A MODEL BASED ON ACCESS CONTROL LIST AND INTRUSION DETECTION SYSTEM FOR IMPROVED CYBER SECURITY IN HIGHER LEARNING INSTITUTIONS IN RWANDA,

A Case of University of Kigali

By MUNYANEZA Alphonse
Co-Author : Dr. Hakizimana Leopord

ABSTRACT

In twenty first century, education sector is turned into digital education, with technology advancing every day, our society is becoming more connected than we have never been there before. While these advancements make our lives much easier, they also add additional risks to our sensitive data. The goal of this research was to put in place a Model based on Access Control List and Intrusion Detection System for improved Cyber Security in Higher Learning Institutions in Rwanda with reference to University of Kigali. The study identified the existing techniques and technology used for Cyber Security at University of Kigali, proposed a new model based on access control list and intrusion detection system framework for improved Cyber Security at University of Kigali, design the communication system and apply ACL and IDS as improved cyber security strategy and the designed model was tested. Questionnaire survey method was used. 5 respondents were University of Kigali IT related staffs who day to day interact with University of Kigali network. The findings indicated that despite the fact that there are existing techniques used for Cyber Security at University of Kigali, they are not enough to guarantee the safety of the university against various attacks. The study recommended that University of Kigali should implement the Model based on ACL and IDS for improving Cyber Security to embrace the benefits of the model based on ACL and IDS for improved cyber security in higher education institutions as 80 % of our respondents stated.

CHAPTER ONE
GENERAL INTRODUCTION

1.1 Introduction

This section "outlines the introduction for this research, the study's context, problem statement, and objective of the study, research questions, the scope and limitations of the research and significance of the study".

1.2. Background to the Study

In twenty first century, "education sector is turned into digital education, with technology advancing every day our society is becoming more connected than we have never been

there before. While "these advances make our lives much easier, they also introduce new risks to our private information." When most people make an online purchase, check their email, or use social media, they do not consider the possibility of their identities being stolen. However, every time you put your personal information on the Internet, you run the risk of it being stolen. This is especially true for students, who spend a lot of time online doing school assignments. With a growing number of individuals making their personal information available online than ever before, it's turning into a haven for hackers. Cyber security needs to be more common knowledge and education needs to be more readily available. While cyber security awareness is an important topic for anyone to discuss, it is especially important for students involved in higher education. College students are becoming a target for phishing attacks at increasingly high rates. College students' information is more vulnerable due to the amount of time they spend on the Internet. This is "particularly true for students enrolled in online programs and classes." They are an ideal target for hackers because they spend so much time on the Internet conducting research, interacting with other students, and participating in class activities"(Hunt 2016).

List of data breaches and cyber-attacks in May 2021 indicated that "116 million records breached including universities records such as University of Franche-Comté which was attacked by phishing scam, personal data was stolen from Australian National University and University of Florida Health Shands notifies patients of a breach of privacy of 1,562 records (Irwin, 2021). In a statement posted on its website, the University of Utah revealed that "it paid a ransomware gang $457,059 in order to avoid having hackers leak student information online." According to the university, it avoided a major ransomware incident and that the hackers only attempted to encrypt 0.02 percent of the data kept on its data centers (Cimpanu, 2020). Located in British Columbia, Canada, Simon Fraser University informed its staff and student body of a cyberattack that breached one of their servers in February."

The data of some 200,000 people could have been put at risk as a result of the cyberattack. In 2021 the University of California, "San Francisco was obliged to pay a $1.14 million to ransom after its School of Medicine was forced to shut down due to a ransomware attack. Because higher educational institutions host so much valuable and confidential research makes them a prime target for state sponsored hackers. Another reason is large deposits of personal identifiable information of large student populations. Cybercriminals can use the fresh credit histories of young people and utilize them for years. Colleges and universities are also more prone to pay ransoms than other types of organizations as they want to limit teach disruption to a minimum. Besides being target rich environments for hackers, the open culture and lack of security controls make educational institutions extra vulnerable (Stankard, 2021)."

The records of Mount Kenya University 211,373 "students both past and present, from admission lists to student and administrative information, were also exposed. Some hackers have shared data from Mount Kenya on various forums, including names, addresses, and phone numbers (Paul, 2020).

"In Rwanda, higher education is provided by both public and private higher learning institutions spread across the country. It is also divided into research-based universities and technical polytechnics, with 31 universities and 9 polytechnics. Higher learning institutions in Rwanda are dominated by private higher learning institutions, which account for 37 of the country's 40 higher learning institutions. Despite enrolling 43 percent of students, the number of public HEIs is small. There are only three public HEIs in the country: The Institute of Legal Practice and Development (ILPD) and the University of Rwanda (UR) (ILPD), Rwanda's dedicated postgraduate legal education institution; and Rwanda Polytechnic (RP). It should be noted, however, that both UR and RP are large, multicampus institutions. With 14 campuses and 26,345 students, UR is the country's largest and preeminent multi-faculty research university (mineduc, 2021)."

Private higher education institutions in Rwanda includes: University of Kigali (UoK), African Institute of Mathematical Sciences Rwanda (AIMS-Rwanda) ,Adventist University of Central Africa (AUCA), Carnegie Mellon University Africa (CMUA), Catholic University of Rwanda (CUR), College of Surgeons of East Central and Southern Africa (COSECSA), East African University - Rwanda (EAUR), Independent Institute of Lay Adventists of Kigali(INILAK), Institut Catholique de Kabgayi (ICK), Institut d'Enseignement Supérieur de Ruhengeri (INES), Institut Polytechnique de Byumba (IPB), Kibogora Polytechnics (KP), Kigali Independent University (ULK), Kigali Institute of Management (KIM), Mount Kenya University (MKU), Premier Early Childhood Teachers Development College (PECDTC), Protestant Institute of Arts and Social Sciences (PIASS), Ruli Higher Institute of Health Sainte Rose de Lima(RHIH), Rwanda Tourism College (RTUC), Institut Superieur Pedagogique de Gitwe (ISPG), University of Global Health Equity (UGHE), Vatel School Rwanda, Oklahoma Christian University (OCU) and Ngoma Adventist College of Health Sciences (NACHS) (hec, 2021)."

