

**DE-TECH: RASPBERRY PI – BASED NETWORK BEHAVIOR
ANALYSIS INTRUSION DETECTION SYSTEM (NBAIDS)
USING ENSEMBLE LEARNING APPROACH**

A Project Study Presented to the Faculty of

Electronics Engineering Department

College of Engineering

Technological University of the Philippines – Manila

In Partial Fulfilment of the Course Requirements for the Degree of

Bachelor of Science in Electronics Engineering

Submitted by:

Ponciano, Mary Grace C.

Felipe, Aliah Fhae A.

Isaias, Judiel A.

Delos Reyes, Khylla Krizel S.

Pengson, Aila Marie S.

Caseria, Ranah Mae M.

Adviser:

Engr. Jay Fel C. Quijano

June 2024

APPROVAL SHEET

This project study entitled "**De-TECH: Raspberry Pi-based Network Behavior Analysis Intrusion Detection System using Ensemble Learning Approach**" has been prepared and submitted by the following proponents:

Ponciano, Mary Grace C.

Delos Reyes, Khylla Krizel S.

Felipe, Aliah Fhae A.

Pengson, Aila Marie S.

Isaias, Judiel A.

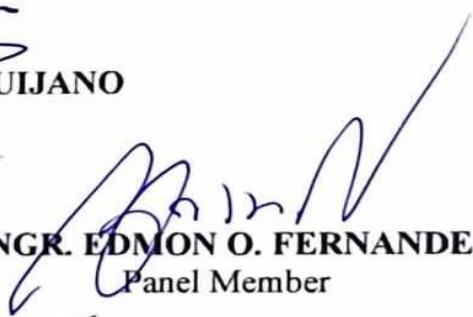
Caseria, Ranah Mae M.

In partial fulfillment of the requirements for the degree of Bachelor of Science in Electronics Engineering is hereby recommended for approval.


ENGR. JAY FEL C. QUIJANO

Project Adviser


ENGR. NILO M. ARAGO
Panel Member


ENGR. EDMON O. FERNANDEZ
Panel Member


ENGR. TIMOTHY M. AMADO
Panel Member

Accepted and approved in partial fulfillment of the course requirements for the degree of Bachelor of Science in Electronics Engineering.


ENGR. CHERRY G. PASCIÓN
Head, ECE Department


ENGR. LEAN KARLO S. TOLENTINO
Dean, College of Engineering

ABSTRACT

As the technology advances, the threat landscape changes needing a stronger network infrastructure. The study presents a Raspberry Pi-based Network Behavior Analysis Intrusion Detection System (NBAIDS) using Ensemble Learning Approach. The primary objective of this research was to develop a NBAIDS that can capture and classify network traffic as normal or malicious. The ensemble learning model used was trained using CTU-13 and CSE-CIC-IDS2018 datasets with the combination of weak learners such as SVM, Naïve Bayes and Decision Tree models. Moreover, the findings of the study showed that the ensemble learning model outperformed the individual algorithms. The ensemble model with 26 features had the highest performance with an accuracy of 96.39%, precision of 95.82%, recall of 96.39%, and F1-score of 95.66% using the validation data. But when tested on generated traffic, its performance decreased with an accuracy of 60.94%. And during deployment at ValACE and TUP-Manila, the model detected 76.04% to 92.18% of malicious traffic.

In summary, the developed Raspberry Pi-based NBAIDS showed its effectiveness in capturing and analyzing network traffic using ensemble learning model despite varying performance of the model depending on the nature and complexity of the network traffic being analyzed. The system also met the required standards for quality based on the ISO 9126 standard and showed potential for practical applications in network security.

ACKNOWLEDGEMENT

The successful completion of this research project would not have been possible without the support and guidance of many.

Our deepest appreciation goes to our esteemed research advisor, Engr. Jay Fel C. Quijano. His constant support, insightful feedback, and unwavering dedication were instrumental in shaping this project.

We would like to express our sincere gratitude to our entire research panel: Engr. Edmon O. Fernandez, Engr. Timothy M. Amado, and Engr. Nilo M. Arago, who also served as our Capstone professor. Their insightful critiques and constructive suggestions during the panel presentation significantly improved the quality of our research.

We acknowledge the invaluable role of the Electronics Engineering Department, led by Engr. Cherry G. Pascion. Their provision of necessary resources and fostering a supportive learning environment nurtured our research endeavors. We are also grateful to Engr. Lean Karlo S. Tolentino, Dean of the College of Engineering, for his leadership and commitment to academic excellence, which inspires continuous improvement.

We are particularly indebted to the cybersecurity and IT experts who generously shared their knowledge and expertise. Their insights significantly enriched our research and provided valuable direction.

We also acknowledge the Valenzuela City Academic Center for Excellence (ValACE) and UITC, the deployment sites for our research. Their willingness to collaborate and provide real-world application proved instrumental to the project's success.

