IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 5, Ser. II (Sep - Oct 2019), PP 01-09
www.iosrjournals.org

Security Shortcomings of Electronic Web Based Voting Systems for Universities in Kenya

Prestone Simiyu[1], Dr. Samuel Mbugua[2], Dr. Daniel Otanga[3]
[1](Department of Information Technology /Kibabii University, Kenya)
[2](Department of Computer Science / Kibabii University, Kenya)
[3](Department of Computer Science / MasindeMuliroUniversity of Science and Technology,Kenya)
Corresponding Author: Prestone Simiyu

Abstract: *Electronic Voting can deliver free and fair elections as well as ensuring on time release of results. One factor fueling the adoption of e-voting is the access to internet and more so GSM network, by majority of the world population. However, with this adoption of electronic voting around the world, some concern are being raised regarding the process. Technically, it's hard to achieve availability, integrity and confidentiality which are the pillars of a free and fair elections while using electronic voting. It is because of this issues that the purpose of this research was to examine security shortcomings for existing web based electronic voting frameworks. A mixed research design was used for the study covering both descriptive survey design and content analysis. The target population of the study was 13700 students, 60 student's council leaders, 64 electoral Officials, 4 dean of student office officer, 6 ICT directorate staff and 29 top management from Catholic University and Kenya College of Accounting University both located in Kenya. Purposive sampling was used to select electoral commission chair, Dean of students while random sampling was used to select 6 management officers, 6 ICT directorate staff, 376 students, 14 electoral officials' staff and 12 student leaders giving a sample of 420. Data collection Instruments were questioners, interview schedule and observation and the data collected was analyzed using descriptive analysis. It was established from the study that the university voting system of the sampled had issues with availability as they had failed at some point. Also, the systems experienced slow speed on the voting day. Another outcome was that the system had locked out a group of eligible voters. Therefore, the systems had issues with integrity. Finally, it was established that the voting system had not allowed non eligible people to vote as well as the system can link the voter and the voter's ballot which is a confidentiality security concern. The output of the paper is a framework for solvingthe current security issues of the electronic voting web based system for Kenyan universities. The findings of the study are significant to electoral commissions of different institution, voters and policy makers.*

Keywords: *Electronic Voting, Web based system Security, Kenyan Universities*

Date of Submission: 18-09-2019 Date of acceptance: 03-10-2019

I. Introduction

Election is a process at the heart of a democratic society. An election cycle can be divided into three periods; pre-election period, election period and post-election period. The pre-election periods begins when electoral agencies prepare the voters and the voting process. It may involve procurement of electoral materials which include, ballot boxes, ballot papers and electronics, training of electoral staff and testing of the system to be used. The election period main process is voting. The post-election process may have the following activates counting of votes and dissemination of electoral results. Therefore, voting is the process that enables a specific group of people to make a decision over a given number of options. Voting can either use a full manual, a full electronic system or a combination of the two systems[4]. Notably, the Council of Europe recommendations define electronic voting as the use of electronic means in at least the casting of the vote. Also, this council has divided electronic voting into two; the first on being an electronic voting supervised by the physical presence of representatives (an example of this is electronic voting machines at poll sites popularly known as Direct Recording Electronics) and the other being an electronic voting within the voter's sole influence (remote e-voting). Furthermore, in electronic remote voting, there is nophysical supervision by representatives. An example of the remote electronic voting is voting from one's own or another person's computer via the internet (Web based system), by mobile phones platform (web based and using Short Message Service, SMS) [7]

In Kenya, electronic voting is gaining popularity with the national government adopting it for the country's general election for 2013 and 2017. Also, electronic voting is being used by different institution in Kenya including the Senate, Parliament Chambers and different universities. One of the factor increasing the adoption of remote electronic voting is the mobile technology. This mobile technologies include web based

systems, Short Messaging services and the Unstructured Supplementary Service Data (USSD) and the technology that can be integrated to electronic voting for better systems.

