A SMART ZERO TRUST SECURITY FRAMEWORK FOR COMBATING AI-DRIVEN CYBERATTACKS IN FINANCIAL INSTITUTIONS

GUEMBE, BLESSING
(17PCG01640)
B.Sc Computer Science, Niger Delta University, Amassoma
M.Sc Computer Science, Covenant University, Ota

JUNE, 2023

A SMART ZERO TRUST SECURITY FRAMEWORK FOR COMBATING AI-DRIVEN CYBERATTACKS IN FINANCIAL INSTITUTIONS

BY

GUEMBE, BLESSING
(17PCG01640)
B.Sc Computer Science, Niger Delta University, Amassoma
M.Sc Computer Science, Covenant University, Ota

A THESIS SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF DOCTOR OF PHILOSOPHY (Ph.D) DEGREE IN COMPUTER SCIENCE, DEPARTMENT OF COMPUTER AND INFORMATION SCIENCES, COLLEGE OF SCIENCE AND TECHNOLOGY, COVENANT UNIVERSITY, OTA, OGUN STATE, NIGERIA

JUNE, 2023

ACCEPTANCE

This is to attest that this thesis is accepted in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy in Computer Science in the Department of Computer and Information Sciences, College of Science and Technology, Covenant University, Ota, Ogun State, Nigeria.

Ms Adefunke F. Oyinloye
(Secretary, School of Postgraduate Studies) **Signature and Date**

Prof. Akan B. Williams
(Dean, School of Postgraduate Studies) **Signature and Date**

DECLARATION

I, GUEMBE, BLESSING (17PCG01640), hereby declare that this research was carried out by me under the supervision of Prof. Ambrose A. Azeta of the Department of Computer and Information Sciences, Covenant University, Ota and Prof. Victor C. Osamor of the Department of Computer and Information Sciences, Covenant University, Ota. I attest that the thesis has not been presented either wholly or partly for the award of any degree elsewhere. All sources of data and scholarly information used in this thesis are duly acknowledged.

GUEMBE, BLESSING

Signature and Date

CERTIFICATION

This is to certify that the research work titled "**A SMART ZERO TRUST SECURITY FRAMEWORK FOR COMBATING AI-DRIVEN CYBERATTACKS IN FINANCIAL INSTITUTIONS**" is an original research work carried out by **GUEMBE, BLESSING (17PCG01640)**, in the Department of Computer and Information Sciences, Covenant University, Ota, Ogun State, Nigeria, under the supervision of Prof. Ambrose A. Azeta and Prof. Victor C. Osamor. We have examined and found the work acceptable for its contribution to knowledge and literary presentation.

Prof. Ambrose A. Azeta
(Supervisor) **Signature and Date**

Prof. Victor C. Osamor
(Co-Supervisor) **Signature and Date**

Prof. Olufunke O. Oladipupo
(Head of Department) **Signature and Date**

Prof. Boniface K. Alese
(External Examiner) **Signature and Date**

Prof. Akan B. Williams
(Dean, School of Post-Graduate Studies) **Signature and Date**

DEDICATION

I dedicate this thesis to my Heavenly Father, who is the source of my wisdom and strength, and in whom I place my hope for supply. I also dedicate it to my mum Mrs. Comfort Guembe and my entire Family.

ACKNOWLEDGEMENTS

First, I acknowledge the inspiration of the Almighty God that gives understanding without which this thesis may never have been successful.

I wish to express my deep sense of gratitude and thanks to the Chancellor and Chairman, Board of Regents, Covenant University, Dr. David O. Oyedepo, for the academic and spiritual platform created. I sincerely thank the Vice-Chancellor, Prof. Abiodun H. Adebayo, the Deputy Vice-Chancellor Prof. Olujide A. Adekeye and the management team of Covenant University for running the vision. My special appreciation goes to the Dean, School of Postgraduate Studies, Prof. Akan B. Williams, for his dedication towards creating an enabling research environment and producing world-class researchers. I also applaud the Sub-Dean, School of Postgraduate Studies, Dr. Emmanuel O. Amoo, for his steadfast counsel throughout my programme.

My special thanks also go to Prof. Olufunke O. Oladipupo (the Head of Department), and all the Faculty and Staff of the Computer and Information Science Department, Covenant University, for their contribution, encouragement, and support towards the realisation of this thesis.