Finally, we express our heartfelt gratitude to our friends and family. Their unwavering support, encouragement, and understanding fueled our motivation and perseverance throughout this journey.

And above all, we are eternally grateful to Almighty God for His blessings, strength, and wisdom that saw us through challenging moments.

- The Researchers

TABLE OF CONTENTS

Title Page	ii
Approval Sheet	ii
Abstract	iii
Acknoledgement	iv
Table of Contents	vi
List of Figures	xi
List of Tables	xiii
 Chapter 1 – The Problem and Its Background		
1.1 Introduction	1
1.2 Background of the Study	2
1.3 Research Gap	4
1.4 Research Objectives	5
1.4.1 General Objective	5
1.4.2 Specific Objectives	5
1.5 Significance of the Study	6
1.6 Scope and Limitations	6
1.7 Definition of Terms	7
 Chapter 2 – Review of Related Literature and Studies		
2.1 Conceptual Literature	9
2.1.1 Internetwork Systems	9
2.1.1.1 Local Area Network (LAN)	9
2.1.1.2 Wide Area Network (WAN)	10
2.1.1.3 Point-to-Point Connection	10
2.1.1.4 The Internet: World Wide Web (WWW)	11
2.1.1.5 Virtualization	11
2.1.2 Cyber Threats	12

2.1.2.1 Malware	12
2.1.2.2 Botnets	13
2.1.2.3 Denial of Service (DoS)	13
2.1.2.4 Bruteforce	14
2.1.2.5 Infiltration	14
2.1.3 Raspberry Pi	15
2.1.4 Datasets	16
2.1.4.1 CTU-13 Dataset	16
2.1.4.2 CSE-CIC-IDS2018 Dataset	18
2.1.4.2.1 Limitations of Datasets	21
2.1.5 Machine Learning Algorithms	21
2.1.5.1 SVM	21
2.1.5.2 Decision Tree	22
2.1.5.3 Naive Bayes	23
2.1.5.4 XG Boost	24
2.1.5.5 Ensemble Learning	24
2.1.6 Web Application	25
2.1.6.1 GUI	26
2.1.7 Intrusion Detection System	26
2.1.7.1 IDS based on Detection	28
2.1.7.2 IDS based on Application	29
2.2 Related Studies	30
2.2.1. Internetwork Systems	30
2.2.1.1. A low-cost embedded IDS to monitor and prevent Man-in-the-Middle attacks on wired LAN environments	30
2.2.2 Cyber Threats	31
2.2.2.1 Botnet Attack Detection using Machine Learning	31
2.2.3 Raspberry Pi	32
2.2.3.1 Snort IDPS using Raspberry Pi 4	32

2.2.3.2 Raspberry Pi as an Intrusion Detection System, a Honeypot and a Packet Analyzer	32
2.2.3.3 RpiIDS: Raspberry Pi IDS A Fruitful Intrusion Detection System for IoT	33
2.2.3.4 IDS on Raspberry Pi: A Performance Evaluation	33
2.2.3.5 Pi-IDS: Evaluation of Open-source intrusion detection systems on Raspberry Pi 2	34
2.2.4 Dataset	34
2.2.4.1 Deep learning-based botnet detection using the CTU-13 dataset	34
2.2.4.2 HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System	35
2.2.4.3 FastTrafficAnalyzer: An Efficient Method for Intrusion Detection Systems to Analyze Network Traffic	36
2.2.5 Machine Learning Algorithms	36
2.2.5.1 Intrusion detection system using XGBoost algorithm on CICIDS 2017 dataset	36
2.2.6 Web Application	37
2.2.6.1 Web application testing: A systematic literature review	37
2.2.6.2 A Graphical User Interface Framework for detecting Intrusions using Bro IDS	38
2.2.7 Intrusion Detection System	39
2.2.7.1 Efficient detection of botnet traffic by features selection and decision trees	39
2.2.7.2 An Ensemble Approach for Intrusion Detection system using Machine Learning Algorithms	39
2.2.7.3 An efficient XGBoost–DNN-based classification model for network intrusion detection system	40

Chapter 3 – Methodology	42
3.1 Theoretical Framework	42
3.2 Conceptual Framework	43
3.2.1 IPO Diagram	43
3.2.2 Block Diagram	45
3.2.3 Network Diagram	46
3.2.4 One-Line Diagram	47
3.2.5 System Architecture	48
3.3 Research Locale	49
3.4 Research Design	49
3.4.1 Hardware Design	49
3.4.2 Software Design	51
3.4.2.1 Algorithm Selection	51
3.4.2.2 Flow Chart of Processes	52
3.4.2.3 Web Application Design	58
3.5 Testing Procedure	61
3.5.1 Cross-validation Procedure	62
3.5.1.1 Malicious Traffic Scenario	63
3.5.1.2 Normal Traffic Scenario	64
3.6 Functionality Testing	65
3.7 ISO 9126 Standard Testing	66
3.8 Statistical Treatment	66
3.8.1 Percentage Frequency Distribution	66
3.8.2 Confusion Matrix	66
Chapter 4 - Results and Discussion	70
4.1 Project Technical Description	70
4.2 Project Structural Organization	70
4.2.1 Packet Capturing Tool	70
4.2.2 Device Limitations	71
4.3 Experimental and Data Analysis	72

