BUSITEMA UNIVERSITY
Pursuing Excellence

P.O.Box 236, Tororo, Uganda
Tel: +256-45-4448834
Fax: +256-454436517
Email: info@adm.busitema.ac.ug
Website: www.busitema.ac.ug

DIRECTORATE OF GRADUATE STUDIES, RESEARCH AND INNOVATIONS

DEVELOPMENT OF AN INVESTIGATIVE PROCESS MODEL TO MONITOR E-LEARNING SYSTEM

A CASE OF BUSITEMA UNIVERSITY

BY

OKUMU WILFRED MAYIRA

REGISTRATION NUMBER

BU/GS18/MCF/4

STUDENT'S NUMBER

1800403969

SUPERVISORS

DR. MUSINGUZI WILSON BABU

DR. GODLIVER OWOMUGISHA

MR. MATOVU DAVIS

AREPORT SUBMITTED TO THE DIRECTORATE OD GRADUATE STUDIES, RESEARCH AND INNOVATIONS IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF MASTER OF COMPUTER FORENSICS

MAY 2022

DECLARATION

I Okumu Wilfred Mayira, Declare that this research is my original work except where due acknowledgement has been made. I declare that this work has never been submitted to any institution for funding or award.

Student Name: Okumu Wilfred Mayira

Registration Number: **BU/GS18/MCF/4**

Signature:……...

Date:……..

APPROVAL

This research is submitted as partial fulfilment of Award of Master of Computer Forensics of Busitema University with my approval as the academic Supervisors

1. Supervisor:
   Dr. Godliver Owomugisha (PhD)
   Signature----------
   Date----------

2. Supervisor:
   Mr. Davis Matovu
   Signature ----------
   Date----------

3. Supervisor:
   Dr. Wilson Babu Musinguzi (PhD)
   Signature……..
   Date……

DEDICATION

Dedicate to my parents **Wandera John Mayira(RIP), Nandera Lusalya, Wafula Wilson Mayira** and all my family members for inspirational insights towards the accomplishment of the Master in Computer Forensics program.

ACKNOWLEDGEMENT

I do acknowledge number of authors that I cited in this report who worked tirelessly to make sure their journey and articles were published that positively contributed to the completion of this research dissertation.

To the gratitude i extend my sincere gratitude to all those who provided constructive critique and help during the preparation of the proposal; more especially **Dr. Godliver Owomugisha, Dr. Wilson Babu Musinguzi** and Mr. **Davis Matovu** upon their wonderful supervision whose outcomes are seen in the research dissertation.

My special appreciation goes to all those who provided material and financial support towards my education more especially: all my lecturers, my late daddy Mr. Wandera John Mayira and Management of Busitema University, Post Graduate Directorate.

Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

CD-ROM	Compact D Read Only Memory
E-LEARNING	Electronic Learning
ICT	Information Communication Technology
IoTs	Internet of Things
LDB	Log Database
HTML	HyperText Makeup Language
SQL	Structured Query Language
XSS	Cross site Scripting
CSRF	Cross site Request Forgery
DoS	Denial of Service
HTTPS	HyperText Transfer Protocol Secure
OS	Operating System
URL	Unified Resource Locator
IT	Information Technology
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
NIDS	Network based and Intrusion and Detection System
HIDS	Host based Intrusion and Detection System
WAN	Wide Area Network
RAM	Random Access Memory

ABSTRACT

High rate of digital technologies and increased interest in the computerization of systems in education have contributed to e-learning through electronic media like internet, world wide websites and others, areas of system security, integrity and confidentiality within which college has to integrate the technology challenges in their teaching. Plagiarism and communication still stand as challenges in question. This study developed an investigative process model to monitor E-Learning system and prevent cyber-attacks a case of Busitema University. The adopted case technique that sought to address the concerns under investigations Further, having considered a case study strategy, mixed methods were adapted such as qualitative and quantitative. Additionally, research adopted design science strategy since the study developed a model as the final artifact.