I appreciate the profound contributions of my supervisor, Prof. Ambrose A. Azeta who has been a role model and mentor. Thank you, sir, for being always available and putting great faith in me even when I did not believe I could accomplish anything worthwhile. The lessons learnt from you and your humility throughout the process of this research will remain with me for life. I thank God for connecting me to your academic leadership. I am certain your kind and humble nature has rubbed off on me even as I move to accomplish higher things in the nearest future. Also, I acknowledge my co-supervisor, Prof. Victor C. Osamor, who has been a great mentor and inspiration to me throughout the course of this program. I thank God for the opportunity to have followed your academic leadership up until now. I will never take this for granted.

I am grateful to Dr. Itunuoluwa Isewon (the Postgraduate Coordinator) whose leadership contributed positively to the completion of this thesis.

I am indebted to my Friend and Roommate Mr. John Abubakar for his support, encouragement, and assistance towards the formatting of this thesis.

Special thanks go to my family members who would not let me rest until I had completed this work satisfactorily. Foremost among whom includes my mum Mrs. Comfort Guembe and my siblings for constant support and encouragement. Be blessed by the Lord Most High.

I would also like to thank all those people who have contributed in some ways both directly and indirectly to the success of this research.

TABLE OF CONTENTS

CONTENT **PAGES**

COVER PAGE **i**

TITLE PAGE **ii**

ACCEPTANCE **iii**
DECLARATION **iv**
CERTIFICATION **v**
DEDICATION **vi**
ACKNOWLEDGEMENTS **vii**
TABLE OF CONTENTS **ix**
LIST OF FIGURES **xiii**
LIST OF TABLES **xvi**
LIST OF ABBREVIATIONS **xviii**
ABSTRACT **xx**

CHAPTER ONE: INTRODUCTION **1**
1.1 Background to the Study 1
1.2 Statement of the Problem 4
1.3 Aim and Objectives of the Study 5
1.4 Justification of the Study 7
1.5 Significance of the Study 7
1.6 Scope of the Study 7
1.7 Glossary and Definitions of Terms 8

CHAPTER TWO: LITERATURE REVIEW **10**
2.1 Preamble 10
2.2 Concept of Cybersecurity 10
2.3 Cyberattack on Financial Institutions 12
2.3.1 Cybersecurity Operational Cost in Financial Institutions 13
2.3.2 Impact of Cyberattack on Financial Institutions 14
2.3.3 Impact of Cyberattack on Nigeria's Financial Industry and the Economy 15
2.4 Classifications of Cyberattack 16
2.5 Categories of Cyberattack 17
2.6 Cyberattack and AI-Driven Cyberattack 19
2.6.1 Difference Between Traditional and AI-Driven Cyberattacks 20
2.7 AI-Driven Cyberattack 21
2.7.1 Autonomous Cyberattack Techniques 23
2.7.2 AI Against AI 24
2.7.3 AI-Driven Cyberattack Evasion Techniques 25
2.7.4 Bio-Inspired and Swarm Intelligence 27
2.8 AI-Driven Attack Proof of Work 28
2.8.1 Application of Generative AI in Cyber Threat Hiding 35
2.9 AI-Driven Attack Cybersecurity Kill Chain 36
2.10 Cybersecurity Defense Strategies 42
2.10.1 Continuous Intelligent Analysis and Threat Monitoring 44
2.11 Smart-Dos Cybersecurity 44

2.12 Machine Learning in Cybersecurity 45
2.13 Explainable AI for Trustworthy Cybersecurity 49
2.13.1 XAI Methods in Cyber Threat Modelling 51
2.13.2 Trade-off Between XAI and Black-Box Model in Trustworthy Cybersecurity 52
2.13.3 Need and Impact of XAI in Cybersecurity 53
2.13.4 Transparent Machine Learning Techniques 54
2.13.5 Output Confidence of XAI 58
2.13.6 Rationale Explanation with XAI in Data Science 59
2.14 Zero Trust Security Framework 59
2.14.1 Security in Zero Trust Environment 60
2.14.2 Existing Zero Trust Security Framework 62
2.14.3 Challenges of Zero Trust Security Framework 63
2.15 AI Model Cybersecurity 65
2.15.1 AI Cybersecurity Defense Layered 68
2.15.2 AI Defense Techniques for Evasive Cyberattacks 69
2.15.3 Defence Techniques for Data Poisoning Attacks 70
2.15.4 Defence Techniques for Backdoor Cyberattacks 71
2.15.5 Defence Techniques for Model/Data Hijacking 71
2.16 Review Related Works 72
2.17 Summary of Findings from Related Works 77
2.18 Chapter Summary 77