4.3.1 Using Validation Data	72
4.3.2 Using Generated Traffic	74
4.3.3 Using Traffic from Deployment Sites	75
4.3.4 Chosen Ensemble Model	75
4.3.5 Web Application Evaluation	78
Chapter 5 - Conclusion And Recommendations	83
5.1 Summary of Findings	83
5.2 Conclusions	83
5.3 Recommendations	84
References	86
Appendices	97
A. Bill of Materials	97
B. Codes	97
a) Raspberry Pi	97
b) Machine Learning Model Training	102
c) Web App (Frontend)	123
d) Web App (Backend)	272
C. Manual of Operation	301
D. Project Duplication Manual	304
E. Survey Form	307
F. Tabulation	308
G. Proponent's Profile	358

LIST OF FIGURES

2.1	Classification of Data by Support Vector Machines (García, E. et al., 2016)	22
2.2	Decision Tree (Cortes & Vapnik, 1995)	23
2.3	Comparative analysis of the proposed model and the existing models with different K-folds (Devan & Khare, 2020)	41
3.1	Theoretical Framework	42
3.2	Block Diagram of Intrusion Detection System using Ensemble Learning Approach	45
3.3	Network Diagram	46
3.4	One-Line Diagram	47
3.5	System Architecture Diagram	48
3.6	Hardware Specifications	50
3.7	RPi-based IDS Attached to the Point-to-point Connected Devices	51
3.8	Flow Chart of Intrusion Detection System using Ensemble Learning	53
3.9	Flow Chart of Data Flow of NBAIDS	54
3.10	Flow Chart of the Backend of the Web Application of NBAIDS	56
3.11	Flow Chart of the Frontend of the Web Application of NBAIDS	57
3.12	Access Page of De-TECH Web Application	58
3.13	Home Page of De-TECH Web Application	59
3.14	Detect Feature of De-TECH Web Application	59
3.15	Analysis Feature of De-TECH Web Application	60
3.16a	Dashboard Feature of De-TECH Web Application	60
3.16b	Dashboard Feature of De-TECH Web Application	61
4.1	De-TECH Hardware	71
4.2	De-TECH connected in the switch using LAN cable	71

4.3	Confusion Matrix of Decision Tree Model	76
4.4	Confusion Matrix of Naïve Bayes Model	77
4.5	Confusion Matrix of SVM Model	77
4.6	Confusion Matrix of Ensemble Model	78

LIST OF TABLES

2.1	Characteristics of botnet scenarios (García et al.,2014)	17
2.2	Amount of data on each botnet scenario (García et al.,2014)	17
2.3	Distribution of labels in the NetFlows for each scenario in the dataset (García et al.,2014)	17
2.4	List of executed attacks and duration (IDS 2018 Datasets Research Canadian Institute for Cybersecurity UNB, n.d.)	19
2.5	Overview of the extracted features of the CSE-CIC IDS2018 dataset (IDS 2018 Datasets Research Canadian Institute for Cybersecurity UNB, n.d.)	20
2.6	Comparison of to previous version of CSE-CIC IDS2018 dataset	21
2.7	Comparison of the CSE-CIC 2018 ID dataset with CICIDS-2017 (Muhammad Ashfaq Khan, 2021)	35
2.8	Efficiency Analysis with Making use of Ensemble Approach using Bagging for KDDcup99 Data Set (Ravindra Kumar Gautam & Amit Doegar, 2018)	40
2.9	Comparative analysis of the proposed model and the existing models based on accuracy (Devan & Khare, 2020)	41
3.1	Input-Process-Output Diagram	44
3.2	Notable Attributes from CTU-13 Dataset (Kasimov, 2018)	61
3.3	Table of Detection Result for Different Malicious Traffic	63
3.4	Table of Detection Result for Different Normal Traffic	64
3.5	Confusion Matrix	67
3.6	Summary Performance Results of the Supervised Model	69
4.1	Durating the Raspberry Pi ran in the Deployment Sites	72