However, the electronic voting being adopted is a web based system with a 3 tier (Client, network and server) architecture that has the following security issues; Man in the Middle (MAM) attack security issues at the client; distributed denial of service(DDOS) attack at the network and both MAM and DDOS at the server. Integrity and Confidentiality of the voting system are affected by the MAM attack that can be used to change or monitor the voter's intention. The other security aspect availability is affected by DDOS. Furthermore, in the current universities web based system, a vote who successfully casts a vote will receive an SMS, however if unsuccessful there is no communication to the voter. Hence a voter can be denied a chance to vote unknowingly affecting the integrity of the system.

II. Related studies

According to Al-Amen &Talab, 2013, the security of the system in an election should be given high priority. This is because any process that has the potential to threaten the integrity of the system or even the perceived integrity of the system is a high profile attack. This attacks attracts the best hackers who would try to manipulate the results of the election without being noticed. The security of an election can be from different points of view. This research seeks to address the technology aspect. Notably, Voter Authenticity, Voter Anonymity, System Integrity, Data Integrity, Secrecy, Non-Credibility, Reliability, Availability, system Disclosability, simplicity testing and certification, system accountability, personnel integrity, Operator Authentication and control and distribution are the requirements of a secure electronic voting system[2]. Also, an e- voting security attack can be initiated in either the hardware, software or the Human ware parts of the system. To understand this attacks, the following sections discusses different types of attacks.

Types of Security Attack

Security attacks can be divided into two; The Client and Server Attacks and The Communication Infrastructure Attacks. Man in the middle attack targets the client and server directly while denial of service attacks target the communication infrastructure that links the server and the client, [1]

Client and Server Attacks

Rubin notes that attacks to the client and server are done by a malicious payload, [8]. He further defines a payload as a software designed to do the penetration to a system. Penetration attacks involves the use of a delivery mechanism to transport a malicious payload to the server in form of a Trojan or a remote control program. Ones the software is installed in the sever, the malicious payload can be used to spy on the ballots, prevent voters from casting votes or modify votes. This attack can be carried out successfully without detection and security mechanisms such as encryption and authentication like secure socket layer and hypertext transport protocol (https) are impotent against this kind of attack. This is because the payload is below the level of abstraction at which this mechanism operates. Furthermore, intrusion detection software and antivirus are also powerless to this attack as the two search for known signatures for malicious softwares or other signs of unauthorized activity. Malicious payload operates from unknown or modified programs and alter system files to effectively "authorize" the changes made. Also, an attack can originate from anywhere in the world and can be delivered to the sever using different ways including email, optical drives, downloads or by exploiting bugs and security flaws in program installed in the server. Activation of such a program can be based on time or a trigger such downloading of the software or opening of an email,[1]. Notably, if the software is installed in the client part of the voter, then the voting process can be monitored through man in the middle attack, denied or even changed before being passed to the communication infrastructure. With many people voting from different places, it is really hard for each of the voters to identify a malicious payload operating in the device being used to cast the vote, [10]. One possible solution to this attack is monitoring and controlling the client side software to ensure that there is no connection with any other internet host apart from the correct servers. The clients can also be set to reject any installation or introduction of new software other than the application software. However, with this attacks can be triggered from an insider [1].

Buffer overflows is another attack mechanism targeting the client and the server. The main aim of this attack is to target the memory in a way that more data is assigned to a specific memory location. Notably, Web server based applications and browsers are vulnerable to this attack as long as the attack is initiated. It is a very common attack targeting the server and client of a system, [10]. ActiveX controls that are on the web server and are attached to the content are used to execute different programs. If the browser being used allows ActiveX controls to be executed, then Trojan horses can be downloaded and executed with the knowledge of the user and hence be used to monitor, change or redirect the voters intention of an election.

According to [10], Distributed Denial of Service (DDOS) attack targets two parts of a system; the communication infrastructure and the Server. With the server, the attacker using various and many computers

called "Zombies" floods a sever with a lot of information flowing in at a first rate and high volumes. The main intention is to keep the server busy working on this "Junk" data and hence ends up hanging or avoids its main duty of receiving and processing of voters intentions. Sychryen Notes that SSL protected website are vulnerable to this attack. This is because cryptographic process that should be done in the SSL protocol takes a lot of time. If a DDOS attack can completely lock a server from receiving data from the clients, an election can be halted.