CHAPTER THREE: METHODOLOGY 79
3.1 Preamble 79
3.2 Research Design 79
3.2.1 Research Strategy 79
3.2.2 Research Appraisal 80
3.3 CBN Risk-Based Cybersecurity Framework 81
3.3.1 Gathering of the Nigeria Banks Cybersecurity Incident Dataset 84
3.4 Components of the Smart-DOS Framework 84
3.4.1 Component of the DevOpsSec 85
3.4.2 Component of the Smart Policy Engine 87
3.4.3 Problem Definition of the Smart Policy Engine 90
3.4.4 Component of the Federated Pipeline 92
3.4.5 Model-agnostic Post-hoc Explainability 95
3.4.6 Local Explainer Problem Definition 96
3.4.7 Global Explainer Problem Definition 98
3.4.8 Systolic Addressing Problem Definition 100
3.5 Experimental Setup 103
3.5.1 Amazon SageMaker 104
3.5.2 Choice of Programming Language 104
3.5.3 Dataset Description 105
3.6 Machine Learning Evaluation Metrics 108
3.7 Chapter Summary 110

CHAPTER FOUR: RESULTS AND DISCUSSION 112
4.1 Preamble 112
4.2 Dataset Exploration and Discussion 112
4.2.1 Exploratory Data Analysis of the Zeek and Intelligent Security Group Dataset 112
4.2.2 Pre-processing of the Zeek and Intelligent Security Group Dataset 115
4.2.3 Eliminate Irrelevant Observations of the Zeek and Intelligent Security Group Dataset 115
4.2.4 Data Duplication of the Zeek and Intelligent Security Group Dataset 116
4.2.5 Data Transformation and Normalisation of the Zeek and Intelligent Security Group Dataset 116
4.2.6 Feature Selection of the Zeek and Intelligent Security Group Dataset 116
4.2.7 Local Model Implementation on Imbalanced Zeek and Intelligent Security Group Dataset 118
4.2.8 Sampling the Zeek and Intelligent Security Group Dataset 119
4.2.9 Local Model Implementation on Balanced Zeek and Intelligent Security Group Dataset 121
4.2.10 Multi-Class Classification Implementation on Imbalanced Zeek and Intelligent Security Group Dataset 121
4.2.11 Multi-Class Classification Implementation on Balanced Zeek and Intelligent Security Group Dataset 124
4.3 Exploratory Data Analysis of the Nigeria Banks Dataset 126
4.3.1 Pre-processing of the Nigeria Banks Dataset 129
4.3.2 Dealing with Missing Values in the Nigeria Banks Dataset 129
4.3.3 Data Type Transformation of the Nigeria Banks Dataset 129
4.3.5 Encoding the Nigeria Banks Dataset 130
4.3.6 Feature Selection of the Nigeria Banks Dataset 130
4.3.7 Sampling the Nigeria Banks Dataset 131
4.3.8 Nigeria Banks Dataset Resampling with SMOTE Technique for Multi-Class 133
4.4 Implementation of the Federated Averaging 134
4.5 Implementing the Systolic Addressing Model 134
4.6 Deployment 135
4.7 Method of Benchmarking 136
4.8 Vulnerability Assessment Techniques 137
4.9 Binary Class Result of the Zeek and Intelligent Security Group Imbalanced Dataset 141
4.9.1 Federated Averaging for the Imbalanced Dataset 144
4.9.2 Binary Class Result for Zeek and Intelligent Security Group Balanced Dataset 145
4.9.3 Federated Averaging for the Zeek and Intelligent Security Group Balanced Dataset 149
4.9.4 Evaluation of the Multi-Class Classification Model Based on the Zeek and Intelligent Security Group Imbalanced Dataset 149
4.9.5 Evaluation of the Multi-Class Classification Model of the Zeek and Intelligent Security Group Balanced Dataset 150
4.9.6 Feature Importance 152
4.9.7 Binary Classification Result for the Imbalanced Nigeria Banks Dataset 153
4.9.8 Federated Averaging for the Imbalanced Nigeria Banks Dataset 155
4.9.9 Binary Classification Result for the Balanced Nigeria Banks Dataset 156

4.9.10 Federated Averaging for the Balanced Nigeria Banks Dataset 156
4.9.11 Evaluation of the Multi-Class Classification Model Based on the Imbalanced Nigeria Banks Dataset 157
4.9.12 Evaluation of the Multi-Class Classification Model Based on the Balanced Nigeria Banks Dataset 158
4.10 Result of the XSec Explainer 159
4.11 Benchmarking of Proposed Model with Existing Models 162
4.12 Results and Evaluation of the Systolic Addressing 164
4.13 Vulnerability Assessment Report 167
4.13.1 Vulnerability Result Analysis 168
4.14 Chapter Summary 168