4.2	Performance Results of different Ensemble Models using Validation Data	73
4.3	Performance Results of different Ensemble Models using Generated Traffic	74
4.4	Results from Deployment Sites	75
4.5	Summary Performance Results of the Model 26	76
4.6	Project Evaluators	79
4.7	Frequency-Percentage Distribution Table of the Web App Evaluation using Questionnaire De-Tech Web Application Questionnaire	80
4.8	Weighted Score and Average Table of the Web App Evaluation using Questionnaire De-Tech Web Application Questionnaire	81
5.1	Results of Day 1 Deployment Testing of De-TECH on ValACE using Model 20	308
5.2	Results of Day 2 Deployment Testing of De-TECH on ValACE using Model 20	309
5.3	Results of Day 2 Deployment Testing of De-TECH on ValACE using Model 39	310
5.4	Results of Day 3 Deployment Testing of De-TECH on ValACE using Model 39	313
5.5	Results of Day 4 Deployment Testing of De-TECH on ValACE using Model 39	317
5.6	Results of Day 5 Deployment Testing of De-TECH on ValACE using Model 39	323
5.7	Results of Day 6 Deployment Testing of De-TECH on ValACE using Model 39	327
5.8	Results of Day 6 Deployment Testing of De-TECH on ValACE using Model 20	332
5.9	Results of Day 7 Deployment Testing of De-TECH on ValACE using Model 26	333
5.10	Results of Day 8 Deployment Testing of De-TECH on ValACE using Model 26	338
5.11	Results of Day 9 Deployment Testing of De-TECH on UITC using Model 26	343

5.12	Results of Testing Model 20 (Ibraheem, Hypertuned) using Generated Traffic	349
5.13	Confusion Matrix and Performance Results of Model 20 (Ibraheem, Hypertuned) using Generated Traffic	351
5.14	Results of Testing Model 26 using Generated Traffic	351
5.15	Confusion Matrix and Performance Results of Model 26 using Generated Traffic	352
5.16	Results of Testing Model 39 (reduced 50-50, Linear Regression-Hypertuned) using Generated Traffic	352
5.17	Confusion Matrix and Performance Results of Model 39 (reduced 50-50, Linear Regression-Hypertuned) using Generated Traffic	354
5.18	Functionality Evaluation of each Respondents	354
5.19	Reliability Evaluation of each Respondents	355
5.20	Usability Evaluation of each Respondents	355
5.21	Efficiency Evaluation of each Respondents	355
5.22	Maintability Evaluation of each Respondents	356
5.23	Portability Evaluation of each Respondents	356
5.24	All Characteristics Evaluation of each Respondents	357

Chapter 1

THE PROBLEM AND ITS BACKGROUND

1.1 Introduction

The Internet has transformed how we work, socialize, and live, connecting computers worldwide and revolutionizing communication and information sharing. Its influence spans business, education, entertainment, and personal connections, surpassing previous transformations. In April 2023, Statista reported that approximately 5.18 billion people, equivalent to around 64.6 percent of the global population, actively used the Internet (Petrosyan, 2023). The Internet's extensive reach and role in global LAN adoption are significant. LANs can exhibit security weaknesses, including misconfigurations, weak access controls, outdated systems, and insider threats, which enable unauthorized access and internal network-based attacks. Such vulnerabilities manifest in various forms and stem from different factors. A comprehensive examination of cyber security weaknesses, threats, attacks, and potential solutions provides a comprehensive understanding of the issue (Aslan et al., 2023). Addressing the prevalent cyber threats and inadequate network security necessitates immediate attention and action to safeguard data integrity, confidentiality, and system availability. Take proactive measures and deploy effective intrusion detection systems (IDS) to create a secure digital environment and protect against evolving malware threats.

1.2 Background of the Study

The expeditious improvement of the technology is also the increase in the utilization of computer systems connected through networks and the exchange of information among them, as well as the creation of applications designed to run on different platforms, presenting a significant threat to the web server's security. As of 2022, social media is utilized by half of the global population, accounting for 50%. This translates to a staggering 3.98 billion individuals engaging in social media platforms worldwide (Flynn, 2023). Currently, the Internet connects a vast array of computers and networks across the globe. It comprises numerous local area networks (LANs) spread worldwide, linked by a central vast area network (WAN). LANs usually function at speeds ranging from 10 to 100 Mbps. According to Rodda and Shankar (2016), the increase in malicious attacks on web servers has raised concerns. The vast amount of network traffic makes manual monitoring impossible. Any unauthorized access to a system that compromises data availability, confidentiality, and integrity constitutes an attack. The Internet has become a worldwide tool that enormously impacts education, health, wealth, government, and business. Flynn (2023) reported that in 2021, the global number of active internet users reached 4.9 billion, accounting for 62% of the world population.

Unauthorized access to a computer system can disrupt servers, clients, or computer networks. Malicious software, also called malware, is invasive software created by hackers or cybercriminals. This malware aims to inflict harm and pilfer data from computers or computer systems. The number of Windows malware detections on business endpoints worldwide rose by 13 percent, and attack techniques were divided into categories targeting consumers and those impacting organizations' networks, as outlined in the Malwarebytes

Labs 2020 State of Malware Report. The automatic monitoring of the network flow to effectively recognize malicious attacks from regular traffic is called an Intrusion Detection System.

