

BUSITEMA UNIVERSITY
FACULTY OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF COMPUTER ENGINEERING AND
INFOMATICS

FINAL YEAR PROJECT REPORT

**DEVELOPMENT OF AN ALGORITHM FOR CYBER
INCIDENT ANALYSIS AND RESPONSE: THE CASE
OF UNIVERSITIES IN EASTERN UGANDA**

By

GERALD KISANGALA

REG NO: BU/GS22/MCF/5

**This Master research report is submitted to the Directorate of Graduate Studies,
Research, and Innovation in Partial Fulfillment of the Requirement for the Award
of the Degree of Master of Computer Forensics of Busitema University**

October 2025

Abstract

Universities in Eastern Uganda increasingly rely on digital systems for teaching, learning, and administration, yet they face persistent cyber threats such as phishing, malware, and application-level attacks. These challenges are intensified by limited computational resources, weak network infrastructure, insufficient funding, and shortages of skilled IT personnel. Most existing intrusion detection and response systems (IDS) are highly complex and resource-intensive, making them impractical for these institutions.

This study addressed that gap by designing and testing a lightweight, rule-based cyber incident detection and response algorithm specifically tailored for resource-constrained universities. These constraints include limited budgets, aging servers and software, few qualified IT staff, and low-capacity, intermittently reliable ISP connectivity typical of remote campuses, which together restrict deployment of enterprise security solutions. A hybrid research approach combining qualitative and quantitative techniques was employed, using Design Science Method (DSM) to guide the structured development, demonstration, and evaluation of the algorithm. Data was gathered from five universities to establish contextual threats and system constraints, while simulation experiments were conducted to evaluate the algorithm's effectiveness under realistic attack scenarios.

The resulting system was modular and adaptive, implemented with a PHP-MySQL backend and an administrative dashboard for IT staff. It focused on detecting SQL injections, fake bots, and header tampering, while a correlation engine linked events into multi-stage attack chains. Results demonstrated detection accuracy above 92%, precision above 91%, and median response times below 100 ms, sustaining up to 450 requests per second before degradation. Compared to Snort, the algorithm achieved higher precision and lower resource use, though Snort maintained slightly higher recall.

This work demonstrates that lightweight, resource-efficient detection systems can significantly strengthen cybersecurity in low-capacity university environments. It further extends the application of the Defense-in-Depth model and Resource-Based View theory by aligning cybersecurity design with available institutional capabilities and infrastructure limitations.

Declaration

I, Gerald Kisangala, declare that this master's research proposal, titled "Development of an Algorithm for Cyber Incident Analysis and Response: The Case of Universities in Eastern Uganda," is my original work. It has not been submitted to any other institution for any academic award. Where the work of others has been consulted or used, it has been properly acknowledged in accordance with the guidelines of Busitema University.

Gerald Kisangala

BU/GS22/MCF/5 - 2200401961

Signature:

Date:

Dedication

This work is dedicated to my family for their unwavering support, and to future young researchers in the field of Computer Forensics who strive to advance knowledge and innovation.

Approval

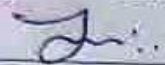
This research report submitted as a partial fulfillment for the award Master of Computer Forensics of Busitema University, with our approval as the academic supervisor(s)

Assoc. Prof. Gilbert Gilibrays Ocen (PhD)

Rank: Associate Professor

Department: Computer Engineering and Informatics

Faculty: Engineering and Technology

Signature: 

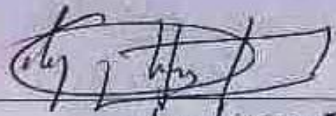
Date: 22/10/2025

Dr. Odongtoo Godfrey (PhD)

Rank: Senior Lecturer

Department: Computer Engineering and Informatics

Faculty: Engineering and Technology

Signature: 

Date: 22/10/2025

Acknowledgement

I wish to express my profound gratitude to all those who supported and guided me throughout this research journey. I am especially thankful to my study colleague, Ivan Bageya, as well as Ms. Rosemary Nalwanga and Mr. Oboth Andrew Okoth, whose encouragement and companionship greatly sustained me.

I am deeply indebted to my supervisors, Assoc. Prof. Gilbert Gilibrays Ocen and Dr. Godfrey Odongtoo, whose invaluable guidance, constructive insights, and unwavering commitment have shaped this work from its inception to completion. Their mentorship has been a constant source of inspiration and professional growth.

