THE JOURNAL OF COMPUTER SCIENCE AND ITS APPLICATION
AN INTERNATIONAL JOURNAL OF THE NIGERIA COMPUTER SOCIETY (NCS)
Vol. 19 No.1, June, 2012

nigeria computer society
www.ncs.org.ng.

PERCEPTION OF SECURITY INDICATORS IN ONLINE SITES

[1]Emmanuel A. Onibere and [2]Annie. O. Egwali
1/2Department of Computer Science, University of Benin, P. O. Box 1154, Benin City. Nigeria.
***Corresponding author**:* egwali.annie@yahoo.com

ABSTRACT

Internet banking provides alternatives for faster delivery of banking services to a wider range of customers. These services have attracted the attention of legitimate and illegitimate online banking practices. Customers are liable to criminal activities, fraud, thefts and other similar threats. Criminals focus on stealing user's online banking credentials because the username and password combination is relatively easy to acquire and utilize to access Internet banking accounts and commit financial fraud. To alert users, many banking sites are now including Security Indicators (SI) to their sites. This paper describes a user study conducted using questionnaires to investigate user's perception of factors influencing the effective implementation of existing SI objectives and evaluate the effectiveness of SI in banking web browsers using the Communication-Human Information Processing Model (C-HIP). Thirteen (13) banks in Nigeria were randomly selected for the study. Data analysis revealed that SI are not very effective at alerting and shielding users from revealing sensitive information to spoofed sites because 27(19.7%) of the 137 participants never even noticed that a warning appeared. These outcomes may help the management of banks develop effective security strategies for the future of electronic banking in Nigeria.

1.0 INTRODUCTION

The Internet is the medium for an escalating amount of business and other sensitive transactions, including online banking and e-commerce. Secured Socket Layer and Transport Layer Security (SSL/TLS) is often used to protect traffic coming from and going to web applications. While this type of protection achieves the goal of data protection, unfortunately current browsers, still allow web spoofing, i.e. customers are tricked into revealing personal or financial information through a fraudulent website or e-mail message. The goal of attackers is often to obtain user-ID's, passwords and other personal and financial information, and abuse it e.g. for identity theft, larceny, or fraud. As customers increasingly rely on the Internet for business, personal finance, and investment, Internet fraud becomes a greater threat. Internet fraud takes many forms, from phony items offered for sale to scams that promise customers great riches if assistance can be given to foreign financial transaction through the customer's own bank account. A common online phishing scam starts with an e-mail message that looks like an official notice from a trusted source, such as a bank, credit card company, or reputable online merchant. In the e-mail message, recipients are directed to a fraudulent website where they are asked to provide personal information, such as an account number or password.

A study by [3], confirmed that about eight out of ten respondents have visited a spoofed web site and over 15% provided personal data to a spoofed site. A user study was conducted by [4] and it was discovered that about two million users revealed sensitive information to spoofed web sites, and estimate a loss of about $1.2 billion to credit card issuers and U.S. banks in the year 2003. As asserted by [1], indirect losses are much higher, including customer service expenses, account replacement costs, and higher expenses due to decreased use of online services in the face of widespread fear about the security of online financial transactions. Spoofing attacks also cause substantial hardship for victimized consumers, due to the difficulty of repairing credit damaged by fraudulent activity. Both the frequency of spoofing attacks and their sophistication is increasing dramatically.

These demerits in Internet banking practices are really having a great impact in the adoption of Internet banking in Nigeria. As posited by [9], Internet banking is slowly being embraced by customers because Internet practice in Nigeria

has been abused by cyber attackers who use real and deceptive banking websites to scoop user's sensitive information and funds. If a deceptive spoofed site can be revealed as fraudulent to the intended customer, the attack can be thwarted. Thus customers are commonly advised by online security tips to pay attention to these indicators whenever they access a website. Unfortunately, online Security Indicators (SI) have historically failed users because users do not understand or believe them.

The prevalence of spoofed sites has prompted the design of many new online SI. Since site spoofing is a semantic attack that relies on confusing customers, it is difficult to automatically detect these attacks with complete accuracy. Presently, there are two types of SI tools used to alert or block users to probable spoof sites: Passive and Active SI. Passive SI indicates an impending danger by providing certain textual information, changing colors, or through other means without interrupting the user's online activity. Active warnings force the user to take notice of the warnings by interrupting the user's main online activity. However, research has shown that passive indicators are failing users because users often fail to notice them or do not trust them [18]. In this study both passive and active SI tools are referred to as SI.

Customers rarely pay attention to SI displayed in the peripheral area of the browser compared to the large main window that displays the web content at the right times to notice an attack. If SI makes mistakes and identifies legitimate sites as spoofed sites, customers may learn to distrust the indicator. Then, when the indicator correctly identifies a spoofed site, the customer may not believe it. The need for indepth knowledge of existing SI practices cannot be overemphasized. These warnings serve as the last defense against users revealing sensitive information to attackers particularly during authentication into Internet banking sites. This paper describes a user study performed to investigate users perception of factors influencing the effective implementation of existing SI objectives and to evaluate the effectiveness of SI in banking web browsers using the Communication-Human Information Processing Model (C-HIP), a model proposed in the field of warning sciences by researchers [17].

2.0 REVIEW OF LITERATURE

An emergent number of user studies are investigating why phishing attacks are so effective against computer users. [12] analyzed concerns about the potential risks and harms of web usage on consumers and evaluated the web practices of 72 participants. It was discovered that consumers are really at risk. Large empirical studies were conducted by [11] to reveal how consumers evaluate websites; guidelines were proposed that encourages trustworthiness on websites. A user study was carried by [18] to examine the effect of SI in preventing phishing attacks. In the study, users spend 34% of their time providing sensitive information to spoofed site even when toolbars were used to give notice of security concerns. In an interview on web security, [12] showed four screen shots of a browser connecting to a website and asked participants to state if the connection was secure or not secure and to affirm the motivating factor for their appraisal. It was discovered that about 72 participants cannot tell if a connection is secure.

An eye-tracker was used by [16] to study user behavior with respect to browser SI and discovered that although subjects glanced at the lock icon in the status bar, however, they hardly ever clicked on it. In a web survey, [15] studied how well users can distinguish phishing emails from legitimate ones. Screenshots of ten emails were shown to subjects and about 28% of the time, phishing emails was incorrectly identified as legitimate by the users. A pragmatic research in online trust by [5] included a study of how manipulating merchant's feedback ratings can influence consumer trust in a merchant's site.

A study by [13] discovered that phishing attacks from trusted sites are more successful at compromising user's sensitive information than sites not trusted. In the study, data were collected from the internet and used to create a social network map of university students. Faked phishing email from the map that appeared to be from friend's spoofed address succeeded in deceiving 72% of the respondents while only 16% were deceived by spoofed sited from unknown addresses. A study by [13] established the fact that social context makes phishing attacks very far more successful. Phishing emails were sent to phishing sites that asked for the subject's university username and password, and validated them. About 72% subject's usernames and passwords were compromised.

Concerns for customers' internet banking practices motivated some organizations to mount phishing attacks against their own members, with the goal of teaching them to protect themselves. A report by [6] on how a US Military Academy at West Point revealed that more than 80% of its cadets succumbed to a phishing attack by a fictional colonel. Similarly, the State of New York mounted two attacks on its 10,000 employees; 15%

were spoofed by the first attack, but only 8% by the second, which came three months later.

A study was conducted by [2] to evaluate the motivational strength of software warnings. Participants were shown a series of dialog boxes with differing text and icons and were instructed to estimate the severity of the warnings using a 10-point Likert scale. The researchers also examined the extent to which individuals will continue to pay attention to a warning after seeing it multiple times. Participant's choice in both icon and warning words greatly affected how each severity was ranked. It was discovered that users dismissed warnings without reading them after viewing them multiple times. This behavior continued even when using a similar but different warning in a different situation. In a survey on the state of Internet banking in New Zealand [7], it was confirmed that security and complication of Internet banking are some of the factors limiting the full acceptance of Internet banking.

3.0 RESEARCH METHODOLOGY

The following section gives a details overview of the research methodology employed in this study.

3.1 Research Design

The intention of the study is two-fold: to analyze user's perception of factors influencing the effective implementation of existing SI objectives and to evaluate the effectiveness of SI in these banking web browsers. Thirteen banks in Nigeria were surveyed, representing 52% of the consolidated banks in Nigeria. The selection criteria were based on proximity of these banks within the southern part of the country and the availability of their online services. The study was conducted in the University of Benin, situated very close to where eleven branches of the banks are located. Users were informed to visit the online banking sites proposed for the study and attempt to perform normal online transaction. Users then filled in a post-task questionnaire on their online experiences.

The study commences with the use of a written survey that was designed to analyze user perception of SI and the effectiveness of SI. Participants were instructed to complete the questionnaires during class hours. The questionnaires are divided into three sections. The first section is for the profile of participants, the second section is to analyze users' perception of factors influencing the effective implementation of existing SI objectives while the third is to examine the effectiveness of SI in these banking web browsers using the Communication-Human Information Processing Model (C-HIP) model.

The first section includes participant's sex, age and banking practices (bank category, banking practice and bank location). The second section analyzes users' perception of factors influencing the effective implementation of existing SI objectives. Participants are to express themselves using seven factors: Time of popups, Indicator-type (passive/active), Choice of icon, Message contents, Display size, Background colour and Display position. The third section verified the effectiveness of SI included in online banking web browsers using a model similar to that proposed by Wogalter in 2006.

For the survey, questionnaires designed consisted of a 5 Likert scale point, 5 for strongly agree (SA), 4 for agree (A), 3 for indifferent (I), 2 for disagree (D) and 1 for strongly disagree (SA). It was initially discovered that the customers' were not clear about the terminologies used in the questionnaire but this matter was solved through detailed explanation and by one to one discussion. The instructions requested respondents to tick the response, which best describe their affirmation. Respondents were assured of the confidentiality of their responses.

3.2 Response Rate

300 level students of Computer Science Department with basic web experiences and who were highly connected with internet services offered by banks were requested to complete the survey forms, which included series of questions to facilitate the categorizing of banking sites SI as being effective or ineffective. The questionnaires were distributed and completed during class hours. Out of the 200 questionnaires, a total of 137 questionnaires were completely filled and used for the purpose of analysis.

3.3 Data Analysis Method

Studies on the sample banks were conducted between February and March, 2008. For data analysis on users perception of factors influencing the effective implementation of existing SI objectives, tests for significant interactions amongst variables were performed using the classical chi-squared. The study also tested reliability of the instruments in order to produce a robust and valid result. Finally, the study employed the Communication-Human Information Processing Model (C-HIP) similar to that proposed by Wogalter in 2006 to determine the effectiveness of SI in thirteen Internet banking web browsers.

3.4 Research Model

The effectiveness of SI in present online banking web browsers, particularly during customer's authentication phase, was analyzed using a model similar to the Communication-Human Information Processing Model (C-HIP) proposed by [17]. The model assists in ascertaining if SIs are effective or not. The model involves various phases for analyzing SI effectiveness. The various phases of the Communication-Human Information Processing Model (C-HIP) includes source, channel, delivery, attention switch, attention maintenance, comprehension memory, attitude and beliefs, motivation, behavior and environment stimuli. To analyze SI effectiveness as it relates to users internet banking practices, the model will be implemented from the *source* phase to the *environment stimuli* phase as these phases affect the users directly while authenticating into internet banking sites. The different phases as shown in figure 1 are:

Source: The source of the warning.
Channel: The channel through which the source warning appears.
Delivery: The delivering nature of the warning.
Attention Switch: The immediate attention capturing capacity of the SI.
Attention Maintenance: The degree at which Users attention capacity is maintained.
Comprehension Memory: Users knowledge of the purpose of the indicators and corresponding actions to take.
Attitude /Beliefs: Users trust of the intention of the indicators
Motivation: The incentive to take the recommended actions.
Behavior: The actual performance of the recommended actions.
Environment stimuli: The interaction of SI with other indicators and other stimuli.

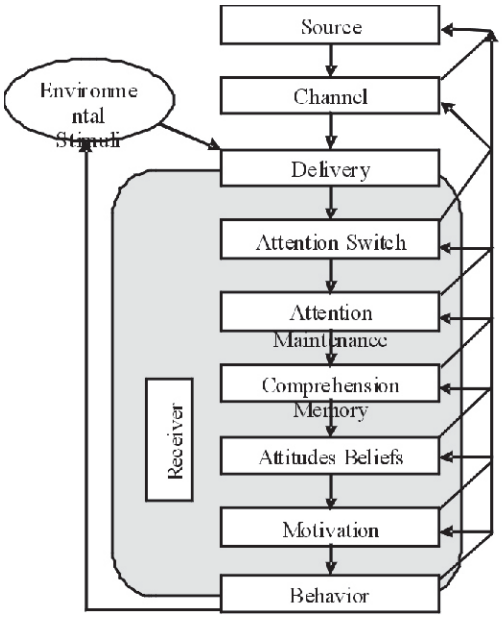


Figure 1. Communication-Human Information Processing Model (C-HIP) [17].

4.0 RESULTS AND DISCUSSIONS

a. Correspondents Profile

Table 1 shows the profile of respondents. The respondents were made up of 79 males (57.7%) and 58 females (42.3%). The age ranged was between 18 20 years (38.7%), 21 25 years (51.8) and 26 35 years (9.5%). As their primary banking category, 1 respondent (0.7%) used First City Monument Bank, 9 (6.6%) used Zenith, 12 (8.8%) used Unity, 3 (2.2%) used Union, 23 (16.8%) used United Bank of Africa, 16 (11.7%) used Skye, 7 (5.1%) used Oceanic, 27 (19.7%) used Intercontinental, 4 (2.9%) used Guaranty Trust, 2 (1.5%) used Afribank, 11 (8.0%) used Access, 5 (3.65) reported using diamond, and 17 (12.4%) used First Bank. In performing banking transaction, 82 participants (59.8%) carried out transaction offline only while 55 (40.2%) carried out both online and offline transactions. As their primary banking location, 41 correspondents (29.9%) carried out banking transaction outside the campus, 27 (19.7%) bank only in the

campus, and 69 (50.5%) carried out banking transactions either on-campus or off-campus.

Table 1: Profile of Respondents

		N = 137	%
Sex	Male	79	57.7
	Female	58	42.3
Age Range	18-20 years	53	38.7
	21-25 years	71	51.8
	26 – 35 years	13	9.5
Bank Category	First City Monument Bank	1	0.7
	Zenith Bank Plc.	9	6.6
	Unity Bank	12	8.8
	Union Bank	3	2.2
	United Bank of Africa	23	16.8
	Skye Bank	16	11.7
	Oceanic Bank	7	5.1
	Intercontinental Bank	27	19.7
	Guaranty Trust Bank	4	2.9
	Afribank	2	1.5
	Access Bank	11	8.0
	Diamond Bank	5	3.6
	First Bank Plc	17	12.4
Banking Practice	Offline only	82	59.8
	Online and Offline	55	40.2
Bank Location	Off Campus only	41	29.9
	On Campus only	27	19.7
	Off Campus and On Campus	69	50.4

The second section analyzes the effectiveness of SI at alerting users by endeavoring to find out the SI perceptive level of customers, participants are to express themselves using seven factors: Time of popups, Indicator-type (passive/active), Choice of icon, Message contents, Display size, Background colour and Display position. The third section verified the effectiveness of SI included in online banking web browsers using a model similar to that proposed by Wogalter in 2006.

b. Users Perception of SI factors

From Table 2, the following can be deduced:

i. Respondents agreed to the fact that the time SI are popped up or display to alert web users of the

Insecurity in using a site has much effect on the subsequent behavior of the user. It contributes to either being alert to obey the warning instructions on time or ignoring the warning altogether.

ii. Respondents consented to the fact that the choice of icon display has a lot of impact on the user subsequent behaviour to reduce vulnerability level.

iii. The least factor with any effect on users is the background colour used for displaying the SI.

Table 2: Users perception of factors influencing the effective implementation of SI objectives.

Table 2: Users perception of factors influencing the effective implementation of SI objectives.

S/N	Statements	SA	A	I	D	SD
1	Time of popups	27	24	16	2	9
2	Indicator-type (passive/active)	11	19	23	5	25
3	Choice of icon	21	21	16	7	21
4	Message Contents	16	18	22	11	12
5	Display size	11	27	11	6	17
6	Background colour	10	21	18	13	33
7	Display Position	13	7	20	9	6
	TOTAL	**109**	**137**	**127**	**53**	**123**
	MEAN	**15.6**	**19.6**	**18.1**	**7.6**	**17.6**

From the Chi square analysis of the resultant data in table 2, the derived result (table 3) is significant beyond the 0.001 level ($p < 0.001$). This gives a 99 percent confidence that the differences between the observed and expected patterns of frequencies does not result from mere random variability.

Table 3: Chi-Square Analysis

X	O	E	(O – E)	$(O-E)^2$	$X^2 = \frac{(O-E)^2}{E}$
SA	109	109.8	-0.8	0.64	0.006
A	137	109.8	27.2	739.84	6.74
I	127	109.8	17.2	295.84	2.69
D	53	109.8	-56.8	3226.24	29.38
SD	123	109.8	13.2	174.24	1.59
TOTAL	**549**	**549**			**40.406**

Table 4: Results of the effectiveness of Internet Banking SI based on the (C-HIP) model

C-HIP Phases	Statements	N = 137	
Attention Switch	Never noticed the appearance of a passive SI	27	19.7%
	Noticed the appearance of a passive SI	110	80.3%
Attention Maintenance	Familiar with the different types of SI displayed	43	31.4%
	Read entire warning message	75	54.8%
	Aware of the consequences of not taking note of such warnings.	43	31.4%
	Saw warning and left site	13	9.5%
Warning Comprehension	Did not understand the full meaning of the SI.	37	27%
	Comprehended that the sites were prone using spoofed sites to steal sensitive information.	11	8%
	Saw the SI revealed that they thought they were expected to log out of the banking sites immediately and discontinue the entering of sensitive information.	12	8.8%
	Saw warnings and believed the site can be spoofed.	7	5.1%
Attitudes and Beliefs	Saw warnings but ignored them	19	13.9%
	Confused some of the warnings that appear alike.	23	16.8%
Motivation	Motivated to log out of the banking sites	19	13.9%
	Motivated to pay attention because the warnings made them believe they were about to be attacked.	21	15.3%
	Submitted information because they were unaware of the risks, used to ignoring similarly designed warnings or because they did not understand the choices that the warnings presented.	25	18.3%
Environmental Stimuli	Ignored SI and entered sensitive information because of trusting the site	18	13.1%

c. ***Effectiveness of Internet Banking SI***

Table 4 shows the results obtained from analyzing the effectiveness of Internet Banking SI (warnings) using **the** (C-HIP) model.

Attention Switch

At the "attention switch" phase, a warning will not be noticed on time if it is incapable of capturing user's attention from the user's present online activity. For sites with passive warnings, 27 of the 137 (19.7%) participants never noticed that a warning appeared because their focus was either on the keyboard and they were ignorant of the fact that such messages exist and will be popup at that point in time. This finding is similar to those of earlier studies made by [19]. The timing for the appearance of the warning messages in 7 sites was about 8 seconds, thus a user who is ignorant of such warning messages can in the course of typing dismiss the warning. In the case of active warnings, 9 of the sites captured user's attention by interrupting user with a warning message; users are then left with the choice of continuing or exiting the current banking site. This type of warning succeeded because user's tasks were interrupted.

Attention Maintenance

For SI to be effective, then it must not only be able to capture user's attention but also be able to sustain the attention of users long enough for them to understand the significance of the SI.

43(31.4%) participants claimed to be familiar with the different types of SI displayed in the different banking sites because they have seen them before and know what they denote. These same participants also claimed to have read the warnings because they were aware of the consequences of not taking note of such warnings. But it is likely that some users will not bother to read the full contents of warning messages even though some of these warnings are to some extent different and more severe. Thus, it is very likely that if a message is recognized, users are less prone to reading such messages. 75(54.8%) participants claimed to have read the entire warning message that was displayed. 13(9.5%) participants said they left the site when the warning message was displayed because they felt that it was a spoofed site. In this case the SI did not protect the users but their ignorance did.

Warning Comprehension

An ingenious warning must be correctly understood, it must communicate a sense of danger and present suggested actions. Users do not need to completely read it to know the appropriate actions to take. Participants were asked what their understanding of each SI meant.

37 participants did not understand the full meaning of the SI. It was observed that 11 of the 110 participants who noticed the SI were able to comprehend that the sites were prone using spoofed sites to steal sensitive information. 12 of the participants who saw the SI revealed that they thought they were expected to log out of the banking sites immediately and discontinue the entering of sensitive information. While 7 participants who saw some of the warnings claimed to the belief that their actions will result in the site being spoofed.

Attitudes and Beliefs

Well designed SI should be able to influence user's attitude and trust of the intention of the warnings depicted. Participants were asked how their attitudes and beliefs influenced their SI perceptions and it was discovered that there is a significant correlation between believing the SI and allowing them to influence the attitudes of participants. The study revealed the fact that 19 (13.9%) participants ignored the warnings completely, a finding similar to that of [8]. 16.8% of the participants confuse some of the warnings that appear alike. Thus gross warnings can be confused for minor ones if the warning formats are similar.

Motivation

An SI should be designed in such a way that it stimulates and affect the desired users' behavior. The study revealed the fact that passive SI is less motivational than active SI. 19(13.9%) participants who saw the SI were motivated to log out of the banking sites, an action that although might seem good at the time but is liable to different approach. 21 of the 74 participants who saw the SI were motivated to pay attention because the warnings made them believe they were about to be attacked. 25(18.3%) participants who chose to submit information said that they did so because they were unaware of the risks (because they did not read the warnings) or were used to ignoring similarly designed warnings (habituation), or because they did not understand the choices that the warnings presented.

Environmental Stimuli

Site was confidence gained as a result of environmental stimuli. 18(13.1%) participants who ignored the warnings said they did so because they have absolute confidence in the sites. This finding is similar to those of [10, 14].

5.0 CONCLUSION

This study reveals the effectiveness of SI in Internet banking sites in some selected banks in Nigeria as it relates to users revealing sensitive information to spoofed sites. SI designed to alert

users and to signal site trustworthiness were not fully comprehended by many participants. 37 (27%) participants did not understand the full meaning of the SI noticed in the banking sites while the attention of some users were not captured enough, for they ignored the warnings completely. Even with the presence of SI, 25(18.3%) participants still went ahead to submit sensitive information.

As spoofing attacks on user's sensitive information continue to advance, attackers' success at compromising customers credentials will become rampant. While it has been suggested that SI be designed in such a way that they interrupt the user's primary task, clearly convey the recommended actions to take, fail in a secure manner if the user does not understand or ignores them, draw trust away from the suspected spoofed banking website, and prevent the user from becoming over familiar with the sites. A different approach is needed in order to adequately secure customers sensitive information in website during authentication particularly banking sites. The appearance of SI under trusted or mistrusted conditions is not enough. SI positioned outside the immediate eye range of users or the use of passive SI will continue to be ineffective. An adequate solution must take into cognizance an enhance authentication procedure that is customers friendly and that will be secured even in an unsecured environment.

5.1 RECOMMENDATION

For Users of Internet Banking Sites

a. Caution should be taken when entering into banking sites in Nigeria. The location of the IS should be inspected. SI appearing as part of the web page should not be trusted.

b. Users of Internet banking facilities should use browsers with improved security and identification indicators. If possible indicators should be customized at significant sites.

c. Banking sites should be contacted by typing their address in the location bar, using a bookmark or following a link from a secure site, preferably protected by SSL/TLS.

d. Internet banking services should be instructed to limit online transactions in personal account to only what is really needed in order to restrict the damages due to spoofing.

For Owners of Internet Banking Sites

a. Shielded authentication operation that is not vulnerable to web spoofing should be employed in all banking sites in Nigeria. In particular, fingerprint authentication merged with the use of customized graphical models that employs the `challenge response` and one-time user authentication mechanisms would be effective against offline and online spoofing attacks.

b. SI should be designed to interrupt the user's task such that a user can continue transaction only after reading and implementing the required instruction. Active warnings are always more effective because they facilitated attention switch and maintenance.

c. SI should be designed to provide the user with clear options on how to proceed, rather than simply displaying a block of text.

d. The design pattern of less serious warnings should be different from that of more serious warnings to reflect the magnitude of the attack.

e. User's sensitive information should be transmitted using Secure Socket Layer.

Finally there should be constant educational programmes organized for users to alert them on how to identify real sites from spoofed sites and how to always ensure secured online transaction.

REFERENCES

[1]. Aaron, E. (2005) **Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures.** Available at: http://www.dictionary.com/cgi-bin/dict.pl?term=radixlabs. [doi>10.1.1.61.9231]

[2]. Amer, T. S. and Maris, J. B. (2005) Signal words and signal icons in application control and information technology exception messages hazard matching and habituation effects. Tech. Rep. Working Paper Series06-05, Northern Arizona University, Flagstaff, AZ, October 2006.

[3]. Anti-Phishing Working Group. Phishing Activity Trends Report, January 2006. http://www.antiphishing.org/reports/apwg_report_jan_2006.pdf [doi>10.1.1.122.7122].

[4]. Avivah L. (2003) Phishing Attack Victims Likely Targets for Identity Theft, Gartner FirstTake, FT-22-8873, Gartner Research.

[5]. Ba, S. and Pavlov P. (2002) Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. *MIS Quarterly*, 26 (3), 243-268.

[6]. Bank, D. (2005). 'Spear Phishing' Tests Educate People About Online Scams. *The Wall Street Journal*. August 17.

[7]. Chung, W and Paynter, J (2002) An evaluation of Internet Banking in New Zealand. *Proceedings of the 35th Hawarii international conference in system sciences*. IEEE Hawarii, September 2002, pp. 1-9.

[8]. Downs, J. S., Holbrook, M., and Cranor, L. (2006) Decision Strategies and Susceptibility to Phishing. In *Proceedings of The 2006 Symposium on Usable Privacy and Security*. Pittsburgh, PA, July 12-14.

[9]. Ezeoha, A.E (2006), Regulating Internet Banking in Nigeria, Problem and Challenges-Part 2. *Journal of Internet Banking and Commerce*, April, 11(1).