The rapid expansion of the Internet of Things (IoT) has dramatically increased the number of devices connected to the Internet. While this technological advancement has revolutionized connectivity, it has also introduced significant vulnerabilities, particularly in IoT devices that often lack robust security measures. The proliferation of such devices has not only heightened the risk of botnet attacks, where a botmaster controls compromised devices to execute illegal activities (Feily et al., 2009), but also made these devices susceptible to sophisticated cyber threats. These include Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which aim to overwhelm a target's resources and render systems inaccessible. Research shows that IoT devices are particularly vulnerable to DDoS attacks due to low power and susceptibility to traffic flooding (Mathews et al., 2022; Sachidananda et al., 2019; Mohammed et al., 2019).

Additionally, brute force attacks, which systematically check all possible passwords or keys, have become more prevalent with the increase in online devices. Infiltration techniques, exploiting software vulnerabilities and phishing scams, are also escalating in complexity, posing a significant risk to network security. The urgent need for comprehensive cybersecurity strategies is highlighted by these cyber threats' wide range and complexity, which address the numerous vulnerabilities in the constantly changing digital environment.

1.3. Research Gap

Despite the exploration of ensemble learning techniques for intrusion detection systems (IDS) in studies such as those conducted by Gautam and Doegar (2018) and Devan and Khare (2020), a significant gap persists in the application of these approaches to resource-constrained devices like the Raspberry Pi. This study addresses this gap by developing an ensemble learning-based IDS tailored to the Raspberry Pi platform, advancing cost-effective and energy-efficient security solutions.

Moreover, most of the existing research evaluates ensemble learning techniques on benchmark datasets such as KDD CUP 99 and NSL-KDD (Gautam & Doeger, 2018; Devan & Khare, 2020), neglecting the assessment of performance and accuracy on real-world network traffic, which may exhibit distinct characteristics from synthetic datasets. Consequently, this study proposes to evaluate the developed system on authentic network traffic, bridging the identified research gap.

Furthermore, while the proposed approach integrates network behavior analysis (NBA) and ensemble learning, a paucity of studies exploring this combination exists. As highlighted by Youssef and Emam (2011), incorporating NBA with data mining techniques could overcome limitations in current IDS. Therefore, this research wants to investigate the potential synergies between NBA and ensemble learning for intrusion detection, addressing a notable gap in the existing literature.

An additional research gap lies in the lack of user-friendly interfaces for IDS, as noted in the study by Gupta and Goel (2012), which emphasizes the need for a GUI framework to enhance the usability of IDS tools. The present research addresses this gap.

By incorporating an intuitive graphical user interface (GUI) for visualizing and interpreting the results of the ensemble learning-based IDS.

Finally, as cyber threats continue to evolve, a lack of research persists on the adaptability and robustness of ensemble learning-based IDS in detecting new and unknown threats. Studies like those by Chen et al. (2019) and Khan (2021) have explored deep learning and hybrid approaches for botnet detection, but the focus on ensemble learning for evolving threats still needs to be expanded. The present research aims to contribute to this area by evaluating the developed system's ability to adapt and detect evolving cyber threats.

1.4 Research Objectives

1.4.1 General Objective:

This study aims to develop a Raspberry Pi-based Network Behavior Analysis Intrusion Detection System (NBAIDS) using ensemble learning approach

1.4.2 Specific Objectives:

1. To develop an Intrusion Detection System using Raspberry Pi 4 model B that will identify and analyze captured traffic
2. To compare and analyse the accuracy of the developed ensemble machine learning algorithm using Naïve Bayes, Support Vector Machine, Decision Tree, and XGBoost to the individual algorithms
3. To develop an adaptive web application that will display the result of the IDS based on the specified start and end time of the captured data
4. To evaluate the created Network Behavior Analysis Intrusion Detection System (NBAIDS) using the ISO 9126 standard

1.5 Significance of the Study

This research offers a significant contribution to the ever-evolving digital landscape and cybersecurity by proposing a study on an ensemble learning approach for detecting malicious traffic in networks.

By developing an Intrusion Detection System (IDS) that utilizes ensemble learning for malicious traffic detection, this study aims to improve passive and conventional detection mechanisms against malware. This improvement will ultimately lead to a reduction in the number of attacks on computer networks. It will help safeguard the confidentiality and integrity of sensitive data, especially in today's interconnected digital world.

Additionally, by assessing the accuracy and effectiveness of ensemble learning methods to identify and detect malicious traffic patterns, this research empowers organizations with a deeper understanding of the relationship between machine learning and cybersecurity risks. This enhanced understanding allows organizations to research and address these threats more effectively, decreasing the risk of data breaches and unauthorized access.

Finally, this study aims to strengthen the security posture of computer networks by effectively and accurately recognizing and classifying newly developed and modified malware attacks.