Institutions of higher learning in Rwanda used full face-to-face learning and teaching prior to the COVID-19 pandemic, and they shifted to remote online instructing and studying using different platforms such as Moodle and other electronic learning platforms as a result of the COVID-19 total lockdown imposed in Rwanda in March 2020. The teaching staff had to upload the course content online, whereas students had to download the online course. (Uwizeyimana, 2021), Halting their education would not be an option for students "studying at the University of Kigali," because the University was prepared to continue with the teaching, learning, and assessment on the e-Learning platform (Moodle) (Wasajja, 2021)."

Universities and academic institutions have become lucrative targets for cyber-attacks and have already been subjected to a number of high-impact incidents. Academic institutions" manage large amount of important research and sensitive personal information, making them an appealing target for cyber-criminals, espionage, and hacktivists(Wangen 2021). For that case education system cyber space needs to be strengthened and secured in all higher learning institutions. And the purpose of this research is to implement a Model based on access control list (ACL) and intrusion detection system (IDS) for improved Cyber Security in Higher Learning Institutions in Rwanda. Higher education (HE) serves an essential societal function charged within research, development, and education. Autonomy, individuality, and freedom of choice characterize the HE environment, with few restrictions regarding collaboration and knowledge dissemination. These properties differ from industry, where trade secrets are common and often vital to thrive in business. In contrast to cybersecurity's emphasis on secrecy, the academic environment thrives upon openness, building on a tradition of trust, information exchange, and discussion (Wangen, 2021)."

Therefore, typical characteristics of universities are to be open and including, "meaning few physical perimeters and that strong access control is uncommon. HE is also

characterized by the yearly enrollment of new students and temporary staff and visiting researchers. Faculties often operate autonomous entities and build their own IT networks designed to support research, development, and teaching activities. The networks are often locally managed with a low degree of centralized control(Wangen, 2021)"

Many institutions of higher learning are massively engaging in building their Cyberspaces in a bid to advance their service delivery to their highest level best almost all the time (Maranga, 2019).

Cyber Security therefore "becomes very critical especially because it plays a central role in information technology, service delivery and meeting the ever increasing and overrated customer expectations (Maranga, 2019)."

The process of securing organizational data, "their information, infrastructure and other internal resources such as trade secrets, and copyrights etc. which largely depend on the deployed technology is becoming one of the biggest challenges to many organizations. This has complicated people's imaginations to an extent that whenever there is a thought about cyberspace and cyber security, one thing comes to people's mind is, 'cybercrime'. Various institutions including governments and other private sector corporations are taking numerous measures to could potentially thwart these crimes. Above and beyond the various measures, cyber security remains a huge concern to many companies and governments (Maranga, 2019)."

In education, "there are issues of online advertisements, sale of admission forms, online admissions, online payment of school fees, online transcripts processing system and e-meetings, e-academic board meetings, online call for papers and chapters, open access scholarly communication and general online publications. There are also online universities, e-learning institutions; online educational programmes at certificate, diploma and degree levels, and learning management systems, automation of library routines and digitization of print materials especially grey literature in libraries and development of institutional repositories, among others".(Igwe, 2017) Akuta, Ong 'a and Jones (2011) put it unashamedly when they say that "Literature indicates that, out of the top ten countries in the world with high levels of cybercrime prevalence, sub-Sahara Africa is host to four of these countries namely Nigeria, Cameroon, Ghana and South Africa". The main reason forwarded for the increase of cybercrime particularly in Africa is the sudden increase in the use of information communication technologies (ICTs) in a number of African countries (Kritzinger, 2021)."

Jensen (as cited in Kritzinger, 2021) believes that "African countries can make leapfrog jumps forward in communication connectedness by adopting new technologies – necessarily using different strategies than developed countries followed". Additionally, a number of cyber factors have led Africa to becoming a cybercrime hub. According to Von Solms and Kritzinger, these factors include the increasing bandwidth, increasing use of wireless technologies and infrastructure, lack of cyber security awareness, ineffective legislation and policies, and lack of technical cyber security measures."

In the Kenyan context for instance, the Public Sector ICT Survey Report on cybercrime confirm that cyber-attacks are launched comparatively more in institutions of higher learning compared to other public sector organizations (Maranga, 2019).

As defined by Kenya Information and Communications Act (2013) cyber security is "the collection of tools, policies, security concepts, security safeguards, guidelines, actions, training, best practices that can be used to protect the cyber environment," (Maranga, 2019).

To ensure that institutions of higher learning in Rwanda are able to protect how students, faculty and staff interact, "collaborate, and conduct business in the cyberspace, there will be a necessity to provide comprehensive cyber security adopting a re-architect Security. This is one of the few real solutions to make security a built-in feature of all computing elements. Yes, it's time to abandon the assumptions that computers are only used by well-intentioned professors, that the only treasured data stored on those computers is drafts of research papers, and that the only other users on the network are university colleagues Instead, there is a need to take several specific steps including: Implementing cyber security techniques such as access control and password security, authentication and authorization of data, malware scanners, firewalls, antivirus software and data backups (Gashyama, 2020)."