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS 171
5.1 Preamble 171
5.2 Summary 171
5.3 Contribution to Knowledge 172
5.4 Conclusion 173
5.5 Recommendations 173

REFERENCES 174
Appendix A 190
Appendix B 190
Appendix C 194
Appendix D 196

LIST OF FIGURES

FIGURES	TITLE OF FIGURES	PAGES
2.1	Traditional Cyberattack Decision Logic	20
2.2	AI-Driven Attack Complex Decision Logic	21
2.3	AI-Driven Cyberattack Techniques	23
2.4	Application of Deep Learning in Evolving Cyber Threat	27
2.5	Traditional Dictionary-Based Password Brute-Force Attacks	30
2.6	AI-Driven Password Brute-Force Attacks	31
2.7	GAN Architecture	35
2.8	MalGAN Architecture	36
2.9	AI-Driven Attack Cybersecurity Kill Chain	37
2.10	Clustering Technique for Cyberattack Detection	47
2.11	Machine Learning Application in Malware Detection	48
2.12	Zero Trust Security Model	62
2.13	AI Model Cybersecurity	66
2.14	AI Cybersecurity defence Layer	69
3.1	Methodology Workflow	80
3.2	CBN Risk-Based Cybersecurity Framework	81
3.3	Use-Case of Central Bank of Nigeria Risk-Based Cybersecurity Framework	83
3.4	The Proposed Smart-DOS Zero Trust Security Model	85
3.5	Component of the Smart DevOpsSec	86
3.6	Component of the Local Smart Policy Engine Model	87
3.7	Component of Smart-DOS Brute-Force Attack Detection	88
3.8	Data Preprocessing Pipeline	89
3.9	Component of the Federated Pipeline	92
3.10	Global Model Insights	95
3.11	Local Explainable Model	97
3.12	Flowchart of the Global Explainer Decision Logic	100
3.13	Systolic Addressing Modelling	101
3.14	Amazon SageMaker Environmental Setup	102
3.15	Tubular Representation of Confusion Matrix	110

4.1 Head Structure of the Dataset 113
4.2 Output of the data info function 114
4.3 Output of the data info function 114
4.4 Summary Statistics of the Dataset 115
4.5 Class Ratio of the Original Dataset 119
4.6 Dataset After Oversampling 121
4.7 Class Distribution of the Original Dataset 123
4.8 Pie Chart Distribution of Multi-class Imbalanced Dataset 124
4.9 AI-Driven Class Distribution of Multi-Class Balanced Dataset 126
4.10 Data Info of the Nigeria Banks Dataset 127
4.11 Attack Types and Distribution of the Nigeria Banks Dataset 127
4.12 Attack Distribution of the Nigeria Banks Dataset for Binary Class 128
4.13 Attack Distribution of the Indigenous for Multi-Class 128
4.14 Summary of Missing Values in the Nigeria Banks Dataset 129
4.15 Results of Data Type Transformation of the Nigeria Banks Dataset 130
4.16 Pairwise Correlation Matrix 131
4.17 Nigeria Banks Dataset Distribution After Preprocessing 132
4.18 Nigeria Banks Dataset Distribution After Oversampling 133
4.19 Training and Deployment of the Proposed Model with Amazon SageMaker 135
4.20 Vulnerability Assessment Architecture 137
4.21 Modified Attack Phase with Discovery Phase Iteration Architecture 138
4.22 CVVS Based Score Decision Tree 139
4.23 Confusion Matrix of the Zeek and Intelligent Security Group Imbalanced Dataset 143
4.24 AUC-ROC Curve of the Zeek and Intelligent Security Group Imbalanced Dataset 143
4.25 Precision-Recall Curve of the Zeek and Intelligent Security Group Imbalanced Dataset 144
4.26 Confusion Matrix of the Zeek and Intelligent Security Group Balanced Dataset 147
4.27 AUC-ROC Curve of the Zeek and Intelligent Security Group Balanced Dataset 148