This capability significantly reduces risks and vulnerabilities within the network. This research contributes to a more robust, adaptable, and accessible cybersecurity landscape.

1.7 Definition of Terms

Algorithm – a series of directions that a computer can follow to address a specific issue.

Background Traffic – Background traffic is traffic that is not malicious but is not essential to the operation of a network

Botnet – a collection of computers that have been infected by harmful software that a hacker controls

Brute Force Attack – a hacking technique that relies on a systematic trial-and-error approach to break passwords, login credentials, and encryption keys.

Denial of Service (DoS) – an attack designed to render a machine or network inoperable, making it inaccessible to its intended users.

Ensemble Learning – a method of machine learning that enhances the overall accuracy by merging the predictions of several models.

Infiltration – malicious software designed to infiltrate and harm a user's computer.

Intrusion Detection System (IDS) – a security system that monitors network traffic for malicious activity

Malicious Traffic – traffic not expected on a network, such as attack or spam traffic. An irregular pattern of behavior typically characterizes it.

Network Behavior Analysis (NBA) – a type of IDS that analyzes network traffic to identify unusual or suspicious behavior and does not rely on signatures of known attacks

Network Behavior Analysis Intrusion Detection System (NBAIDS) – an IDS that combines NBA with other IDS techniques.

Normal Traffic – traffic that is expected to be on a network and characterized by a regular pattern of behavior

Packets - data units transmitted over a network.

Traffic – the flow of packets over a network and can be classified as either normal traffic or malicious traffic

Chapter 2

REVIEW OF RELATED LITERATURE AND STUDIES

2.1 Conceptual Literature

2.1.1 Internetwork Systems

An internetwork system encompasses a computer network structure that extends over numerous individual networks, facilitating effective communication and resource sharing. Routing involves the distribution of information across the internetwork. Internetworking has emerged as a crucial element in contemporary computer communication systems and has found applications in diverse fields such as teleradiology and the advancement of internetwork research. The significance of internetworking lies in its ability to facilitate collaboration and communication among diverse networks, thus enabling efficient resource sharing and effective communication (Park et al., 2012).

2.1.1.1 Local Area Network (LAN)

The group of gadgets and other relevant tools that connect to a machine using a wireless signal or a shared transmission is called a local area network (LAN). In a LAN, the networking equipment or computers are situated near one another, enabling communication, resource sharing, and information exchange among them (Bhardwaj, 2020).

An Ethernet cable, referred to as a LAN cable, serves as a conductor that establishes connections between devices within a Local Area Network (LAN) using a network connector. There is a specific sort of interconnection

that enables the routers, wireless routers, PCs and other machines to communicate with one another. Ethernet cable is sometimes abbreviated as LAN (Stein, 2022).

2.1.1.2 Wide Area Network (WAN)

A Wide Area Network (WAN) can be used to transmit information, pictures, sound and even videos over a large region like one country, a continent or even the whole world. The complexity of a WAN can vary greatly, from intricate backbone networks that interconnect the Internet to straightforward dial-up connections that link a personal computer to the Internet (Forouzan & Sophia Chung Fegan, 2007). Information obtained from news wire services and other sources via a wide area network (WAN) possesses unique characteristics in terms of its timeliness, duration, audience, and volume. With its constantly changing and disorganized environment, this data presents difficulties but also provides a rich setting for the creation and assessment of AI classification and extraction methods (Wyle, n.d.).

2.1.1.3 Point-to-Point Connection

Computer structures, connections, and telecommunications all frequently employ this kind of connectivity. It provides a dedicated and private pathway for data transfer between the two connected points. A point-to-point connection refers to a secure and direct link established between two or more private data service sites. It is a network data transport

service that operates independently of the Internet, ensuring inherent security and eliminating the necessity for data encryption (Azap, 2022).

2.1.1.4 The Internet: World Wide Web (WWW)

The development of the World-Wide Web aimed to create a vast collection of human knowledge, enabling individuals in distant locations to collaborate and share ideas related to shared projects. The inspiration for the Web emerged from a favorable encounter with a personalized hypertext system, known as a “home-brew,” which effectively managed personal information within a distributed project (Berners-Lee et al., 1994). The World Wide Web allows the display of textual, graphical, auditory, and visual information, regardless of the platform, through the utilization of hypertext (Hirsch, 1995).

The “a” option and utilization of the Internet, along with its various applications, do not inherently bring about transformative changes in individuals’ lives. Instead, they become integrated into the natural process of societal evolution. Consequently, it becomes evident that the mere substitution of one aspect with another is improbable, as numerous consequential events continue to shape individuals’ lives (Anderson & Tracey, 2001).