1.3 Statement of the Problem

Without adequate protection of network in high learning institutions, many individuals, businesses, and governments are at risk of losing that asset. "In education sector connecting more than two sites rely on internet in order to share resources, each time that you put your personal information on the Internet you are at risk of that information getting stolen (Hunt,2016) Universities and academic institutions have become lucrative targets for cyber-attacks and have already suffered multiple high impact incidents. Academic institutions manage large amounts of valuable research, and sensitive personal data, which makes them an attractive target for cyber-criminals, espionage, and hacktivists (Wangen 2021).in addition there is a variation of internet speed which negatively affect communication and resource sharing. Often broadband speed varies because there are more users on larger home networks. Speed slowdowns can be caused by factors internal and external to the household. Internal factors include bandwidth intensive applications choking a

connection, old computing equipment causing stalls or multiple people using the internet simultaneously creating bottlenecks. External factors include the access technology itself (e.g., cable) (Chetty, Haslem, 2011)."

Higher learning institutions in Rwanda are working online during COVID 19 pandemic period using different e-learning platforms such as Moodle, "Cyber-attacks on e-learning platforms coming from the approach of the training module which is on eLearning platforms and they are part of an ERP enterprise platform which containing complex modules asset management of a company: human resources, material resources acquisitions planning, financial planning and so on. So, the company's ERP (Enterprise resource planning) system contains these learning modules. The essence of e-learning platforms is: free time management and training mobility. Because training mobility, the legal restrictions to access training modules are not, and many of which modules, which are part of a company specific ERP system, can be accessed from outside the corporate network. In this context, eLearning platforms became a gate for cyber-attack scenarios because these are open for access to information and the access control is low. Generally, these education platforms are open source and the system used is open system. In these circumstances, the eLearning platforms have many vulnerabilities and elements which can be exploited and these modules may become a gate to ERP company and the hackers may be attacked the information system of company. University of Kigali as our case study is now using Physical firewall which has many drawbacks such as Hardware firewalls treat outgoing traffic from the local network as safe, which can be a hazard if malware, such as a worm, penetrates your network and attempts to connect to the Internet and also hardware firewalls are more difficult to configure, especially for novices (Scheeres, 2006) and these misconfigurations can cause major network failures such as security violations which can lead to University data loss or theft."

So, it is beneficial to address cyber security in two ways: "on the one hand as a collection of policies and actions used to protect the connected network (including computers, hardware, information stored or transmitted) from unauthorized access, modification, theft, interruption or other threat, and secondly, as a process of permanent monitoring and evaluation of these policies and actions in order to ensure improvement of the quality of security to the changing nature of threats (droiu, 2017).Therefore, there is a need to fill the gap from existing literature in Rwandan higher learning institutions context on cyber security enhancement by implementing a Model based on ACL and IDS for improved Cyber Security in Higher Learning Institutions in Rwanda reference made to University of Kigali."

1.3. Objectives

The current study has both specific and general objectives.

1.3.1. General Objective

The general objective of this study is to implement a Model based on ACL and IDS for improved Cyber Security in Rwandan higher learning institutions, with a focus on the University of Kigali.

1.3.2. Specific Objectives

i. To identify the existing Cyber Security techniques and technology used at the University of Kigali.
ii. To propose a new model based on access control list and intrusion detection system framework for improved Cyber Security within University of Kigali;
iii. To design the network and apply ACL and IDS as improved cyber security strategy;
iv. To examine the relevance of Model based on access control list and intrusion detection system framework for improved Cyber Security within University of Kigali.

1.4 Research questions

i. What are the existing techniques used for Cyber Security within University of Kigali?
ii. To what extent is the model based on access control list and intrusion detection system framework for improved Cyber Security within University of Kigali?
iii. How can ACL and IDS be applied as improved cyber security strategy on a designed network within University of Kigali?
iv. How relevant is model based on access control list and intrusion detection system framework for improved Cyber Security at University of Kigali?

1.5. The Research's Scope

For the requirement of this study, researcher designed the study with reference to university of Kigali as an example of major private University that is recognized as the model of well-established Higher Learning institutions in Rwanda having multiple campuses. This university has one campus in Kigali and another in Musanze town. In this study, the researcher put emphasis on applying Virtual Private Network (VPN) technology and the combination of ACL and IDS for Improved Cyber Security."

1.6 The Study's Significance

1.6.1 To the Lecturer

Lecturers will enjoy the system since all updated educational resources are accessible on the server and well secured at all times.

1.6.2 To the Researcher

This project's implementation can be beneficial to the Researcher because this research will help the researcher to

explore the usefulness of Cyber security hence improves the skills and knowledge. Furthermore, the research will be submitted as part of the requirements for the Master of Science in Information Technology award.

1.6.3 Staffs' side

The University supporting staffs (non-academic staffs) will have secured directories through which they receive order and they report their work, this improves paperless system.

CHAPTER TWO: RESEARCH METHODOLOGY

2.0 Introduction

This chapter explains the methodology used to develop the model, methods that were used to collect data, how respondents were selected and how findings were obtained. In addition, a summary of how the data have been processed and analyzed is presented. The challenges expected during the research process and how they were handled to facilitate the research process was also analyzed in this section.

2.2 Research design

According to Churchill (1976), research design is the schedule for a study that serves as a guide in collection and analysis of data. The present study has used quantitative methods and experimental methods. First of all, the quantitative aspect of this study is explained by the fact that questionnaires used in data collection from the field and the data collected have been analyzed by counting respondents' number for each item and the corresponding percentages. The quantitative approach was adopted because it clarified things easily to everyone who used this research report and the experimental approach was adopted to show the working principle of the developed system.

2.3 Research population

Research population refers to the large groups of people or things on which the study is carried out (Dahlia, 2011:61). In this context, the population of this study included five IT related staff of university of Kigali. The size of the population is very reasonable to adopt the census for the entire population based on the central limit theorem.

2.4 Sample design

2.3.1 Sampling procedure

Sampling is "a method or technique for selecting a subset of a population to participate in a study; it is the process of selecting a group of people for a study in such a way that the individuals chosen represent the large group from which they were chosen (Ogula, 2005). The universal sampling was used for this study for five IT related staff at University

of Kigali.