Communication Infrastructure

DDOS attack can also target the communication infrastructure with the main aim blocking client data movement to the server. The attacker forwards IP packets using the internet as a means of communication to the server and receives the same packets from the server with the main aim of "Jamming" or keeping the communication channel busy. If this IP packets are sent from various devices posing as clients, then the looping of the system will be high and hence a chance of the targeted channel failing. The communication channel fails when the router of that channel fails.

Another way to attack the communication channel according to [8]in a research done in the AT &T Labs is to have an algorithmic that grows in size split into many small fragments and stored in different computers in the network work called "daemon". This computer is coordinated and activates by a "Master" on the same network. When the attack is initiated, the small fragment makes loops from the sever to the router. The fragments have ability to merge into one and once merged, grow in size. This is done until the size of the algorithm exceed the bandwidth of the communication infrastructure. Once this is done the network is brought to a standstill and no connection to the server or from the server will be done. [8]notes that the DDOS targeting the communication channel are potent from the results of a test of a program called Tribe Flood Network (TFN). He notes that another program "Ping of Death" is a fatal one used to initiate the fragment DDOS attack. Rubin says that the reason why DDOS on the communication channel are very potent is that the programs used to initiate this attacks can be accessed by anyone and that a network can receive more than one attack at the same time. DDOS can also target the Domain Name Service (DNS) server. DNS are servers that are used to map IP address to domain names. If a DDOS attack is successfully implemented to a DNS Server, then there will be no communication to the server for voters who don't know the IP address of the server. The known date and time for elections fully exposes the voting system to this attack and from anywhere around the world.

Man in the Middle attack is another attack that targets the communication channel. It can be done in various way the first one being DNS spoofing. In this attack, an image of the correct IP address overwrites it with the same functionality. The voter follows instructions for voting and thus communicates with the hacker unknowingly revealing all private and sensitive information. For example, the voter might be looted to vote on a page that is similar to the correct one and once the voter inputs the username and password, the attacker logs in the correct IP address and votes for the voter. This attack can happen in the context of social engineering where an attacker sends emails to the voters containing links to the attacker's machines. [10]Notes that this attacks can be effectively addressed with digital certificates of websites, however, a large number of the current population are not familiar with this certificates therefore wont check for the validity of the voting website. This attacks can be used during registration of voters, where voters miss on the register because of registering using a fake IP address.

Security Short Coming of Web Based Existing Voting System

The following section looks at security shortcomings of two commonly used electronic voting systems

Bio Metric Voter Registration and Identification Web Based Voting System

Biometric refers to physiological and individual characteristics that can be automatically verified. Biometric system is a system for the automatic recognition of individuals based on their behavioral and biological characteristics. There are two types of biometric systems; Physical biometric and biological biometric system. Biometrics uses artificial intelligence technologies and can use one or a combination of the following; facial recognition, finger print, hand geometry, iris scan, retinal scan, vascular patterns, deoxyribonucleic acid (DNA), ear print and voice recognition. Each one of this technologies has its own security short comings but in general the security shortcomings can be divided into two; false reject (FR) and false accept (FA). False reject causes the system to deny an eligible voter a chance to vote while false accept allows a non-eligible person to vote. The first shortcoming of Biometric Electronic voting is that it is affected by environment and usage equipment. Once there is change in environment and equipment used the features being recorded might vary. Secondly some daily jobs like a person who deals with chemicals might alter the patterns of the finger prints or eye iris. For voice recognition sickness and aging might cause slight variance to a person voice as well one person voice can be the same as other person voice. For voice there is chance that voice can be recorded and used without the person being there as well as finger prints and eye iris can be cut sorted and used with the approval of the person. Facial recognition is affected by light and glass for a person who uses spectacles. DNA

is the most reliable source of biometric recognition but should be noted that it takes time and is very expensive. With election being time bound, DNA is not a favorite. Also with DNA someone can get access to an individual sample and use it without the user noticing. Also, for most biometric system, the biometric part is used to verify and identification of voters and election officials. However, transmission and storage used other technologies which are not biometric protected. That means that the framework is still exposed at the transmission channel and storage place. Some biometric systems have the voters registered stored in their hardware while some must connect to a server before verifying a voter. For those that must connect to sever still can experience DDOS and man in the middle attack at the communication channel and storage.