2.1.1.5 Virtualization

Virtualization refers to the process of creating virtual or simulated versions of computer resources, such as servers, operating systems, storage devices, or networks. It provides a flexible and efficient approach to

maximizing the utilization of computing resources, enhancing scalability, and simplifying management and maintenance. Virtualization is the technological advancement that enables the concurrent operation of multiple instances, known as virtual machines, on a single machine, which is typically a physical server (Virtualization| Solutions, n.d.).

2.1.2 Cyber Threats

The severity and number of cyberattacks have risen, delivering a major problem for an enterprise that attempts to protect their networks and information from skilled attackers. These individuals, sovereign attackers to wealthy institutions, work together as members of an illegal business or represent an entire nation. Attackers use several kinds of tactics, methods, and procedures (TTPs) to harm infrastructure, damage services, execute financial fraud, reveal or exploit trademarks, and other confidential data. Considering the risks these threats create, enterprises have to exchange cyber threat intelligence and utilize it to enhance their safety measures (Johnson et al., 2016).

2.1.2.1 Malware

Opposing harmful programs is one of the primary cybersecurity issues of nowadays. "Malware samples" are typically precisely developed software applications that have been developed to remain unidentified when conducting extensive asset and architecture analysis. Commonly, infected devices link together through a telecommunication network to develop what is known as a "botnet," which is effortlessly and systematically controlled by cybercriminals for a range of malicious uses, including ransomware,

SPAM dissemination, DDoS harm, fraud, and confidential information theft (Kozik, 2018). According to Check Point Software Report of 2022, Education/Research, Government/Military, and Healthcare are the most attacked industries globally with 38% increased, compared to 2021. The top malware families reported by Check Point Software Report of April 2022 discovered that, with 6% of corporations affected globally, Emotet remains as the most prevalent threat. Formbook, with 3% of corporations affected, and AgentTesla, with 2% of corporations globally affected, are the next the majority common malwares.

2.1.2.2 Botnets

A bot (bad bot) is a minor program that executes any form of malicious behavior that, without the authorized consumer's awareness, could constantly harm the machine. A botnet is a collection of bots that are operated by a botmaster. A botnet comprises various devices with internet access that attackers may have purposely infected to transmit infection. Botnets have the ability to perform distributed denial of service (DDoS) assaults, transmit spam, acquire confidential user data, and execute widespread computing functions for malicious purposes. A kind of malicious operation that affects or shuts down a web page, a computing system, a system, or a network device through a collection of computer networks is called a botnet attack. The only goal of this attack is to cause disruption to typical corporate operations or damage the affected system's overall efficiency (Haq & Singh, 2018).

2.1.2.3 Denial of Service (DoS)

It is one of the most harmful categories of cyberattacks. This leads to a machine or disk capacity becoming overloaded by generating an enormous amount of traffic, making it impossible to respond to requests from system users who have been granted permission (Gupta, 2020).

It is a kind of attack that includes mailbomb, neptune, smurf, land, apache2, teardrop, bank, processtable, udpstorm, and pod (Khan et al., 2018).

2.1.2.4 Bruteforce

Attacks utilizing brute-force continue to be an established and ongoing threat (Alrowaily et al., 2019). It is an attack typically used to decode Data Encryption Standard (DES) codes, break passwords, and locate hidden web pages or information (IMPROVING the EFFICIENCY of BRUTE-FORCE ATTACK DETECTION USING DECISION TREES: AN ANALYSIS STUDY, 2023). The convenience and accuracy of brute-force attacks might render them especially harmful. By using specific devices or algorithms, hackers have the capacity to develop an enormous range of password configurations, which could bypass safety measures and possibly compromise computers. This emphasizes how important it is to establish reliable and effective techniques for recognizing and avoiding brute-force attacks (Alrowaily et al., 2019).

2.1.2.5 Infiltration

Adobe Acrobat/Reader is generally enhancing an unsafe piece of software as a threatening component that seeks to penetrate or harm the system's internal components (Alrowaily et al., 2019). Once an intruder has effectively broken into an infrastructure through surveillance and gained access to it, the transfer of privileges typically occurs after the attack. Subsequently, the hacker must access the attacked machine by using indirect motion to locate all of the necessary components and gadgets (Hagar & Gawali, 2022). In addition, hackers employ programs and penetration techniques to gain full unauthorized access to connected system data (Manimurugan et al., 2020).

2.1.3 Raspberry Pi

The Raspberry Pi Foundation's primary objective is to increase every individual's global utilization of electronics and multimedia. They accomplish this by providing people with powerful, reasonably priced machines that enable them to gain knowledge, address challenges, and have fun. In order to increase the utilization of machines and electronic manufacturing, the organization also runs awareness and learning initiatives. Individuals create free tools to help people learn how to use machines for creative projects and for processing, and they educate instructors so that they can help others gain these abilities as well (B. Nuttall, 2021). Raspberry Pi can connect with external devices and supports programming languages like Scratch and Python. It operates on low power, making it energy-efficient, and can be effortlessly configured to set up intrusion

detection systems for enhancing network security. This microprocessor is a controlled hardware like the motherboard of a computer, but it doesn't have built-in storage or peripherals. An SD card that has the software required for the Raspberry Pi computer to begin operating has to be placed into the correct socket in order to start it up. The Linux operating system works with Raspberry Pi machines, lowering storage needs and enabling a more flexible programming platform (Raspberry Pi Models and Features, n.d.).