2.5 Methods of data collection

The researcher used a questionnaire survey method. Questionnaire respondents were IT related staff who day to day interact with University of Kigali network. Both primary and secondary data were collected so that we could arrive at satisfactory results. Different techniques and research instruments for gathering information used; these include Books, reports, journals, questionnaires, etc.

2.5.1 Questionnaire

A questionnaire is basically a structured method for gathering primary data. It is typically a series of written questions to which respondents must respond (Bell 1999). The present study used questionnaires for collecting data from IT department staffs of University of Kigali. The questionnaire was made up of structured questions, which required the answers like "yes" or "no" and/or multiple-choice questions.

2.6 Validity and reliability

The validity of the information collected through the questionnaire was guaranteed by the appropriate respondent and the comfortable place and time. These instruments helped the researcher to obtain in depth and valid answers but also the reliability was verified by pretesting data collection instruments in order to make sure that the instruments are relevant and understandable

2.7 Analysis of Data

Data from questionnaires have been collected, compiled, sorted, edited, classified and coded into a coding sheet and analyzed using a computerized data analysis package known as statistical Package for Social Science. (SPSS) vision IBM SPSS Statistics V21.0 and for implementing the system I used simulation software such as VMware which allowed us to install windows server operating systems, GNS3 was initially utilized to supply CISCO routers. on which access control lists were configured and SNORT was installed in windows Machines to work as IDS.

2.8 Ethical considerations

Creswell (2003) states that the researcher has an obligation to respect the rights, needs, values and desires of the informants. Among the normally unexpected concerns relating to ethical issues is the cultural sensitivity. Silverman (2000) argues that the researcher-subject relationship during data collection must be considered in terms of the researcher's values and cultural considerations. Therefore, appropriate steps were taken to adhere to strict ethical guidelines in to uphold participants' privacy, confidentiality, dignity, rights, and anonymity. The researcher will obtain an introductory letter from the University of Kigali's Office of Postgraduate Studies. The researcher will also request permission from University of

Kigali before approaching sampled Employees concerned. The researcher ensures that the information gathered is only used for the intended purpose and that it is treated with confidentiality.

2.1 Methodology for implementing the model

To implement the model, "the prototyping model was used where the design team's focus in the prototyping methodology is to create an early model of the new system, software, or application. This prototype will not be fully functional or thoroughly tested, but it will provide customers and other stakeholders with an idea of what is to come. Then, during the SDLC phases that follow, feedback can be gathered and implemented. The client can get an actual feel of the system by interacting with the prototype, as interactions with the prototype can help the client better understand the requirements of the desired system. For complex and large systems, prototyping is an appealing idea where there is no manual system or preexisting system to assist in gathering the requirements. The prototype is usually not a complete system, and many of the information are not comprised. The objective is to provide overall functionality to a system.

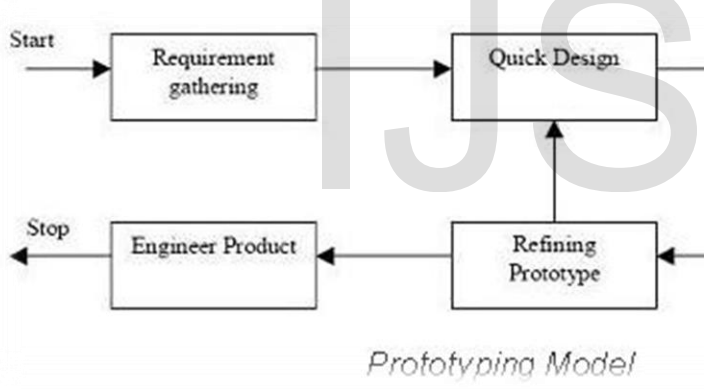

Figure 1: Diagram of Prototype model

Source: (QA, 2020)

Step 1: Gathering and analyzing requirements

A prototyping model starts with requirement analysis. In this phase, the requirements of the system are defined in detail.

Step 2: Design

The second phase is a preliminary design, also known as a quick design. At this stage, a basic system design is created. It is, however, not a complete design. It provides the user with a high-level overview of the system. The quick design aids in the prototype's development.

Step 3: Create a Prototype

"An actual prototype is designed based on the information gathered from quick design" during this phase. It's a scaled-down workable system of the required system.

Step 4: Customer feedback

The proposed system is presented to the client for an initial evaluation at this stage. It aids in determining the working model's strengths and weaknesses. Customer feedback and suggestions are gathered and forwarded to the developer.".

Step 5: Prototype refinement

If a user isn't "extremely happy with the existing design," you must "refine the prototype based on the constructive criticism and suggestions from the users "

This step will not be successfully completed until all of the requirements stated by the user have been met. When the user is satisfied with the prototype that has been created, a final system based on the approved final prototype is created.

Step 6: Engineering Product

Following the development of the final prototype, the final system is thoroughly tested and deployed to production. Routine maintenance is performed on the system to minimize downtime and avoid major breakdowns.

2.9 TOOLS and Methods when installing system

For implementing the project, the following simulation software were used:

- VMware which allowed us to install windows server operating systems.
- GNS3 to supply CISCO routers on which extended access control lists were configured.
- SNORT was installed in windows Machines and worked as IDS.

2.10 Working Principle

The utilization of an access control list together with the intrusion detection system (IDS) is used here for improving the security on our servers. ACL verifies packets crossing LAN interfaces of routers toward the severs basing on the given criteria. If packets are arriving from a UOK remote branch, such as 172.16.10.0 network to server 192.168.10.2 or 192.168.10.0 network to server 172.16.10.2; they will be accepted to reach the destination server. Otherwise, they will be dropped. It is widely assumed that internet packet may originate from hackers who have skilled to penetrate the routers' interfaces configured with access control lists. In

case Access control list are defeated, SNORT working as IDS/IPS in servers will detect intruders and will disconnect them from servers based on rules established.

CHAPTER THREE: PRESENTATION AND ANALYSIS OF RESEARCH FINDINGS, MODEL DESIGN, TESTING.