[10]. Florencio, D., and Herley, C. (2007) A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web (WWW '07),* New York, NY, USA, ACM Press, pp. 657666.

[11]. Fogg, B. J. (2002) Stanford Guidelines for Web Credibility. *Res. Sum. Stanford Persuasive Tech. Lab.*

[12]. Friedman, B. et al. (2002) Users' Conceptions of Risks and Harms on the Web: A Comparative Study. *Ext. Abs. CHI*, 614-615.

[13]. Jagatic, T., Johnson N., & M. Jakobsson. (2005) *Phishing Attacks Using Social Networks*, *Indiana U. Human Subject Study 05-9892 & 05-9893*.

[14]. Moore, T., and Clayton, R. (2007) An empirical analysis of the current state of phishing attack and defence. In *Proceedings of the 2007 Workshop on the Economics of Information Security (WEIS2007)*. http://www.cl.cam.ac.uk/ twm29/weis07-phishing.pdf. [doi>10.1.1.98.6098]

[15]. Sullivan B. (2004) Consumers still falling for phish. MSNBC. Available at: http://www.stargeek.com/item/212081.html. [doi>10.1.1.87.668]

[16]. Whalen T. and Inkpen K.. (2005). Gathering Evidence: Use of Visual Security Cues in Web Browsing. In Graphics Interface. Available at: http://portal.acm.org/ft_gateway.cfm?id=1089532&type=pdf&coll=GUIDE&dl=GUIDE&CFID=2824950&CFTOKEN=18618081 [doi>10.1.1.133.8698]

[17]. Wogalter, M. S. (2006). Communication-Human Information Processing (C-HIP) Model. In Handbook of Warnings, M. S. Wogalter, Ed. Lawrence Erlbaum Associates, pp. 5161.

[18]. Wu, M., Miller, R. & Garfinkel, S. (2006) Do Security Toolbars Actually Prevent Phishing Attacks? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Held in Montreal*. ACM Press, pp. 601610.

[19]. Zhang, Y., Egelman, S., Cranor, L. F., and Hong, J. (2007) Phinding phish: Evaluating anti-phishing tools. In *Proceedings of the 14th Annual Network & Distributed System Security Symposium (NDSS 2007)*.

THE JOURNAL OF COMPUTER SCIENCE AND ITS APPLICATION
AN INTERNATIONAL JOURNAL OF THE NIGERIA COMPUTER SOCIETY (NCS)
Vol. 19 No.1, June, 2012

nigeria computer society
www.ncs.org.ng.

Genetic Neuro-Fuzzy System for the Intelligent Recognition of Stroke

Obi, Jonathan Chukwuyeni[*], Imianvan, Anthony Agboizebeta[*] and Ekong, Victor Eshiet[**]
[*]Department of Computer Science, University of Benin, Benin City, Edo State, Nigeria.
[**]Department of Computer Science, University of Uyo, Akwa Ibom State, Nigeria.
tripplejo2k2@yahoo.com, tonyvanni@yahoo.com, victor_eshiet_ekong@yahoo.co.uk

Abstract
Stroke is a global pandemic, affecting both developed and developing countries. In Nigeria, a steady rise in affected patients is becoming noticeable to all which inspired the development of this research. Stroke is caused by high blood pressure, smoking cigarettes, family history of stroke, high cholesterol, diabetes, obesity, overweight and cardiovascular diseases which affect the brain and damage part of the body (legs, hand) coordinated by that part of the brain. The symptoms of stroke vary from numbness of the affected body part to poor speech recognition and loss of balance. In this work, geno-neurofuzzy system for the intelligent recognition of stroke is designed. Genetic algorithm is used for optimizing fuzzy set or rules, neural network provides the self-learning paradigm while fuzzy logic handles vagueness or imprecision of fuzzy set. The evaluation results show an effective way of determining and assessing the three different levels of stroke. This provides a decision support for the tele-medical diagnosis of stroke within the health sector.

Keywords: Fuzzy logic, Genetic Algorithm, Neural Network, Stroke

1.0 INTRODUCTION

Brain cell function requires a constant delivery of oxygen and glucose from the bloodstream. Cerebro-Vascular Accident (CVA) or stroke [1, 2], occurs when blood supply to part of the brain is disrupted, causing brain cells to die. Blood flow can be compromised by a variety of mechanisms. **Blockage of an artery or narrowing of the small arteries within the brain** can cause a lacunar stroke, (lacune means "empty space"). Blockage of a single arteriole can affect a tiny area of brain causing that tissue to die (infarct) or **hardening of the arteries (atherosclerosis) leading to the brain.** There are four major blood vessels that supply the brain with blood. **The anterior circulation** of the brain that controls most motor activity, sensation, thought, speech, and emotion is supplied by the carotid arteries. **The posterior circulation**, which supplies the brainstem and the cerebellum, is supplied by the vertebra basilararteries [2]. If these arteries become narrow as a result of atherosclerosis, plaque or cholesterol, debris can break off and float downstream, clogging the blood supply to a part of the brain. As opposed to lacunar strokes, larger parts of the brain can lose blood supply, and this may produce more symptoms than a lacunar stroke such as, **embolism to the brain from the heart.** In some instances blood clots can form within the heart and the potential exists for them to break off and travel (embolism) to the arteries in the brain and cause a stroke and **Cerebral hemorrhage** (bleeding within the brain substance or **Rupture of an artery)**. The most common reason to have bleeding within the brain is uncontrolled high blood pressure. Other situations include aneurysms that leak or rupture or arteriovenous malformations (AVM) in which there is an abnormal collection of blood vessels that are fragile and can bleed.

The two main types of stroke include ischemic stroke and hemorrhagic stroke. Ischemic stroke accounts for about 75% of all strokes and occurs when a blood clot, or thrombus, forms that blocks blood flow to part of the brain. If a blood clot forms somewhere in the body and breaks off to become free-floating, it is called an embolus. This wandering clot may be carried through the bloodstream to the brain where it can cause ischemic stroke. A hemorrhagic stroke occurs when a blood vessel on the brain's surface ruptures and fills the space between the brain and skull with blood (subarachnoid hemorrhage) or when a defective artery in the brain bursts and fills the surrounding tissue with blood (cerebral

hemorrhage). Both result in a lack of blood flow to the brain and a buildup of blood that puts too much pressure on the brain [3].

The risk factors for stroke include: high blood pressure (hypertension), high cholesterol, diabetes, and smoking. The symptoms of stroke includes; sudden numbness or weakness of the affected area, sudden confusion or trouble speaking or understanding, sudden troubling seeing in one or both eye, dizziness, loss of balance or coordination, severe headache with no known cause, sudden confusion or trouble understanding simple statements.

In this work, geno-neurofuzzy system for the intelligent recognition of stroke is designed. Genetic algorithm is used for optimizing fuzzy set or rules, neural network provides the self-learning paradigm while fuzzy logic handles vagueness or imprecision of fuzzy set.

2.0 LITERATURE REVIEW

A stroke is a medical emergency, and anyone suspected of having a stroke should be taken to a hospital immediately so that tests can be run and the correct treatment can be provided as quickly as possible. Physicians have several tools available to screen for stroke risk and diagnose an active stroke. These include [3]:

a. *Physical assessment* - blood pressure tests and blood tests to see cholesterol levels, blood sugar levels, and amino acid levels.
b. *Ultrasound* - a wand waved over the carotid arteries in the neck can provide a picture that indicates any narrowing or clotting.
c. *Arteriography* - a catheter is inserted into the arteries to inject a dye that can be picked up by X-rays.
d. *Computerized tomography* (CT) *scan* - a scanning device that creates a 3-D image that can show aneurysms, bleeding, or abnormal vessels within the brain.
e. *Magnetic resonance imaging* (MRI) - a magnetic field generates a 3-D view of the brain to see tissue damaged by stroke.
f. *CT and MRI with angiography* - scans that are aided by a dye that is injected into the blood vessels in order to provide clearer and more detailed images.
g. *Echocardiography* - an ultrasound that makes images of the heart to check for embolus.

2.1 Neural network

Neural network (NN) consists of an interconnected group of neurons [4]. Artificial Neural Network (ANN) is made up of interconnecting artificial neurons (Programming constructs that mimic the properties of biological neurons). A Neural Network is an analog and parallel computing system. A neural network is made up of a number of very simple processing elements that communicate through a rich set of interconnections with variable weights or strength. ANN (subsequently referred to as NN) is used in solving artificial intelligence problems without creating a model of a real biological system. NN processes information using connectionist approach to computation. It changes it structures based on internal or external information that flows through the network during the learning phase. NN can be used to model complex relationship between input and output or find patterns in data. The term network in the term "Artificial Neural Network" arises because the function f(x) is defined as a composition of other function $g_i(x)$ which can further be defined as a composition of other functions [5]. Figure 1 presents a simple NN which comprises of three layers (Input, Hidden and Output layers). The NN presented in Figure 1, comprises of a layer of "input" connected to a layer of "hidden" units, which is in turn connected to a layer of "output" units. The activity of the input unit represents the raw information that is fed into the network; the activity of the hidden units is determined by the activity of the input unit and the weights between the hidden and output units. The hidden units are free to construct their own representation of the input; the weights between the input and hidden units determine when each hidden unit is active, and so by modifying these weights, a hidden unit can choose what it represents [6].

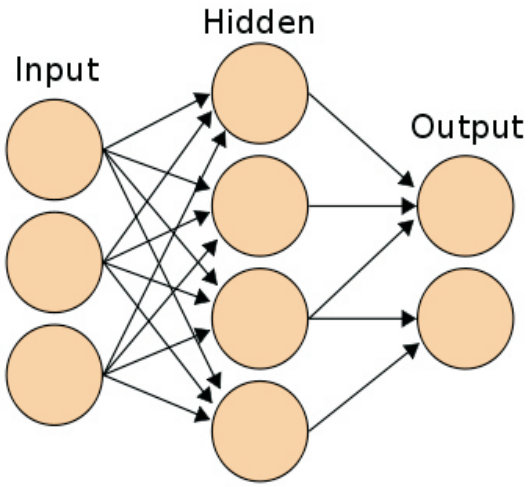


Figure 1: A simple Neural Network

NN employs learning paradigm that includes supervised, unsupervised and reinforcement learning [7]. NN has been applied in stock market prediction, credit assignment, monitoring the condition of machinery and medical diagnosis [7, 8, 9, 10, and 11]. Application of NN in medical diagnosis includes electronic noses, diagnosis of cardiovascular systems, [7, 12]. Tuberculosis has also been explored [13] while breast cancer [14]. They learn by example, hence details of how to recognize the disease is not needed. What is needed is set of examples that are representatives of all the variation of the disease. However, NN cannot handle linguistic information and also cannot manage imprecise or vague information [15].

2.2 Genetic Fuzzy Classifier System

Computational Intelligence techniques such as fuzzy logic and genetic algorithms (GAs) are popular research subjects, since they can deal with complex engineering problems which are difficult to solve by classical methods [16]. Fuzzy systems are fundamental methodologies to represent and process information, with mechanisms to deal with uncertainty and imprecision. With such remarkable attributes, fuzzy systems have been widely and successfully applied to control, classification and modeling problems. One of the most important tasks in the development of fuzzy systems is the design of its knowledge base. An expressive effort has been devised lately to develop or adapt methodologies that are capable of automatically extracting the knowledge base from numerical data. Fuzzy systems are particularly suitable for modeling and classification problems as a human expert is able to analyze and comprehend the knowledge stored in the form of linguistic variables and rules. Although fuzzy systems have been successfully applied in a large number of applications, they lack the ability to extract knowledge from a set of training data. Therefore, over the past years more research has been devoted to augment the approximate reasoning method of fuzzy systems with the learning capabilities of neural networks and evolutionary algorithms [17]. Over the past decade, there has been an increasing interest in evolutionary algorithms that adapt the knowledge base of a fuzzy system. Genetic algorithms have demonstrated to be a powerful tool to perform tasks such as generation of fuzzy rule-base, optimization of fuzzy rule bases, generation of membership functions, and tuning of membership functions. These approaches are described by the general term Genetic Fuzzy Rule Based Systems (GFRBS) [17]. The role of the evolutionary algorithm is to either tune the parameters of a fuzzy rule based system or to completely automate the fuzzy knowledge base design. A Genetic Fuzzy System (GFS) [18] is basically a fuzzy system augmented by a learning process based on evolutionary computation, such as genetic algorithms [19].

3.0 METHODOLOGY

The genetic neuro-fuzzy system for the intelligent identification of stroke is presented in Figure 2. The system is developed in an environment characterized by Microsoft Window XP Professional operating system, Microsoft Access Database Management system, Visual Basic Application Language, Microsoft Excel and xI bit 1.1 (genetic algorithm tool) was used to optimized both the fuzzy rule and sets to derive the best rules and symptoms. Neuro-Solution and Crystal Report were used for Neural Networks analysis and graphical representation respectively. The process for the clinical diagnosis of stroke starts when an individual consults a physician (doctor) and presents a set of clinical complaints (symptoms). The physician then requests further information from the patient or from others close to him who knows about the patient's symptoms in severe cases.

Data collected include patient's previous state of health, living condition and other medical conditions. A physical examination of the patient condition is conducted and in most cases, a medical observation along with medical test(s) is carried out on the patient prior to medical treatment. From the symptoms presented by the patient, the physician narrows down the possibilities of the illness that corresponds to the apparent symptoms and make a list of the conditions that could account for what is wrong with the patient. The physician then conducts a physical examination of the patient, studies his or her medical records and ask further questions, as he goes in an effort to rule out as many of the potential conditions as possible. When the list has been narrowed down to a single condition, it is called differential diagnosis and provides the basis for a hypothesis of what is ailing the patient. Until the physician is certain of the condition present; further medical test are performed or schedule such as medical imaging, scan, X-rays in part to conform or disprove the diagnosis or to update the patient medical history. Other Physicians, specialist and expert in the field may be consulted (sought) for further advice. The focal point of this research centers on tuning fuzzy rules utilizing Genetic Algorithm (GA) which help optimize the fuzzy set (parameters or symptoms and then yield the Fuzzy IF-Then rule, in other to obtain the best results). Neural network was

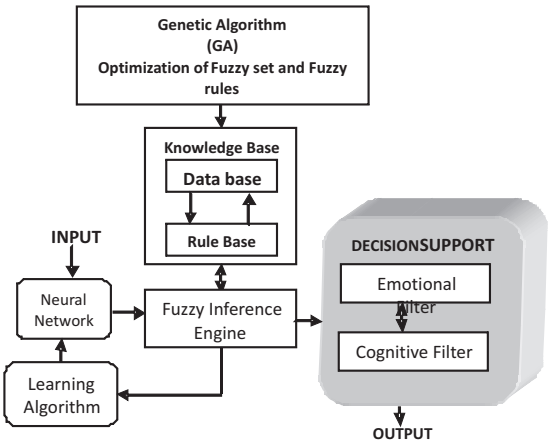


Figure 2: Genetic-Neurofuzzy system for Stroke diagnosis

To design our Genetic-Neuro-Fuzzy system for diagnosis of stroke, we designed a system which consists of a set of clinical symptoms needed for the diagnosis (here, we are using seven optimized clinical symptoms of stroke):

a. Sudden numbness or weakness of the affected area
b. Sudden confusion or trouble speaking or understanding
c. Sudden troubling seeing in one or both eye
d. Dizziness
e. Loss of balance or coordination
f. Severe headache with no known cause
g. Confusion understanding simple statements

The knowledge base consists of the database and Rule base. The knowledgebase houses the clinical symptoms of stroke. The values of the parameters are often vague (fuzzy) and imprecise hence the adoption of fuzzy logic in the model as means of analyzing these data. These parameters therefore constitute the fuzzy parameter of the knowledge base. The system parades two input variables X_1 and X_2 which are symptoms of stroke. The training data are categorized by two classes C_1 and C_2. Each input is represented by the two linguistic terms, thus we have four rules.

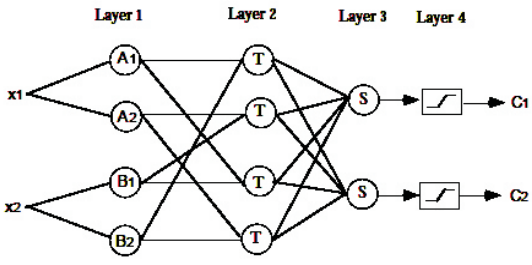


Figure 3: Fuzzy Classifier System for the Diagnosis of Stroke

Layer 1: The output of the node is the degree to which the given input satisfies the linguistic label associated to this node. This is governed by the bell-shaped membership functions

$$A_i(u) = \exp\left[-\frac{1}{2}\left(\frac{u - a_{i1}}{b_{i1}}\right)^2\right],$$

$$B_i(v) = \exp\left[-\frac{1}{2}\left(\frac{v - a_{i2}}{b_{i2}}\right)^2\right],$$

which represent the linguistic terms, where $\{a_{i1}, a_{i2}, b_{i1}, b_{i2}\}$ is the *parameter set, where* ***u*** *and* ***v*** *is the total parameter set*. As the values of these parameters change, the bell-shaped functions vary accordingly, thus exhibiting various forms of membership functions on linguistic labels A_i and B_i. In fact, any continuum, such as trapezoidal and triangular-shaped membership functions are also quantified candidates for node functions in this layer. The initial values of the parameters are set in such a way that the membership functions along each axis satisfy:-completeness, normality and convexity. The parameters are then tuned with a descent-type method.

Layer 2: Each node generates the signal corresponding to the conjunctive combination of individual degrees of match of stroke symptoms. The output signal is the firing strength of the fuzzy rule with respect to stroke.

We take the linear combination of the firing strengths of the rules at *Layer 3* and apply sigmoidal function at *Layer 4* to calculate the degree of belonging to a certain class. Given training set $\{(x^k, y^k), k = 1, \ldots, K\}$ where x^k refers to the k^{th} input pattern then

$$y^k = \begin{cases} (1,0)^T & \text{if } x^k \text{ belongs to Class 1} \\ (0,1)^T & \text{if } x^k \text{ belongs to Class 2} \end{cases}$$

the error function for pattern k can be defined by:

$$E_k = \frac{1}{2}\left[(o_1^k - y_1^k)^2 + (o_2^k - y_2^k)^2\right]$$

Where y^k is the desired output and o^k is the computed output.

Using fuzzy IF-THEN rules to describe a classifier, assume that K patterns $x_p = (x_{p1}, x_{pn}), p = 1, \ldots, K$ are

given from two classes, where x_p is an n-dimensional crisp vector. Typical fuzzy classification rules for $n = 2$ are like:

IF x_{p1} is *small* and x_{p2} is *very large* THEN $x_p = (x_{p1}, x_{p2})$ belongs to Class C_1

IF x_{p1} is *large* and x_{p2} is *very small* THEN $x_p = (x_{p1}, x_{p2})$ belongs to Class C_2

where x_{p1} and x_{p2} are the features of pattern (or object) p, *small* and *very large* are linguistic terms characterized by appropriate membership functions.

The task of *fuzzy classification of stroke* is to generate an appropriate fuzzy partition of the feature space. In this context the word *appropriate* means that the number of misclassified patterns is very small or zero. Then the rule base should be optimized by deleting rules which are not used. The scheme is extensible to any number of input and classes. The fuzzy set of parameters is represented by 'X', which is defined as X= $\{X_1, X_2 \ldots, X_n\}$ where X_i represents the j^{th} parameter and n is the number of parameter. A neural network provides the learning structure for the parameters, which serves as a platform for the inference engine. The inference engine consists of reasoning algorithm driven by production rules. These production rules are evaluated by using the forward chaining approach of reasoning [20, 21]. The inference mechanism is fuzzy logic driven. The cognitive filter of the decision support engine takes as input the output report of the inference engine and applies the objective rules to rank the individual on the presence or absence of stroke. The emotional filter takes as input the output report of the cognitive filter and applies the subjective rules in the domain of studies in order to rank individuals on the extent of stroke.

Genetic Algorithm is used for optimizing the knowledgebase, which houses both the database and Fuzzy rule-base. The genetic algorithm comprises of five components which are fitness function, selection, mutation, reproduction and crossover. **The fitness function**, also called evaluation function, rates a potential solution by calculating how good they are relative to the current problem domain. **Selection** is used to move towards promising regions in the search space. The individuals with high fitness are selected and they will have a higher probability of survival to the next generation. **Mutation** prevents stagnation at any local optima. **Crossover** takes two of the fittest genetic strings in a population and combines the two of them to generate new genetic strings. **Reproduction** causes evolution to better solution.

The fuzzy partition for each input feature consists of clinical symptoms of stroke. However, it can occur that if the fuzzy partition of stroke is not set up correctly, or if the number of linguistic terms for the input features is not large enough, then some patterns will be misclassified. The rules that can be generated from the initial fuzzy partitions of the classification of stroke is thus

a. Not experiencing Stroke (C_1)
b. Experiencing Partial Stroke (C_2)
c. Experiencing Severe Stroke (C_3)

If the patient is experiencing three or less symptoms *THEN* (C_1), if the patient is experiencing at least four symptoms *THEN* (C_2) and if the patients is experiencing five or more symptoms *THEN* (C_3).

The Fuzzy IF-THEN Rules (R_i) for stroke is

R1: IF the patient is experiencing numbness sudden numbness or weakness of the affected area THEN he/she has class C_1.

R2: IF the patient is experiencing sudden numbness or weakness of the affected area and sudden confusion or trouble speaking or understanding THEN he/she has class C_1.

R3: IF the patient is experiencing sudden numbness or weakness of the affected area, sudden confusion or trouble speaking or understanding and sudden troubling seeing in one or both eye THEN he/she has class C_1.

R4: IF the patient is experiencing sudden numbness or weakness of the affected area, sudden confusion or trouble speaking or understanding, sudden troubling seeing in one or both eye and dizziness THEN he/she has class C_2.

R5: IF the patient is experiencing sudden numbness or weakness of the affected area, sudden confusion or trouble speaking or understanding, sudden troubling seeing in one or both eye, dizziness and loss of balance or coordination, THEN he/she has class C_3.

R6: IF the patient is experiencing sudden numbness or weakness of the affected area, sudden confusion or trouble speaking or understanding, sudden troubling seeing in one or both eye, dizziness, loss of balance or coordination and severe headache with no known cause THEN he/she has class C_3.

R7: IF the patient is experiencing sudden numbness or weakness of the affected area, sudden confusion or trouble speaking or understanding, sudden troubling seeing in one or both eye, dizziness, loss of balance or coordination, severe headache with no

known cause and confusion understanding simple statements THEN he/she has class C_3.

4.0 RESULTS AND DISCUSSION

The dataset for the diagnosis of stroke is presented in Table 1. The degree of membership ranges, from *0.00-1.00 (below 0.5, low degree of membership function and 0.5 and above high degree of membership function).* The graph clearly shows a symptoms with high degree of "Not Experiencing Stroke" in Cluster 1, four symptoms with high degree of "Experiencing Partial Stroke" in Cluster 2 and five symptoms with high degree of "Experiencing Severe Stroke" in Cluster 3.

Table 1: Data Set showing the Degree of membership of stroke Symptoms; Scale (0.00 1.00)

PARAMETERS OR FUZZY SETS	CODES	DEGREE OF INTENSITY OF STROKE		
		Cluster 1 (C_1)	Cluster 2 (C_2)	Cluster 3 (C_3)
Sudden numbness or weakness of the affected area	P01	0.10	0.10	0.80
Sudden confusion or trouble speaking or understanding	P02	0.10	0.10	0.80
Sudden troubling seeing in one or both eye	P03	0.50	0.15	0.50
Dizziness	P04	0.00	0.50	0.50
Loss of balance or coordination	P05	0.29	0.59	0.12
Severe headache with no known cause	P06	0.00	0.50	0.50
Confusion understanding simple statements	P07	0.18	0.70	0.12
RESULTS		NOT EXPERIENCING STROKE	EXPERIENCING PARTIAL STROKE	EXPERIENCING SEVERE STROKE

5.0 CCONCLUSION

Stroke is becoming is a global health problem. The need to design a model that would assist physician in tele-medical diagnosis of stroke cannot be over emphasized. This paper demonstrates the practical application of soft computing (combination of artificial intelligence, fuzzy logic, neural networks, genetic algorithm and probabilistic reasoning) in the health sector. It presents an hybrid of fuzzy logic, genetic algorithm and neural network to generate a genetic-neurofuzzy model to help in diagnosis of stroke. This model which uses a set of fuzzified data set incorporated into neural network system is more precise

than the traditional system. The system designed is an interactive system that tells the patient his current condition as regards stroke. It should however be noted that the model was not designed to give prescription or treatment on stroke but can also be expanded to do so in subsequent research. A system of this nature that has the ability to diagnose a person suffering from stroke should be introduced in health care delivery centers and hospitals to help ease the work of physicians.

REFERENCES

[1] Healthline (2009) Stroke, Retrieve from: http://healthline.com?Adamcontent/numbness-and-tingling.

[2] MedicineNet (2011) Stroke, Retrieve from: http://MedicineNet.com/stroke/article.htm

[3] MNT: Medical News Today (2009) Stroke, Retrieve from: *www.**medicalnewstoday**.com/articles/7624.php*

[4] Ponniyin, S.K. (2009) Neural Network, Retrieve from: http://www.Icann2007.org/neural.networks

[5] Gary, R. G and Cardullo F. (1999) Research paper on, Application of Neuro Fuzzy System to Behavioral Representation in Computer Generated Forces, Retrieve from: http://citeseer.ist.psu.edu/george99application.html

[6] Christos, S. and Dimitros, S. (2008) Neural Network, Retrieve from: http://docs.toc.com/doc/1505/neural-networks.