Internet Web Based Voting System

Remote Internet Voting enables eligible voters to cast their votes from anywhere as long as they can access the internet and a gadget with the voting software. Most remote voting systems allows the user to place a vote more than one time but the final vote is the one that will be counted. Estonian Internet voting accounts for almost 30 percent of the national votes casted being the leading national internet voting system. Estonian Internet voting was first deployed for use in national election in Estonia in 2005 being the first country to use remote internet voting. However the system is controversial with security critics in Estonia and around the world questioning the security aspect of the system, [3]. According to [9]report on the dangers of internet voting, internet voting issues are not going to be resolved any time soon. Spakovsky notes that to create a secure online voting system with the current technology is an idea that is dangerously mistaken. This is because internet voting is vulnerable to cyber-attack and fraud hardware and software multifunctioning, as well as the basic manner in which the Internet is organized. 32 Computer Technologists' Statement on Internet Voting in 2008 notes the following technical security issues facing internet voting systems.

Malicious softwares which can be installed either on the server or client computer, firmware or hardware that have the ability to change, create or delete voter's intention, change the appearance of the ballot or switch input of the voter, leaking information about votes to enable voter coercion, denying and passing information to discourage voting, or performing online electioneering through algorithms. Denial of service attacks which targets the communication channel through the client computers (called "botnets"), with an aim of jamming the network or redirecting traffic of votes to a different destination. This attacks can be initiated by anybody with access to the internet. Also, accountability of the internet voting system might be wanting. With the large number of votes casted it is next to impossible to investigate each vote one by one. The investigation is left for the machine. With this scenario, the computer scientists noted that a change can be made from people with access to the system such as the equipment manufacturers, technicians, system administrator and electrical official and be undetected. The Scientists note that the challenges might look simple and could have various solutions but can't be fully eliminated. There is no hardware or software that currently exists the can overcome this challenge, [9]. Furthermore, the internet architecture makes it vulnerable to almost all cyber-attacks yet a number of the attacks are difficult to track the origin. The computer scientists recommended against Pilot studies of any Internet Voting system because the apparent success of such a study absolutely cannot show the absence of problems that by their nature may go undetected, [11].

III. Research Methodology

The study was done on university systems for Catholic University of East Africa and Kenya College of Accounting University. The two university were randomly selected from a target of four university that were identified from documented evidence. This two university gave a target population of 13863 with 13700 being students, 60 student's council leaders, 64 electoral Officials, 4 dean of student office officer, 6 ICT directorate staff and 29 top management. Purposive sampling was used to select key informants that included, Dean of students, director ICT and chair of election commission, while stratified random sampling was used to select 6 management officers, 6 ICT directorate staff, 376 students, 14 electoral officials' staff and 12 student leaders giving a sample of 420. Interview schedules and questionnaire were validated and tested for reliability before being issued to respondents with the aim of collecting data. The collected data was analyzed using descriptive survey and the output was represented using graphs and tables.

IV. Result and Discussion

The research had a respondent rate of 81.43 percent having collected views of 342 out of 420 respondents. Among the 342, 210 were from Catholic University of East Africa (CUEA) while 132 came from Kenya College of Accounting University (KCAU). Also, 180 where male while 162 where female. The study was well balanced across different specialization with a majority of the respondents being between 18 and 25 years. The research noted that all the respondents had used electronic voting at least once and that the majority of the respondent's phones could access 3G network. This information is summarized in the table 4.1 and 4.2 below

Table no 1: Respondents Categorized by Gender

Gender of Respondent	CUEA	%	KCA	%	Total	%
Male	109	31.8%	71	20.8%	180	52.6%
Female	101	29.6%	61	17.8%	162	47.4%
Total	210	61.4%	132	38.6%	210	100%