3.0 Introduction

The researcher in this section presented the findings in table formats using both descriptive and regression analysis to help the readers have a deep understanding of research findings. The findings are presented by respecting the objectives of this study. This research presents both the background information and descriptive statistics by using frequency tables and bar charts, this chapter illustrate also the design and testing of model.

3.1 Presentation and examination of research findings

	Frequency	Percentage
Respondent saying that UoK has Network out of 5 respondents	5	100.0

Table 1: Possession of Network

When asked whether UoK has a network, The large number of respondents (100%) came to an agreement that UoK has a network.

	Frequency	Percent
Repondent saying that UoK has a server	5	100.0

Table 2: Possession of server

When asked whether UoK has a server connected to its network, The large number of respondents (100%) came to an agreement that UoK has a server.

	Frequency	Percent
Respondents saying that UoK has Internet	5	100.0

Table 3: Internet possession

When asked whether UoK has internet, the majority of respondents (100%) came to an agreement that UoK has an internet.

	Frequency	Percent
Firewall and ACL	5	100.0

Table 4: Current Cyber Security Techniques used at UoK

When asked about Cyber Security Techniques currently used at UoK, 100% of respondents responded they are using firewall with Access control list.

	Frequency	Percent
Yes	5	100.0

Table 5: Is UoK router configured with ACL?

When asked whether UoK router is configured with ACL, 100% of respondents responded that UoK router is configured with ACL.

	Frequency	Percent
Yes	5	100.0

Table 6: Asking if they have met ACL misconfiguration problem

When asked whether they have met misconfiguration problem of ACL, 100% of respondents responded that they have met ACL misconfiguration problem.

	Frequency	Percent
Both Network security violation and Network reachability problem	5	100.0

Table 7: Asking about challenges met after misconfiguration of ACL

When asked about challenges met after misconfiguration problem of ACL, 100% reported both network security violation and network reachability problem.

	Frequency	Percent
No	5	100.0

Table 8: Is UoK Server configured with IDS?

When asked whether UoK server is configured with IDS, 100% of respondents responded that UoK server has no IDS.

	Frequency	Percent
Respondents who said Yes	1	20.0
Respondents who said No	4	80.0
Total	5	100.0

Table 9: Are the current techniques used for Cyber Security at University of Kigali enough to ensure the university is safe from the attack?

When asked if the current techniques used for Cyber Security at University of Kigali are enough to ensure the university is safe from the attack, 20% of respondents agreed that the current techniques used for Cyber Security at University of Kigali are enough to ensure the university is safe from the attack while 80% disagreed, which means that the current techniques used for Cyber Security at University of Kigali are not enough to ensure the safety from the attack.

	Frequency	Percent
Strongly disagree	2	40.0
Disagree	3	60.0
Total	5	100.0

Table 10: Respondents appreciating that service offered by ACL are enough

When asked if the service of ACL when it is used alone on the network is well secured, 40% of respondents strongly disagreed while 60% disagreed.

	Frequency	Percent
Strongly disagree	2	40.0
disagree	3	60.0
Total	5	100.0

Table 11: Respondents appreciating that service offered by IDS are enough

When asked if the service of IDS when it is used alone on the network is well secured, 40% of respondents strongly disagreed while 60% disagreed.

	Frequency	Percent
Agree	2	40.0
Strongly agree	3	60.0
Total	5	100.0

Table 12: Respondents appreciating that service of both ACL and IDS is more secured

When asked if the service of both ACL and IDS when combined on the network is more secured, 40% of respondents agreed while 60% strongly agreed.

	Frequency	Percent
Yes	4	80.0
No	1	20.0
Total	5	100.0

Table 13: Do you recommend UoK to implement this model based on ACL and IDS for improved Cyber Security?

3.2 Model Design

Figure 2: Working Structure of Model based on ACL and IDS in phase no1

In phase one: the user packet is sent to the router through the internet, the router uses rules to see if the user packet should be permitted or denied access. In case where user packet is permitted access, the router directs the user packet to IDS and IPS for the next phase otherwise Access is denied by the router.

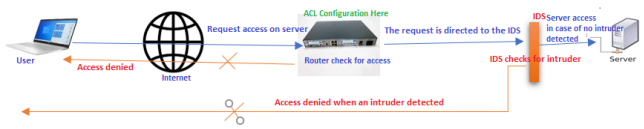

Figure 31: Working Structure of Model based on ACL and IDS in phase no2

In phase Two: The user packet is received by the IDS and IPS to be checked for intruder. In case an intruder detected the packet is thrown away otherwise it is granted server's access.

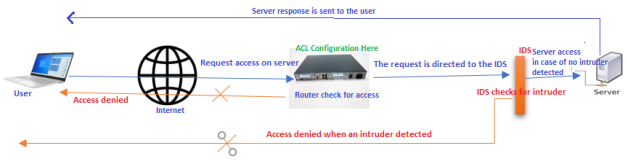

Figure 4: Working Structure of Model based on ACL and IDS in phase no3

In phase Three: The user packet is received on the server, processed and the server return the output to the user.