[7] Wikipedia (2010), "Artificial Neural Network", Retrieve from: http://en.Wikipedia.org/wiki/Artificial-neural-network

[8] Dase, R. K and Pawar, D.D. (2010) Application of Neural network to stock market prediction: A review of literature, Retrieve from: http://www.bioinfo.in/uploadfiles/12843156482_2_3_IJMI.pdf

[9] Hiroshi, S., Kentaro, K., Kazuo, O. and Masato, O. (2011) Statistical mechanics of Structural and temporal credit assignment effects on learning in neural Networks, Retrieve from: http://pre.aps.org/abstract/PRE/v83/i5/e051125

[10] Adyles, A. J. and Fabrício, C. L. A. (2010) **Automatic Faults Diagnosis by Application of Neural Network System and Condition-based Monitoring Using Vibration Signals, Retrieve from: http://www.informatics.org.cn/doc/ucit201001/ucit20100104.pdf**

[11] Vahid, K., Gholam, A. M (2009) Intuitionistic fuzzy set vs. fuzzy set application in medical pattern recognition, *Artificial Intelligence in Medicine*, Vol. 47, No. 1, pp. 43-52, DOI:10.1016.j.artmed.2009.03.002.

[12] Jionghua, T., Suhuan, W., Jingzhou, Z. and Xue, W. (2010) Neuro-fuzzy logic based fusion algorithm of medical images, *3rd IEEE Int'l Congress on Image and Signal processing (CISP2010)*, Vol. 4, pp 1552-1556, DOI: 10.1109/CISP.2010.5646958.

[13] Imianvan, A.A. and Obi J.C (2011) Fuzzy Cluster Means Expert System for the Diagnosis of Tuberculosis, *Global Journal of Computer Science & Technology*, Vol. 11, No. 6, ISSN: 0975-4175.

[14] Obi, J.C. and Imianvan, A.A. (2011) **Breast cancer recognition using fuzzy classifier,** *International Journal of Academic Research*, Vol. 3. No. 3, Retrieved from: http://www.ijar.lit.az/pdf/11/2011%2811-68%29.pdf

[15] Akinyokun, O.C. (2002) Neuro-fuzzy expert system for evaluation of human Resource
Performance, First Bank of Nigeria Endowment Fund lectures Federal University of technology, Akure, Nigeria.

[16] Francisco, H. (2008) Genetic fuzzy systems: taxonomy, current research trends and prospects, *Journal of Evol. Intel*, Vol.1, Pp.2746, DOI: 10.1007/s12066-007-0001-5.

[17] Hoffmann, F (2001) Boosting a Genetic Fuzzy Classifier, *IFSA World congress and 20th NAFIPS Int'l Conf.*, Stockholm, Vol. 3, pp. 1564-1569, DOI: 10.1109/NAFIPS.2001.943725.

[18] Magdalena, L., Cordon, O., Gomide, F. Herrera, F. and Hoffmann, F. (2001) Ten Years of Genetic Fuzzy Systems Current Framework and New Trends, *IFSA World congress and 20th NAFIPS Int'l Conf.*, Stockholm, Vol. 3, pp. 1241-1246, DOI: 10.1109/NAFIPS.2001.943725.

[19] Eiben, A.E, and Smith, J.E. (2003) *Introduction to Evolutionary Computation,* Springer, Berlin, pp. 33-35, ISBN: 3-540-40184-9.

[20] Georgios, M. and Nick, B. (2009) DLEJena: A Practical Forward-Chaining OWL 2 RL Reasoner Combining Jena and Pellet, Retrieved from: http://www.DLEJena.com/A Practical

Forward- Chaining OWL2 RL Reasoner Combining Jena and Pellet

[21] Obi, J. C. and Imianvan, A. A. (2011) Decision Support System for the Intelligent Identification of Alzheimer using Neuro Fuzzy logic, *Int'l Journal on Soft Computing (IJSC)*, Vol. 2, No. 2, pp. 25-38, DOI:10.5121/ijsc.2011.2203.

THE JOURNAL OF COMPUTER SCIENCE AND ITS APPLICATION
AN INTERNATIONAL JOURNAL OF THE NIGERIA COMPUTER SOCIETY (NCS)
Vol. 19 No.1, June, 2012

nigeria computer society
www.ncs.org.ng.

Assessing Network Services and Security in Nigeria Universities

*O. A. T. Aladesanmi (taladesanmi@oauife.edu.ng)
**B.S. Afolabi (bafox@oauife.edu.ng)
***T.O Oyebisi (toyebisi@oauife.edu.ng)
*Information Technology and Communications Unit, Obafemi Awolowo University, Ile-Ife, Nigeria
**Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria
***Technology Planning and Development Unit, Obafemi Awolowo University, Ile-Ife, Nigeria

ABSTRACT
The paper investigated sources of threats and vulnerabilities to Nigerian university computer networks and assessed the adequacy of security controls in place to mitigate the occurrence of successful intrusion. This was with a view to enhancing the integrity of data transactions on the Universities' computer networks. Data for the study were sourced from 18 purposively selected universities in Southwestern Nigeria. Three universities, each representing federal, state and private were selected from each of the six states in the zone. Primary data were obtained through the use of validated questionnaire. The result revealed that 81.3% of the universities had internet presence. The Universities' Organisation Information Criticality Matrix (OICM) showed the bursary unit with highest weighted average. The result further showed that web services posed the greatest source of threat and vulnerability to the university networks. Indeed, 72% of the universities ran e-portal services that incorporated electronic payment but none of the universities was digitally signed with Certificate Authority (CA). The result also showed that single factor authentication using usernames and passwords were the only network access identifier employed by all the universities. The study noted that the security controls to safe guard the integrity and non-repudiation of network transactions in the universities were weak and high potential existed for possible compromise of the network system. The study therefore concluded by proposing a layered approach to managing security on the university network.

1.0 INTRODUCTION

It is almost universally accepted that technological change and other kinds of innovations are the most important sources of productivity growth and increased material welfare [1] and thus, have a decisive impact on the competitive structure and capital creation in many industries and at many levels [2, 3]. One of the most significant drivers of strategic change in the world is technological innovation. In particular, the application of innovative information technology (IT) is radically altering the basis of business competition [4]. The benefit of exploiting IT not only relates to making business processes and tasks more efficient. Instead, IT also enables the creation of products, services, distribution channels, and links with customers, suppliers, and other stakeholders. IT is virtually interwoven with almost every aspect of modern organizations, their business network, and their environment as a whole. In the universities, ICT is used to support, enrich and improve education and provide more flexibility in teaching delivery. The entire academic landscape, including the teaching and learning process, the research process, libraries and information services; and university administration and management now partially or wholly rely on ICT [5]. ICTs are being reflected in university strategic plans and institutional guidelines. More and more African universities are seeing the benefits of adding "e" to learning. Universities like Eduardo Mondlane University (Mozambique), Makerere University (Uganda), University of Dar es Salaam (Tanzania) and Obafemi Awolowo University (Nigeria) have ICT institutional guidelines that are aligned to their university strategic plans [5].

Internet usage in Nigeria has grown rapidly resulting in the explosion of Internet Service Providers (ISPs) and Internet access points. This has had several positive impacts on the socio-economic and educational developments in the country. Unfortunately, the country's image has also suffered as a result of the nefarious activities of some Nigerians, that has now turn the Internet into a cheap channel for the perpetration of criminal spamming activities known as the 'Advanced Fee Fraud' [6]. More worrisome is the capture of Al Qaeda's operative, Muhammad Naeem Noor Khan, which provided the Pakistani and American Intelligence Authority with some of

Al Qaeda's Internet Communication Strategy and also identified that Nigerian Websites and Email System were used by Al Qaeda to disseminate Internet information [7]. Universities networks in Nigeria are not immune from these nefarious activities. Globally, Universities have been a target of attackers, because there is a wealth of information there that is useful for exploitation. There are young students there who have credit cards, Social Security numbers, bank accounts and other types of online assets that are valuable to criminals [8]. Paradoxically, while corporations may have large security budgets and IT staff, universities often do not enjoy the same level of resources to safeguard information. Universities have unique challenges that are extremely difficult to manage. They often have a very large number of users and support a wide range of computers. They are typically understaffed, and their IT employees often are undertrained to deal with computer security [8].

Computer threats and attacks over the years have become both increasingly numerous and sophisticated [9]. Many organizations are having trouble determining which new threats and vulnerabilities pose the greatest risk and how resources should be allocated to ensure that the most probable and damaging attacks are dealt with first. These incidents, their rising sophistication and the vulnerability of even the best defenses are unfortunate reminders that the potential exists for severe damage.

Managing security threats and vulnerabilities in computer networks is a fundamental challenge to universities in Nigeria. Studies on Universities computer network management in Nigeria and their capabilities for evaluating computer security incidents are scarce giving credence to Okonigene and Adekanle, (2009) that Nigeria is an innocent and ignorant passive player in cyberspace knowledge Olympiad.

The paper profiles the information asset of some selected universities in Nigeria and went to build an organizational information criticality matrix (OICM). It also investigated sources of threats and vulnerabilities to the University computer networks. This is with view to identify areas of weakness, achieve better implementation of security controls, reduce the number and impact of major incidents, encourage development of security policies, standards and controls and improve enterprise-wide security awareness.

2.0 METHODOLOGY

In achieving these objectives, a set of structured questionnaire was administered on senior ICT staff of selected universities in Southwest, Nigeria. The universities were selected from the southwest because the zone hosts the oldest federal, state and private universities in Nigeria. The Universities were purposively selected to also reflect ownership structure (Federal, State and privately owned). The questionnaire probe the amount of information residing in various major units of the Universities namely the bursary, library, registry, human resource and academic units. The questionnaire went further to seek information on the security controls (operational, technical and administrative) implemented on data containers such as storage devices and data that moves across communication channels among data containers.

3.0 DISCUSSION OF RESULTS

a. Organisation Information Criticality Matrix (OICM)

The OICM helped in differentiating and characterising information based on its level of criticality. The criticality is measured in terms of three data attributes namely confidentiality, integrity and availability. The study revealed that the bursary services which comprise of budget preparation, implementation monitoring; reporting and evaluation, revenue & grant management, fixed assets management, payroll and salaries were the most computerised units in the universities. In addition, as shown in Table 1, the OICM of the universities ranked in terms of respondent perception of confidentiality, integrity and availability of the data. The Mean Weighted Value of OICM is depicted in Table 2. From the two tables, bursary records rank most critical in all the three data attributes of confidentiality, integrity and availability. This is followed in decreasing order by registry (1.87), library (1.64), academic services (1.49) and HRM (1.21). That is, a loss of university bursary data would have the greatest adverse impact on the Universities. Unexpectedly, academic services comprising of course design, development and integration, e-learning, test and assessment ranked poor in the OICM. This on the face value presented a case of priority misplacement since academic and research work form the core function of the university. However, a deeper probing showed that digitisation of records and automation of services in the Universities commenced with the bursary unit and services (most especially salaries and payroll). Technology driven learning was a recent event

which is yet to take a firm root and in majority of the universities, only limited to student online registration generically referred to as e-portal services in the Universities.

Table 1 Weighted Average of OICM

University Services/ Operations	Confidentiality	Integrity	Availability
Library	1.54	2.00	1.39
Registry	1.93	2.23	1.46
Bursary	2.31	2.31	1.46
Human Resource Mgt	1.39	1.39	0.85
Academic Services	1.31	1.69	1.46

Table 2 Mean Weighted Average Value for OICM

University Services/Operations	Weighted Average
Library	1.64
Registry	1.87
Bursary	2.04
Human Resource Mgt	1.21
Academic Services	1.49

b. Network services availability

Figure 1 shows the various hosted network services being provided in the universities.

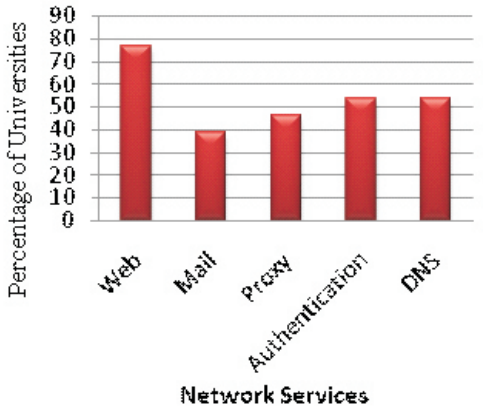


Figure 1 Network Services Provided by Universities

From figure 1, it can be seen that 76.9% of the universities offered web services. Other services offered were authentication (53.8%), domain name system (53.8%), proxy (46.2%) and mail (38.5%). As further seen in Table 3, web services accounted for the highest level of threat among the services provided therefore constituting greatest source of threat and vulnerability in the universities. Conversely, the Domain Name System (DNS) service is the least vulnerable service and the least threatened also. Websites have been known to be the face

Table 3 Threat and Vulnerabilities to Network Services

Network Services Vulnerabilities Assessment					
Service	Web	Mail	Proxy	Authentication	DNS
Most Vulnerable	2.2	2.2	1.9	2.0	1.7
Most Threatened	2.4	2.2	1.9	2.0	1.7

of any organization in the cyberspace; the first contact intruders will likely come to

of any organization in the cyberspace; the first contact intruders will likely come to meet. There is substantial industry documentation on web browser security because the web browser is a frequently used vector of attack [10]. This result is consistent with [11] where it was submitted that 9 in 10 websites contain serious security issues and therefore a prime target for malicious hackers. It further lend credence to the submission of Okonigene and Adekanle (2009) that Nigeria websites were used as part of Al Qaeda activities.

It is particularly interesting to note that 84% of the universities claimed to have e-portal services running on their network with 72% of the said portal system incorporating electronic payment. However, only 18.2% of the Universities have their portal digitally signed. None of the Universities was digitally signed with with any of the accredited Certificate Authorities. Digital Certificates support integrity services by confirming that the

information in a certificate has not been altered by unauthorized methods and belongs to the proper subject [12]. The underlying intent for digital certificates is in terms of supporting a transitive trust relationship that allows a relying party to verify the authenticity of a signed artifact through verification of the signer's key using the public key infrastructure (PKI) [13].

An examination of security controls on the network revealed a gap between current practices by the universities and established best practices. For instance, 84.6% of the universities deployed wireless access (Table 4). Generally speaking, a significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot [14], hence, wireless network security is more concentrated and complex than that of a wired network [15]. In securing the wireless network, 35.5% of the Universities deploy MAC filtering (Figure 2). This was followed by Wired Equivalent Privacy (WEP) (30.8%) and Wi-Fi Protected Access (WPA) (15.4%). Literature had established flaws in each of this protection technique. The use of MAC filtering is prone to MAC spoofing. An attacker can have unauthorized access to the network by using a wireless NIC card with a spoofed MAC address [12].

Table 4: Network Media and Internet Connection

Media Used	Percentage (%)
Wireless	84.6
Ethernet Cable	92.3
Fibre optics cable	61.5
Others	7.7
Means of Internet Connection	**Frequency (%)**
Satellite (VSAT)	84.6
Fibre optics cable	15.4
Terrestrial Radio	0
Others	0

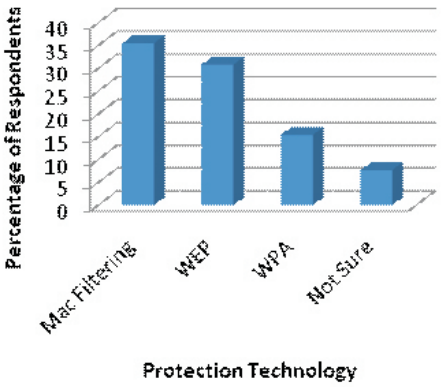


Figure 2: Technique for securing Wireless Network

This position is further strengthened in [16] where it was argued that MAC filtering provides only primitive protection against attackers. Lack of scalability constitute another downside of MAC filtering, it becomes cumbersome having to manually enter the MAC address of every PC in the university. Also, each MAC address addition on Access Point increases the load thereby putting stress on the Central Processing Unit (CPU) and the memory.

WEP which ranked second in the list of protection mechanism used by the university is also fraught with weaknesses. WEP uses shared secret and generates a pseudo-random key stream from the shared secret key. As noted by [17], the shared key can be discovered by guesswork based on a certain amount of social engineering regarding the administrator who configures the wireless LAN and all its users. This is possible because the WEP key has to be shared with all users of the network. In addition, some client software (Microsoft Vista for example) stores the WEP keys in the operating system registry or initialization scripts which can easily be retrieved and decoded. In addition, the Federal Bureau of Investigation (FBI) has demonstrated using tools such as kismet and aircrack the possibility of cracking WEP keys in less than three minutes.

It becomes worrisome knowing that all the universities sampled uses single factor authentication with username and password as the only source of accessing services on the network including those that required elevated privileges (Table 5). This result posed a fundamental question: how come the universities portal system in Nigeria has survived thus far with this obvious porosity. The fact that there has not been significant cases of computer attack does not imply a good security

control exist but stems from the fact that resources currently residing on the network as seen in the OICM are not sufficiently attractive to warrant attack.

See Http://www.youtube.com/watch?v=gruJc4oc51o&feature=related for a youtube demonstration.

The general operation of the portal system which (in all the universities) only acts as

Table 5: Access Method

Network access identifier	Percentage of Respondents
Usernames and password	100%
Swipe card	0
Thumb print	0
Voice Recognition	0
Retina Detection	0
Others	0
Identifier for access critical system resources with	**Percentage of Respondents**
Usernames and password	100%
Swipe card	0
Thumb print	0
Voice Recognition	0
Retina Detection	0
Others	0

a conductor i.e an interface to make payment, whereas the actual containers of the payment records are within the receiving merchants in this case, banks with better and improved security measures. There is potentials for sophisticated attack and internal threat in particular as network resources becomes more valuable.

To address this therefore, the study proposes a three layer approach.

1. Managerial Control: there is need by every university to first evolve a distinct but interdependent security policy that guides the use and deployment of information resources on network. The policy should reflect the current security situation in each of the university with provision for regular review to accommodate new challenges. It is important that the policy should also have institutional backing to make it enforceable, so it is just not an IT department creation but a university creation.
2. Operational Control: Capabilities of ICT staff should be improved through continuous focus training specifically in areas of security. There is need for establishment of configuration management system.
3. Technical Control: The technical controls are the actual implementations of the operations controls which itself should align with objectives already set in the universities security policies.

In the immediate however, it is recommended that network access to critical resources should employ a multi-factor authentication mechanism beyond the current practice of single factor usernames and passwords. Furthermore, to attain reasonable level of transaction integrity and non repudiation, universities offering online payment solution should consider using public key infrastructure.

5.0 CONCLUSION

University network in Nigeria is growing and much emphasis is placed on providing network access, digitisation and computerization of records and technology driven learning. Logically, recent study on university networks in Nigeria focused on the impact of these evolving areas. The study assessed the network services provisioned in the universities by determining the university information resources, investigating the sources of threat and vulnerability and assessing the security controls in place. This was necessitated on the premise that the functioning of universities in Nigeria, as it is in most organisations and institutions in the globe, is becoming more and more dependent on ICT and sensitive data reside

on the university networks. Literature has also established that information as a critical organisation asset is central to decision making and competitive advantage.

In achieving the objectives set in the study, institutional questionnaires were administered on Technical Head of ICT units in some selected universities in Southwest of Nigeria. The study revealed that Ethernet cabling remains the primary form of network access by users on the network closely followed by wireless technology and fibre. VSAT technology was the major technology in connecting to the Internet. In terms of computerization of records, bursary operations were the most computerized. Furthermore, the university provides different network based services with web services accounting for the highest. The study also showed that web service was the most vulnerable and the most threatened of all the network services. Most of the university runs an e-portal system which as well incorporates electronic payment. However, this is done over an unsecured internet link. As such, web portends the greatest source of threat and vulnerability to the university network.

The study revealed predominant use of wireless access. However, the two commonest security controls on the wireless network were MAC filtering and WEP, both with serious flaws. The study finally proposed the need for the universities to evolve security policies geared towards addressing potential security breach and incident management.

The study recommended that universities offering electronic portal services with integrated electronic payment should be digitally signed to guarantee the integrity of transaction on the networks. Capabilities of ICT staff should be improved through continuous focus training specifically in areas of security. There is also need to overhaul existing ICT policies to integrate and address security concerns, disaster recovery mechanism, roles and responsibilities based on the current realities of evolving security threats.

REFERENCES

[1] Edquist, C. (1997). Systems of Innovation Approaches-Their Emergence and Characteristics in Systems of Innovation. Ed. John de la Mote

[2] Ernst, H. (2003). Patent Information for Strategic Technology Management. World Patent Information. Vol. 25, Issue 3, September 2003, pp 233242. Retrieved from http://aspheramedia.com/v2/wp-content/uploads/2011/02/Patent-information-for-strategic-technology-management.pdf (Accessed June 2010).

[3] Laosirihongthong, T. and Lim, L. K. (2008). Skill Inexistence and Knowledge Requirements of Technology Marketing and Management Programs in Emerging Thailand and Vietnam. *International Journal of Business and Management, Vol. 3, No. 5. pp 151 -160.*

[4] Van Der Zee J.T.M. and Berend , D. (1999). Alignment Is Not Enough: Integrating Business and Information Technology Management with the Balanced Business Scorecard**. *Journal of Management Information Systems* Fall 1999, Vol. 16, No. 2.**

[5] Beebe, M.A. (2004). Impact of ICT Revolution on the African Academic Landscape. Proceedings of CODESRIA Conference on Electronic Publishing and Dissemination, Dakar, Senegal 1 -2 September, 2004. Retrieved from www.codesria.org/Links/conferences/el_publ/beebe.pdf.

[6] Longe, O.B. and Chiemeke S.C.(2008). *Cyber Crime and Criminality in Nigeria What Roles are Internet Access Points in Playing?* ***European Journal of Social Sciences Volume 6, Number 4(2008). pp 132-139.***

[7] Okonigene, R.E. and Adekanle, B. (2009). Cybercrime In Nigeria**. *Business Intelligence Journal - January, 2010 Vol.3 No.1. pp. 93-98.***

[8] LeClaire, J. (2006). *Hackers Target University Computer Assets*. http://www.technewsworld.com/story/50799.html?wlc=1282640602. (Accessed August 2010).

[9] Hansman, S. and Hunt, R. (2004). A Taxonomy of Computer Attacks. *Computers & Security*. Volume 24, Issue 1, February 2005, pp31-43.
1983, Pages 9-13.

[10] Crowley, C. (2009). Preventing Incidents with a Hardened Web Browser.

www.sans.org/reading.../preventing-incidents-hardened-web-browser_33244. (Accessed June, 2010).

[11] WhiteHat (2008). Vulnerability Assessment Plus Web Application Firewall. Retrieved from *www.whitehatsec.com/home/assets/WP_WAF061708.pdf*

[12] Park, J.S. and Decoi, D. (2003). WLAN Security: Current and Future. *Internet Computing. IEEE* Volume: 7 Issue: 5, Sept.-Oct. 2003. pp. 60 65.

[13] Huston, G. (2009). Resource Certification. IETF Journal Volume 4, Issue 3. pp. 21-26.

[14] Karygiannis, T. and Owens, L. (2002). **Wireless Network Security 802.11, Bluetooth and Handheld Devices. Computer Security: *NIST Special Publication 800-48.***

[15] Abiona, O.O, Aladesanmi, A.T., Onime, C.O., Adewara, K. and Kehinde, L.O. (2007). **Enhancing University Wireless Network Security Using Peer-to-Peer Authentication Security Model. *Proceedings of the 2nd International Conference on Application of ICT to Training, Research and Administration, AICTTRA* 2007, Ile-Ife, Nigeria, 146-155.**

[16] Haataja, K. (2000). Security in Bluetooth, WLAN and IrDA: A comparison. Retrieved from http://www.cs.uku.fi/research/publications/reports/A-2006-1.pdf

[17] Mateti, P. (2005). The Handbook of Information Security, Ed. Hossein Bidgoli, John Wiley & Sons, Inc., 2005.

THE JOURNAL OF COMPUTER SCIENCE AND ITS APPLICATION
AN INTERNATIONAL JOURNAL OF THE NIGERIA COMPUTER SOCIETY (NCS)
Vol. 19 No.1, June, 2012

nigeria computer society
www.ncs.org.ng.

A SECURED PROTOCOL FOR PREVENTING ONLINE DICTIONARY ATTACK

Onashoga, S. Adebukola and Akinwale, A. Taofik
Dept. of Computer Science, Federal University of Agriculture, Abeokuta, Ogun State, Nigeria
Corresponding Author: **bookyy2k@yahoo.com**

ABSTRACT

The use of passwords is a major point of vulnerablility in computer security as passwords are often easy to guess by automated programs running dictionary attacks. Several attempts have been made by researchers in order to counter online dictionary attack but with one drawback or the other, for example storing passwords in plain text, denial of service and so on. This paper employs Diffie-Hellman Key Exchange Scheme to impose more challenges to the attackers with three guesses as against one in the referenced protocol. Two way hash functions were used to generate two indices which were encrypted so that the attackers would not be able to compromise with the Server. The new scheme requires a high computatioal time of 1.743years as against 1.6625years proposed by other researchers for discouraging online dictionary attacks.

Keywords: authentication, identification, hash functions, online dictionary attacks, disrcete logarithm theorem.

1.0 INTRODUCTION

One of the first steps toward securing an IT system is the ability to verify the identity of its users. The process of verifying a user's identity is typically referred to as user identification and authentication. Passwords are the methods used most often for authenticating computer users, but this approach has often proven inadequate in preventing unauthorized access to computer resources when used as the sole means of authentication. Determining if a user is authorized to use an IT system includes the distinct steps of identification and authentication. Identification concerns the manner in which a user provides his unique identity to the IT system. The identity must be unique so that the system can distinguish among different users. Depending on operational requirements, one "identity" may actually describe one individual, more than another.

Authentication is the process of associating an individual with his unique identity, that is, the manner in which the individual establishes the validity of his claimed identity. There are three basic authentication means by which an individual may use to authenticate his identity. These are:

- Something an individual knows(e.g a password, Personal Identification Number (PIN), the combination of a set of facts from a person's background).
- Something an individual possesses(e.g a token or card, a physical key to a lock)
- Something an individual is (e.g personal characteristics or "biometrics" such as a fingerprint or voice pattern) [4].

The introduction of passwords which only the customer will possess was to avoid identity theft, monetary fraud, and loss of privacy. Obtaining passwords is a common and effective attack approach because they are the most commonly used mechanism to authenticate users to an information system. The following are types of password guessing attacks:

i. Brute force : Brute-force password guessing means using a random approach by trying different passwords and hoping that one works.

ii. Dictionary attack : A dictionary attack is one in which a dictionary of common passwords is used in an attempt to gain access to a user's computer and network [7].

iii. Hybrid attack : An hybrid attack is a combination of the dictionary attack and the brute force attack. It

combines a wordlist with some mutations on the entropy.