Table no 2: Respondents by Speed and Operating system of their Phone

Phone Operating System	4G	%	3G	%	2G	%	Total	%
Mac (IPhone, Apple)	8	2.3%	18	5.2%	0	0%	26	7.7%
Windows	20	5.8%	31	9.1%	0	0%	51	14.9%
Android	103	30%	150	43.9%	0	0%	253	73.9%
Others	0	0%	0	0%	12	3.5%	12	3.5%
Total	131	38.3%	199	58.2%	12	3.5%	342	100%

Table no 3: Respondents by number of times for using web based system

Number of times of using the System	CUEA	%	KCA	%	Total	%
1	111	32.5%	132	38.6%	243	71.1%
2	99	28.9%	0	0%	99	28.9%
Total	210	61.4%	132	38.6%	342	100%

In order to examine the security shortcoming of existing web based voting system, the research started by finding out if the population understood the three pillars of security (Availability, Integrity and Confidentiality). The study established 259 of 342 respondents and 284 of 342 respondents strongly agreed to a secure web based voting system observing integrity and availability. This formed 75.7 and 83 percent of the population suggesting that the voter were comfortable with a system that is always available and observes integrity. On confidentiality, the study established that the population was divided with 32.5 percent strongly agreeing to secure web based system should observe confidentiality. This division could be because some of the population had no problem with their intention being made public while others had an issue. This information is summarized in the table 4.4, 4.5 and 4.6.

Table no 4: Respondents Categorized by secure electronic voting system should always be available

Specialization		Strongly Agree	Agree	No Idea	Disagree	Total
Information Technology	Count	89	35	2	2	128
	% of Total	26.0%	10.2%	0.6%	0.6%	37.4%
Business and Management	Count	80	12	2	0	94
	% of Total	23.4%	3.5%	0.6%	0%	27.5%
Teaching and Academics	Count	73	19	1	4	97
	% of Total	21.3%	5.6%	0.3%	1.2%	28.4%
Engineering and Science	Count	3	1	0	0	4
	% of Total	.9%	0.3%	0%	0%	1.2%
Health	Count	3	0	0	0	3
	% of Total	0.9%	0%	0%	0%	0.9%
Others	Count	11	2	0	3	16
	% of Total	3.2%	0.6%	0%	0.9%	4.7%
Total	Count	259	69	5	9	342
	% of Total	75.7%	20.2%	1.5%	2.6%	100.0%

Table no 5: Respondents Categorized by secure electronic voting system always maintaining integrity

Specialization		Strongly Agree	Agree	No Idea	Disagree	Total
Information Technology	Count	101	25	1	1	128
	% of Total	29.5%	7.3%	0.3%	0.3%	37.4%
Business and Management	Count	82	10	2	0	94
	% of Total	24.0%	2.9%	0.6%	0%	27.5%
Teaching and Academics	Count	81	14	0	2	97
	% of Total	23.7%	4.1%	0%	0.6%	28.4%
Engineering and Science	Count	4	0	0	0	4
	% of Total	1.2%	0%	0%	0%	1.2%
Health	Count	3	0	0	0	3
	% of Total	0.9%	0%	0%	0%	0.9%

Others	Count	13	2	0	1	16
	% of Total	3.8%	0.6%	0%	0.3%	4.7%
Total	Count	284	51	3	4	342
	% of Total	83.0%	14.9%	0.9%	1.2%	100.0%

Table no 6: Respondents Categorized by secure electronic voting system always observe confidentiality

Specialization		Strongly Agree	Agree	No Idea	Disagree	Strongly Disagree	Total
Information Technology	Count	38	27	0	25	38	128
	% of Total	11.1%	7.9%	.0%	7.3%	11.1%	37.4%
Business and Management	Count	32	16	1	29	16	94
	% of Total	9.4%	4.7%	.3%	8.5%	4.7%	27.5%
Teaching and Academics	Count	35	18	0	24	20	97
	% of Total	10.2%	5.3%	0%	7.0%	5.8%	28.4%
Engineering and Science	Count	2	0	0	0	2	4
	% of Total	0.6%	0%	0%	0%	0.6%	1.2%
Health	Count	1	0	0	1	1	3
	% of Total	0.3%	0%	0%	0.3%	0.3%	0.9%
Others	Count	3	2	0	10	1	16
	% of Total	0.9%	0.6%	0%	2.9%	0.3%	4.7%
Total	Count	111	63	1	89	78	342
	% of Total	32.5%	18.4%	0.3%	26.0%	22.8%	100%