Model based on ACL and IDS for improved cyber security

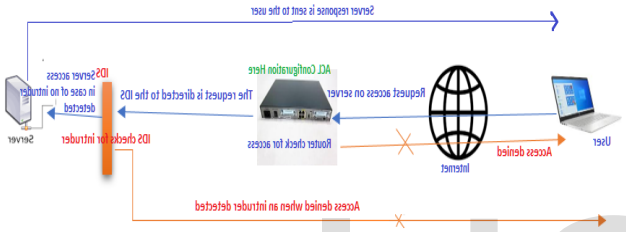

Figure 5: Model based on ACL and IDS for improved Cyber Security

3.3. Model Testing

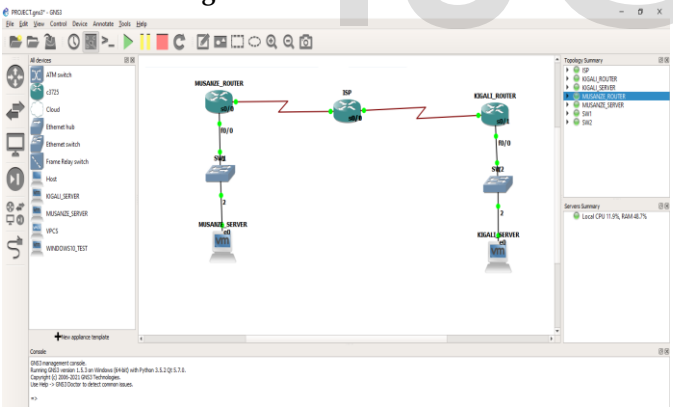

Figure 6: Model testing

MUSANZE ROUTER CONFIGURATION

Interfaces configuration

Router>enable
Router#configure terminal
Router(config)#hostname MUSANZE
MUSANZE (config)#interface GigabitEthernet0/0
MUSANZE (config-if)#ip address 172.16.10.1 255.255.255.0
MUSANZE (config-if)#no shutdown
MUSANZE(config-if)#exit
MUSANZE(config)#interface Serial0/0/0
MUSANZE(config-if)#ip address 15.0.0.1 255.0.0.0
MUSANZE(config-if)# clock rate 9600
MUSANZE(config-if)#no shutdown
MUSANZE(config-if)#EXIT

NAT with interface overload to connect to internet

MUSANZE(config)#IP nat inside source list 50 interface S0/0/0 overload
MUSANZE(config)#access-list 50 permit 172.16.10.0 0.0.0.255
MUSANZE(config)#int gigabitEthernet 0/0
MUSANZE(config-if)#ip nat inside
MUSANZE(config-if)#exit
MUSANZE(config)#int s0/0/0
MUSANZE(config-if)#ip nat outside
MUSANZE(config-if)#exit

Default static route configuration

MUSANZE(config)#ip route 0.0.0.0 0.0.0.0 15.0.0.2
MUSANZE(config)#^Z
MUSANZE#
MUSANZE#copy running-config startup-config

Configuring P2P over internet (GRE) on MUSANZE router

Step1

R1(config)# int tunnel 15
R1(config-if)#tunnel source s0/0/0
R1(config-if)#tunnel destination 25.0.0.1
R1(config-if)#ip address 10.0.0.1 255.0.0.0

……

STEP 2: CONFIGURING ROUTING PROTOCOL

MUSANZE (config)#router eigrp 10
MUSANZE (config-router)#network 172.16.10.0 0.0.0.255
MUSANZE (config-router)#network 10.0.0.0 0.0.0.255

EXTENDED ACL CONFIGURATION ON MUSANZE ROUTER

MUSANZE(config)#access-list 150 permit tcp 192.168.10.0 0.0.0.255 host 172.16.10.2 eq ftp
MUSANZE(config)#access-list 150 permit tcp 192.168.10.0 0.0.0.255 host 172.16.10.2 eq www
MUSANZE(config)#access-list 150 deny tcp any any
MUSANZE(config)#interface g0/0
MUSANZE(config-if)#ip access-group 150 out

ISP CONFIGURATION

Interfaces configuration

Router>enable
Router#configure terminal
Router(config)#hostname ISP
ISP(config)#interface s0/0/0
ISP(config-if)#ip address 15.0.0.2 255.0.0.0
ISP(config-if)#no shutdown
ISP(config-if)#exit

ISP(config)#interface s0/0/1
ISP(config-if)#ip address 25.0.0.2 255.0.0.0
ISP(config-if)#clock rate 9600
ISP(config-if)#no shutdown
ISP(config-if)#exit

Default static route configuration

ISP(config)#ip route 15.0.0.0 255.0.0.0 15.0.0.1
ISP(config)#ip route 25.0.0.0 255.0.0.0 25.0.0.1
ISP(config)#exit
ISP# copy running-config startup-config

KIGALI ROUTER CONFIGURATION

Interfaces configuration

Router>enable
Router#configure terminal
Router(config)#hostname KIGALI
KIGALI (config)#interface GigabitEthernet0/0
KIGALI (config-if)#ip address 192.168.10.1 255.255.255.0
KIGALI (config-if)#no shutdown
KIGALI(config-if)#exit
KIGALI (config)#interface Serial0/0/1
KIGALI(config-if)#ip address 25.0.0.1 255.0.0.0
KIGALI(config-if)#no shutdown
KIGALI(config-if)#EXIT

NAT with interface overload to connect to internet

KIGALI (config)#IP nat inside source list 50 interface S0/0/1 overload
KIGALI (config)#access-list 50 permit 192.168.10.0 0.0.0.255
KIGALI (config)#interface gigabitEthernet 0/0
KIGALI (config-if)#ip nat inside
KIGALI (config-if)#exit
KIGALI (config)#int s0/0/1
KIGALI (config-if)#ip nat outside
KIGALI (config-if)#exit

Default static route configuration

KIGALI (config)#ip route 0.0.0.0 0.0.0.0 25.0.0.2
KIGALI (config)#^Z
KIGALI # copy running-config startup-config

Configuring P2P over internet (GRE) on KIGALI router

Step1

KIGALI (config)# int tunnel 25

KIGALI (config-if)#tunnel source s0/0/0

KIGALI (config-if)#tunnel destination 15.0.0.1

KIGALI (config-if)#ip address 10.0.0.2 255.0.0.0

…….

