



DEVELOPMENT OF AN ADVANCED CYBERSECURITY
FRAMEWORK THROUGH CENTRALIZED
SECURITY PLATFORM

UNDERGRADUATE THESIS

Submitted as one of the requirements to obtain
Sarjana Komputer

By:

NAJLA ADELLINE ZAHRA

001202200151

FACULTY OF COMPUTER SCIENCE

INFORMATICS STUDY PROGRAM

CIKARANG

AUG, 2025

SIMILARITY INDEX REPORT

chapter 1-5

ORIGINALITY REPORT

11%	9%	4%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Gloucestershire Student Paper	1%
2	Submitted to Open University Student Paper	<1%
3	github.com Internet Source	<1%
4	mailtrap.io Internet Source	<1%
5	www.raymondcamden.com Internet Source	<1%
6	Submitted to University of Northampton Student Paper	<1%
7	ai.google.dev Internet Source	<1%
8	Submitted to University of Essex Student Paper	<1%
9	Submitted to University of East London Student Paper	<1%

AI Report

We predict this text is

Human Generated

AI Probability

3%

This number is the probability that the document is AI generated, not a percentage of AI text in the document.

Plagiarism



The plagiarism scan was not run for this document. Go to gptzero.me to check for plagiarism.

INDIVIDUAL REPORT - Najla Adelline.pdf - 7/21/2025

NAJLA ZAHRA

Development of an Advanced Cybersecurity Framework Through Centralized Security Platform

UNDERGRADUATE THESIS

Submitted as one of the requirements to obtain

Sarjana Komputer

By:

NAJLA ADELLINE ZAHRA

001202200151

ABSTRACT

This final project discusses the problem of employees lack of cybersecurity awareness and associated weaknesses that expose companies to data breaches and network attacks. There is often a lack of monitoring, basic education and real-time oversight in today's environment, leading to the exposure to ever-changing cyber threats. This project suggests creating an Advanced Cybersecurity Framework with a Centralized Security Platform at its core in order to address these issues.

An integrated system intended to give an extensive overview of a company's safety record is the planned Centralized Cyber Security Platform. Strong Network Security protocols, sophisticated Security Awareness tools, and advanced SIEM (Security Information and Event Management) tools along with Web Threat Analysis for proactive threat mitigation are some of its primary features. A Security Chatbot will also be included to help in the event of a security breach, identify malicious communications, and offer real-time assistance with cybersecurity queries.

The successful implementation of this framework is expected to result in significant benefits, including an extensive decrease in cyberattack risk, improved overall cybersecurity adaptability, a decreased number of data breaches, increased employee protection, and more accessible cybersecurity guidance. The project intends to provide comprehensive, real-time security management and cultivate a security-conscious culture

in order to strengthen organizational defenses against a threat landscape that is becoming more complicated.

Keywords: Cybersecurity Framework, URL Threat Analysis, Security Chatbot, Phishing Simulation, Employee Awareness, Centralized Security Platform.

TABLE OF CONTENTS

	Page
DEDICATION	viii
ACKNOWLEDGMENTS	ix
TABLE OF CONTENTS	x
LIST OF TABLES	xii
LIST OF FIGURES	xiii
CHAPTER	
I. INTRODUCTION	1
1.1 Background	1
1.2 Problem Formulation	1
1.3 Problem Limitation	2
1.4 Research Objectives	3
1.5 Research Methods	3
II. LITERATURE REVIEWS	5
2.1 URL-Based Threats	5
2.2 Tools and Technologies for URL Threat Analysis Feature	5
2.3 Chatbots in Cybersecurity	5
2.4 AI Integration with Gemini API	6
2.5 Frontend Implementation with React.js	6
2.6 Backend Implementation with Node.js	7
III. SYSTEM ANALYSIS	8
3.1 System Analysis	8
3.2 Product Perspective	8
3.3 Product Function	9
3.4 System Overview	17
IV. SYSTEM IMPLEMENTATION AND TESTING	19
4.1 System Interface Implementation	19
4.2 The Web Threat Analysis Code And Explanation	30
4.3 Security ChatBot: Cyra AI Code And Explanation	45
	xi

4.4	Software Functionality Testing	62
V.	CONCLUSION	66
	REFERENCES	67

LIST OF TABLES

Table 3. 1 Table Description Use Case Diagram.....	10
Table 3. 2 Table Description Use Case Diagram.....	12
Table 3. 3 Table Description Use Case Diagram.....	13
Table 3. 4 Table Description Use Case Diagram.....	15
Table 4.1 Security Awareness Tools Testing.....	62
Table 4.2 Network Security Tools Testing.....	63
Table 4.3 Web Threat Analysis Tools Testing.....	64
Table 4.4 Security ChatBot Testing.....	65

LIST OF FIGURES

Figure 3. 1 Use Case Diagram.....	9
Figure 3. 2 ERD.....	16
Figure 3. 3 Class Diagram.....	17
Figure 4.1 Page Interface login page.....	19
Figure 4. 2 Homepage.....	20
Figure 4. 3 Super user homepage.....	20
Figure 4. 3 Regular user homepage.....	21
Figure 4. 3 Phishing Dashboard.....	21
Figure 4. 4 Create Phishing Campaign Page.....	22
Figure 4. 5 Create Target Campaign Page.....	23
Figure 4. 6 Create Email Template Page.....	23
Figure 4. 7 Create Landing Page.....	24
Figure 4. 8 Create Sending Profile Page.....	25
Figure 4. 9 Create User Management Page.....	25
Figure 4.10 Web threat analysis feature is displayed.....	26
Figure 4.11 The web threat analysis result UI.....	26
Figure 4.12 Whitelist Page.....	27
Figure 4.13 Create Whitelist Rule.....	27
Figure 4.14 Firewall Policy.....	28
Figure 4.15 Create Firewall Policy.....	28
Figure 4.16 Logs.....	29
Figure 4.17 Security ChatBot AI: Cyra AI.....	29
Figure 4.18 Example interactive with Cyra AI	30