The study sort to know from the population if their university system had experienced security breach by asking questions that touched on the availability, integrity and confidentiality of the system. On availability the study asked two question; the first one if their university system had ever failed and the second question if their university system had experienced slow speed on the voting day. The research noted that the voting system for the two universities had failed at some point and experienced slow speed on voting day. This results are summarized by table 4.7 and 4.8

Table no 7: Respondents categorized by failing of the universities electronic voting

University		Strongly Agree	Agree	No Idea	Disagree	Strongly Disagree	Total
CUEA	Count	92	59	15	44	0	210
	% within University of Respondent	43.8%	28.1%	7.1%	21.0%	0%	100.0%
KCA	Count	58	38	0	25	11	132
	% within University of Respondent	43.9%	28.8%	0%	18.9%	8.3%	100.0%
Total	Count	150	97	15	69	11	342
% within University of Respondent		43.9%	28.4%	4.4%	20.2%	3.2%	100.0%

Table no 8 Respondents categorized by experiencing slow transmission rate during voting day

University		Strongly Agree	Agree	No Idea	Total
CUEA	Count	188	21	1	210
	% within University of Respondent	89.5%	10.0%	0.5%	100.0%
KCA	Count	108	23	1	132
	% within University of Respondent	81.8%	17.4%	0.8%	100.0%
Total	Count	296	44	2	342
% within University of Respondent		86.5%	12.9%	0.6%	100.0%

To test both confidentiality and integrity, the study asked two questions; one to establish if their university voting system has ever allowed a non-eligible voter to vote and if the system had ever denied a eligible voter a chance to vote. The study established that the sampled population was confident that the system had not allowed a non-eligible voter while the two the system had at some point locked out eligible voters a chance to vote. This information is summarized in the table 4.9 and 4.10 below

Table no 9: Respondents categorized by electronic voting denying an eligible voter a chance to vote

University		Strongly Agree	Agree	**No Idea**	**Disagree**	
CUEA	Count	188	19	1	2	210
	% within University of Respondent	89.5%	9.0%	0.5%	1.0%	100.0%
KCA	Count	108	20	2	2	132
	% within University of Respondent	81.8%	15.2%	1.5%	1.5%	100.0%
Count		296	39	**3**	**4**	**342**
% within University of Respondent		86.5%	11.4%	**0.9%**	**1.2%**	**100.0%**

Table no 10: Respondents categorized by electronic voting allowing a non-eligible voter to vote

University		Strongly Agree	Agree	No Idea	Disagree	Strongly Disagree	Total
CUEA	Count	12	13	31	61	93	210
	% within University of Respondent	5.7%	6.2%	14.8%	29.0%	44.3%	100.0%
KCA	Count	8	12	29	27	56	132
	% within University of Respondent	6.1%	9.1%	22.0%	20.5%	42.4%	100.0%
Total	Count	20	25	60	88	149	342
% within University of Respondent		5.8%	7.3%	17.5%	25.7%	43.6%	100.0%

Proposed Solution for the current web based voting system security issues

The study established that the population knew that availability and integrity were indicators of security. The study noticed that the population was divided on confidentiality as an indicator of security. From table 4.7, the study noted that the current web based system had failed at some point because of different issues. Also, the system experienced slow transmission speed on the voting day. From this we can conclude that the current web based voting system lacked availability. Integrity and Confidentiality were tested together. First the study asked the respondents if the current voting system had allowed a non-eligible voter a chance to vote. The study established that the current voting system had not allowed a non-eligible voter to vote with 43.6% strongly supporting this. On the man in the middle question, the study established that 79.6% of the population had no idea. The study noted that 12 staff from Information technology had agreed to this. Since the Information Technology department is the host of the system, then they could be the ones only aware of such an attack. From this we can say the current web based system has issues that affects all the three indicators of security.