List of Abbreviations

DoS:	Denial Of Services Attack
MiM:	Man in the Middle
RBV:	Resource-Based View
DiD:	Defense-in-Depth
DSM:	Design Science Methodology
APTs:	Advanced Persistent Threats
LSTM:	Long Short-Term Memory
IDPS:	Intrusion Detection and Prevention System
SDN:	Software Defined Networking
GRU:	Gated Recurrent Units
VMs:	Virtual Machines
FGDs:	Focus Discussion Groups
MMs:	Virtual Machines
VS:	Visual Studio Code
UCSF:	The University of California, San Francisco
CERT:	Computer Emergency Response Team
PHP:	HyperText Processor
REST:	Relational State Transfer
API:	Application Programming Interface
RDBMS:	Relational Database Management Systems
IDS:	Intrusion Detection System
IT:	Information Technology
CIAR:	Cyber Incident Analysis and Response

List of Tables

Table 1. 1 - Operational Definitions	IX
Table 1. 2 - Universities of Contact	4
Table 2. 1 - Current cyber threats faced by academic institutions.....	10
Table 2. 2 - Existing cyber security frameworks and their limitations	12
Table 2. 3 - Comparison with the study's contribution	13
Table 3. 1 - How DSM guided design	17
Table 3. 2 - Universities of Contact	18
Table 3. 3 - Respondents by University.....	20
Table 3. 4 - Algorithm Performance Metrics	23
Table 3. 5 - Security Evaluation Metrics	24
Table 3. 6 - Thematic / Content Analysis of Qualitative data	25
Table 3. 7 - Cybersecurity themes and related metrics	26
Table 3. 8 - Simulation environmental setup	27
Table 3. 9 - Data Model description	35
Table 4. 1 - Resource utilization results.....	50
Table 4. 2 - Comparative benchmarking.....	51
Table 5. 1 - Summary of conclusions, limitations and recommendations	56

List of Figures

Figure 1. 1 Conceptual framework	6
Figure 3. 1 Design Science Overview.....	16
Figure 3. 2 - Geographical locations of the Universities of Contact.	19
Figure 3. 3 - Algorithms Internal Architecture	29
Figure 3. 4 - Algorithm's use case	30
Figure 3. 5 - Context diagram of the Cyber Incident Analysis and Response Algorithm	31
Figure 3. 6 - Level 1 Data Flow Diagram.....	32
Figure 3. 7 - Level 2 Data Flow Diagram.....	33
Figure 3. 8 - Level 3 Data Flow Diagram.....	34
Figure 3. 9 - CIAR Algorithm's Database Schema Mysql Extract.....	35
Figure 3. 10 - CIAR Logical Database Schema.....	36
Figure 3. 11 - Event Injection Pseudocode	37
Figure 3. 12 - Rule Engine Pseudocode	38
Figure 3. 13 - Correlation & Response Engine Pseudocode.....	38
Figure 4. 1 Respondents by Role	44
Figure 4. 2 - Respondents by University	44
Figure 4. 3 - Awareness of Cybersecurity Risks.....	45
Figure 4. 3 - Awareness of Cybersecurity Risks.....	45
Figure 4. 4 - Most Frequently Observed Cyber Threats	45
Figure 4. 5 - Effectiveness of current cybersecurity measures	46
Figure 4. 6 - Existence of Cybersecurity Framework/Protocols.....	47
Figure 4. 7 - CIAR Algorithm Dashboard	48
Figure 4. 8 - Confidence in the CIAR Algorithm	49

Operational Definitions

<i>Term (s)</i>	<i>Definitions</i>
<i>Attack surface</i>	The total number of attack-vectors an attacker can use to manipulate a network or computer system or extract data.
<i>Data breach</i>	Any security incident where sensitive, protected, or confidential data is accessed or stolen by an unauthorized party
<i>Multi-stage attack</i>	Multi-stage attack is a kind of sophisticated intrusion strategy that attackers use for penetrating the well protected network infrastructures. It is a combination of attack vectors or techniques to compromise a target network or application