STEP 2: CONFIGURING ROUTING PROTOCOL

KIGALI (config)#router eigrp 10

KIGALI (config-router)#network 192.168.10.0 0.0.0.255

KIGALI (config-router)#network 10.0.0.0 0.0.0.255

EXTENDED ACL CONFIGURATION ON MUSANZE ROUTER

KIGALI(config)#access-list 150 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.2 eq ftp
KIGALI (config)#access-list 150 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.2 eq www
KIGALI (config)#access-list 150 deny tcp any
KIGALI (config)#interface g0/0
KIGALI (config-if)#ip access-group 150

3.4 Findings and comparison with the existing related

According to a study in 2018 published by DePaul University which stated that the increasing complexity of managing access control configurations due to larger networks and longer policies makes configuration errors highly likely and these misconfigurations can cause major network failures such as reachability problems, security violations, and network vulnerabilities. In our research when asked if some time they meet Access Control Misconfiguration problem, The large number of respondents (100%) agreed that they had encountered the issue of access control misconfiguration and when asked about challenges met after access control misconfiguration problem, 100% of respondents reported network reachability problem and when asked if the service of ACL while configured alone on the system assist in ensuring that the system is well secured, 60% disagreed. As the outcome, our research demonstrated that larger networks necessitated different configurations of access control which sometimes resulted in network misconfiguration and these misconfigurations result in significant network problems including reachability issues and security breaches.

Referring to a report in 2016 published by National Institute of Standards and Technology which stated that IDS cannot substitute for other types of security measures (for example Identification and Authentication, encryption, single sign on, firewalls or ACL), they cannot by themselves completely protect a system from all security threats. In our research when asked if the service of IDS in case where it is used alone on the network ensure the network is well secured, 40% of respondents strongly disagreed while 60% disagreed. Therefore, our research also proved that Intrusion Detection Systems cannot substitute for other types of security mechanisms and they cannot, by themselves, completely protect a system from all security threats.

CHAPTER FOUR: CONCLUSION

4.1. Conclusion

This study was a success in relation to achieving objectives that was set at the beginning of this journey; objectives

including but not limited (1) to determine the existing techniques and technology used for Cyber Security at University of Kigali, and the findings shows that techniques and technology used for Cyber Security there is firewall with Access control list as indicated on table 4. (2) to propose a new model based on ACL and IDS framework for improved Cyber Security at University of Kigali, this study confirmed that the model based on ACL and IDS framework for improved Cyber Security at University of Kigali is needed as indicated on table 12, (3) to design the model and apply ACL and IDS as improved cyber security strategy, our study designed the model and ACL and IDS was applied to the designed network as indicated on figure 6. (4) to test the relevance of Model based on ACL and IDS framework for improved Cyber Security at University of Kigali, the model was tested by using GNS3 and VMware as indicated on Fig 23 for laying a secured network accessible by only authorized users but if and only if user have security credentials to securely monitor and manipulate network connected servers. Once implemented, this model will make a significant contribution to cyber security at the University of Kigali and other higher learning institutions in Rwanda and around the world

ACKNOWLEDGEMENT

I'd like to pay my respectful appreciation to Dr HAKIZIMANA Leopord for the keen interest and invaluable guidance rendered to me under whose able guidance and motivation, this research has been carried out from start to finish. I am grateful to him for always being a source of encouragement and inspiration, without whom this journey would have been a figment of my imagination.

I'd also want to express my deepest thankfulness to my classmates. my classmates for giving valuable suggestions during the course of preparing this paper time to time. I recognize my lecturers Dr Luc NGEND and Dr MBANZABUGABO Jean Baptiste for their encouragement and support. Above all, I bow my gratitude to the Almighty whose grace enabled me to complete this thesis.

References

Alabady, S. (2009). Design and Implementation of a Network Security Model for Cooperative Network. *International Arab Journal of e-Technology*, 26.

Alabady, S. (2009). Design and Implementation of a Network Security Model for Cooperative Network. *International Arab Journal of e-Technology*, 28.

Alabady, S. (2009). International Arab Journal of e-Technology. *Design and Implementation of a Network Security Model for Cooperative Network*, 28.

Ali, M Irfan. (1992). Frame relay in public networks. *IEEE Communications Magazine*, 72-78.

Amit Kumar, Harish Chandra Maurya et al. (2013). A Research Paper on Hybrid Intrusion Detection System. *International Journal of Engineering and Advanced Technology (IJEAT)*.

Bace, Rebecca et al. (2016). *NIST special publication on intrusion detection systems.* NIST.

Britannica, T. E. (2016, March 3). *Higher education. Encyclopedia Britannica. https://www.britannica.com/topic/higher-education*. Retrieved from https://www.britannica.com: https://www.britannica.com/topic/higher-education

Buchanan, William. (2000). *Computer busses.* Elsevier.

Cimpanu, C. (2020, August 21). */article/university-of-utah-pays-457000-to-ransomware-gang/*. Retrieved from https://www.zdnet.com: https://www.zdnet.com/article/university-of-utah-pays-457000-to-ransomware-gang/

Cisco. (2021, August 29). *what-is-vpn.html*. Retrieved from www.cisco.com: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 2.

Dosal, E. (2018, 3 12). */blog/firewall-threats-vulnerabilities*. Retrieved from https://www.compuquip.com: https://www.compuquip.com/blog/firewall-threats-vulnerabilities

Dov Dori and Yaniv Mordecai. (2021, May 19). *Why_Model%3F*. Retrieved from

https://www.sebokwiki.org/: https://www.sebokwiki.org/wiki/Why_Model%3F

droiu, A. M. (2017). The cybersecurity of elearning platforms. *Conference proceedings of» eLearning and Software for Education «(eLSE)* (pp. 374-379). "Carol I" National Defence University Publishing House.

Easttom, C. (2016). *Computer Security Fundamentals.* y Pearson Education.

Ehab Al-Shaer,Will Marrero et al. (2018). *Global Verification and Analysis of Network Access.* DePaul University.