Availability of the system is the most affected. One of the main cause of systems to be unavailable is traffic congestion. This could be because of poor monitored usage of system, low bandwidth allocation or a denial of service attack. Monitoring can be done by human beings with the help of different software. Low bandwidth can be caused by poor management of the communication channel. For example if a number of voters stay on the communication channel for 30 minutes knowingly or unknowingly, this might cause congestion. One of the possible solution to this is using a technology that is session bounded. This means each session is given a specific time, after that time the voter will be locked out. However, this should be done in a way that the time allocated to each voter is sufficient

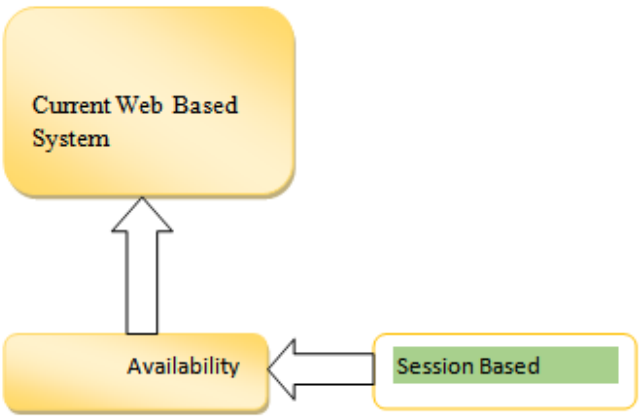

Figure no 1: Session Based technology to increase availability of the system

Another main challenge with the current voting system is that one is able to link the vote to the specific person who voted. This can lead to a lot of voting malpractice like buying of voters or coerced voting. This way voters may not place their intention in a free and fair way. To solve this a technology that does not store specific voters intention and as well as communicates to the voter in real time till the end of the voting process should be used.

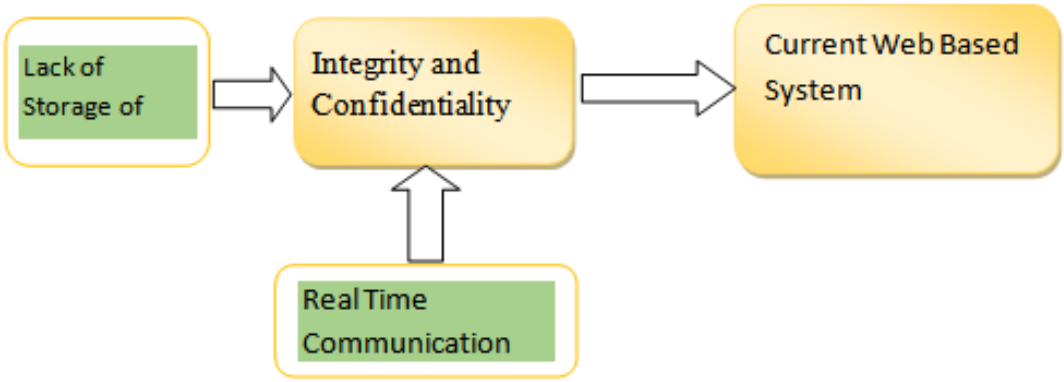

Figure no 2: Real time and Lack of Storage of messages technology to increase integrity and confidentiality

Moderating variables of the study were political influence and User literacy. For political influence, the study ensured that the sampled population was well balanced from both political sides. This way the study captured views of both the wining and loosing political parties. The study targeted the literate population and hence was not affected by the illiterate population.

Combining figure 5.1, figure 5.2 and figure 5.3 gives a good representation of the proposed solution to the current web based security issues of electronic voting.