Table 1. 1 - Operational Definitions

Contents

Abstract	I
Declaration	II
Dedication	III
Approval	IV
Acknowledgement	V
List of Abbreviations	VI
List of Tables	VII
List of Figures	VIII
Operational Definitions	IX
CHAPTER ONE: INTRODUCTION	1
1.0 Introduction.....	1
1.1 Background of the Study	1
1.2 Statistical Background of the Study.....	2
1.3 Problem Statement	3
1.4 Objectives of the Study	3
1.4.1 Main Objective.....	3
1.4.2 Specific Objectives	3
1.5 Research Questions	3
1.6 Scope of the Study	4
1.6.1 Content Scope	4
1.6.2 Geographical Scope	4
1.6.3 Time Scope	4
1.7 Justification	5
1.8 Significance of the Study	5
1.9 Theoretical and Conceptual Framework	5
1.10 Novelty of the Study	6

1.11 Chapter One Conclusion	7
CHAPTER TWO: LITERATURE REVIEW	8
2.0 Introduction.....	8
2.1 Cybersecurity Threats in Academic Institutions.....	8
2.2 Design of cyber incident analysis and Response Algorithms for Limited-Resource Environments	10
2.3 Evaluating Detection Frameworks: Scalability and Adaptability.....	11
2.4 Summary of Existing Cybersecurity Frameworks and Algorithms.....	12
2.5 Chapter Two Conclusion	13
CHAPTER THREE: METHODOLOGY	15
3.0 Introduction.....	15
3.1 Research Design.....	15
3.1.1 Design Science Method	15
3.2 Research Approach	17
3.3 Geographical Area of the Study.....	18
3.4 Population of the Study.....	19
3.5 Sampling Strategy	20
3.6 Data Collection Methods	20
3.7 Data Quality Control.....	21
3.8 Measurements	21
3.9 Data Analysis	22
3.9.1 Quantitative Analysis.....	22
3.9.2 Qualitative Analysis.....	25
3.9.3 Integrated Analysis	25
3.10 Materials	26
3.11 Algorithm Architecture and Workflow.....	27
3.11.1 Requirements Derivation	27

3.11.2 Architectural Overview.....	27
3.11.3 Workflow Diagram	29
3.12 System Design Specifications.....	29
3.12.1 Context Diagram.....	31
3.12.2 Data Flow Diagrams	32
3.12.3 Data Model Overview.....	34
3.12.4 Pseudocodes.....	37
3.13 Analysis Techniques/Procedures	39
3.13.1 Development of the Algorithm	39
3.13.2 Simulation Environment	39
3.13.3 Attack Models and Scenario	40
3.13.4 Performance Evaluation.....	41
3.13.5 Refinement Process.....	42
3.13.6 Replicability	42
4.14 Chapter three conclusion.....	42
CHAPTER FOUR: RESULTS AND DISCUSSION	44
4.0 Introduction.....	44
4.1 Results for Objective 1: Assessment of Cybersecurity Threats.....	44
4.1.1 Participant Demographics.....	44
4.1.2 Awareness of Cybersecurity Risks	45
4.1.3 Observed Cyber Threats	45
4.1.4 Frequency of Incidents.....	46
4.1.5 Effectiveness of Current Measures	46
4.1.6 Institutional Challenges and Frameworks.....	46
4.2 Results for Objective 2: Algorithm Design	47
4.2.1 Administrative Dashboard	47
4.2.2 Motivation for Adoption.....	48

4.2.3 Confidence in the Algorithm	49
4.3 Results for Objective 3: Implementation in Simulation	49
4.3.1 Simulation Setup.....	49
4.4 Results for Objective 4: Evaluation of Algorithm Effectiveness.....	50
4.4.1 Detection Effectiveness	50
4.4.2 Response Latency	50
4.4.3 Resource Utilization.....	50
4.4.4 Correlation and Chaining Results	51
4.4.5 Comparative Benchmarking	51
4.5 Discussion of Results.....	51
4.6 Summary	52
CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS	53
5.0 Introduction.....	53
5.1 Conclusions.....	53
5.2 Limitations of the Study.....	54
5.3 Recommendations.....	54
5.3.1 For Universities and Practitioners.....	54
5.3.2 For Policymakers and Regulators	55
5.3.3 For Future Research.....	55
5.4 Summary	55
References.....	57
Appendix I: Rule Sets, Thresholds, and Configurations.....	59
Appendix II: Sample Payloads and Simulation Scripts	61