Another direction in strengthening password-based schemes is to protect the schemes from being broken even if the passwords can be easily guessed. The dictionary attacks are classified into offline dictionary attacks and online dictionary attacks. By eavesdropping communications between the client and the server, the offline attacks try all possible passwords to find the correct one without direct interaction with the server. On the contrary, in online attacks, each guessed password requires the participation of the server to verify if the guess is correct [11]. Offline attacks can be countered by cryptographic mechanisms, i.e. SSL protocol or many other password-based authentication protocols secure against offline dictionary attack [3].
The measures that are commonly used against online attacks in practice are quite simple. One measure is delayed response to a login attempt in order to slow down attacks; the other is account locking after several failed login attempts [11]. However, these two methods not only maybe vulnerable to denial of service attacks, but also cannot prevent global online dictionary attacks. In global attacks, an adversary can try many user accounts simultaneously with one attempt for one account, or several attempts below the account-locking threshold for one account. It is easy to see that the above two measures can be circumvented by global online dictionary attacks.

Several other strategies, apart from the aforementioned, have been proposed in countering dictionary attack such as challenge response system, use of Reverse Turing Test (RTT), Hash Card [11] and so on. This paper focuses on designing a suitable algorithm against dictionary attack using the Hash Card approach. In Hash Card approach, the client is asked to solve a computational problem before getting the login OK or Error response from the server. The computational problem is to find the pre-image of a cryptographic hash function. The main drawback of this approach is that the clients' computation capacity is varied, and some of them are too slow to solve the problem in acceptable time [11]. In order to overcome this problem, a formal description that justifies the proposed model is described with the presentation of the computational time for an attacker to break in.

The rest of the paper is organized as follows: Section 2 reviews related works. Section 3 discusses the improvement and modification over the protocol proposed by Goyal et. al. [10] and section 4 shows the result while section 5 concludes the work.

2.0 RELATED WORKS

This section reviews extant researches in this direction as described in the subsections.

Existing Strong Password Authentication and Key Agreement (SPAKA) protocols protect passwords from passive eavesdropping-offline dictionary attacks, but not from active online dictionary attacks. [15] eliminates the threat of initiation of parallel attacks in SPAKA by requiring the client to solve a puzzle with an aim to keep the attacker busy and reduce the number of sessions that an attacker can initiate Their protocol, ($SPAKA^{+}$) strengthens password-based authentication protocols and helps prevent online dictionary attacks as well as many-to-many attacks common to 3-pass SPAKA protocols. $SPAKA^{+}$ significantly increases the computational burden of an attacker trying to launch online dictionary attacks, while imposing negligible load on legitimate clients as well as on the authentication server.

[9] introduced a Server-assisted generation of a strong secret from a password in which passwords are effectively protected through distribution of trust across multiple servers. The scheme of Ford and Kaliski can also be called password hardening mechanism. In their system, a client parlays a weak password into a strong one through interaction with one or multiple hardening servers, each one of which blindly transforms the password using a server secret. In essence, the client in their protocol obtains what may be regarded as a function 8_i blindly evaluated by each of the servers with which the client is interacting. The function in question is based on a secret unique to each server and user account. The client combines the set of shares into a single secret 8_i a strong key that the user may then use to decrypt credentials, authenticate herself, and so on [9].

A protocol to counter online dictionary attacks was proposed by looking at the various instances of online dictionary attacks [10].
This is a four pass protocol and only hash computations are employed throughout the protocol. Two out of four messages are simple message exchange without any encryption. The remaining two messages involve hash computation: once by the user and once by the server. The protocol presents a challenge for the

user by the server and the user can login only after cracking the presented challenge which requires some computation time. This computation time can be easily increased or decreased by the server at will. In the protocol, hashed passwords of users were stored on a database, which can be easily compromised if an attacker has knowledge of the hash algorithm. Also, if these passwords are stored in an encrypted form, an attacker might get a pre-computed hash of passwords and compare with the encrypted passwords in the database thereby getting the actual password that was used. The proposed protocol is not complex enough going by the computational time it took to break into a resource.

Goyal et. al's scheme is summarised below:

Message 1. Alice ⟶ Bob: Alice
Message 2. Bob ⟶ Alice: H(r, R), R, H(H(r, P), Alice, K_{Bob}, n)
Message 3. Alice ⟶ Bob: Alice, H(r, P), MAC
Message 4. Bob ⟶ Alice: Success/Fail

[11] considered a scheme based on RTT by presenting a formal model of online work of dictionary attacks based on a decision function as an improvement over [12, 13] . RTT is a method to distinguish human being from computer programs e.g. CAPTCHA (Completely Automated Public Turing Test To Tell Computers and Human Apart). The decision function, D_3 is defined as a probability function such that for every username stored in the database, there exists a secret key k_i. As part of the definition of D_3, a hash function of the username, password and k_i is created. On login attempt, a user enters a username and a password, the server now checks whether the username is valid and whether the password is correct for the username. A user is asked to answer an RTT if $D_3 = 1$, else denied access if $D_3 = 0$. The major contribution of these authors lies in the presentation of a formal model with different assumptions. The limitation of this work is in the storage of the plaintext of the username and password before a hash function is defined. The system could be compromised if an attacker is able to access the unsecured database. Also, the work majorly focused on defeating attacks by automated programs and not on human users.

A distributed dictionary attacks are usually executed in a network environment either over LAN or WAN. They are also distinguished as online or offline attacks and may be executed in both cases depending on the target. The authors of [14] typically describe a distributed dictionary attack for a social network. It analyses the attack amplification over time as well as its geographical distribution. It gives different scenario of dictionary attacks considering the "rush hour" period. The experiment as carried out by the authors involves performing a distributed dictionary attack on a targeted server. The time stamps for the different experiments were recorded.

Hence, based on these weaknesses and strength of these works, a new protocol is designed to efficiently counter online dictionary attack.

3.0 METHODOLOGY

The proposed protocol involves using the notion of Disrcete Logarithm Theorem which is used in Diffie-Hellman scheme [5] to authenticate the user's identity. Section 3.1 describes the theorem. In section 3.2, we modify the protocol by introducing 3 parameters instead of 2 used by [10] in order to make the protocol more difficult for an attacker to break in. The encryption technique is based on the standard AES [17].

3.1 Discrete Logarithm Theorem

In discrete logarithm theorem, if g is a primitive root of , then the equation

$$g^x \equiv g^y \pmod{n} \quad holds$$
$$\Leftrightarrow \quad x \equiv y \pmod{\phi(n)}$$

Proof:

$$x \equiv y \pmod{\phi(n)}$$

Suppose that $x = y + k\phi(n)$ *for some integer k*

$$therefore: g^x \equiv g^{y+k\phi(n)} \bmod (n)$$
$$\equiv g^y . g^{\phi(n)k} \bmod (n)$$
$$\equiv g^y . 1^k \bmod (n)$$
$$\equiv g^y \bmod (n)$$

therefore, if

$g^x \equiv g^y \pmod{n}$ *then we must have*

$x \equiv y \pmod{\phi(n)}$

$$if\ x \equiv y (\mathrm{mod} \phi(n))$$

$$there\ exists\ an\ integer\ s\ such\ that$$

$$a = b + sm$$

$$so\ that\ a - b = sm$$

$$then\ a^k - b^k = (a-b)(a^{k-1} + a^{k+2}b + ... + ab^{k-2} + b^{k-1})$$

k = 2 is also a multiple of m, it follows that

$$a^k \equiv b^k \ (\mathrm{mod}\ m)$$

3.2 The Modified Protocol

The following notations are used: U stands for the user and S for the server; It is assumed that User, *U* is registered with Password, *P*; Prime number, *M* and Username, K_{user}.

K_{server} = secret key of the server.
N = number of unsuccesful login attempt,
r = a 20-bit random number,
R = a 128-bit random number,
E() = encryption function,
MAC = message authentication code,
H(H(A)) = Two way hash value of A, where H(A) is based on Robert, J. Jenkin's standard hash function and H(H(A)) based on Peter J. Weinberger's standard hash functions as used by [1].

The different passes of the protocol after this modification are as follows:
Message 1: U ⟶ S: User
User asks for a request to login.

Message 2: S ⟶ U: E(H(H(r, P, M))), R, MAC
MAC = C, H(H(r, P, M), User, K_{server}, n)

$C = H(H(r^{Kserver} \bmod M, R, M)), R, M$
The Server sends User a challenge, MAC involving another challenge, C.

Message 3: U ⟶ S: User, E(H(H(r, P, M))), MAC

In order to get the MAC, User calculates the reply C as follows:
$C = H(H(r^{Kserver} \bmod M)^{Kuser} \bmod M)$
and sends C to the Server

Message 4: S ⟶ U: Success/Fail

The server with the knowledge of K_{user}, M and MAC, also computes C

$$C = H(H(r^{Kuser} \bmod M)^{Kserver} \bmod M)$$

and compares it with the value received from the User. If the two values match, the User is authenticated else it goes back to login again.

Note:
$H(H(r^{Kuser} \bmod M)^{Kserver} \bmod M) = H(H(r^{Kserver} \bmod M)^{Kuser} \bmod M)$
Both User and Server have arrived at the same value according to Diffie-Hellman Key Exchange. Moreso, K_{Server}, K_{User} and $r^{KserverKuser}$ and $r^{KuserKserver}$ are kept secret between the User and Server.

3.3 Proof of the proposed protocol

Goyal et al. (2005) protocol takes 5 seconds approximately by the User to compute the value of r. Moreso, it is also proved that it would take offline attackers 52, 428, 800 seconds (1.6625 years) since they do not know the value of P as well as r.
In this new function, two way hash functions are used to hash password, prime number and user secret key to derive two indices of hash values which are encrypted in the database.The attacker must know the encrypted hashed values of the three parameters as against two.

For online dictionary attacks, it will take the probability of ? to guess the three challenges. Table 1 illustrates the chance for attackers to gain access into the system and the expected value is

$$E(X) = \sum P(X = r) r$$

= 3/2 which is very high.

Table 1: Chance for the Attackers

P=password	Key =Server	M=prime number	Attacker's chance to gain access
0	0	0	Attacker fails to obtain any challenge
0	0	1	Attacker obtains only prime number challenge
0	1	0	Attacker obtains Server key challenge
0	1	1	Attaker fails to obtain password challenge
1	0	0	Attacker obtains passwrd challenge
1	0	1	Attacker fails to obtain Server key challenge
1	1	0	Attacker fails to get prime number challenge
1	1	1	Attacker gains access into the system

Since the attacker does not know the values of r, k and M, to find the correct value of C from message 2, he will require $2^{20}.2^{20}$ x n hash computations. Taking the standard value of n to be 10 millions as suggested by [10], the time required will be

$R = 2^{20}.2^{20} X\ 10{,}000{,}000 X\ 0.005 X\ 0.001$
$= 549755813880\ seconds$
$= 1.743\ years$

and the time to compute prime number and the key of the user are as follows:

K_{user} = 10,000,000 X 0.005 X 0.001
= 50seconds
Prime number = 10,000,000 X 0.005 X 0.001
= 50seconds
Total Time = (5.4975580s + 50s + 50s)
= 105.4975580s
= 3.345 years

The challenge for users to compute r is 5seconds and for our new scheme is 15seconds. For attackers to guess P and r using the proposed protocol, it will take 1.743 years. To guess the three parameters, it will take 3.345 years.

4.0 IMPLEMENTATION AND RESULTS

The proposed scheme is implemented on a pentium III intel microprocessor with Microsoft C# as the programming language. 150 data sample of users (90 legitimate and 60 illegitimate users) were tested on. On login, the user enters his name, password and an agreed prime number which has already been stored in the database, so as to discourage any permutation of characters. Figure 1 shows the login interface of the prototype of the proposed protocol during one of the testing phase. The Time shown indicates the least time it takes to compute r for that particular username displayed.

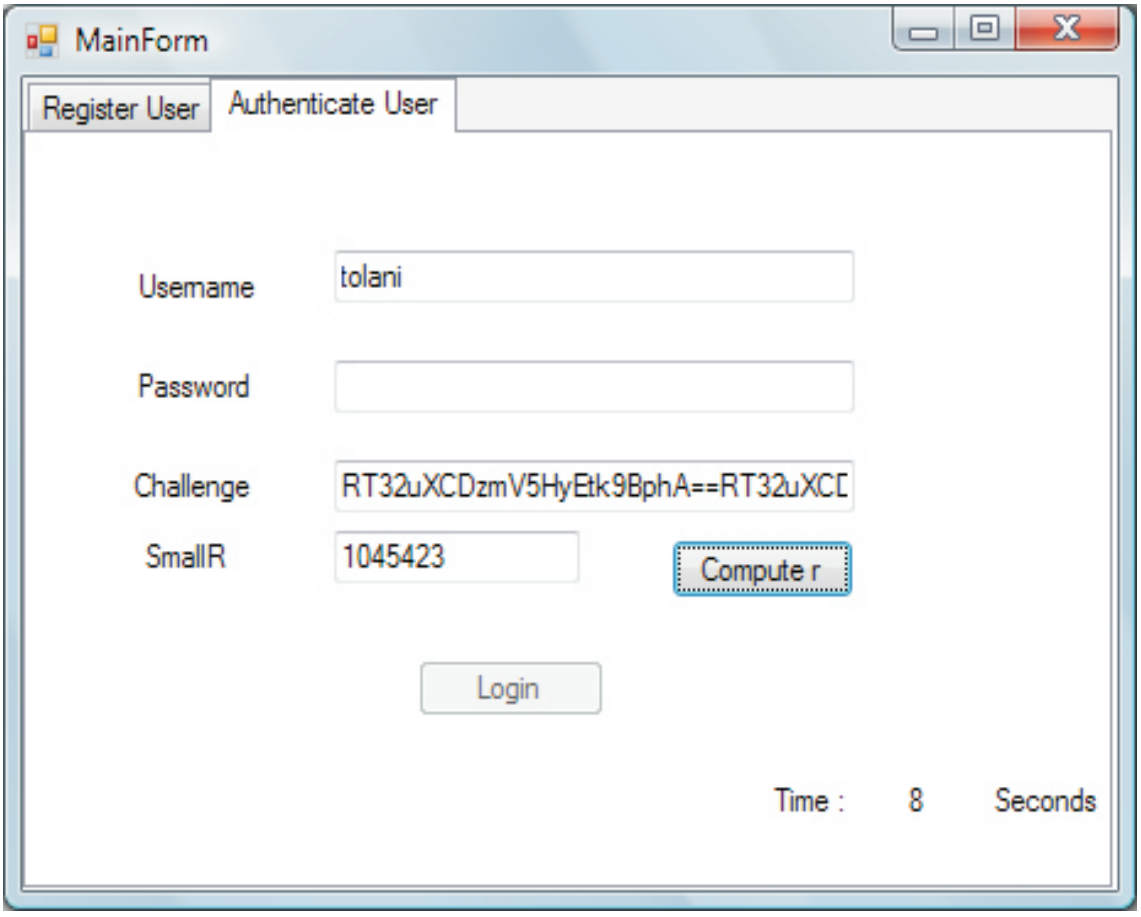


Figure 1: A Login interface

The result shows a time between 8 and 12 seconds for the legitimate users while the illegitimate ones were not given access.

5.0 CONCLUSION

It is safe to invest much on security, since prevention is better than cure. The paper made use of Diffie-Hellman to improve on Goyal et al. scheme. The improvement used two-way hash functions to compute the three parameters posed and their hash values were encrypted so that attackers would not be able to compromise with the server. The server at its own end makes use of an infix salt added to the password, this acts as a way of discouraging permutations that could be made by attackers. The whole process is a way forward to discourage online dictionary attack. The improved protocol proposed is very effective in preventing dictionary attack. Further future work in consideration is modifying this scheme for other attacks.

REFERENCES

1. Akinwale, A. T. and Ibharalu, F. T. (2009). "The Usefulness of Multilevel Hash Tables with Multiple Hash Functions in Large Database", Journal of Computer Science Series, Vol 7, No. 1. pp 11 20.
2. Arora, A. (2007). "Statistics Hacking Exploiting Volnerabilities in News Websites". International Journal of Computer Science and Network Security, Vol. 7, pp 342 - 347.
3. Bellovin, S.M., Merritt, M. (1992). Encrypted Key Exchange: Password-based Protocols Secure Against Dictionary Attacks, *Proceedings of the 1992 IEEE Computer Society Conference on Research in Security and Privacy, 1992*, pp 72-84
4. Murali, K. R. D. (2007). "Design and Analysis of hash Functions", Master's thesis submitted to the School of Computer Science and Mathematics, Victoria University, 2007
5. Carts, D. A. (2001). "A Review of the Diffie-Helman Algorithm and its use in Secure Internet Protocols", A report from SANS Institute Reading Room, Nov. 2001.
6. Cormen, T. H., Leiserson, C. E., Rivest, R.L. (1992). "Introduction to Algorithms", MIT Press Cambgridge, Massachusetts, London, England, 1992.
7. Cole Eric, Krutz Ronald & Conely James(2005). "The Security Threat and the Response" *Network Security Bible,* Pg 592 623 .
8. Computer and Technology News Paper, USA(2008). http://www.computerworld.com/
9. Ford W. & Kaliski B. S (2005) "Server assisted generation of a string secret for a password". *In proceedings of the IEEE 9th International Workshop on Enabling Technologies (WETICE)*
10. Goyal V, Kumar V, Singh M, Abraham A. & Sanyal S. (2005). "A new protocol to counter online dictionary attack". *Elsevier Journal of Computer and Security.*
11. He, Y. & Han, Z. (2009). "User Authentication with Provable Security against Online Dictionary Attacks". *Journal of Networks*, VOL. 4, NO. 3, May 2009, pp. 200- 207
12. Murali, K. R. D. (2007). "Design and Analysis of hash Functions", Master's thesis submitted to the School of Computer Science and Mathematics, Victoria University, 2007
13. Pinkas, B. & Sander, T, (2002). "Securing Password against Dictionary Attack". *Proceedings of the 9th ACM conference on Computer and communications security, ACM press*, 2002
14. Oorschot, P.C.V., Stubblebine,S. (2006). "On Countering Online Dictionary Attacks with Login Histories and Humans-inthe-Loop". *ACM Transaction on Information and System Security, Vol. 9, No.3, August 2006,* pp235-258.
15. Soroka, E. V. and Iracleous, D. P. **(2010). Social Networks as a Platform for Distributed Dictionary Attack** , Recent Researches in Communications and IT, pp 101 106.
16. Wang P, Kim Y, Kher V & Kwon T. (2005). "Strengthening Password Based-Authentication Protocols against Online Dictionary Attacks". *Computer Science and Engineering, University of Minnesota-Twin Cities, Minnesota, USA and School of Computer Engineering, Sejong University, Seoul, Korea.*

Joshua Holden & Rose-Hulman (2010). "A Simplified AES Algorithm", Note retrieved from http://www.rose-hulman.edu/~holden/Preprints/s-aes.pdf

THE JOURNAL OF COMPUTER SCIENCE AND ITS APPLICATION
AN INTERNATIONAL JOURNAL OF THE NIGERIA COMPUTER SOCIETY (NCS)
Vol. 19 No.1, June, 2012

nigeria computer society
www.ncs.org.ng.

A Conceptual Trust Model for Managing E-Commerce Environment

Vincent, O. R. and Agbola O. E.
Department of Computer Science,
University of Agriculture, Abeokuta, Ogun State, Nigeria
vincent.rebecca@gmail.com and agbolaoe@yahoo.com

ABTRACT

E-commerce helps businesses to increase production flexibility by ensuring timely availability of components from suppliers. However, of paramount concern is the issue of trust. Some trust models such as Pretty Good Privacy (PGP) and Public Key Infrastructure based on X.509 (PKIX) are based on the notion of delegation whereby one entity gives some of its authority to other entities. The problems with these models are: leaked public-key certificate, false owner's identity and how to manage the details about certificate. This study presents a flexible trust model based on human interactions. It involves dynamic evolution of trust between entities which is independent of the usage of certificates from trusted third parties. We describe trust in three folds: the default, initial and final trust. A prototype of this model was implemented using ASP.NET and C#. The result shows that while initial trust bestowed on a consumer is unstable and unpredictable, final trust of a consumer is partially stable and therefore fulfils integrity, competence and benevolence.

Keywords: E-Commerce, Trust, Integrity, Open Distributed environment, Trust Management.

1.0 INTRODUCTION

In our world of Information Technology (IT), e-commerce is seen as an electronic business application aimed at commercial transactions. It entails information about products, events, services, suppliers, transaction advanced search algorithms, transactional security and authentication, e.t.c. [10]. E-commerce offers customers convenient shopping methods for products, information and services, electronic banking, and personal finance management. Through e-commerce, it is easier for consumers to find their desired products and services that match their requirements, and compare prices [21]. Several business models have been developed to support various customers' needs. Among them are online portals, content providers, transaction brokers and community creators.

Lack of physical contact and face-to-face communication has limited the consumer's ability for assessing the quality and suitability of these products [12, 15]. The absence of a live social interaction between a buyer and a seller has made quality assessment of products and services difficult in the e-commerce environment [14, 23]; thereby resulting in inability to assess the integrity and benevolence by the customer. The lack of control and the limitation of tracking of the purchase procedures after sending information from the consumer to an e-commerce site is also a strong challenge to trust. Therefore, the level of uncertainty in e-commerce environment, which is higher than the traditional commerce, has made trust a very important issue in e-commerce [11, 20].

Recently trust has been recognized as one of the main factors affecting electronic commerce. According to WISTA International E-Commerce Survey, trust (26%) is the most important barrier to electronic commerce in 27 surveyed countries. The survey recognized "trust as significant stumbling block in electronic commerce development, due to the fact that electronic commerce is global and its international reach means that participants must deal with unknown or anonymous individuals and companies". The survey established the impact of trust in electronic commerce (42%, moderately 35%) [9]. Trust has been identified as an important component in a security infrastructure for communication between two parties.

In traditional commerce, trust is created through face to face communication and over a

period of time whereas in the online commerce time is dramatically compressed. Senses are also used to evaluate the quality of a product and its compatibility with people's needs. In contrast, with online shopping the consumer has to trust what he/she is seeing on the web vendor interface and vice versa, rather than being able to examine the product through her or his senses [3, 6, 7, 22]. This is called initial trust. Initial trust has been recognised as a vital factor for many types of e-based commerce. This is due to its role in creating initial relationships with customers in the business to-customer commerce [13,16]. Initial trust is defined as "one that invokes and maintains an initial relationship before the relationship becomes a committed one" [17, 22].

Though, the Internet has been termed an untrusted environment for commerce activities, a desired trusted environment can be achieved by creating a shopping environment that will constitute some unique and identifiable set of rules to determine customer trust when transacting [1,4,21]. The main goal of this work is to develop a trust model for managing e-commerce environment which will be independent of the usage of certificates from trusted third parties and also providing a platform where both the buyers and the sellers are protected during online transactions.

2.0 CURRENT TRUST MODELS

Some trust models have emerged as public key technology and have grown beyond local domains to satisfy needs of larger and more diverse communities, such as PGP trust web. These systems are based on the notion of delegation, whereby one entity gives some of its authority to other entities [2,9,15]. The two well-known certificate systems are those of PGP and Public Key Infrastructure based on X.509 (PKIX).

PGP uses a convenient means of using trust, associating trust with public keys, and exploiting trust information. PGP employs a structure called key ring to implement an "introducer mechanism". Similarly, each individual must create his own key pair and disseminate his own public key. No central infrastructure needs to be developed. This model works very well for small groups, who have pre-existing relationships, but does not scale well for large groups especially where consistency in trading is required. Communication of certificate status to relying parties is also very difficult with this model [8,16].

The PKIX authentication framework attempts to solve the same part of the trust management problem that PGP's introducer mechanism attempts to solve, namely the need to find a suitably trustworthy copy of the public key of someone with whom one wants to communicate [10, 20]. However, PKIX differs sharply from PGP in its level of centralization of information. The PKIX framework requires that everyone will obtain certificates from a certification authority (CA). Relying parties who share a common CA can trust each other directly. Certificates from different CAs cannot trust each other unless there is pre-trust relationship between the CAs. It is impossible to organize all CAs into a global "certifying authority tree" and to have keys signed by CAs with a common ancestor in this global tree. However, the primary concern is that user must manage all the details about certificates.

The Independent Trust Intermediary Service (ITIS) is a facility for distributing certificates of CAs in a manner that ensures their authenticity and integrity. Multi-ITISs connect each other to form a trust web. Relying party who consumes the service of a selected ITIS can deem it as "trust anchor" to form a trust chain. Relying parties offload the burden of trust management to the selected ITIS and maintain a few certificates of their selected ITISs [5]. The concern is that ITIS will first evaluate the registration information to make a decision before accepting these certificates. This give lots of rigorous searching before transaction communication.

Erickson *et al* (2010) described the issues of trust in online retailing and agreed that the problem has to do with the absence of face-to-face contact and other contextual factors that usually enhance confidence in an exchange. Institutional credibility solutions such as external certifications, user reviews, and brand building activities have helped to build trust in virtual environments, resulting in the recent rapid growth of e-retailing [3,6]. The work compares trust levels and more specific aspects of trust across various items related to institutional credibility and community.

This paper proposes a trust management and assessment model that is based on reliable evidence about systems and remote transaction partners in computer networks. This is imperative to correct some of the identified problems.