Enumeration, C. W. (2021, June 26). *data/definitions/284.html*. Retrieved from https://cwe.mitre.org: https://cwe.mitre.org/data/definitions/284.html

Gashyama, V. (2020). *Impact of cyber threat to the security of Rwanda.* kampala: Makerere University.

hec. (2021, July 30). *index.php?id=65*. Retrieved from https://hec.gov.rw/: https://hec.gov.rw/index.php?id=65

Hunt, T. (2016). *Cyber Security Awareness in Higher Education.* Washington: Central Washington University.

Igwe, K. (2017). *Imperative of Cyber Ethics Education to Cyber Crimes Prevention and Cyber Security in Nigeria.* Ebonyi State.

Irwin, L. (2021, June 1). */blog/list-of-data-breaches-and-cyber-attacks-in-may-2021-116-million-records-breached*. Retrieved from https://www.itgovernance.co.uk: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-may-2021-116-million-records-breached

Jadidoleslamy, H. (2012). WEAKNESSES, VULNERABILITIES AND ELUSION STRATEGIES AGAINST INTRUSION DETECTION SYSTEMS. *International Journal of Computer Science & Engineering Survey*.

John N. Davies,Vic Grout et al. (2010). *Improving the Performance of IP Filtering using a Hybrid Approach to ACLs.* Wrexham: Glyndwr University.

Jonard B. Bolanio&Rolysent K. Paredes*. (2021). Network Security Policy for Higher Education Institutions based on ISO Standards. *Mediterranean Journal of Basic and Applied Sciences (MJBAS)*, 12.

Kaushik, Sharat, and Anita Tomar. (2014). Access Control List Implementation in a Private Networ. *International Journal of Information & Computation Technology*.

Kritzinger, E. (2021). A Framework for Cyber Security in Africa. *Akuta, Ong'oa and Jones put it* , 1.

Liu, Ming, Xue, Zhi et al. (2018). Host-Based Intrusion Detection System with System Calls:Review and future trends. *ACM Computing Surveys (CSUR)*, 1-36.

Maranga, M. J. (2019). Emerging Issues in Cyber Security for Institutions of Higher Education. *International Journal of Computer Science and Network*, 371.

Marshini Chetty, David Haslem,*. (2011). *Why Is My Internet Slow?: Making Network Speeds Visible.*

Md. Asif Raihan&Marzia Afroze. (2016). *SECURING A NETWORK BY USING VLAN, PORT SECURITY AND ACCESS CONTROL LIST.* East West University.

mineduc. (2021, July 30). *higher-learning-institutions*. Retrieved from www.mineduc.gov.rw: https://www.mineduc.gov.rw/higher-learning-institutions

N-able. (2019, October 16). *blog/types-of-network-security*. Retrieved from www.n-able.com: https://www.n-able.com/blog/types-of-network-security

Odii J. N.,Nwokoma F.O. et al. (2017). NETWORK CONGESTION CONTROL SYSTEM USING FRAME RELAY TECHNOLOGY. *International Research Journal of Computer Science (IRJCS)* .

Paul, E. (2020, June 1). */2020/06/01/nigerian-kenyan-universities-hacked/*. Retrieved from https://techpoint.africa: https://techpoint.africa/2020/06/01/nigerian-kenyan-universities-hacked/

QA, T. (2020, August 22). *what-is-prototype-model-advantages-disadvantages-and-when-to-use-it/*. Retrieved from http://tryqa.com/: http://tryqa.com/what-is-prototype-model-advantages-disadvantages-and-when-to-use-it/

Quamar Niyaz, W. S. (2016). *A Deep Learning Approach for Network Intrusion Detection System.* ICST.

Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam. (2016). *A Deep Learning Approach for Network Intrusion Detection System.* New York .

Rademacher, L. (2021, June 26). *the-disadvantages-of-intrusion-detection-systems*. Retrieved from https://www.techwalla.com: https://www.techwalla.com/articles/the-disadvantages-of-intrusion-detection-systems

Rjaibi, N. (2012). Cyber Security Measurement in Depth for E-learning Systems. *International Journal of Advanced Research in Computer Science and Software Engineering*, 1.

Scheeres, J. (2006, 11). */security/articles/200611/hardwarevsoftwarefirewall.html*. Retrieved from https://www.inc.com: https://www.inc.com/security/articles/200611/hardwarevsoftwarefirewall.html

Sharat Kaushik, Anita Tomar et al. (2014). Access Control List Implementation in a Private Network. *International Journal of Information & Computation Technology*, 1361-1366.

Stankard, T. (2021, 4 13). */blog/colleges-continue-to-withstand-cyberattacks-in-2021/*. Retrieved from https://www.titanhq.com: https://www.titanhq.com/blog/colleges-continue-to-withstand-cyberattacks-in-2021/

Subramanian, Viswanath. (1995). *Frame Relay Networks-a survey.*

subscription.packtpub. (2021, August 13). *book/networking_and_servers/9781787128873/2/ch02lvl1sec17/intrusion-detection-system*. Retrieved from https://subscription.packtpub.com: https://subscription.packtpub.com/book/networking_and_servers/9781787128873/2/ch02lvl1sec17/intrusion-detection-system

Tutorialspoint. (2021, August 13). *computer-science/computer-network-tutorials/types-of-firewall-and-possible-attacks*. Retrieved from https://tutorialspoint.dev: https://tutorialspoint.dev/computer-science/computer-network-tutorials/types-of-firewall-and-possible-attacks

Uwizeyimana, V. (2021). 5The University of Rwanda response to COVID-19. *ResearchGate*.

Wallarm. (2021). *what/whats-the-access-control-list-acl*. Retrieved from https://www.wallarm.com: https://www.wallarm.com/what/whats-the-access-control-list-acl

Wangen, J. B. (2021). *A Systematic Review of Cybersecurity Risks in.*

Wasajja, J. (2021, July 21). *uok-online-studies-and-students-progression*. Retrieved from https://uok.ac.rw: https://uok.ac.rw/uok-online-studies-and-students-progression/