4.28 Precision-Recall Curve of the Zeek and Intelligent Security Group Balanced Dataset 148
4.29 Actual Values Versus Predicted Values of the Zeek and Intelligent Security Group Balanced Dataset 151
4.30 ROC Curve for the Multi-Class Classification of the Zeek and Intelligent Security Group Balanced Dataset 152
4.31 Top Ten Important Features of the Zeek and Intelligent Security Group Balanced Dataset 153
4.32 Global Explainer for Summary Plot 160
4.33 Shap Explainer Value for the Dependency Plot 161
4.34 Shap Explainer Value for Dependence Plot 162
4.35 Benchmarking of Proposed Model with Existing Binary Class Models Based on Performance Accuracy 163
4.36 Benchmarking of Proposed Model with Existing Multi-Class Models Based on Performance Accuracy 164
4.37 Scattered Plot of the Systolic Addressing Showing Legitimate Flow 165
4.38 Scattered Systolic Addressing Showing AI-Driven Attacks 166
4.39 Vulnerability Assessment Result Based on CVSS Score 168

LIST OF TABLES

TABLES	TITLE OF TABLES	PAGES
1.1	Objectives and Methodology Mapping	6
2.1	Ranking of Cyberattacks in the Top Ten Industry	13
2.2	AI Techniques in the Reconnaissance Stage of Cybersecurity Kill Chain	38
2.3	AI Techniques in the Cybersecurity Kill Chain Access and Penetration Stage	39
2.4	AI Techniques in the Delivery Stage of the Cybersecurity Kill Chain	40
2.5	AI Techniques in the Exploitation Phase of Cybersecurity Kill Chain	41
2.6	AI Techniques in the C2 Stage of the Cybersecurity Kill	42
3.1	Activities of the Key Stakeholders of the CBN Risk-Based Framework	82
3.2	Systolic Addressing Requirement Description	102
3.3	Systolic Addressing Technical Description	103
3.4	Features of the Zeek and Intelligent Security Group Dataset	106
3.5	Attack Distribution in the Zeek and Intelligent Security Group Dataset	107
3.6	Features of the Nigeria Banks Dataset	108
3.7	Attack Distribution in the Nigeria Banks Dataset	108
4.1	Top Ten Selected Features of the Dataset	117
4.2	Data Resampling with SMOTE Technique for Binary Class	120
4.3	Class Distribution of the Original Dataset	122
4.4	Data Resampling with SMOTE Technique for Multi-Class	125
4.5	Data Resampling of the Nigeria Banks Dataset	132
4.6	Nigeria Banks Dataset Resampling with SMOTE Technique for Multi-Class	133
4.7	Maximum Attack Level Based on DRS	140
4.8	Classification Result of the Zeek and Intelligent Security Group Imbalanced Dataset	141
4.9	Classification Report of the Zeek and Intelligent Security Group Imbalanced Dataset	142
4.10	Actual versus Predicted Result of the Zeek and Intelligent Security Group Imbalanced Dataset	142
4.11	Performance Accuracy of the Centralised and Federated Model of the Zeek and Intelligent Security Group Imbalanced Dataset	144

4.12 Classification Result of the Zeek and Intelligent Security Group Balanced Dataset 145
4.13 Classification Report of the Zeek and Intelligent Security Group Balanced Dataset 146
4.14 Actual versus Predicted Result of the Zeek and Intelligent Security Group Balanced Dataset 146
4.15 Performance Accuracy of the Centralised and Federated Model for Zeek and Intelligent Security Group Balanced Dataset 149
4.16 Multi-Class Classification Result of the Zeek and Intelligent Security Group Imbalanced Dataset 149
4.17 Multi-Class Classification Result of the Zeek and Intelligent Security Group Balanced Dataset 150
4.18 Actual Versus Predicted Result of the Multi-Class Classification on the Zeek and Intelligent Security Group Balanced Dataset 150
4.19 Classification Result of the Imbalanced Nigeria Banks Dataset 153
4.20 Classification Report of the Imbalanced Nigeria Banks Dataset 154
4.21 Actual Versus Predicted Samples for the Imbalanced Nigeria Banks Dataset 155
4.22 Performance Accuracy of the Centralised and Federated Model for the Imbalance Nigeria Banks Dataset 155
4.23 Classification Result of the Balanced Nigeria Banks Dataset 156
4.24 Classification Report of the Balanced Nigeria Banks Dataset 156
4.25 Performance Accuracy of the Centralised and Federated Model for the Balanced Nigeria Banks Dataset 157
4.26 Multi-Class Classification Result of the Imbalanced Nigeria Banks Dataset 157
4.27 Multi-class Classification for the Imbalanced Nigeria Banks Dataset 158
4.28 Multi-Class Classification Result of the Balanced Nigeria Banks Dataset 158
4.29 Multi-class Classification for the Balanced Nigeria Banks Dataset 159
4.30 Benchmarking of Proposed Model with Existing Binary Class Models 162
4.31 Benchmarking of Proposed Model with Existing Multi-class Models 163
4.32 Benchmarking the Systolic Addressing with Existing Model 166
4.33 Vulnerability Assessment Score 167
4.34 Vulnerability Assessment Result Based on DRS Score 168