3.0 A TRUST SCHEME FOR MANAGING E-COMMERCE ENVIRONMENT

In this paper, a typical e-commerce site is presented with a trust induction mechanism. Trust mechanism is the first acceptable condition for any

e-commerce site to operate. There is a general trust that appropriate security measures have been taken to protect businesses and consumers from misuse and fraud in the network. *The procedure involves the assumption that communication between hosts is by the use of public and private keys for authentication. Each host defines its own levels of access depending on the use of its resources. A secure host may allow very limited access while a host of an e-business may allow greater access to its resources. Trust is usually built up over time, starting from a predefined level between two entities that communicate. The fluctuations in trust level could lead to an independent scheme of certification, and is based mostly on mutual interaction.*

A network environment with at least four hosts is described. Host A is represented by H_A and the trust between hosts A and B as T_{AB}. Assuming that H_A communicates with H_B, H_C and H_D. The trust level T, that H_A has with H_B is T_{AB}, the one with H_C is T_{AC}, while that of H_D is T_{AD} and so on. It should be noted here that the trust level may not be symmetric, that is, T_{AB} may not be same as T_{BA}. If H_A trusts H_B at T_{AB}, and H_B trusts H_C at T_{BC}, then, H_A would trust H_C at $T_{AB} \times T_{BC}$, whereas if H_A communicates with H_C directly, the trust level is T_{AC} which may not be same as $T_{AB} \times T_{BC}$. The interactions via neighbouring hosts reduce trust level, and therefore are not desirable. Hence, this scheme encourages direct interactions between hosts.

The trust value has the range between 0 and 1, where 0 indicates no trust and 1 means full trust. If H_A trusts H_B at 0.9 level, and H_B trusts H_C at 0.9 level, then H_A trusts H_C at 0.81 level. This value is used as the initial level of trust between H_A and H_C when the first contact is made. However, if H_A directly interacted with H_C, then the start trust level is 0.81 and this can go up or down depending on the results of interaction between them. If this chain of indirect interaction were to increase, then the resulting trust level will go down, as it happens in case of human interactions. The Trust metric adapted from [17] is defined as:

$$T_{AB} = T_0 + \frac{\sum_{i=1}^{n} w_i E_i}{\sum_{i=1}^{n} w_i} + f(t) \quad (1)$$

where T_0 is the base level trust or the default value of the trust between the host A and B. The trust parameter takes values between 0 and 1. E_i are the events called services that the visiting host carries from the host; w_i are the weights assigned to the events. I is the initial trust value given to the consumer. The tracks of event E_i records are kept by the host H_B. The weights w_i for the event E_i are defined by H_A and each host defines its own weights depending on its needs. The weighted events are summed over n events. Since the weights can be negative, the trust parameter can go down as well.

It is assumed that the human receives a certain experience at each time point, the E is the experience gained as a result of events that occurred and is it calculated directly with time. The experience is assumed to reside on the interval [0, 1]. The term f(t) is included to reflect any time-dependent activity to suggest gain or loss of reliability. If the host is not accessible due to network problem, then the trust level is reduced. At this stage, there is no association of any trust parameter to the path that the host may take to reach its destination. The trust level can go down temporarily if the route to a host is down. If this state continues then the reliability of the host goes down. This would be reflected in the trust level. The algorithm for the trust metric in equation 1 is given as follows:

A generic Algorithm for Trust in E-commerce Environment

Inputs: W_i and E_i
Outputs: T_{AB}
Step 1: Begin
Step 2: Initialize SumWeightEvent to be = 0
Step 3: Initialize SumWeight to be = 0
Step 4: For i = 1 to n
Step 5: SumWeightEvent = SumWeight + ($w_i * e_i$)
Step 6: End
Step 7: For i = 1 to n
Step 8: SumWeight = SumWeight + w_i
Step 9: End
Step 10: $T_{AB} = T_0$ + (SumWeightEvent/ SumWeight) + f(t)
Step 11: End.

Figure 1 shows the trust metric framework for this scenario. If a host H_C sends a for malicious activity to H_D. H_C may have defined H_D as a trusted host but H_D may note that H_C is not a trusted host if it can find out malicious activity by its attributes. Eventually, after many interactions, H_C would be noted as an untrusted host by many hosts. H_S denotes a strange host hoping to make transaction within the network. The scheme does not require authentication by trusted third party in terms of certificates. The trust

is based on one-to-one interaction and is developed over time. Each destination host should be associated with a measure of its reliability. Figure 2 shows the metric flow for consumers.

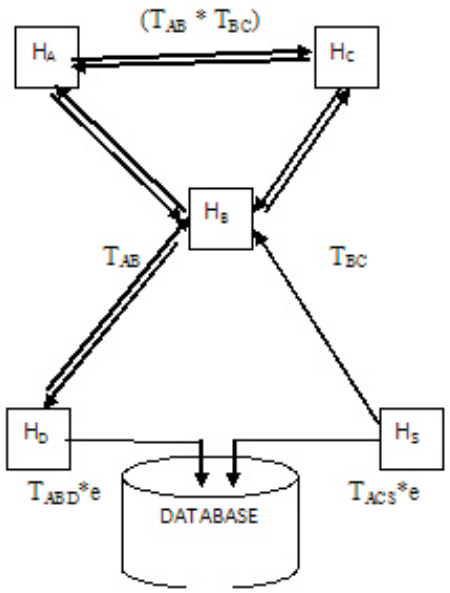


Figure 1: Trust Metric Framework

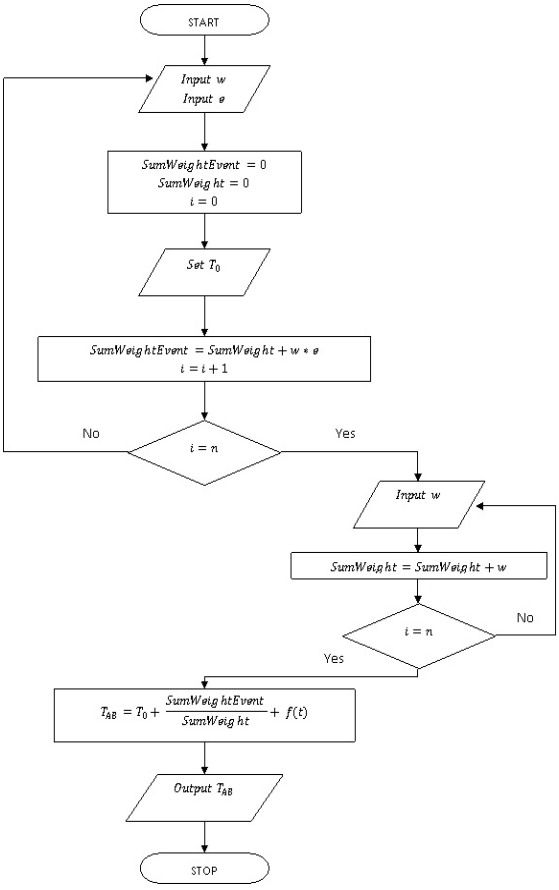


Figure 2: A Trust Metric Flow for Consumers

4.0 A PROTOTYPE E-COMMERCE ENVIRONMENT

The prototype is developed by using ASP.net and C-Sharp which were used to simulate the design. The .NET environment is used because it allows e-business issues such as interaction between the buyer and the seller. A prototype Internet Information Server was configured to provide for efficient network service. An e-commerce environment is created where customer could buy and make payments on the goods bought at the home page site. When customer registers his intention for transaction, the system immediately recognizes the address of host. On registering, the menu page which can be used by both the administrator and the customer appears. From the menu page, the customer could click on the product pack page which makes the customer to see the product on sale and where the customer could also choose from the packs of products. Here, the customer choose from the list of products and then add them to cart, after he might have chosen from the packs of products in the previous page.

Figure 3: The Cart Page

Figure 3 shows the cart page where the customer can edit the quantity of products that is to be bought or even delete products not to be purchased any longer. The customer can log out after and then order the products. At the administration page, the administrator can decide to add new products or view the products that are on for sale. The administrator can track the state of any transaction. Figure 4 shows the product page where the

products bought are displayed and total price calculated. The trusts on the transactions made are computed based on the way the products were chosen in percentage. The trust percentage fields in figure 4 shows the flexibility of the scheme, whereby the host can decide on the initial trust for the customer. The administrator can edit any field of product if there is any mistake when adding a new product.

Figure 4: Product Edit Page

Figure 5: Customer Order Page

The customer ordered page in figure 5 shows list of the customers on the site and it is where the administrator decides either to lock the account of the customer if the trust percentage is very low or unlock if otherwise. On the next entry of the customer to site, if his/her account has been locked by the administrator, the system will show the restriction message from entering to the site.

4.2 Trust Level Evaluation

Table 1 shows the trust level evaluation of the designed e-commerce site. The Initial trust was measured using the trust metric as the condition for the first contact. The initial trust represents the weight (w_i) of each events and the final trust was also measured after orders have been made. This table 1 shows the product-*id* representing each event (E_i) that occurred in the transaction, registering initial trust. The order-*id* represents each order made by the customer, with the final trust for each order. This final trust increases and decreases depending on each order made by the customer or a visiting host.

Table 1: TRUST LEVEL EVALUATION TABLE

TRUST LEVEL EVALUATION			
PRODUCT-ID	INITIAL TRUST (in percentage)	ORDER-ID	FINAL TRUST (in percentage)
1d5ad121	60	43ec4c75	1.34
4f113c07	10	569ccd2e	1.3.4
632e635d	20	573332ec	0.7
7a5bd3e3	80	5cb1378d	4.49
9a437cf4	70	a465d8dd	1.34
e68c6997	70	c47a0ed8	1.34
eb30f557	90	c601a481	1.34
f33de02b	80	d57d501b	2.21

4.3 Trust Evaluation Graph

Figure 6 shows the graph of customer trust against products displayed. This is done to measure the initial trust of the customer. Figure 7 shows the graph of trust against the product ordered for. In figure 6, it was found that the initial trust of customers is never stable; it changes from customer to customer. The drastic variation and fluctuations in the initial trust shows that a customer can never be judged by the initial trust. In figure 7, however, it is found that the final trust of a customer may be stable for some time. However, this stability may not count for future transaction.

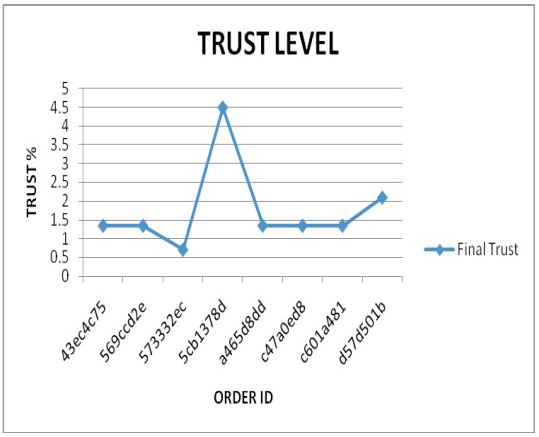


Figure 7: Trust against Product Ordered

5.0 CONCLUSION

This trust model is based on human experience of trust. The level of access given to the visiting customer depends on the initial trust the host has for the visitor. When a customer visits an e-commerce site for the first time, it is expected that the customer has a little trust value. This trust value can increase or decrease depending on the nature of interactions called events.

Another customer may determine a different trust level from the same set of actions as their requirements may be different; these variations are called the weights. If a strange customer applied to the same site, two solutions may be applied: firstly, a default trust value may be assigned to the stranger and start to build up trust from there; secondly, if the customer could recognize a well trusted customer, then the stranger will be given a benefit of doubt to make transaction. In this case, the trust value is a function time and the actions for the customer in question. Obviously, positive interactions gives higher trust. In general, the host has the flexibility to select the weights as well as the functional form of the actions to determine its trust level. However, the general trust value given to any networked environment is known as trust propensity.

The model described in the paper differs from other models in literature. First, it requires neither certificates nor the recommendations from third parties. This system will ease the stress of looking for recommendations from third parties. In addition, once the account is created, it can be used several times and for several purchases until the initial trust percentage is less than 50%. The trust measures in this model are dynamic and flexible parameters. It is based on one-to-one interactions. Trust parameter can also increase or decrease depending on the activity of the trusted entity.

REFERENCES

[1] Capra, L. (2004), "Engineering Human Trust in Mobile System Collaborations", Proc of the 12th International Symposium of the Foundations of Software Engineering, 107-116

[2] Carbone M., Nielsen M. and Sassone V., (2003) "A formal Model for Trust in Dynamic Networks", Proceedings of *1st* International Conference on Software Engineering and Formal Methods Brisbane, Australia, 54-63.

[3] Corritore, C. L., Kracher, B. and Wiedenbeck, S. (2003): On-line trust: Concepts, evolving themes, a model, International Journal of Human-Host Studies, 58, 737-758.

[4] Cyr, D., Hassanein, K., Head, M., and Ivanov, A. (2007). "The Role of Social Presence in Establishing Loyalty in E-Service Environments", *Interacting with Hosts,* 19, 43-56.

[5] Eastlick, M. A., Lotz, S. L., and Warrington, P. (2006)."Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment", *Journal of Business Research,* 59, 877886.

[6] Erickson, G. S., Komaromi, K, and Unsal, F. (2010), " Sociol Networks and Trust in E-commerce", International Journal of Dependable and Trustworthy Information Systems, 1(1), 1-15.

[7] Heijden, H. v. d., Verhagen, T. and Creemers, M. (2003): Understanding online purchase intentions: contributions from technology and trust perspectives, European Journal of Information Systems, 12, 41-48.

[8] Holsapple C. W. and Sasidharan S. (2005). "The dynamics of trust in B2C e-commerce: a research model and agenda", *Information Systems and E-Business Management*, 3(4), 377-403.

[9] Huang, S., Li, C. and Lin C. (2007), "Trust Model for E-commerce", Issues on Information Systems, 8(2), 63-69.

[10] Ketchpel S.P. and Garcia-Molina H., (1996), "Making Trust Explicit in Distributed Commerce Transaction", Proceedings 16th Int'l

Conf. Distributed Computing Systems, IEEE CS Press, Los Alamitos, Calif, 45.

[11] Khandelwal, A. S. (2011), "Enhancing Trust Beliefs in E-commerce Through Whitelist Website Security Paradigm", *Indian Journal of Computer Science and Engineering*, 2(2), 248-254.

[12] Khazaei, A. (2006), **The Impact of Initial Trust on Consumer Behaviour in E-Commerce (B2C);** A Study submitted in partial fulfilment of the requirements for the degree of Master of Science in information Management at the University of Sheffield, United Kingdom.

[13] Kim, B and Han I. (2009), " The role of trust belief and its antecedents in a community-driven knowledge environment", *Journal of the American Society for Information Science and Technology*, 60(5), 1012-1026.

[14] Krauter, S.G. and Kaluscha, A, E. (2003). "Empirical research in online trust: a review and critical assessment". *International Journal of Computer Studies*, 58, 783-812.

[15] Lee, K. O., Matthew, and Turban, E. (2001). "A trust model for consumer Internet shopping", *International Journal of Electronic Commerce,* 6(1), 75 91.

[16] Mahmood O. and Selvakennedy Selvadurai, (2006), "Modeling Web of Trust with Web 2.0", World Academy of Science, Engineering and Technology, 123-124.

[17] Dimitrakos, T. and Martinell, F. (2005), "Formal aspects in security and trust", International Federation of Information Processing, Springer Verlag.

[18] Sandy C. C. and Gurpreet S. D. (2003). "Interpreting Dimensions of Consumer Trust in E-commerce", *Information Technology and Management, 4*, 303-318.

[19] Shi, J., Bochman, G. V. and Adams, C. (2004), "A trust model with Statistical Foundation, Workshop on Formal Aspects in Security and Trust" (FAST'04) Toulouse, France 18th IFIP World Host Congress, 169-181.

[20] Suh B. and Han I. (2003), "The Impact of Customer Trust and Perception of Security control on the acceptance of Electronic Commerce, 7(3), 135-161.

[21] Tsiakis, T., Stephanides G. and Pekos, G. (April 2005), "Trust and Security in Electronic Payment: What We Have and Need to know?" *Proceedings of World Academy of Sccience, Engineering and Technology*, 5, ISSN 1307-6884.

[22] Wierzbicki, A. (2010), "Trust and Fairness in Open, Distributed Systems", *Studies in Computational Intelligence*, 298, Springer publisher.

[23] Witkowski M., Artikis A. and Pitt J., (2001). "Experiments in Building Experimental Trust in a Society of Objective-Trust Based Agents", *Lecture Notes in Host Science*, 2246, 111-112.

THE JOURNAL OF COMPUTER SCIENCE AND ITS APPLICATION
AN INTERNATIONAL JOURNAL OF THE NIGERIA COMPUTER SOCIETY (NCS)
Vol. 19 No.1, June, 2012

nigeria computer society
www.ncs.org.ng.

WEB-BASED NOVEL ARCHTECTURE FOR INTELLIGENT TUTORING

Japheth[1] B. R. and Patience[2] Spencer
[1]Department of Mathematics/Computer Science, Niger Delta University, Yenagoa, Nigeria
jbunakiye@yahoo.com
[2]Department of Computer Science, University of Education, Port Harcourt, Nigeria
Pakaye_kirime@yahoo.co.uk

ABSTRACT

This paper presents a novel architecture for intelligent tutoring **model that combines both dynamic client design and three-tier server side with database server design.** The **content and dialogue initiations capability of the tutorial model are embedded in the three-tier server side with database server design aspect of the architecture while the dynamic client design is used for the tutorial interactivity aspect. Both aspects were then analyzed as prerequisite knowledge to developing the new web-based architecture for intelligent tutoring.** The architecture combines a client side implementation language, a server side implementation language and a database implementation language. This client side script has all the necessary logic required to process dynamism and interactivity of the system, hence, the interactivity request is made at the client, captured by the client script and processed by the client script. If there are complex data that require processing at the server side, the server script processes it and returns the result as parameters to the script which uses it for further processing. The result is then sent to the web browser for total service delivery and throughput. The evaluation of the system shows the capability of handling millions of lessons effectively depending on the storage disk capacity of the web server.

Key Words: Complex Combination, Three-tier Server Side, Dynamic Client, Storage Disk, Round Tripping, Bandwidth

1.0 INTRODUCTION

Intelligent tutoring systems (ITSs) are computer programs that are designed to incorporate techniques from the artificial intelligence (AI) community. They are designed in such a way that the contents to teach, how to teach it, and who to teach are all incorporated in a software module. AI [2, 13] attempts to produce in a computer behaviour, which if performed by a human, would be described as 'intelligent'. ITSs may similarly be thought of as attempts to produce in a computer behaviour, which if performed by a human, would be described as 'goad teaching'. Much of the research in the domain of educational software involving AI has been conducted in the name of Intelligent Computer-Aided Instruction (ICAI). This evolved out of the name 'Computer-Aided Instruction' (CAI), often referring to the use of computers in education [12, 6, and 7]. The design and development of such tutors lie at the intersection of computer science, cognitive psychology and educational research. H**owever, because of the efforts of some researchers, a great deal has been learnt about how to design and implement ITSs. The intelligent tutoring system described in this paper confirms this fact** [11]**.** The consequence in terms of this architecture is that we need to resort to a distributed architecture in which flexibility in learning is derived from multiple strategies. To fulfill this goal, there is need to develop complex combination architecture with specific characteristics. The rest of this paper is organised as follows. Section 1 presents the introduction to the study. Section 2 discusses literature review. In section 3, the research methodology is described. Section 4 describes the implementation and evaluation procedure. Conclusion and future work are presented in section 5.

2.0 LITERATURE REVIEW

An **intelligent tutoring system** (ITS) [12, 6, and 7] is any computer system that provides direct customized instruction or feedback to students, i.e. without the intervention of human beings, whilst performing a task. An ITS may employ a range of different technologies. Broadly defined, an intelligent tutoring system is educational software containing an artificial intelligence component. The software tracks students' work, tailoring feedback and hints along the way. By collecting information on a particular student's performance, the software [2, 13] can make inferences about

strengths and weaknesses, and can suggest additional work.

2.1 THE INCORPORATION OF ARTIFICIAL INTELLIGENCE

AI scientists concentrated on developing general methods or techniques for building intelligence into specialized programs [2]. These efforts produced expert systems generally conceptualized as depicted in figure **1.** The user makes a consultation through the interface system (the communication hardware and also the software which defines the type of queries and formal language to be used) and the system questions the user through this same interface in order to obtain the essential information upon which a judgment is to be made. Behind this interface are two other sub-systems: the knowledge base, made up of all the domain-specific knowledge that human experts use when solving that category of problems. The inference engine or system performs the necessary reasoning, and uses knowledge from the knowledge base in order to come to a decision with respect to the problem posed [2, 13].

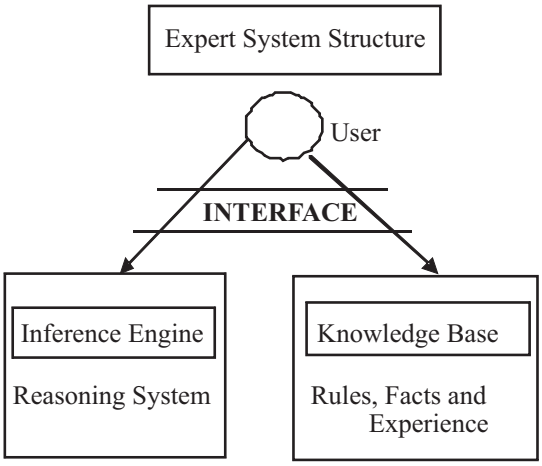


Figure 1: General Conceptualization of Expert System

2.2 LEARNER MODELS

Learning in intelligent tutoring systems has evolved during the last two decades. The goal was to reproduce the behavior of an intelligent human tutor who can adapt his teaching to the learning rhythm of the learner. The fundamental elements of existing intelligent tutoring systems as shown in figure 2 usually include a curriculum/expert system, an inference engine and a learner model. In these systems flexible communication between the learner and the system is often difficult to accomplish due to the lack of a tutorial module that permits various pedagogical interactions [12].

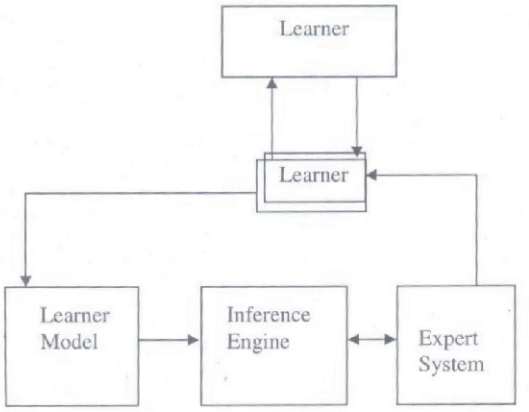


Figure 2: Existing Model of Intelligent Tutoring System

3.0 METHODOLOGY

The present system allows interactions by means of some interface system, receiving information and providing responses to questions or sometimes initiating dialogue by asking questions [9, 12]. The system then must respond to the learner [4, 5] in a manner appropriate to the individual pattern of responses and queries received. The system adapts to the individual learner's needs, learning styles, difficulties, etc. These adaptations are possible because the proposed system incorporates a very well-structured knowledge base comprising the subject matter that is to be taught, the teaching methods and tricks associated specifically with that subject [17]. The elements of this new system include a curriculum/expert system, a learner model, an inference engine and a pedagogical module. In a tutorial system, there is need for a more flexible communication between the learner and the system in order to allow various pedagogical interactions [12]. This flexibility implemented in the tutorial module of the present sytem. This new component will make it possible for the novel architecture to assume a pedagogical role as indicated in figure 3

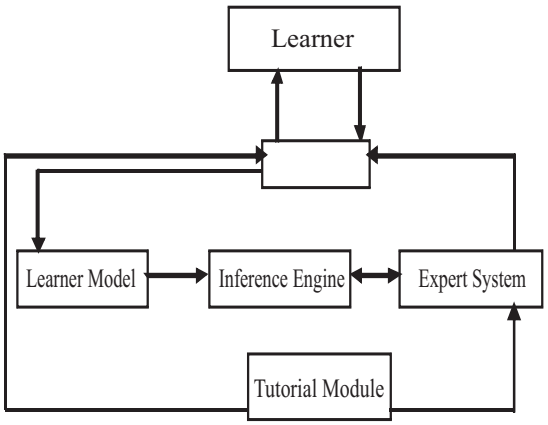


Figure 3: Pedagogical Role of Intelligent Tutor

3.1. DATABASE SIDE

The database schema of this study, as shown in figure 4, entails the external level, which is the user view (UV), the conceptual level (CV), representing the logical meaning of the database and defining the entities and relationships. The internal level represents the entire database, its storage and the physical representation (PR). This schema actually evaluates the contents of three tables: the development table, the lesson table, and the assignment table used in this study.

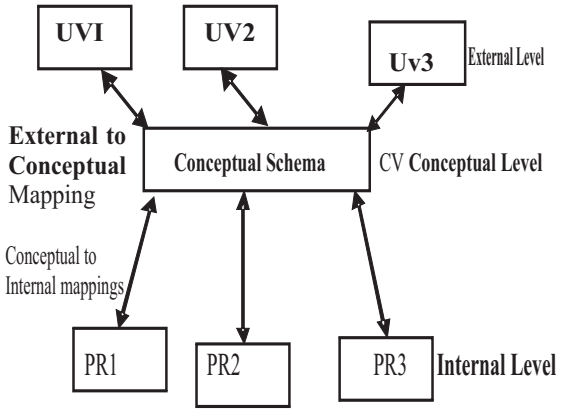


Figure 4: Intelligent Tutor Database Schema

3.2 DESIGN METHODOLOGY

The design methodology used in this study is the multi-tier architecture approach to applications development. The components of this architecture are a complex combination of a dynamic client and a three-tier server side with database server. In the process, a One-tier Dynamic Client Design, a Two-tier Server Side Design, and a **Three-tier Server** Side **with Database Server design methods were adopted. The** one-tier dynamic client design supports client-side programming. This means that the scripts can make the web pages to **be** responsive to user interaction and to be dynamic. If a remote learner makes a **request,** the browser then dynamically sends the page.

