CONTENTS

APPROVAL ii

SELF DECLARATION AGAINST PLAGIARISM iii

ABSTRACT iv

ABSTRAK v

DEDICATION vi

ACKNOWLEDGMENTS vii

PREFACE viii

CONTENTS ix

LIST OF TABLES xiv

LIST OF FIGURES xv

LIST OF TERMS xvi

LIST OF NOTATIONS xviii

1 INTRODUCTION 1

1.1 Rationale . . . 1

1.1.1 Background of the Study . . . 1

1.1.2 Problem Situation: Global, National, and Local Forces . . . 2

1.1.3 Statistical Justification . . . 2

1.1.4 Clinching Statement . . . 3

1.2 Theoretical Framework . . . 3

1.3 Conceptual Framework/Paradigm . . . 4

1.3.1 AIM-CTI Layer Framework Architecture . . . 4

1.3.2 Research Paradigm: AI-Driven CTI Enhancement . . . 6

1.3.3 Framework Flow and Integration . . . 7

1.3.4 CTI-CMM Enhancement Mapping . . . 7

1.3.5 Critical Success Factors . . . 8

1.3.6 Variables Related to the Problem . . . 9

1.3.6.1 Independent Variables . . . 9

1.3.6.2 Dependent Variables . . . 9

1.3.6.3 Mediating Variables . . . 9

1.3.6.4 Moderating Variables 10
1.3.7 Research Paradigm and Schematic Diagram 10
1.3.8 Relationship of Elements/Variables 11
1.4 Statement of the Problem 12
1.5 Objective and Hypotheses 12
1.6 Assumption 13
1.7 Scope and Delimitation 13
1.8 Significance of the Study 14

2 REVIEW OF LITERATURE AND STUDIES 15
2.1 Related Literatures 15
2.1.1 CTI Capability Maturity Models 15
2.1.2 AI and Machine Learning in Cybersecurity 19
2.1.3 Large Language Models in Security Applications 20
2.1.4 Retrieval-Augmented Generation in Information Security 20
2.1.5 CTI Platforms and Practices 21
2.2 Related Studies 22
2.2.1 Research Gap Analysis and Study Positioning 30

3 RESEARCH METHODOLOGY 33
3.1 Research Design 33
3.1.1 System/Product/Method Implementation 33
3.1.1.1 System Requirements and Limitations 33
3.1.1.2 Modular Architecture Design 37
3.1.1.3 OpenCTI-LlamaIndex Connector 38
3.1.1.4 Connector Initialization and Configuration 39
3.1.1.5 Mathematical Foundations 41
3.1.2 Performance and Scalability Metrics 44
3.1.3 Graph Data Model Complexity 44
3.1.4 Retrieval Performance Metrics 45
3.1.4.1 Main Processing Loop 45
3.1.4.2 Report Processing 46
3.1.4.3 Batch Processing Optimization 47
3.1.4.4 API Layer Implementation 49
3.1.4.5 Hybrid Search API Implementation 50
3.1.4.6 User Interface Implementation 51
3.1.4.7 Real-time Response Streaming 52
3.1.4.8 Hybrid Retrieval Framework Implementation 53
3.1.5 Experiment Scenario 54
3.1.5.1 Collecting Queries from Expert 54

3.1.5.2 Generate System Responses . . . 55
3.1.5.3 Evaluating the Results . . . 55
3.1.5.3.1 F1 Score . . . 55
3.1.5.3.2 Rouge N . . . 56
3.1.5.3.3 METEOR . . . 56
3.1.5.4 Expert Validation Analysis . . . 56
3.2 Population/Sampling . . . 57
3.3 Instrumentation and Data Collection . . . 57
3.3.1 OpenCTI Data Connector Pipeline . . . 58
3.3.1.1 Data Collection Procedures . . . 58
3.3.1.2 Neo4j Dual Database Architecture . . . 58
3.3.1.3 Vector Database Schema . . . 60
3.3.1.4 Graph Database Schema . . . 61
3.3.1.5 STIX Validation Process . . . 64
3.3.2 Expert Validation . . . 65
3.4 Tools for Data Analysis . . . 65
3.5 Security Testing and Validation . . . 66
3.5.1 Injection Attack Resistance Testing . . . 66
3.5.1.1 Cypher Injection Vulnerability Assessment . . . 66
3.5.1.2 API Layer Security Testing . . . 67
3.5.1.3 LLM-Specific Security Testing . . . 67
3.5.2 Security Implementation Details . . . 68
3.5.2.1 Implemented Security Measures . . . 68
3.5.2.2 Security Configuration . . . 68

4 PRESENTATION, ANALYSIS AND INTERPRETATION OF DATA 70
4.1 Presentation of Data . . . 70
4.1.1 Evaluation Framework Overview and Data Presentation . . . 70
4.1.2 Query Dataset Analysis with Domain Distribution . . . 70
4.1.3 Ground Truth Establishment . . . 74
4.1.4 System Response Analysis . . . 76
4.1.4.1 Hybrid RAG System Performance . . . 76
4.1.4.2 ChatGPT - System Response . . . 79
4.1.5 Quantitative Performance Analysis . . . 82
4.1.5.1 Hybrid RAG Quantitative Results . . . 82
4.1.5.2 ChatGPT Result . . . 85
4.1.6 Analysis of the Data . . . 88
4.1.6.1 Quantitative Analysis . . . 88
4.1.6.2 Qualitative Analysis . . . 89
4.1.6.2.1 Sample Data . . . 89

4.1.6.2.2 Analysis . . . 92
4.1.6.3 LLM vs Human Expert Judgment Analysis . . . 92
4.1.6.4 Qualitative Result Analysis . . . 93
4.1.6.5 ChatGPT Expert Judgment Evaluation . . . 93
4.1.6.5.1 Comprehensive Comparison: Hybrid RAG vs ChatGPT Expert Judgment . . . 94
4.1.6.5.2 Critical Limitations Analysis of Proposed Method 95
4.1.6.6 Statistical Validation and Comparative Analysis . . . 96
4.1.7 CTI Maturity Evaluation (CTI-CMM Scoring) . . . 97
4.1.7.1 Before Implementation . . . 97
4.1.7.2 After Implementation . . . 101
4.1.8 Security Testing Results . . . 104
4.1.8.1 Injection Attack Resistance Validation . . . 104
4.2 Summary of Findings . . . 105

5 CONCLUSION AND RECOMMENDATIONS 106
5.1 Conclusions . . . 106
5.1.1 Research Problem Resolution . . . 106
5.1.2 Research Objectives Achievement . . . 106
5.1.3 Research Hypothesis Validation . . . 107
5.1.4 Key Research Contributions . . . 107
5.1.5 System Limitations Identified . . . 107
5.2 Recommendations . . . 108
5.2.1 Technical Improvements . . . 108
5.2.1.1 Knowledge Base Enhancement . . . 108
5.2.1.2 Multi-Entity Reasoning Enhancement . . . 108
5.2.2 System Architecture Improvements . . . 108
5.2.2.1 Hardware Requirements . . . 108
5.2.2.2 Scalability Enhancements . . . 108
5.2.3 Security and Compliance . . . 109
5.2.3.1 Security Testing Framework . . . 109
5.2.3.2 Compliance Requirements . . . 109
5.2.4 Future Research Directions . . . 109
5.2.4.1 Methodological Advancement . . . 109
5.2.4.2 Evaluation Methodology Enhancement . . . 110
5.2.4.3 Industrial Integration . . . 110

BIBLIOGRAPHY 111

Appendices 113

A MISCELLANEOUS **115**

A.1 List of Query 115

B Curriculum Vitae **186**