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
BYOD	Bring Your Own Device
C2	Command and Control
CBN	Central Bank of Nigeria
CISO	Chief Information Security Officer
CNN	Convolutional Neural Network
CVSS	Common Vulnerability Scoring System
DA	Document Analysis
DDoS	Denial of Service Attack
DevOpsSec	Development, Operations and Security
DL	Deep Learning
DMBs	Deposit Money Banks
DNN	Deep Neural Network
DRS	DDoS Resiliency Score
DT	Decision Tree
EDA	Exploratory Data Analysis
GAM	General Addictive Model
GAN	Generative Adversarial Networks
GBRT	Gradient Boosted Regression Trees
IDSs	Intrusion Detection Systems
KNN	K-nearest Neighbor
LR	Logistic Regression
LSTM	Long Short-term Memory
ML	Machine Learning
MP	Matching Pursuit
NIBSS	Nigeria Inter-Bank System
NNs	Neural Networks
PA	Policy Administrator
PDP	Policy Decision Point
PE	Policy Engine
PEP	Policy Enforcement Point
PSPs	Payment Service Providers

RF	Random Forest
RNNs	Recurrent Neural Networks
SA	Systolic Addressing
SVM	Support Vector Machine
TA	Trust Algorithm
UCA	Use Case Analysis
URLs	Uniform Resource Locators
VA	Voice Assistance
VM	Virtual Machine
XAI	Explainable Artificial Intelligence
XSec	Explainable Security
ZT	Zero Trust
ZTA	Zero Trust Security Architecture
ZTS	Zero Trust Security

ABSTRACT

Cybercriminals are currently weaponising Artificial Intelligence (AI) to execute convoluted cyberattacks. This new type of cyberattack is known as an AI-driven attack. AI-driven attack incorporates AI into conventional cyberattack tools to elude detection and inflict more damage. Few studies have demonstrated the effectiveness of zero trust security frameworks and AI approaches in combating sophisticated cyberattacks. However, the existing approaches are prone to data poisoning, model weight attack, and data leakage. This study proposed a Smart zero trust security framework for combating AI-driven attacks in financial institutions to address the gaps in the existing approaches. To achieve this, the study investigated the Central Bank of Nigeria risk-based cybersecurity framework to examine the use-case, stakeholders responsibilities, and reusable concepts. The study designed a DevOpsSec technique to distribute security across the development phase. A systolic addressing approach was implemented to ensure continuous threat hunting. The Federated Artificial Intelligence Technology Enabler Framework was adopted to create virtual banks and a central server. The virtual banks collaborate to train the model under the supervision of the central server without exposing their data to others. The Gradient Boosting Decision Tree and SecureBoost techniques were used to train the model. At the same time, the model-agnostic post-hoc explainer was used to explain essential features that influence the model decision. The proposed model was trained on the Zeek and Intelligent Security Group Dataset and the Nigerian Banks dataset. The systolic addressing was simulated in a network lab environment. The implemented model was evaluated with standard machine learning evaluation metrics and benchmarked with state-of-art approaches. The result shows that the implemented model achieved the best performance, with 99.81% and 99.99% prediction accuracy, 100% precision, recall and F1-score for the binary classification on the Zeek and Intelligent Security Group Dataset and Nigerian Banks Dataset. The systolic addressing was able to detect malicious patterns in 56.14 seconds. The model agnostic post-hoc explainer reveals that the “flow_duration_milliseconds” positively impacts detecting AI-driven attacks, while the packet sent has a decreasing effect. The model was also evaluated with the ISO/IEC 27000:2018 cybersecurity vulnerability assessment techniques such as the Common Vulnerability Scoring System and DDoS Resiliency Score. The model achieved a Common Vulnerability Score of 3.15 and a DDoS Resiliency Score of 7.0. This implies that the model is capable of withstanding multiple variant attacks. The result suggests that the model can efficiently be incorporated into the existing zero trust security policy engine to enhance protection.

Keywords: AI-Driven Cyberattack, Cybersecurity, DevOpsSec, Zero trust