Data Collection Methods and Instruments are presented from the Server Computers using Microsoft Excel and Csv files. These helped to capture the information from different stakeholder's paths, the authentic logs analyzed was 10695 making 91.4% while unauthentic logs 1005 making 8.6% over the total number of 11700 logs analyzed. A critical review of the literature was provided and an objective model based on process investigative model for the success in e-learning was developed. In addition, some security challenges are briefly discussed.

CHAPTER ONE

INTRODUCTION

1.0 Introduction

High rate of connections (internet) for user demands like e-learning, financial transactions, e-government and other services has for the past years been positively helpful for faster delivery of services to both government institutions and individuals. The government and other private academic institutions have prioritized the introduction of E-services through connection of internet to ease service delivery to people and therefore an important service.

According to wu et al (2012), defines E-learning as any digital platform for communication of knowledge from sender (instructor) to the receiver (student) among the learners. Most academic institutions like Busitema University, Makerere University, Kyambogo University, Uganda Management Institute and many others in Uganda have developed working policies to adopted E-Learning as a mode of delivering services to students online. The mode of learning requires students to login into the e-learning system in order to access the learning material over internet. The mode of teaching requires an instructor or lecturer to have online live sessions like video conferencing and audios or the instructor, lecturer can upload recorded videos, audios or lecture notes to the platform so that students are able to access them. The mode of learning is considered to be cheaper as it only requires time and data as compared to physical attendance which requires costs like transport, accommodations and other related inconveniences to more so working class. The platform may be opted for Video systems like Zoom, Jitsi, Skype, Moodle, Google Meet and may others. While these sessions are on high demand, the platforms or e-learning systems need to be secure from any kind of security breach. Most concerns that happen as a result of digital technologies in E-learning systems that affects their use negatively, the responsible ones are security risks and vulnerability attacks on e-learning systems and private data and important devices (Kambourakis 2013) Most education system innovations having focused on educational structure and having no considerations to privacy and security as required element (Ciobanu et al. 2012). However, it's evident that such attacks and system weaknesses in technology were

REFERENCES

1. Mugenda, O. M., &Mugenda, A. G. (1999). Research methods: Quantitative and qualitative approaches. Acts press.
2. HY Wu, HY Lin - Computers & Education, 2012 – Elsevier. A hybrid approach to develop an analytical model for enhancing the service quality of e-learning
3. 18th Australian Cyber Warfare Conference 2019 (CWAR 2019), October 7-8, 2019, Melbourne, Victoria, Australia
4. Creswell John W (2014). Research design: Qualitative, quantitative and mixed methods approaches
5. Ciobanu (Defta) Costinela – Lumini, Ciobanu (Iacob) Nicoleta – Magdalena, 2012. E-learning Security Vulnerabilities
6. Alwi, N.H.M. and Fan, I.S. (2010) E-Learning and Information Security Management. International Journal of Digital Society (IJDS), 1, 148-156.
7. WY Oso, D Onen 2008. A Handbook for the Beginning Researchers
8. Reith, M., Carr, C. & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, Vol. 1 No. 3. Online: http://www.ijde.org/docs/02_fall_art2.html [visited 30 June 2004]
9. Ó Ciardhuáin, S. & Gillen, P. (eds.) (2002) Guide to Best Practice in the area of Internet crime Investigation. Report from EU FALCONE Project No. JAI/2001/Falcone/127 "Training: Cyber Crime Investigation — Building a Platform for the Future." Dublin, Ireland: An Garda Síochána.
10. Casey, E. (2000). Digital Evidence and Computer Crime. San Diego: Academic Press.
11. Graeme Byrne and Lorraine Staehr (2002). International Internet Based Video Conferencing in Distance Education: A Low-Cost Option. InSITE – Where Parallels Intersect, pp. 187 – 194.
12. Chris McCuller (2010). Videoconferencing and Distance Learning. Valdosta State University Whitepaper.
13. Polycom inc. (2010). The Top Five Benefits of Video Conferencing. Polycom, inc., Polycom Worldwide Headquarters,
14. Donald Gillies (2008). Student Perspectives on Videoconferencing in Teacher Education at a Distance. Distance Education, Vol. 29, No. 1, pp. 107 – 118,

