauchi, Bauchi State, Nigeria in 2007. She is currently a student pursuing a Master of Technology Degree in Computer Science at the School of Information and Communications Technology, Federal University of Technology, Minna, Niger State, Nigeria. Her main research interests include Computer Security and Development of Intelligent Systems.

Olayemi Mikail Olaniyi is a Senior Lecturer in the Department of Computer Engineering at Federal University of Technology, Minna, Niger State, Nigeria. He obtained his B.Tech. and M.Sc. in Computer Engineering and Electronic and Computer Engineering respectively. He had his Ph.D. in Computer Security from Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria. He has published in reputable journals and learned conferences. His areas of research include Computer Security, Intelligent/Embedded Systems design and Applied Medical Informatics.

Engr. Abdullahi Ibrahim Mohammed obtained a Bachelors of Engineering (B.Eng.) Degree in Electrical and Computer Engineering from the Federal University of Technology, Minna in 2010. He also hold a Masters of Technology (M.Tech.) Degree in Computer Science (Artificial Intelligence and Image Processing) from Ladoke Akintola University of Technology, Ogbomoso, Oyo State, obtained in 2015. He is currently a doctoral student at the School of Electrical Engineering and Technology, Federal University of Technology, Minna, Niger State, Nigeria. His main research interest includes: Computation Intelligence (Development and Analysis of Nature Inspired Algorithms and its application in solving Optimization Problems), Development of Intelligent and Smart Embedded Systems, Application of AI to Computer Security and Digital Image Processing.

Yunusa Simpa Abdulsalam is a passionate researcher in the field of Science and Technology. He is an academic researcher ready to explore the shores of nature to make available resources to please man. He does research in Control Systems Engineering, Communication Engineering and Computer Engineering. Current projects are ‘Tele-medicine’, Cloud and Internet-of-Things Technology and System’ and ‘Wireless Sensor Networks’