The server side design supports server side programming; this feature defines and processes the tutor logic while the server side with database server design supports the storage of lessons in the database using a database server. The **dynamism provided by** this combination allows the server script to communicate with the database server using SQL queries. The lessons stored in the databases are fetched and processed for onward transfer to the browser, and instead of sending everything, only the lessons requested are sent. As as a result, the bandwidth used by the system is reduced. Another significant achievement from this combination is that the code in the server are not sent to the client rather the processed result in form of simple HTML web pages are sent to the client. Hence, proprietary codes are not available to unauthorized users. Subsequently, no identified security problems or risks evolve from sending components to client machine because vital information can be hidden. This process reduces the number of simple HTML pages needed to be created in the server. Only one set of pure HTML code is actually created as an output, the rest is a set of it and the logic that manipulate it before it can be sent to the browser [5, 8]. **3.3THENOVEL ARCHITECTURE FOR INTELLIGENT TUTORING**

This complex combination of dynamic client and three- tier server side with database server design method actually led to the design of a novel architecture for intelligent tutoring as shown in figure 5. In the integration process, issues of inefficiency due to bandwidth problems and round-tripping between the web server and the client browser in one-tier systems were **identified**. Also identified is the fact that in two-tier systems there is no significant reduction in bandwidth problem since the round-tripping between the web server and the client browser still exist. The reduction is only on the size of content fetched in each trip to the server since many objects are sent once and the one lacking in the database are then sent at subsequent requests.

After all these considerations have been made at design time, what became possible in the new design is that the client makes a request and the page is submitted to the client with the client side script. This client side script has all the necessary logic required to process dynamism and interactivity of the system. Hence, the interactivity request is made at the client captured by the client script and processed by the client script. If there are complex data that require processing at the server side, the server script processes it and returns the result as parameters to the script which uses it for further processing and then sends the result to the web browser on all the client. . It is only when the need for special processing like search for a lesson on the database or other related activity is required that the server is round-tripped; this drastically reduces the bandwidth required. It also keeps those processes that are general knowledge on the client and keep the complex processes which need to be protected from unauthorized use in the server.asd

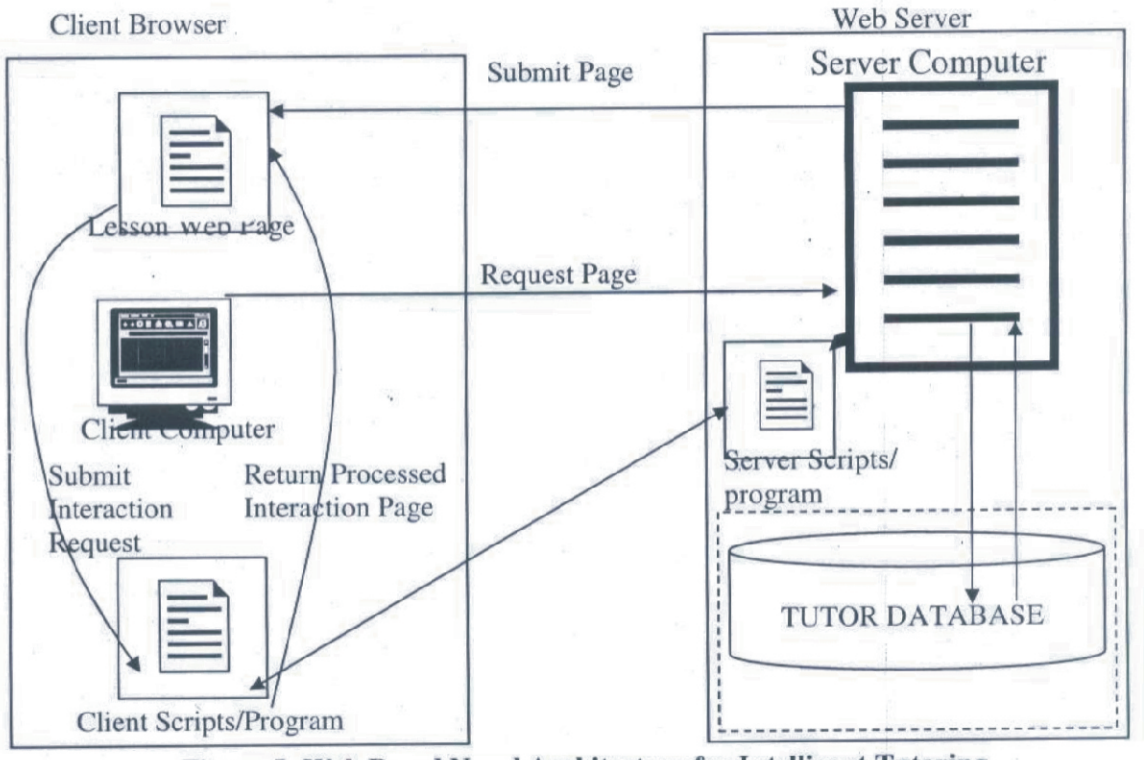
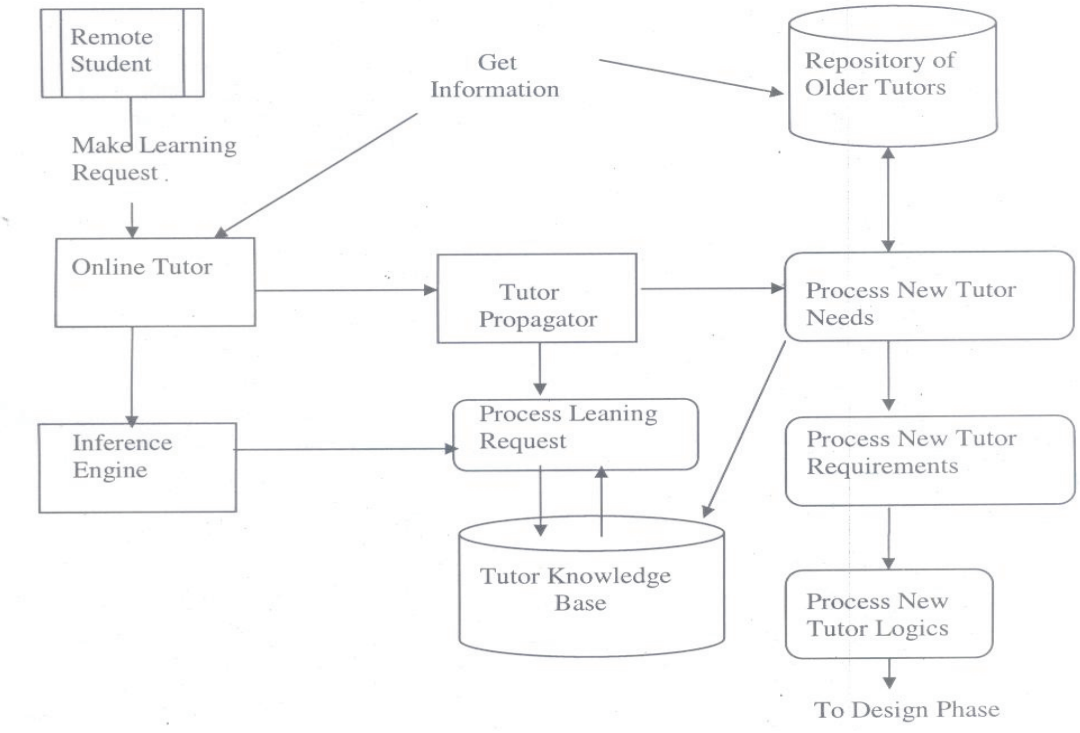


Figure 5: Web Based Novel Architecture for Intelligent Tutoring

3.4 PROCESS MODEL OF THE TUTOR

The process model of the web based tutor shown in figure 6 represents the reality of a tutor teaching some learners in a given class. The difference being that the tutor is on the internet or on the web and the students are in remote locations devoid of a physical classroom.



The process model illustrates the processes from the time the remote learner (user) makes learning request on the online tutor to the time the tutor sends a response. The Online tutor uses the tutor propagator, the inference engine, the knowledge base and the need to process the remote student's request. The new needs generate new requirements for the system and new **logic** for the preparation of lessons that go to design for implementation. The online tutor also uses the information from existing tutors, which are normally stored in the system repository. The extent to which the system utilizes these existing analysis, designs or materials depend on the relevance to the new needs and to the subject matter handled by the tutor [16, 17, and 12].

4.0 IMPLEMENTATION AND EVALUATION

In the implementation, the Apache web server that have both PHP and MySQL in their configuration was used. The system was able to fetch data from the database to populate the web page using the math lesson hyperlink and the answer hyperlink. The search hyperlink also uses the search term to search the database and to produce correct results which are also displayed on the web page. The lesson was followed in the normal way an online user is expected to follow it using the ***development*** link. The system was able to fetch the development information from the ***develop*** table of the ***tutordb*** database and display the result well without mixing the lessons. This was possible due to the implementation of the system using session controls which kept track of the page the user is viewing during navigation. The correct page is then displayed whenever the user clicks next or moves to the answer section. The system use the user interface to display all the results of its operation instead of keeping specific HTML file or Link as a given result or link to a given click event. This makes the system to manage the content of the tutor dynamically. The ***no*** **script** tag is included to take care of a situation where the user disabled JavaScript on his browser. The tag will remind the user that JavaScript has been disabled and that it should be enabled to run the interactive sections.

On the start of the system program the code If ($_CET['page']== "HOME") examines the click event of the user to see if the HOME link, Search link, Lesson link, and answer link have been clicked. If they have been clicked, the program calls home.php, search.php, lesson.php, interact.php and answer.php respectively. On the other hand, when none of this has been clicked, no event listener is returned to the GET method object and welcome.php is returned. This is particularly so when we get to the system first or when the online student enters the web online class. The call to this php files for server processing is done using the include statement such as *include ('home.php');*

The home program file is then processed by the PHP server engine and the result returned to the client machine as simple HTML code. This code is then rendered by the client browser and viewed by the student using the online tutor as a simple we page.

When the Search Link is clicked, the event is sent to the search.php file, which processes the search page and renders a page that provide for the selection of search operation. On submission of the search, the PHP server engine connects to the database and use the SQL query statement presented in lessondb.php file to select the database which it needed to perform the various operations required. The database in our case is the ***tutordb*** . The PHP server engine also uses the select query statement to process the database fetch the results and return to a place holder.

The user must have specified a reasonable term to get a good result, otherwise, the system will return no value. In the interactivity, the PHP server engine processes the code and send the forms for the operations to the client browser as illustrated in our design in figure 5 (**Web Based Novel Architecture for Intelligent Tutoring**). Sample interfaces for the implementation are as shown in figures 7, 8a, 8b, 9a and 9b respectively.

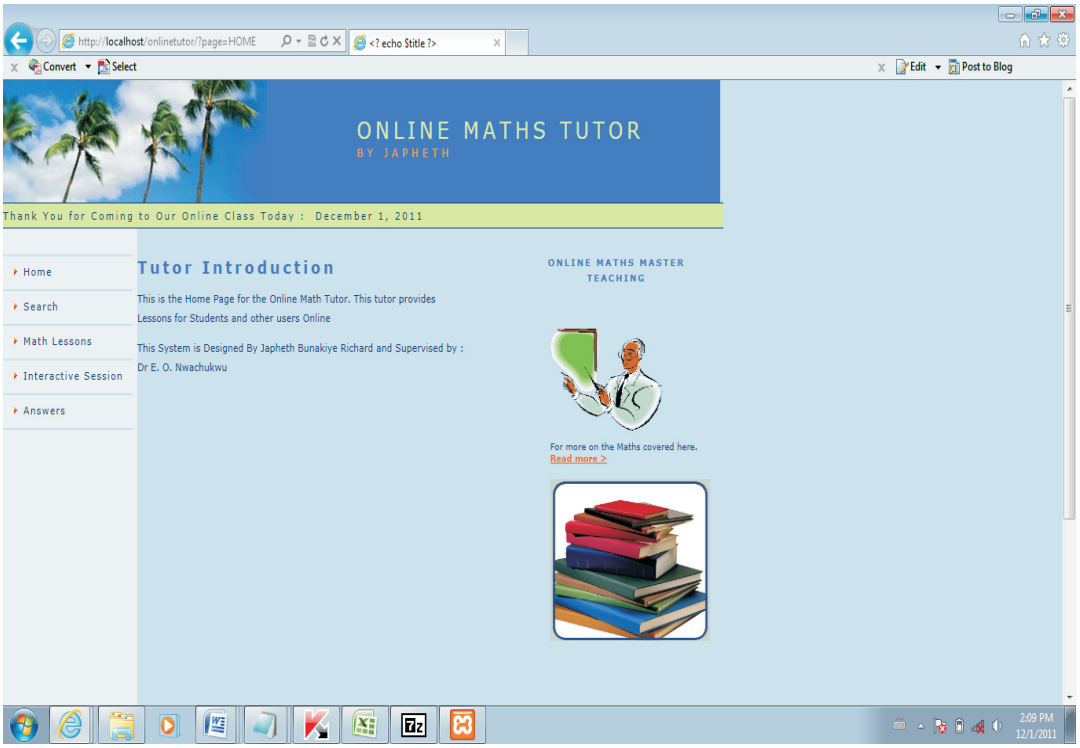


Figure 7: Tutor Home Page with Hyperlinks

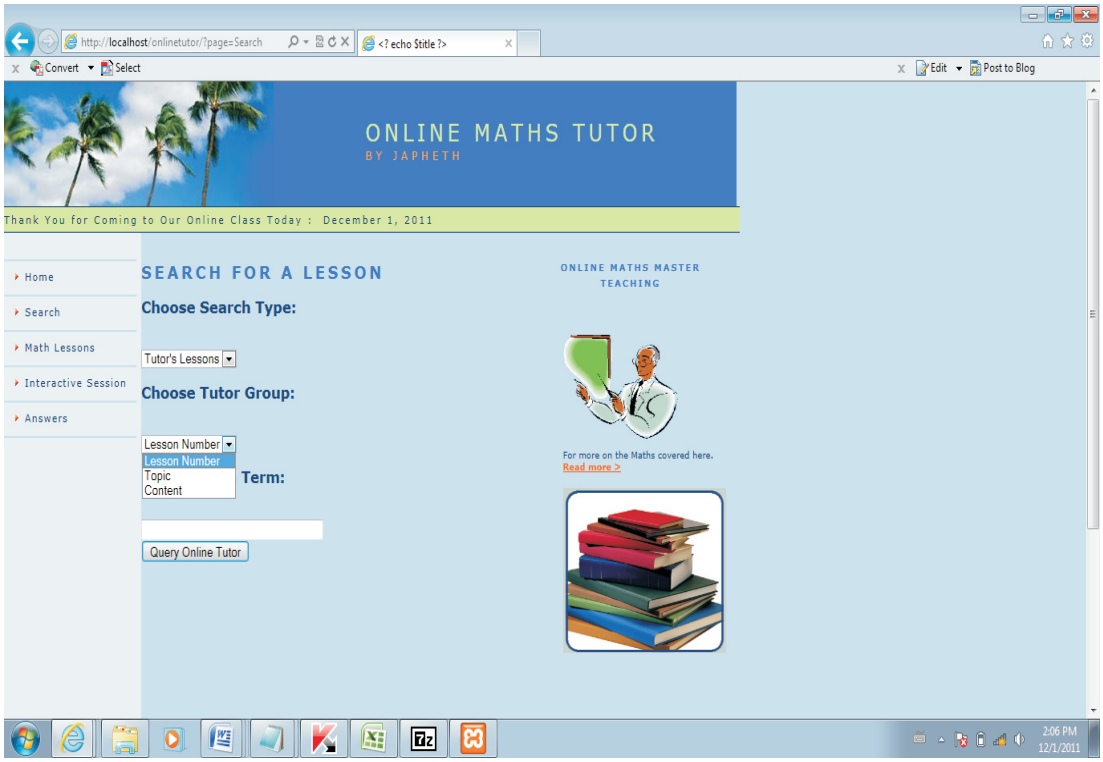


Figure 8a: Tutor Interface Showing Search Link Activation

Figure 8b: Tutor Interface Showing a Choice Search Operation

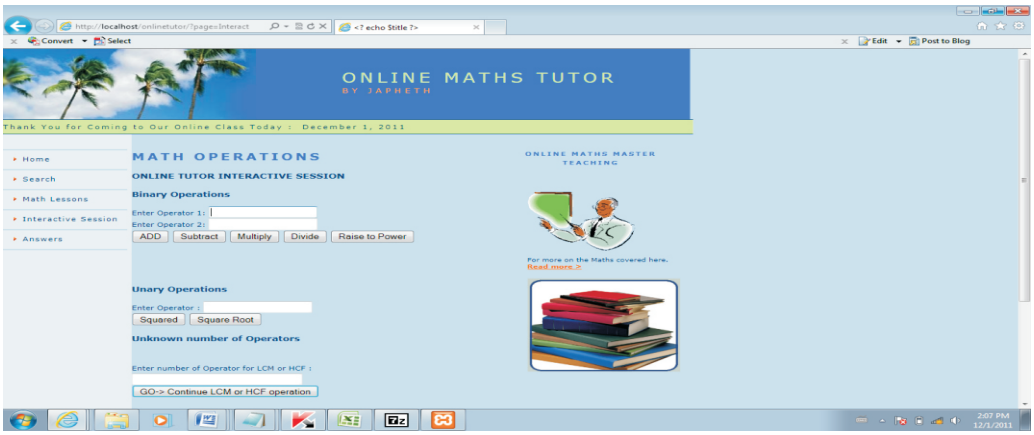


Figure 9a: Tutor Architecture Allowing Interaction for Math Operations

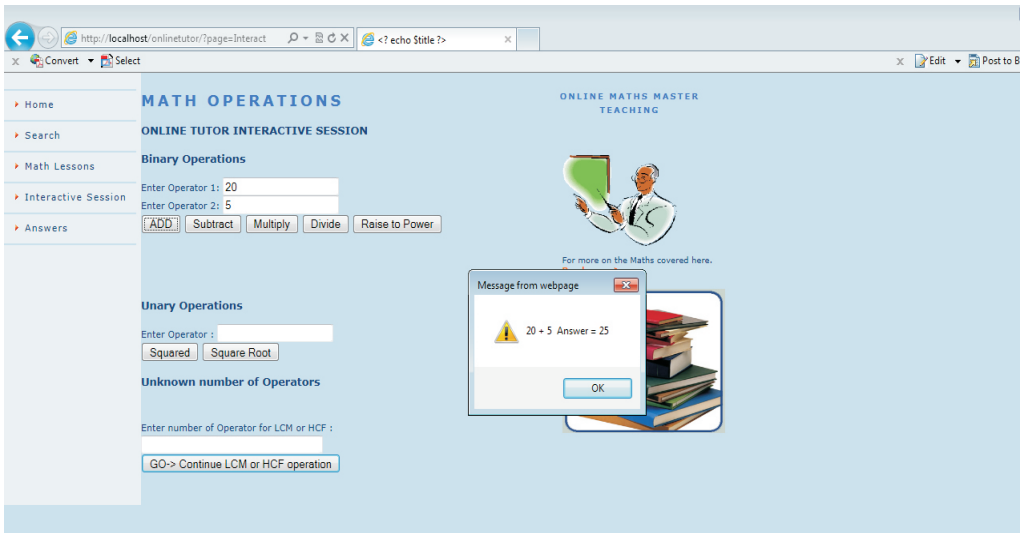


Figure 9b: Tutor Interface Showing Result of Interaction for a Math Operation

4.1 DATABASE IMPLEMENTATION

Illustrated in figure 10, is the entity relationship between the tables in the tutor database. The database is authenticated with MySQL, which is responsible for evaluation of the active services to learners' requests. The evaluation process is such that the database management system server allows only the admin available to the lesson creator to be used for the input of the lessons in the input window. From that point, the server side program will be able to access them [7]. Therefore, each group of users can have a separate external view of the database tailored to the group's specific needs. In the intelligent tutoring system, the user views the external level as simple web page lessons displayed simply on the browser.

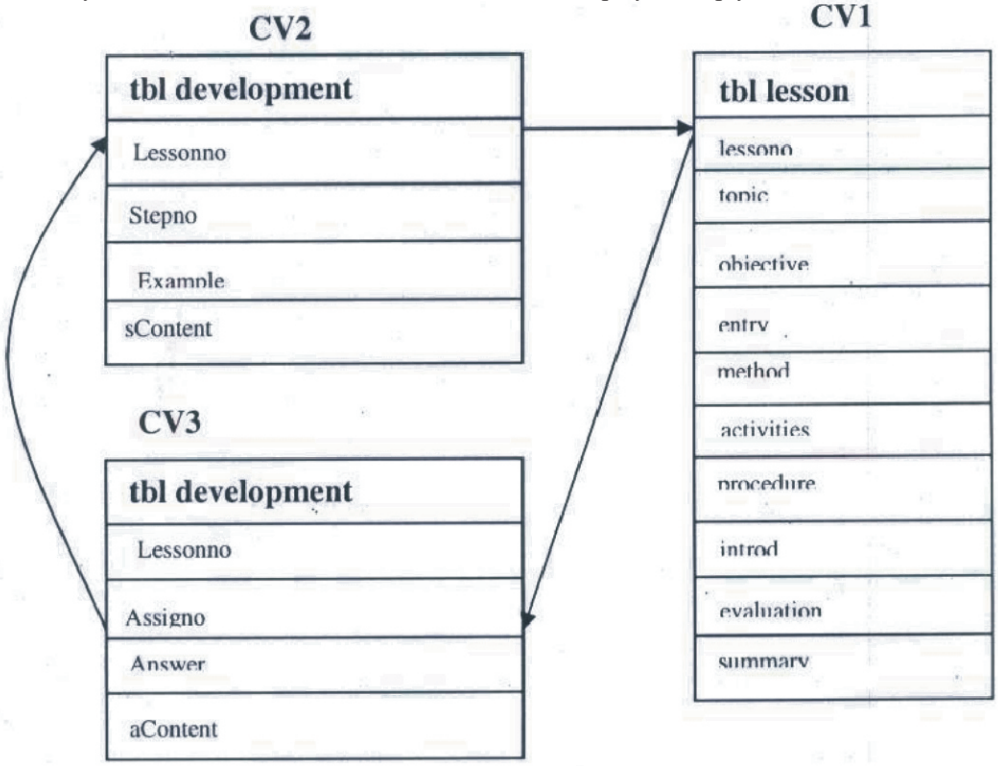


Figure 10: Relationship Representation of tutordb Database

BIOGRAPHY OF AUTHORS

Japheth, B. R. is a Lecturer in the Department of Mathematics/Computer Science, Niger Delta University. He is a Certified Information Technology Practitioner; certified by the Computer Professionals Registration Council of Nigeria. His research interests are Software Engineering, Systems Analysis, Modeling and Simulation

Patience S. is a Lecturer in the Department of Computer Science, University of Education, Port Harcourt. Her research areas are Web Applications and Artificial Intelligent

THE JOURNAL OF COMPUTER SCIENCE AND ITS APPLICATION
AN INTERNATIONAL JOURNAL OF THE NIGERIA COMPUTER SOCIETY (NCS)
Vol. 19 No.1, June, 2012

nigeria computer society
www.ncs.org.ng.

A Trustworthy SMS Based Voting System Architecture

[1]Agbaje M. Olugbenga*, [2]Awodele Oludele, [3]Joshua J. Vincent and [4]Maitanmi, O. Stephen, [5]S.O. Okolie.
Babcock University, Computer Science, Ilishan Remo, Ogun State, Nigeria
Agbajeolugbenga@gmail.com, delealways@yahoo.com,
Jvjoshua@yahoo.co.uk, maitanmi@yahoo.com

Abstract

Short Message Service (**SMS**) is the text communication service component of phone, web or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices. The use of SMS as data application in the world is enormous, with 2.4 billion active users, or 74% of all mobile phone subscribers. This paper develops an SMS voting system that can be used in conducting a trustworthy, secure and robust voting. The design requires the use of a national SIM card module the electoral process. tions, Easy and cheap to implement, Fast election delivery results within 24hrs and generally acceptable electoral conduct base on the legislation of a particular country. It is based on The SIM card can be used for either the Internet voting system or the SMS voting. The model is based on other e-voting schemes and adapted to the Nigerian system of election. The method is cheap and fast and guarantees prompt election result.

Keywords: SMS, SIM, voting, trustworthy, electoral process

1.0 INTRODUCTION

The world has embraced democracy as a type of governance. The use of paper ballots has been bastardized, especially in developing countries where politicians will do anything to rig elections. The manipulation of other electoral system is also still a matter great concern where they are utilized. The need for fast, secure and trustworthy electoral system is therefore a subject of challenge in Information and Communication Technology. The term e-voting refers to an electronic system that allows a voter to record his or her secure and secret ballot electronically by Short Messaging Service (SMS) or other electronic data transmission media [1].

In direct-democratic Switzerland, e-voting is meant to include not only the casting of votes in elections and referendums, but ultimately the giving of 'electronic signatures' for initiatives, referendums and proposals for candidates for membership of the National Council [2]. In Nigeria, a lot of funds that should be used for infrastructural development are being channeled towards voters' registration and electoral system conducts. The use of SMS readily comes to mind because use of mobile phones which is cheap and widely available. The use of SMS is diverse and has been used widely for opinion polls which can serve as a measure of popularity of candidates for a particular position. Therefore, the paper proposes an SMS based electoral voting system that is trustworthy, cheap and adaptable to Nigerian system of government and social system.

There are two methods of SMS widely used in applications; they are the PUSH and PULL. This application can either be used to push or pull messages. A Push SMS application is one whereby a message is been sent from the application to the user. It is a one way message.

A Pull SMS application on the other hand is one whereby a user sends a request and obtains a reply from the application. This is a full duplex scenario.

Types of SMS

Two types of SMS which can be classified by the origin of the message were identified [3]

Mobile Originated (MO): SMS-MO is **sent from** a mobile phone and could be sent either to another mobile phone (such as when a mobile subscriber sends a personal message to another subscriber) or to a computer application that will process the message.

Mobile Terminated (MT): SMS-MT is **transmitted to** a mobile phone. It could also be sent by another mobile phone or generated by a computer application [4, 5].

1.2 Uses and advantages of SMS

SMS are used for personal communication, opinion polls, result checking system, air line booking, electronic appliance control, Result checking system in examination and Medical uses. They have the advantage of being paperless, no electricity problem, fast results processing, cost effectiveness and availability, as most individuals own phone.

1.3 SMS today

In 2008, 4.1 trillion SMS text messages were sent. SMS has become a massive commercial industry, worth over 81 billion dollars globally as of 2006 [6]. The global average price for an SMS message is $ 0.11, while the cost to providers approaches zero. Mobile networks charge each other so-called interconnect fees of at least $0.04 when connecting between different phone networks.