15. Casey, E. (2004). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press, Second Edition
16. Baryamureeba, V and Tushabe, F. (2004). The Enhanced Digital Forensic Investigation Process Model. Proceedings of the Digital Forensic Research Conference, Baltimore USA.
17. Africa cyber security report. (2017). Demystifying Africa's Cyber Security Poverty Line. Kenya, Nairobi.
18. Hassan, N. A. (2019). Digital forensic basics guide using windows OS
19. Mushtaque K, Ahsan K and Umer A. (2015). Digital Forensic Investigation Model. An evolution study Journey of Information system and Technology Management Vol 580 Springer International Publishing AG 2018
20. Africa cyber security report. (2018). A skills gap is the difference between skills that employers want or need, And skills their workforce offer. Kenya, Nairobi
21. Africa Cyber Security Risk. (2019). What's Now and What's Next. Kenya, Nairobi
22. Dumisani Gumbi, (2018). Understanding the threat of Cybercrimes
23. Mahboob Usman, (2015). Cybercrimes a case study of legislation in Pakistan.
24. DFRWS (2001) A Roadmap for Digital Forensic Research report from the first Digital Forensic Research Workshop
25. Baltimore, MD. Citeseer,(2004). In Proceedings of the 4th Annual Digital Forensic Research Workshop,
26. Mugenda, O. M., & Mugenda, A. G. (1999). Research methods: Quantitative and qualitative approaches. Acts press.
27. African cybersecurity research report white paper 2019
28. EC-Council Press (2010) Investigating Network Intrusions and Cybercrime
29. Elsevier (2007) Cyber Crime Investigations: Bridging the Gaps Between, Security Professionals, Law Enforcement, and Prosecutors Copyright,
30. Mike O' Leary (2015) Cyber Operations: Building, Defending, and Attacking Modern Computer Networks
31. Eoghan Casey (2004) Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition by ISBN:0121631044 Academic Press ©
32. Eoghan Casey (2010) Digital Evidence and Computer Crime Third Edition

33. ANDREW S. TANENBAUMHERBERT (2005) Modern Operating Systems BOS **Vrije Universiteit** Amsterdam, The Netherlands
34. Daniel P. Bovet, Marco Cesati (2005) Understanding the Linux Kernel, 3rd Edition
35. Principles of operating system Designs and applications Brian L. Stuart FedEx Labs University of Memphis
36. William stallings (2011) Network Security Essentials 4th Edition
37. William Stallings (2004) Computer Networking with Internet Protocols and Technology
38. Chandra mohan (2013) Operating system by former professoer SV University tirupati
39. Andrew S. Tanenbaum (2010) Operating Systems Design and Implementation, Third Edition Vrije Universiteit Amsterdam
40. Garry H, Watson E (2016) Computer Hacking, Security testing, Penetration Testing and basic security
41. Anthony R, Kevin O'Shea, Jim Steele, Jon R. Hansen, Captain Benjamin R. Jean Thomas R. (2007) Cyber Crime Investigations: Bridging the Gaps Between, Security Professionals, Law Enforcement, and Prosecutors
42. Anderson, D., Frivold, T. and Valdes, A. Next-generation intrusion detection expert system (NIDES): A summary Technical
43. Devikrishna, K. S. and Ramakrishna , B. B. .An Artificial Neural Network based Intrusion Detection System and Classification of Attacks", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Jul-Aug 2013, 3(4): 1959-1964.
44. Karent K, Murugiah S. Guide to Computer Security Log management Sept 2006