References

- Abdul, Syed, Rehman Bukhari, and Mohammad Ali. 2021. "Sample Size Determination Using Krejcie and Morgan Table." doi:10.13140/RG.2.2.11445.19687.
- Bipin Gajbhiye, Shalu Jain, and Om Goel. 2024. "Defense in Depth Strategies for Zero Trust Security Models." *International Journal for Research Publication and Seminar* 15(3):293–305. doi:10.36676/jrps.v15.i3.1497.
- Check Point Research. 2021. "Education Sees 29% Increase in Attacks." <https://cybermagazine.com/cyber-security/check-point-research-education-sees-29-increase-attacks>.
- Check Point Research [Online] Software Blog. 2023. "38% Increase in 2022 Global Cyberattacks." <https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/>.
- Daily Monitor. 2022. "Makerere University Hit by Cyberattacks, Student Portals Disrupted." Available: <https://www.monitor.co.ug/uganda/news/national/makerere-university-hit-by-cyberattacks>.
- INTERPOL. 2023. *AFRICAN CYBERTHREAT ASSESSMENT REPORT 2023*.
- J, Okello. 2023. "Uganda Christian University Warns of Phishing Attacks on Staff Emails." *New Vision*.
- Jessica Davis. 2020. "UCSF Pays \$1.14M to NetWalker Hackers After Ransomware Attack." <https://www.techtarget.com/healthtechsecurity/news/366595656/UCSF-Pays-114M-to-NetWalker-Hackers-After-Ransomware-Attack>.
- Lallie, Harjinder, Harjinder Singh Lallie, Andrew Thompson, Elzbieta Titis, and Paul Stephens. 2021. *Understanding Cyber Threats Against the Universities, Colleges, and Schools*. <https://www.researchgate.net/publication/372655992>.
- Maheswaran, N., S. Bose, and Buvaneswari Natarajan. 2024. "An Adaptive Multistage Intrusion Detection and Prevention System in Software Defined Networking Environment." *Automatika* 65(4):1364–78. doi:10.1080/00051144.2024.2372749.
- Matovu, Mugeni, Gilbert, Simon M. Karume, and Stephen Mutua. 2019. *State of Cyber Security: The Ugandan Perspective*. <http://www.ijser.org>.
- M.D.C, Tongco. 2007. "126-Article Text-454-1-10-20080402." *Ethnobotany Research and Applications* 147–58. doi:10.17348/era.5.0.147-158.

- NITA-U. 2022. *National Information Technology Survey Final Report*.
<https://www.nita.go.ug/publications/reports/national-it-survey/national-information-technology-survey-final-report-2022>.
- PML Daily. 2024. “Experts Warn of Uganda’s Cybersecurity Vulnerability.”
<https://www.pmldaily.com/business/2024/09/experts-warn-of-ugandas-cybersecurity-vulnerability.html>.
- Prey Project. 2024. “Cybersecurity Threats IT Professionals in Education Face.”
<https://preyproject.com/blog/cyber-security-threats-it-professionals-in-education-face>.
- Selim, Sahar, Mohamed Hashem, and Taymoor M. Nazmy. 2011. “Hybrid Multi-Level Intrusion Detection System.” *Article in International Journal of Computer Science and Information Security* 9(5):2. <http://sites.google.com/site/ijcsis/>.
- UCC. 2021. “COMMUNICATIONS-SECTOR-CYBER-SECURITY-POSTURE-January-2021-to-December-2021.”
- Uganda Communication Commission. 2023. *Annual Cybersecurity Report 2023*. Kampala.
<https://www.ucc.co.ug/cybersecurity-report-2023>.
- Verkerken, Miel, Laurens D’Hooge, Didik Sudyana, Ying Dar Lin, Tim Wauters, Bruno Volckaert, and Filip De Turck. 2023. “A Novel Multi-Stage Approach for Hierarchical Intrusion Detection.” *IEEE Transactions on Network and Service Management* 20(3):3915–29. doi:10.1109/TNSM.2023.3259474.
- Zhou, Peng, Gongyan Zhou, Dakui Wu, and Minrui Fei. 2021. “Detecting Multi-Stage Attacks Using Sequence-to-Sequence Model.” *Computers and Security* 105. doi:10.1016/j.cose.2021.102203.