Problems and Vulnerabilities

Technological issues to the security (Integrity, Confidentiality, Availability and Authentication) of Internet/electronic ballots are still significant. Some of the threats include viruses and worms that can easily cause denial of service to the system or modifications to and deletion of ballots data. Hackers can also take advantage of vulnerabilities that exist with the internet. The Global Service for Mobile communications (GSM), with the greatest worldwide number of users, succumbs to several security vulnerabilities. In the GSM, only the airway traffic between the Mobile Station (MS) and the Base Transceiver Station (BTS) is optionally encrypted with a weak and broken stream cipher (A5/1 or A5/2). The authentication is unilateral and also vulnerable. There are also many other security vulnerabilities and shortcomings. Such vulnerabilities are inherent to SMS as one of the superior and well-tried services with a global availability in the GSM networks. SMS messaging has some extra security vulnerabilities due to its store-and-forward feature, and the problem of fake SMS that can be conducted via the Internet. When a user is roaming, SMS content passes through different networks, perhaps including the Internet, and is exposed to various vulnerabilities and attacks. Another concern arises when an adversary gets access to a phone and reads the previous unprotected messages [7].

In October 2005, researchers from Pennsylvania State University published an analysis of vulnerabilities in SMS-capable cellular networks. The researchers speculated that attackers might exploit the open functionality of these networks to disrupt them or cause them to fail, possibly on a nationwide scale.

The objectives of this paper include designing an SMS voting system that is, secure and robust to manipulations, trustworthy, easy and cheap to implement and fast delivery results within 24hrs.

2.0 REVIEW OF EXISTING SYSTEMS

2.1 Introduction

Most countries still go to the polls using the ballot box method while a few now go through I-voting (internet voting). In literature, a national election of any country that is completely based on SMS is not found. The internet based method is still at the infancy stage and still requires strict regulations and control for it to be used. This section takes a look at different types of voting systems.

Internet voting is emerging as significant alternative to other conventional systems in the delivery of trusted elections. Although, certain forms of electronic voting have been used successfully in a number of countries during the national and local elections, Internet voting had not been used in a legally binding political election. In the USA, Internet voting (abbreviated as i-voting or ivoting) had never been used until March 2000when the Arizona Democratic Party held its primary election online. Other countries which have implemented i-voting are: France (2003) and Estonia (2006). Estonia is believed to have held the world's 1st ever successful i-voting election in 2006. Any country with plans to adopt the use of i-voting systems must first get full government election certification and legislations before implementation [8, 9].

Deployment of SMS based voting would be inexpensive and needs also appropriate technical support and usage on the part of the nationals. However, an implementation of SMS voting to communities in geographically difficult to reach terrains with poor communication infrastructure, would allow increased access to the voting process.

2.2 Conventional Elections

The traditional voting systems have been in use to ensure the principles for democratic elections and referenda. This involves the freedom to vote, the secrecy of the vote, the non-modification of the expressed intention of the vote and lack of intimidation during the vote operation. A regular election process, however, is basically made up of the following components:

- formulating a legislation, through Parliament, that will guide and support any election process,
- calling of elections,
- registration of candidates,

- preparation and display of polling list at polling stations,
- voting at polling stations/ centre
- counting of votes,
- declaration of results by the Electoral Body or Commission .

2.2.1 Nigeria Model

Nigeria was fifty in October, 2010 and the country has gone through a lot of electoral reforms. The results of many elections have been contentious and the best election we ever had was June 12, 1992 which was annulled. The system used was called option A4, where voters had to queue up behind the candidate of their choice. Subsequent elections had been marred with a lot of rigging and lack of trust.. The next election comes up in 2015, while the question of trust lingers. A lot of money is normally spent on registration and electoral conduct [10]. The wastages have been huge and a trustworthy system using the SMS can be adopted to achieve a credible election.

2.3 Electronic Voting Systems

Like the traditional/conventional systems, the e-voting systems must deliver reliable and trusted elections. It must therefore be designed and operated to ensure reliability and security of the voting process. The e-voting systems have to be as free, secret, reliable and secure as the conventional voting systems. An e-voting system therefore, should meet the following minimum requirements:
(i) Ensure that only persons with the right to vote are able to cast a vote.
(ii) Ensure that every vote cast is counted and that each vote is counted only once.
(iii) Maintain the voter's right to form and express his or her opinion in a free manner, without any coercion or undue influence.
(iv) Protect the secrecy of the vote at all stages of the voting process.
(v) Guarantee accessibility to as many voters as possible, especially with regard to persons with disabilities.
(vi) Increase voter confidence by maximizing the transparency of information on the functioning of each system.

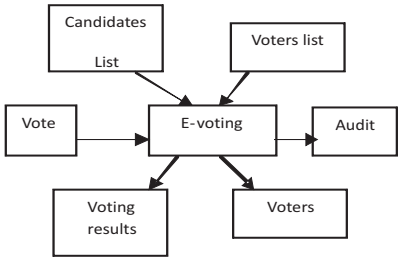


Figure 1: Estonia Voting System Model[11]

The figure 1 shows an e-voting system that was implemented in Estonia [11]. The Estonians had the opportunity and motivation to implement the e-voting project for local government council elections of 2005. The system had its input from:
a) voter lists, b) candidate lists and c) expressed will of the voters. According to the literature available, its output consisted of: a) summarized voting result of e-voters, b) list of voters who used e-voting.
In Estonia scenario, the voters' personal computers and servers were the responsibility of the Estonia's National Election Committee (NEC). The weakest link of the e-voting procedure was probably the voters' personal computers with no control that could be exerted over it. There was high possibility for anyone to control the data servers, errors and attacks, can easily influence a large amount of votes simultaneously.

2.4 Electronic voting in India

Electoral malpractices have reduced with the use of electronic voting machines (EVMs) in India and has resulted in a more efficient elections. The Election Commission of India type of electronic voting machine (EVMs) is a fully standalone machine and is not part of any network. This gives an advantage for control and monitoring with less intrusion from the outside, for example hacking and other threats. The disadvantage is limitation on the use of network technology in the EVM [11].

Electoral Information & Poll Monitoring System for the elections in 2009 in Tripura provides an alternative networking platform using the mobile phone developed to effectively integrate the available communication facilities and the networking technology to further improve the reliability, accuracy and trustworthiness of the electoral process. Election monitoring of the polling stations and the election process was dependent on conventional communication medium like fax, telephone and police wireless and in-person visits for earlier elections. New directives were issued by the Election commission of India (ECI) to develop an effective communication plan and to collect information from the polling stations on strategic parameters by effectively utilizing the communication network to pin point the polling stations where corrective measures are required for the conduct of free and fare election [11].

2.5 Pakistan model

Pakistan is proud to have the world's largest biometric database; National Database and Registration Authority (NADRA) of its citizens. It is secure, reliable, centrally organized, well managed and advances with the passage of time resulting in emergence of products like Machine Readable Passports (MRP), Birth/Death Certificates and Vehicles Identification & Monitoring System (VIMS) ,and so on, from a single source based on Computerized National Identity Card (CNIC).

An impressive use of centralized data is the registration of mobile SIM card with CNIC using an activation service by NADRA and then using the facility to keep track of who owns a particular SIM card(s). It is one great achievement and there is no other elsewhere so publicized, noting that the number of people who owns and use mobile phones in Pakistan is indeed high. The idea of e-voting through SMS that seems good option could indeed be time saving, secure, fast, corruption-less and most cost cutting national election idea ever was proposed, and a supporting model presented [12].

2.5.1 Working Model

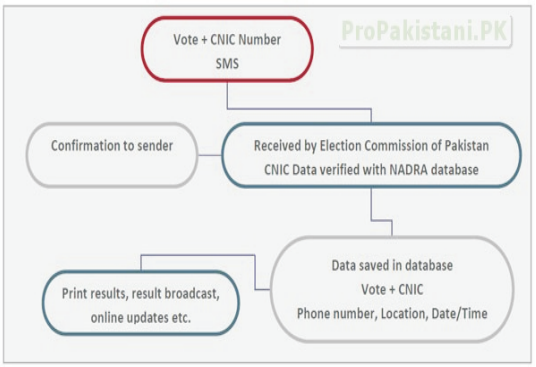


Figure 2: Model of Pakistan election

The figure 2 shows how electoral registered citizen should cast their vote through SMS by sending a short number along with CNIC number. It would be then received by Election Commission of Pakistan and the data checked for confirmation at NADRA database. Subsequently on successful verification, vote is saved for that CNIC; and confirmation SMS is sent back to sender/voter.

Defining a limit and check over posted votes per mobile SIM card would sets spam risk at lower level. The fact that each individual has an exclusively issued CNIC number could be used to ensure compliance to voting rights. Efforts and funds, needed in security concern for days, would be saved, when SMS e-voting is provided with free of charge short number for vote [11] . It should be noted here that some attention should be paid to preservation of voting secrecy.

2. 6 E-voting Encryption Algorithms.

Electronic voting scheme are based on certain schema of which the core is encryption. Two of such algorithms' are Elgamal and Blind signatures, are discussed subsequently.

2.6.1Elgamal Encryption Algorithm

Elgamal encryption algorittm employs homomorphic encryption principle. The e-voting environment consists of M-authorities, A_1 to A_M. Each of them owns a public key pair. Authorities are closely bound to each other through the use of threshold cryptography requiring at least **t** authorities needed to decrypt the result of elections. The number of all voters is given by N, whereby each voter own a public key pair. To cast vote, the voter splist up into M parts, each for one authority [13,16]:

$v_i ? s_{i,1},...,s_{i,j},...,s_{i,M}$ (2.1)

Next, every part of the decomposed vote becomes encrypted with the with public key of the authority for which the part of the vote is intended. One of the shares of the vote dedicated to an authority A_j looks like this:

$(g^{ri,j}, \gamma_j^{ri,j}, g^{Si,j})$ (2.2)

The tupel$(g^r,\gamma^r x)$ stand for the ElGamal encryption algorithm where **g** denotes the generator function and **r** represents random number. This is why it is denoted as randomised encryption algorithm. The variation of this random factor ensures that the encrypted message will vary even if the plain text is the same.

After election, each authority collects valid votes received and calculates the component-wise product of all of them without decrypting the particular votes. Assuming A_j received N shares of votes, whereby all of them are proved for correctness, uniqueness and whether the voter is authorised to cast a vote:

$(g^{r1,j}, \gamma_j^{r1,j}, g^{S1,j}),...,(g^{ri,j}, \gamma_j^{ri,j}, g^{Si,j}),...,(g^{rN,j}, \gamma_j^{rN,j}, g^{SN,j})$., (2.3)

Building the component-wise product of these encrypted shares leads to the following results:

$(g?_i^{ri,j}, \gamma_j ?_i^{ri,j}, g?_i^{Si,j})$ (2.4)

The component $S_j = g?_i^{Si,j}$ contains the resulting sum of all votes cast. Thus by decrypting the result, authority A_j gains this component, and therefore the sum of the shares dedicated to it.

The components of **t** authorities are necessary at the very least to reconstruct the resulting sum according to all votes cast because of the use of threshold encryption. The overall result can be calculated by Lagrange-Interpolation used within threshold cryptography systems:

$\Pi_j(g^{Si,j})\alpha_j = g?_i^{Si,j}\ \alpha_j = g^S$ (2.5)

It is infeasible to gain S due to difficulty of computing discrete logarithms. Since the number of voters is limited by N, It is possible to calculate all possible results, such as $g^0...g^N$ reflecting S=0...S=N since the number of voters is limited to N. The voters' sdecision can easily be determined by comparing the result with these pre-processed values . The major principle in this scheme is that it is not necessary to decrypt each ballot and reconstruct the results by the use of the encrypted votes. Thus the idea is very good for secrecy. The drawback is that the complexity of the scheme grows exponentially with the number of electable options.

2.6.2 Blind signatures

Blind signatures were initially intended for electronic cash systems (e-cash) to ensure the anonymity of its owner. The technique as well applies to e-voting since one of voting rule is to make the voters anonymous. The key technique of blind signature allows a signer to sign a document

without seeing it [14]. This can be compared to giving a handwritten signature on a document wrapped in a flimsy manner. The wrapped document gets signed without seeing it. The mathematical principle used by blind signature is given below:

public(n,e)
private(n,d) (2.6)

The voter wants the authority to sign the vote **v** without knowing what it is (blind signature). Thus, the voter generates a random value **r** satisfying
gcd(n,r)=1 (2.7)

By using the random value r and the authority's public key component e, the voter makes her vote blind and creates a blind vote **x**:

$x=(r^e v) \bmod n$ (2.8)

The voter then request the authority to sign it for authority to derive any useful information from the message **x**, using its private key

$t=x^d \bmod n$ (2.9)

The authority returns the signed vote t to the voter:

$t= x^d \bmod n$
$=(r^e v)^d \bmod n$
$=(r^{ed} v)^d \bmod n$
$=rv^d \bmod n$

The authority is prevented from learning the signal vote **v** [13, 15].

3.0 PROPOSED SYSTEM

3.1 Introduction

This paper proposes a modified use of Pakistan, Estonia and India models. It proposes the use special SIM cards that are legally manufactured for electoral process only to eligible persons. The legislation guiding electronic voting system should be reviewed and passed by the legislators for it to be operational. The number of political parties should be few for efficient and functional system. The system should follow the existing governing structure. In Nigeria for example, it would flow along the local government, the state government and the federal government political structure as shown in Figure 4.

3.2 Proposed scheme

The following modifications to the SMS voting scheme will be done to reflect the modified voting process:

- The registration of voters by the electoral body based on local government to capture data such as: Name, picture, Finger prints ,e.t.c
- Issuance of valid Voter's ID card bearing voter's number and special code for SMS voting.

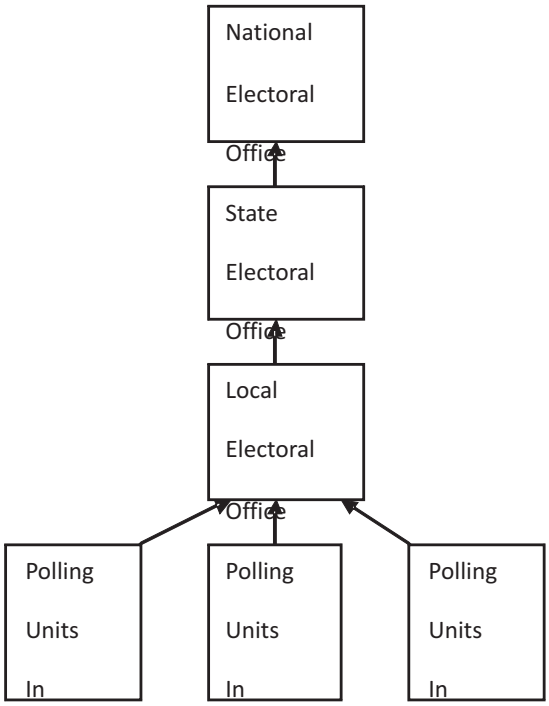


Figure 4: Nigeria Political systems of government.

- Collation of candidate's name, party and candidates ID.
- Local government delineations and SMS code.
- State government delineations and code for secure data transfer.
- Federal code for secure data transfer.
- On voting day the physical presence of voters at polling centers before casting votes.

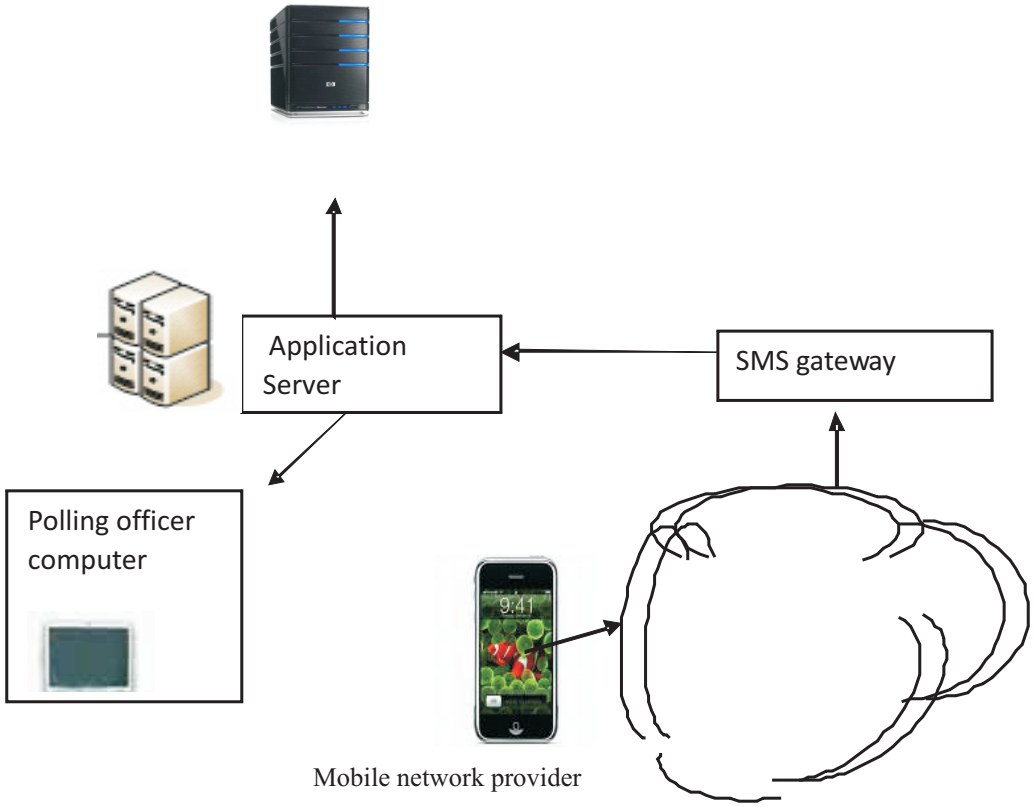


Figure 5: Equipment for polling system.

The required additional equipment beyond what is already in place would vary from country to country depending on their preparedness. Attention now focuses on the peculiar challenges of the Nigerian environment.
Each polling unit should be equipped with:

A laptop containing the entire registered voters with their pictures, fingerprints and other modes of identification that are collated during the registration procedures. The electoral office collation for each polling station should have a server serving as result collation point for other polling units within the local government for transmission to a central server. The final destination should be the national electoral commission such as the presidency.
The processes for state elections would stop at the state level; similarly the processes for local government elections would stop at direct collation from each polling station. Figure 5 shows the SMS polling equipment. The security of the sent message, validations of the identity of the sender and confidentiality would have to be in place for trustworthiness.
Encryption should be performed on the sent message using one of the secure cryptographic protocols for SMS services. The personal SIM card issued should contain information personal to an eligible voter and should be used for authentication. In case of hijacking of SIM cards the process can be tracked to know if the SMS originates from a single phone or in a single location using signal tracking system provided in conjunction with the GSM service providers. Voting is a social responsibility and each voter should require appearing at polling units where the voter's record is made active before vote is cast for confidentiality.

4.0 Implementation
A special SIM card is produced for elections purposes only. Pre-election registration of eligible voters is done by capturing all necessary information and a unique SIM card is issued with the necessary identity card (see Figure 6 for example). The necessary equipment outlined is provided with essential software system. OZEKI SMS server, with applications written in Java and Mysql for database application is been used for test deployment.

The voters would visit the election site on the day of the election and insert the government-approved SIM in his or her phone and register with the polling officer before the vote is cast. The polling officers' laptops although internet enabled would be disabled during the period of election. Only SMS data streams would be allowed. Each voter would send a text consisting of party code, candidate's number and voter's identity number in casting a vote (see figure 8). Every candidate's name, party code and number would be on display as shown in Figure 7. The number that each voter will send the SMS to will be displayed on the election date and it will uniquely identify the polling unit of the voter and the local government of the voters. The voter receives a reply when vote is cast successfully.

The result of the local processing of votes would be viewed by political agents on the screen and the results would be sent to state and then upward to the national headquarters for final collation. Each polling would connect to the secured network and send the election result to respective party headquarters. The votes cast could be recounted and could be used as evidence in court of law in case of election dispute.

A voting scenario

The Identification card/polling card for a Nigerian election can be of the form as depicted the figure 6, 7 and 8.

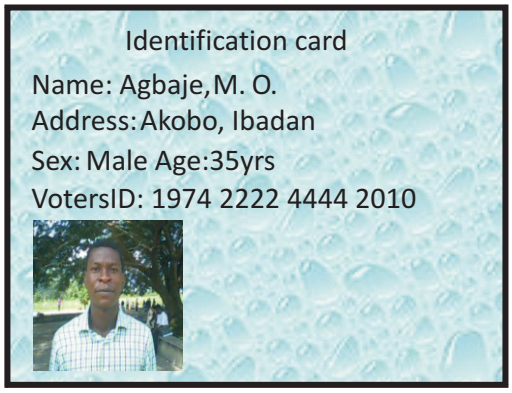


Figure 6: An example of voter's Identification card

Polling Card

Candidates	Party	Candidate ID
S. Ojo	PDP	4001
M. Obilo	AC	4002
J .Abu	CPC	4003

Figure 7: Polling card with candidate's information

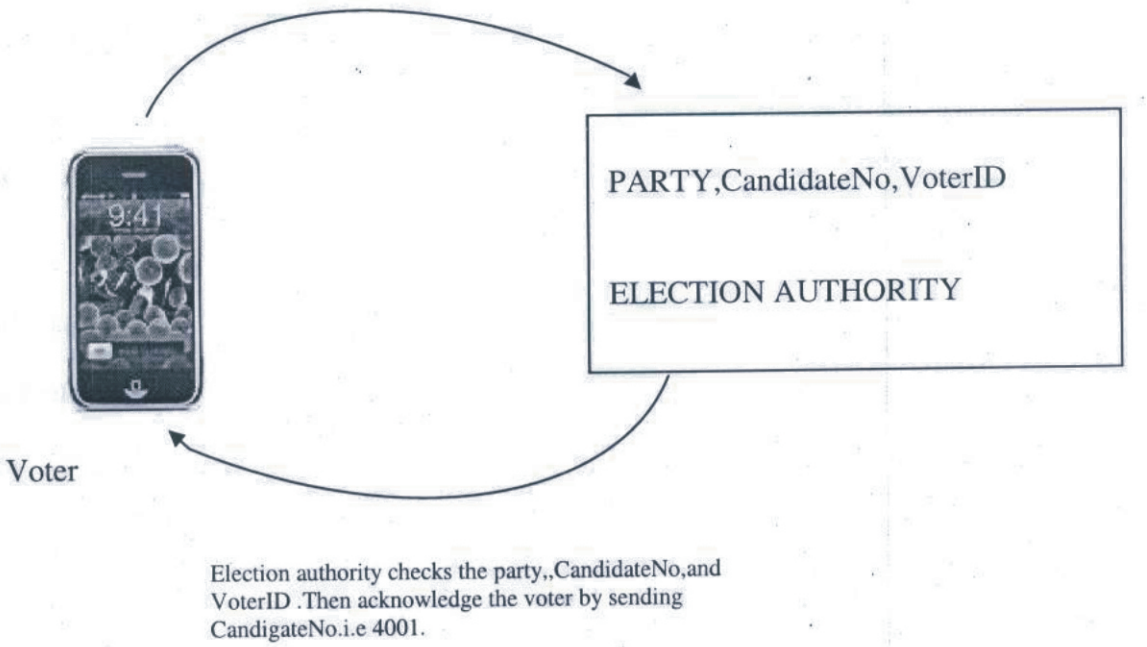


Figure 8: The vote casting process.

5.0 CONCLUSION AND FURTHER WORK The SMS voting system is efficient and will not overload the communication network. Many of the SMS voting system being proposed are not yet legislated for most countries. The incorporation of these medium side by side with the paper balloting elections especially in the regions where the education (awareness) is more will be of importance so as not to exclude the less privileged. Pilot trials will help popularize this mode of election stating with candidates selection at party levels. This paper introduced trustworthiness based on the appearance of voters at polling units before casting their votes using their mobile devices. Further research in the areas of security issues, efficiency and effectiveness measurement, acceptability, and design and creation of necessary application software are essential.

References

[1] Nadja Braun & Daniel Brändli (2006). Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed.

[2] Robert Krimmer (Ed.) (2006). Electronic Voting 2006 2nd International Workshop Co- organized by Council of Europe, ESF TED, IFIP WG 8.5 and E- Voting.CC August, 2nd 4th, 2006 in Castle Hofen, Bregenz, Austria G I - Edition Lecture .Notes in Informatics.

[3] Mavrakis, D. (2004). The Monaco Telematique mobile SMS whitepaper.

[4] Adagunodo, E. R, Awodele, O. & Ajayi, O. B (2007). SMS Banking Services: A 21st Century Innovation in Banking Technology. *Issues in Informing Science and Information Technology Volume 4, 2007.*

[5] Awodele O. (2009). An intelligent SMS based agent for Multi-service application.

[6] ITU internet report (2006). Digital life, chapter 3.

[7] SSMS (2008). A Secure SMS Messaging Protocol for the M-Payment Systems, *Proceedings of the 13th IEEE Symposium on Computers and Communications* (ISCC'08), pp. 700-705, July 2008

[8] Gibson, R. (2001): Elections online: Assessing internet voting in light of the Arizona Democratic Primary, *Political Science Quarterly* 116 (4): doi: 561-583.

[9] Alan, D.S. and John, S.C. (2005): Revolutionalising the voting process through online strategies, *USA Journal on online voting* 29(5). doi: 513-530.

[10] National Mirror, Feb 2, 2011.www.nationalmirroronline.net

[11] Tallinn, (2005). The National Election Committee, Estonia: *E-Voting System Overview*,http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf(accesses03 July,2006).

[12] Jabran (2010). Idea of SMS Based Electoral System (A Proposal): who is student of MSC Web Development at Staffordshire University, UK and one of the top Mapping contributors and Pakistan's ambassador at Google Map Maker.

[13] Thomas Gert ROSSLER(2007). Electronic Voting over the internet-an E-government Specialty,PhD Thesis,University of Tech,Graz,Austria.