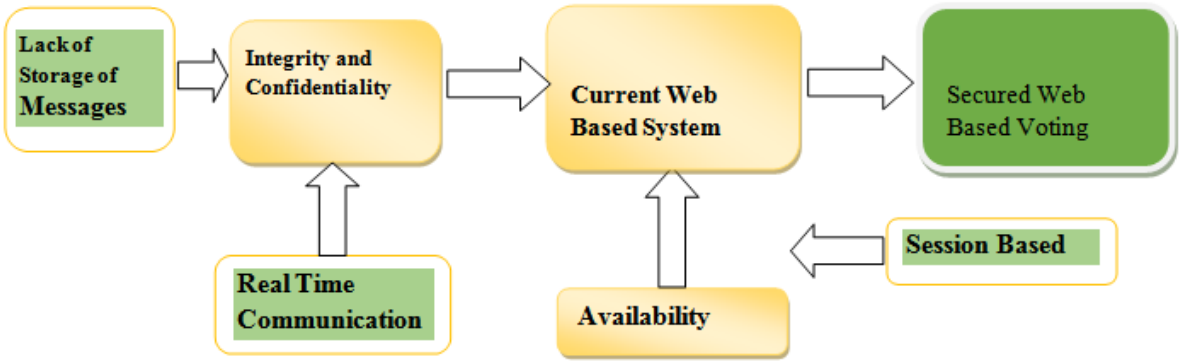

Figure 5.4: Proposed solution for the current security issues for electronic web based voting system

V. Conclusion

The study established that the current voting system for the sampled two universities had failed at some point. This forced the university to revert to manual voting system. This shows that the current web based voting system are not perfect and have issues. The study also established that the two systems have locked out eligible voters. This is a security short coming because it comprises the availability of the system. Notably, the current voting system had not allowed and eligible voter to place a vote for the two universities. On the speed of transmission on voting day, the study established that the voting system experienced slow speeds on the voting day. This could be because of large number of users accessing the system and the system being allocated low bandwidth or miss use of the bandwidth by the voters who keeps on communication to the system even after voting. This low speed can affect the integrity of the system as some voter can assume they have voted yet they have not. The study also established that confidentiality of the system was compromised in the case of a petition of the results. This is because in both system, a list of voters and their pick is always produced. This means the system ties directly the voters and their vote. Furthermore, in both universities a student council is the one that is responsible in case of petitions. Which means voter are able to see how the rest of the voters voted. The study also established that the population was not informed on the different types of attack that the web based system can experience. Majority of the population will have no idea if the web

References

[1]. Al-Amen, A., &Talab, S. A. (2013). E- Voting systems Security Issues. International Journal of Networked Computing and Advanced Information Management, 25-34.

[2]. Bungale, P. P., & Sridhar, S. (2013). Requirements of an Electronic Voting System. Unplublished Thesis, Department of Computer Science, The Johns Hopkins University.

[3]. Drew Springall, T. F. (2014). Security Analysis of the Estonian Internet Voting System. University of Michigan, Ann Arbor, MI, U.S.A, 1-13.

[4]. Dwomfuo, O. G., &Paatey, E. (2011). The Design of an Electronic System. Research Journal of Information Technology 3 (2), 91-98.

[5]. NPR. (2013, March 9th). all tech considered, Tech Culture and Connection. Retrieved from all tech considered: http://www.npr.org/sections/alltechconsidered/2013/03/09/173905754/how-kenyas-high-tech-voting-nearly-lost-the-election

[6]. Obulutsa George, M. F. (2017, Septemeber 20). Reuters. Retrieved from Kenya Supreme Court criticizes election board in verdict on polls: https://www.reuters.com/article/us-kenya-election-court/kenya-supreme-court-criticizes-election-board-in-verdict-on-polls-idUSKCN1BV0QB

[7]. Olusola, O. O., Olusayo, O. E., Olatunde, O. S., &Adesina, G. R. (2012). A Review of the Underlying Concepts of Electronic Voting. Information and Knowledge Management

[8]. Rubin, A. (2011). Security Consideration for Remote Electronic Voting Over the Internet. Florham Park, NJ: AT & T Labs - Research.

[9]. Spakovsky, H. A. (2016). The Dangers of Internet Voting. Washington DC: The Heritage Foundation.

[10]. Sychryen, G. (2010). How Security Problems Can Compromise ReMOTE Internet Voting Sytems. Institute of Business Information Sytems, RWTH Aachen University Templergraben, 12- 23.

[11]. Technologists, C. (2013, March). Verified Voting. Retrieved from Computer Technologists' Statement on Internet Voting: https://www.verifiedvoting.org/downloads/InternetVotingStatement.pdf

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Prestone Simiyu. " Security Shortcomings of Electronic Web Based Voting Systems for Universities in Kenya." IOSR Journal of Computer Engineering (IOSR-JCE) 21.5 (2019): 01-09