[14] David Chaum (1981). Untraceable electronic mail, return addresses and digital pseudonyms, communications of the ACM,24(2):84-86

[15] David Chaum (1983). Blind Signatures for untraceable payments. In proceedings of CRYPTO'82 pg 199-203, New York

[16] Taher Elgamal.(1985). A Public Key Cryptosystem and signature scheme based on discrete logarithms. In proceedings of CRYPTO'84, pg 10-18,NewYork.

THE JOURNAL OF COMPUTER SCIENCE AND ITS APPLICATION
AN INTERNATIONAL JOURNAL OF THE NIGERIA COMPUTER SOCIETY (NCS)
Vol. 19 No.1, June, 2012

nigeria computer society
www.ncs.org.ng.

A Generic Maximum Delay Model of a Packet Switch

M. O. Eyinagho[1], S. O. **Falaki**[2]
[1]Electrical and Information Engineering Department, Covenant University, Ota, Nigeria
eyimon@yahoo.com
[2]Department of Computer Science, Federal University of Technology, Akure, Nigeria

ABSTRACT
There has been a strong trend away from shared medium (in the most recent case, the use of hubs) in local area networks in favor of switched local area networks. The need for deterministic guarantees on delays when designing switched local area networks has also been recognized by many researchers as these delays are useful engineering quantities. This is because, if the maximum delay between two nodes of a network is not known, it is impossible to provide a deterministic guarantee of worst case response time of packets' flows. In this paper, we describe a maximum delay model of a packet switch that can be used for designing maximum end-to-end delays packet switched networks. The packet switch model was obtained by using elementary components such as receive buffers, constant delay lines, multiplexer, first-in-first-out (FIFO) queue. The maximum delay value of the packet switch model was computed from an appropriate aggregation of the maximum delay values for the concatenated network elements. Comparison of the maximum packet delay value of the model with two other values obtained from literature showed that the model is better and much more realistic.

Key words: Packet Switch Model, Maximum End-To-End Delay, Network

1. Introduction

One fundamental characteristics of a packet-switched network is the delay required to deliver a packet from a source to a destination [1]. Delay is the elapsed time for a packet to be passed from the sender through the network to the receiver [2]. End-To-End delay is the sum of the delays experienced at each hop from the source to the destination [3]. It is the delay required to deliver a packet from a source to destination [1].

In certain real-time applications, network designers must know the time needed to transfer data from one node of the network to another [4]. V**oice,** video and an increasing variety of data sessions require upper bounds on delay and lower bounds on loss rate [5]. In [6], it was mentioned that, if the maximum delay between two nodes of a network is not known, it is impossible to provide a deterministic guarantee of worst case response time of packet flows.

The path taken by a packet through a network can be modeled as a sequence of queuing systems [7], [8]. The performance experienced by a packet along the path is the accumulation of the performance experienced along the N queuing systems; for example, the total end-to-end delay is the sum of the individual delays experienced at each system [8]. To determine the maximum end-to-end delay from origin to destination of a switched communication system, we must add the different maximum delays at each switch from origin to destination of a path [7], [8]. It can therefore be seen that there are compelling reasons to have correctly formulated and developed maximum delay models of packet switches. This paper describes such a maximum delay model of a packet switch.

2. Description of the Maximum Delay Model of a Packet Switch

The proposed maximum delay model of a packet switch is Shown in Figure 1. We will then proceed in the next few sections to describe its composition and derive its mathematical equivalent model. The maximum delay packet switch model is based on the following delays/latencies: packet (frame) forwarding latency, packet (frame) routing latency, queuing delay, packet (frame) transmission delay and, concurrent arrival of packets (frames) delay. So the maximum delay which a packet will suffer in a packet switch is given by:
Maximum Packet Delay = Maximum Forwarding (Store and Forward) Latency + Maximum Routing

(Switching) Latency + Maximum Delay as a result of concurrent arrivals of packets + Maximum Queuing Delay + Maximum Transmission Delay (1)

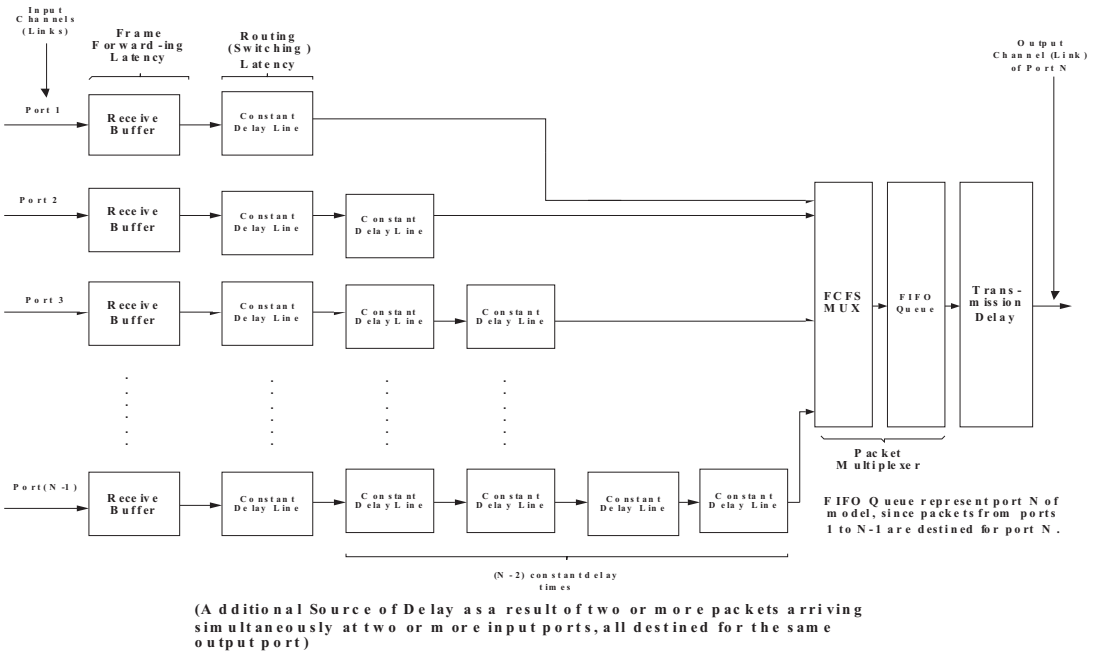


Fig. 1 Maximum Delay Model of a Packet Switch

In the model that is shown in Fig. 1, there are N-1 (where N is the number of ports in the packet switch) receive buffers, representing the input buffering at each of the input ports of a packet switch. According to Cruz in [9], the receive buffer is a useful network element for modeling network nodes which must completely receive a packet before the packet commences exit from the node. Next, there are N-1 constant delay lines. These constant delay lines are each used to model the routing (switching) latency of a data packet in the switch. As averred by Cruz in [9], the constant delay line is a useful network element which can be used in conjunction with other elements to model devices that do not process data instantaneously. We have also used the constant delay line to model the delay suffered by one or more packets in a packet switch when two or more packets arrive at input ports simultaneously, but all of these arriving packets are destined for the same output port. When two packets arrive simultaneously at two input ports, both of them are destined for the same output port, one of them is delayed a fixed constant time (T seconds) before it is sent to the output port.

Next, we have a set of constant delay lines between the first set of constant delay lines and the FCFS MUX (first-come, first-serve multiplexer). The first port (port 1) has no other constant delay line (except the constant delay line that is used to model routing or switching latency). The second port (port 2) has one constant delay line, the third port has two constant delay lines, and so on, up to the $(N-1)^{th}$ port, which has N-2 constant delay. The next component in this model is the FCFS MUX (first come, first serve multiplexer). The MUX has two or more input links and a single output link. The function of the MUX is to merge the streams arriving on the input links onto the output link.

FIFO (first-in, first-out) Queue is the next component in the model. It is used to model the output queuing in packet switches. If a data packet arrives at the input port, after the packet header has been checked to know its destination address, it is then switched (routed) to the output port corresponding to the destination address by the switching fabric. If there are other data packets waiting in the queue of the output port to be transmitted on the transmission line, then it has to wait for the transmission of these other data packets before being transmitted. The FCFS MUX together with the FIFO queue is called packet multiplexer (this is because, apart from multiplexing data

packets from multiple inputs onto a single output, data multiplexers contain buffers for queuing data packets). The last component is a unit that models the transmission delay in a switch (that is, the delay between when the first bit of a data packet is placed on the transmission line that is attached to the output port and when the last bit of the data packet is placed on the same transmission line).

3. Mathematical Model of the Maximum Delay Packet Switch

We note explicitly here that, it is the packet that arrives at input port N-1 that will suffer the maximum delay in the switch.

i. Receive Buffer

According to [10], a packet of length L-bits arriving over a link of bit rate C, will start arriving at time t and will finish arriving at

Time t +.$\frac{L}{C}$ In [9], the backlog in the receive Buffer is bounded by L, where L is the maximum length in bits of a packet.

The maximum delay of any packet passing through the receive buffer is upper-bounded by:

$$D_{buffer} = \frac{L}{Ci} \text{ seconds}$$

where D_{buffer} = maximum delay experienced by a data packet in passing through the receive buffer, L = maximum length in bits of a data packet, C_i = transmission rate in bits/sec of the input channel (line).

ii. Constant Delay Line

The switch model is based on the shared-memory switching fabric, which is the most commonly implemented switching fabric. In this type of switch, the packet transfer rate of the switching fabric is usually at least twice the sum of the input line rates [11], [10]. Therefore, assuming a lower bound of this statement and that there are N ports with input line rates $x_1, x_2, x_3, .., x_N$ in bps. Also, if the speeds of connected medias to input ports 1, 2, 3,..., N of the switch = input rates (c_is) of the receive buffers,

transfer rate of the switching fabric (TRSF) is given as:

TRFS = $[2\times(x_1+x_2+ \ldots+x_N)]$bps =

$$[2\times(c_1+c_2 \ldots+c_N \sum_{i=1}^{N} c_i)]\text{bps} = [2\times()]\text{bps} \quad (3)$$

But Cruz in [9] contends that the operation of a constant delay line is described by a single parameter D, and that all data that arrives in the input stream exits on the output stream exactly D seconds later. We can then say that one packet delay time D in seconds is:

D (seconds)

$$\frac{packet\ length(bits)}{packet\ transfer\ rate(bits/\sec onds)}$$

$$\frac{L(bits)}{packet\ transfer\ rate(bits/\sec onds)}$$

Then, the delay D in seconds of a packet in a constant delay line becomes:

$$D\,(\text{seconds}) = \left(\frac{L}{2\times\sum_{i=1}^{N} c_i} \right)$$

Since the arriving $(N-1)^{th}$ packet will suffer N-2 constant delay times in this model, we then have:

$$D_{CDT}\,(\text{seconds}) = (N-2)\times \left(\frac{L}{2\times\sum_{i=1}^{N} c_i} \right)$$

(5) where, D_{CDT} = maximum delay suffered by a data packet in the switch as a result of N-1 constant delay times, N = the number of I/O ports in the switch, L = maximum length in bits of a data packet, the c_is are the input rates of the receive buffers. For example, c_i, i = 1, 2, 3,…, N for an Ethernet packet switch could be: 10Mbps Ethernet rate, 100Mbps (Fast Ethernet), 1000Mbps (Gigabit Ethernet).

iii. First-Come-First-Served Multiplexer (FCFS MUX)

Our multiplexer is bufferless. In [10], a bufferless multiplexer concept was used in multiplexer analysis. We adopt the notion in that outputs contention resolution (packet scheduling policy) along with output buffering (used for output queuing), both in the switch is called packet multiplexer [10, p.120]. Packets therefore, do not suffer delay in our FCFS MUX. The delay that is supposed to be suffered by packets in the FCFS MUX is represented by the succeeding FIFO Queuing delay.

iv. First-In-First-Out (FIFO) Queue

We have shown in [12] that if;

d_j = maximum delay in seconds incurred by the j^{th} packet in crossing the FIFO Queue, σ = maximum

amount of data traffic that can arrive in a burst in bits, C_{out} = bit rate of the output link (switch port) in bits per second (bps), then d_j is given by Eq. (6).

$$d_j = \frac{\sigma}{C_{out}}$$

6) But, there is no general agreement in the literature on how to characterize bursty traffic (how do we assign a numerical value to σ?) [13], [14]. In this paper, we adopt the recommendations of RFC 2544 in [15]. It was made under the Device Under Test (DUT) recommendations to switch (and other similar devices, like, router manufacturers). It states that tests should be run with burst sizes of 16, 64, 256, and 1024 frames. In this paper therefore, we will use the average of these four recommended burst sizes; that is, the parameter σ is taken as

$$\frac{16+64+256+1024}{4} \text{ Ethernet frames}$$

= 340 Ethernet frames.

v. Transmission Delay

According to [16], [17], [8], if L = length of frame in bits, R = full rate of medium that connects to the output port of the node in bits/sec,

then, the time to transmit the frame at full rate

$$= \frac{L}{R} \text{ secs.}$$

Therefore, if $D_{maxtrans}$ = maximum transmission delay that any packet can incur in the switch in seconds, L = maximum length of a packet in bits, C_{out} = transmission speed of the output port (link) in bits/sec, then;

$$D_{maxtrans} = \frac{L}{C_{out}} \text{ Seconds.}$$

(7) Having derived the maximum delay expressions for each of the components in Eq. (1), we can now proceed to insert these maximum delay expressions into this equation. Therefore, if we replace C_i in Eq. (2) by C_{N-1} (since we have assumed that the data packet that arrived at port N-1 will suffer the maximum delay it is the last to be forwarded to the output port N), we then have (after summing similar terns):

$$D_{max}(\text{seconds}) = \frac{L}{C_{N-1}} + (N\text{-}1) \times \left(\frac{L}{2 \times \sum_{i=1}^{N} C_i} \right) + \frac{\sigma}{C_{out}} + \frac{L}{C_{out}}$$

where; D_{max} = maximum delay in seconds for a packet to cross, any, N-port packet switch;

N = no of input/output ports; C_i, i = 1, 2, 3,.., N = bit rates of ports 1, 2, 3,..,N in bps = channel rates of input ports in bps;

C_{out} = bit rate of the N^{th} output line in bps = output port rate of the N^{th} port (the destination of the other N-1 input traffics);

C_{N-1} = bit rate of the $(N-1)^{th}$ input port in bps; L = maximum length in bits of a data packet; σ = maximum amount of traffic in bits that can arrive in a burst.

4. Evaluation of Switch Model

The contention in this paper that the 'N-port maximum delay switch model' is indeed what the term in quotes suggests, must be adequately substantiated. In the first place, the functionalities and operation of packet switches are largely the same. Their differences are mainly in the choice of switching fabric implementations and in the type of buffering employed (input, output, or input and output). But the challenge that arises in the context of this paper is 'how good is our maximum delay model?' In order words, is there an optimum upper-bound delay by which we can measure our maximum delay model? According to 18], issues that have to do with making comparisons are undoubtedly difficult task. They are difficult because the framework on which a comparison is based must be clearly defined; otherwise, the whole exercise may be meaningless. This is because, the more acceptable this framework is, the more acceptable the results of the comparison is, likely to be.

Some researchers ([19], [20]) have attempted to solve this problem by using network simulation software packages such as OPNET Modeler, NS-2 (Network Simulator-2), Comnet 111 to model network components in order to be able to carry out performance comparisons. [20] used the Comnet 111 to model a 1-switch and 3-hosts network and the upper-bounded end-to-end delay values obtained with the simulator were compared with the upper-bounded end-to-end delay values that were computed using the algorithm that was proposed in the paper. But the values that were obtained from using the network simulator, differed, widely, from the values that were computed using the algorithm. Hence, we may then ask the next pertinent question: how good are the values that are obtained from using network simulators? In [21], it was asserted that 'breach of credibility'

by studies that are based on network simulation tools has been reported in the literature. We therefore, decided on a simple ingenious 'practical' way to validate the 'goodness' of our model in this pape. Incidentally, this ingenious practical method showed that values (for example delay values) obtained from using network simulators can be very misleading. This therefore supports the 'breach of credibility' by network simulators that have been reported in literature as asserted in [21].

4.1 Model Validation by Comparison of Three Maximum Delay Packet Switch Models

Using a channel rate of 100Mbps and the maximum size of an Ethernet (we assumed a switched Ethernet network) frame, typical maximum delay values for the model represented by Eq.(8) are now computed. The extended Ethernet frame has a maximum frame size of 1530 bytes = 1530×8 bits = 12240 bits

For the model represented by Eq.(8),

Forwarding Delay (FWD) = $\frac{L}{C_{N-1}}$ secs., L =

12240 bits, $C_{N-1} = 100\times10^6$ bps, therefore,

FWD = $\frac{12240}{100\times10^6}$ = 12240 × 10^{-8}secs = 0.12240 ms

Routing or Switching Delay (RSD)

$$= \frac{L}{2\times\sum_{i=1}^{N} C_i} \text{ secs.}$$

We assume here that the switch is a Super Stack 11 Ethernet Switch 3900 by 3Com Corp. It is a 24 ports switch. Here, L = 12240 bits, $C_i = 100\times10^6$ bps, N= 24, therefore

RSD = $\frac{12240}{2\times24\times100\times10^6} = \frac{12240\times10^{-8}}{48}$ =

255 ×10^{-8}secs = 0.00255 ms

Simultaneous Arrivals of packets Delay (SAD)

$$= (N-2)\times\left(\frac{L}{[2\times\sum_{i=1}^{N} C_i]}\right) \text{secs.}$$

SAD = (N-2) × RSD = (24-2) × RSD = 22 × 0.00255ms = 0.05610 ms

Frame Transmission Delay (FTD) = $\frac{L}{C_{out}}$ secs.; L = 12240 bits, $C_{out} = 100\times10^6$ bps,

therefore,

FTD = $\frac{12240}{100\times10^6}$ = 12240 × 10^{-8}secs

= 0.12240 ms

Queuing Delay (QD) = $\frac{\sigma}{C_{out}}$ secs., σ =

340×1530×8 = 4,161,600 bits;

therefore,

QD = $\frac{\sigma}{C_{out}} = \frac{4{,}161{,}600\,bits}{100\times10^6\,bits/\sec.}$ =

4,161,600×10^{-8} = 41.616 ms

Adding the five (5) computed delays, the maximum delay of this packet switch model is:

Dmax = 0.12240ms **+ 0.00255ms** + 0.05610ms + 0.12240ms **+ 41.616ms 42 ms**

It has not been easy coming across values for maximum switch delay in the literature. But Georges, Divoux, and Rondeau reported in [20], that the maximum delay obtained with the maximum delay Ethernet packet switch model reported in the paper is 3080 µs, or 3.080 ms; while the COMNET 111 simulation software gave a maximum delay of 450 µs or 0.450 ms. Which of the three (the model that is represented by Eq.(8), the model in [20], or the value given by COMNET 111 as reported in [20]) results can be said to be the better result? We will now use a typical practical switched Ethernet LAN installation scenario in the literature for this comparison.

4.1.1 Selecting an Appropriate Upper Delay Bound

In the view in [22],

- 100 ms is the maximum delay before a user no longer feels that a network is reacting instantaneously,
- 1 second is the maximum delay before a user's flow of thought is interrupted, and
- 10 seconds is the maximum delay before the user looses focus on the current dialog.

This view is in concurrence with IETF RFC 2815: **Integrated Services Mappings on IEEE 802 Networks [23]. Using 100ms as application end-to-end maximum delay, we now make a comparison of the three maximum packet switch delay values.**

i. The maximum delay value in [20] is 3.080 ms.

Using the 100 ms end-to-end application delay bound, it will mean that between two hosts (one, the origin host and the other, the destination host) there can be

$$\frac{100ms}{3.080\,ms} = \textbf{32.5 33 switches.}$$

i. The maximum delay value provided by COMNET 111 as reported in [20] is 0.450 ms.

Between two hosts (one, the origin host and the other, the destination host) there can be

$$\frac{100ms}{0.450\,ms} = 222 \text{ switches.}$$

i. The maximum delay value provided by Eq. (8).is 42 ms.

Between two hosts (one, the origin host and the other, the destination host) there can be

$$\frac{100ms}{42\,ms} = 2.4, \text{ rounded up to 3 switches.}$$

In [24], a switch manufacturer's (Square D) installation instruction bulletin for the installation of the Model SDM 5DE 100, Class 1400 Ethernet packet switch was shown. In was stated in it that switches can be concatenated between devices (hosts) as long as the path between hosts does not exceed four (4) switches and five (5) cable runs. From this information therefore, it can be seen that in practical terms, our model is close to reality (and it is therefore, validated). In fact, we can say with utmost assuredness that the model in [20] and the value provided by COMNET 111 as reported in [20] are very unrealistic as maximum delay bound for an Ethernet packet switch.

5. Conclusion

In this paper, we have explained the development of a maximum delay model of a packet switch. Compared to the maximum delay values of models that were obtained from literature, the value obtained with this model was shown to be very close to practical reality in the context of designing upper-bounded end-to-end delays switched for LANs. Further research efforts are being directed at developing formal methods for designing upper-bounded end-to-end delays switched LANs, using, this model. Determining the maximum amount of traffic that can arrive to a switch, in a burst, that is σ, is a challenge that needed to be confronted. This is presently an area of very intense research activity (see references [13] and [14]). This is because, coming out with an empirically validated value for σ (or how to determine σ) will be a major breakthrough to the Internet and Networking research community.

References

[1] Bolot, J. (1993). Characterizing End-to-End Packet Delay and Loss in the Internet, *Journal of High-Speed Networks*, Vol.2, no. 3, pp. 305-323.

[2] Ferguson, P. and Huston, G. (2009). Quality of Service in the Internet: Facts, Fiction or Compromise?, Retrieved from: http://eprints.kfupm.edu.sa Accessed January, 2010).

[3] Ming-Yang, X., Rong, L. and Huimin, C. (2004). Predicting Internet End-to-End Delay: An Overview, *Proceedings of the IEEE 36th South Eastern Symposium on Information Systems Theory,* pp. 210 214.

[4] Mann, R. and Terplan, K. (1999). Network Design: Management and Technical Perspectives, CRC Press Ltd, New-York, USA.

[5] Bertsekas, D. and Gallager, R. (1992). Data Networks, Prentice-Hall, Englewood, Cliffs, USA.

[6] Martin, S., Minet, P., and Laurent G. (2005). End-To-End Response Time with Fixed Priority Scheduling: Trajectory Approach Versus Holistic Approach, *International Journal of Communication Systems*, Vol. 18, pp.37-56.

[7] Torab, P. and Kamen, E. (1999). Load Analysis of Packet Switched Networks in Control Systems, *Proceedings 25th Annual Conference of the IEEE Industrial Electronics Society*, San Jose, CA, Vol. 3, pp.1222 1227.

[8] Alberto, L. and Widjaja, I. (2004). Communications Networks: Fundamental Concepts and Key Architectures, McGraw Hill, New-York, USA.

[9] Cruz, R. (1991). A Calculus for

Network Delay, Part 1: Network Elements in Isolation, *IEEE Transactions on Information Theory*, Vol. 37, no.1, pp.114-131.

[10] Anurag, K., Manjunath, D. and Kuri, J. (2004). Communication Networking: An Analytical Approach, Morgan Kaufmann Publishers, San Francisco, USA.

[11] Song, Y. (2001). Time Constrained Communication over Switched Ethernet, *Proceedings IFAC International Conference on Fieldbus Systems and their Application*, Nancy, France, pp. 152-169.

[12] Eyinagho, M., Falaki, S. and Atayero, A. (2011). Characterizing the Maximum Queuing Delay of a Packet Switch, *International Journal of Computer and ICT Research*, Vol. 5, Issue 2, pp. 32-37.

[13] Sven, U., Ales, F., and Stanislav, H. (2008). Quantification of Traffic Burstiness with MAPI Middleware, *Proceedings 2008 CESNET (Czech Educational and Scientific Network) Conference*, Prague, Czech Republic, pp.13-22.

[14] Ryousei, T., Yuetsu, K., Tomohiro, K., Motohiko, M., and Fumihiro, O. (2006). Real Time Burstiness Measurement, *Proceedings PFLDnet 2006 Conference, Nara*, Japan, pp.109-115.

[15] Request For Comments 2544, Retrieved from: http://www.ietf.org/rfc/rfc 2544 (Accessed January, 2010).

[16] Kanem, E., Torab, P., Cooper, K., and Custodi, G. (1999). Design and Analysis of Packet Switched Networks for Control Systems, Proceedings1999 *IEEE Conference on Decision and Control*, Phoenix, AZ, pp. 4460-4465.

[17] Reiser, M. (1982). Performance Evaluation of Data Communications Systems, *Proceedings of the 1982 IEEE Conference*, Vol. 70, no. 2, pp.171-194.

[18] Adegbenro, O. (1986). LSI-Oriented Residue Arithmetic Circuits and their Application in the Implementation of a Digital Signal Processor, A Dissertation for the Degree of Doctor of Engineering, Department of Electronic Engineering, Faculty of Engineering Graduate Division, Tohoku University, Sendai, Japan.

[19] Abiona, O. (2005). Development of a Framework for Optimizing Access to WAN Resources, Ph.D Computer Science Thesis, Obafemi Awolowo University, Ile-Ife, Nigeria.

[20] Georges, J., Divoux, T. and Rondeau, E. (2005). Confronting the Performances of a Switched Ethernet Network with Industrial Constraints by using Network Calculus*", International Journal Communications Systems*, Vol.18, pp. 877-903.

[21] Gilberto, F., Marcos, P., Emmanuel, J., Martin, F. and Martin, J. (2009). OPNET Modeler and Ns-2: Comparing the Accuracy of Network Simulators for Packet Level Analysis using a Network Test bed, Retrieved from: http://genie.iitd.ernet.in/ns/weas (Accessed January, 2010).

[22] Nielson, J. (2009). Designing Web Usability, Retrieved from: http://www.amazon.com/Designing-Web-Usability-Jakob-Nielson/dp (Accessed January, 2010).

[23] Integrated Services Mappings on IEEE 802 Networks, Retrieved from: http://tools.ietf.org/html/rfc2815 (Accessed January, 2010).

[24] Square D® Ethernet Switch Model SDM 5DE 100 Installation and Illustration Bulletin, Retrieved from: www.us.Square D® (Accessed January, 2010).