Ample opportunities for coding and development are provided with Raspberry Pi, serving as an excellent tool for individuals who desire to create something but lack a starting point. By utilizing Raspberry Pi as a foundation, it can support a comprehensive range of resources required by anyone. The possibilities for the tools housed within the computer are virtually limitless. Monitoring security is one of the valuable applications of Raspberry Pi, as it has been a necessary component of security toolkits since its introduction in 2012. Practical uses of Raspberry Pi include constructing a security operations center (SOC) dashboard, filtering out malicious network traffic, setting up a personal VPN, and assembling a magic mirror (Rudder, 2020).

2.1.4 Datasets

2.1.4.1 CTU-13 Dataset

The CTU-13 dataset is a set of network traffic captures developed in 2011 by the Czech Technical University (CTU) in Prague. It contains thirteen different botnet sample captures, also referred to as scenarios. The dataset aims to produce a major capture of actual botnets traffic combined with normal and background

traffic. Specific malware was run on each scenario that used various protocols and performed different actions, shown in Figure 2.1 (García et al., 2014).

The CTU-13 is a distinguished dataset because each scenario was examined and labeled manually. NetFlow files were used to do the labeling process. The connection between the number of labels for each scenario's Background, Botnet, C&C Channels, and Normal shows in Figure 2.3 (García et al., 2014).

Researchers have been able to create and test innovative techniques in Anomaly detection, Machine learning based classification, feature selection, and ensemble methods because of the dataset's diverse attack scenarios, labeled data, and large-scale captures. Despite its drawbacks, the CTU-13 dataset continues to make a substantial contribution to the area of network security by influencing the creation of stronger and more reliable intrusion detection algorithms (García et al., 2014).

Table 2.1. Botnet scenario characteristics (García et al., 2014)

Id	IRC	SPAM	CF	PS	DDoS	FF	P2P	US	HTTP	Note
1	✓	✓	✓							
2	✓	✓	✓							
3	✓			✓				✓		
4	✓				✓			✓		UDP and ICMP DDoS.
5		✓		✓					✓	Scan web proxies.
6			✓							Proprietary C&C. RDP.
7								✓		Chinese hosts.
8				✓						Proprietary C&C. Net-BIOS, STUN.
9	✓	✓	✓	✓						
10	✓				✓			✓		UDP DDoS.
11	✓				✓			✓		ICMP DDoS.
12							✓			Synchronization.
13		✓	✓						✓	Captcha. Web mail.

Table 2.2. Amount of data on each botnet scenario (García et al., 2014)

Id	Duration(hrs)	# Packets	#NetFlows	Size	Bot	#Bots
1	6.15	71,971,482	2,824,637	52GB	Neris	1
2	4.21	71,851,300	1,808,123	60GB	Neris	1
3	66.85	167,730,395	4,710,639	121GB	Rbot	1
4	4.21	62,089,135	1,121,077	53GB	Rbot	1
5	11.63	4,481,167	129,833	37.6GB	Virut	1
6	2.18	38,764,357	558,920	30GB	Menti	1
7	0.38	7,467,139	114,078	5.8GB	Sogou	1
8	19.5	155,207,799	2,954,231	123GB	Murlo	1
9	5.18	115,415,321	2,753,885	94GB	Neris	10
10	4.75	90,389,782	1,309,792	73GB	Rbot	10
11	0.26	6,337,202	107,252	5.2GB	Rbot	3
12	1.21	13,212,268	325,472	8.3GB	NSIS.ay	3
13	16.36	50,888,256	1,925,150	34GB	Virut	1

Table 2.3. Distribution of labels in the NetFlows for each scenario in the dataset (García et al.,2014)

Scen.	Total Flows	Botnet Flows	Normal Flows	C&C Flows	Background Flows
1	2,824,636	39,933(1.41%)	30,387(1.07%)	1,026(0.03%)	2,753,290(97.47%)
2	1,808,122	18,839(1.04%)	9,120(0.5%)	2,102(0.11%)	1,778,061(98.33%)
3	4,710,638	26,759(0.56%)	116,887(2.48%)	63(0.001%)	4,566,929(96.94%)
4	1,121,076	1,719(0.15%)	25,268(2.25%)	49(0.004%)	1,094,040(97.58%)
5	129,832	695(0.53%)	4,679(3.6%)	206(1.15%)	124,252(95.7%)
6	558,919	4,431(0.79%)	7,494(1.34%)	199(0.03%)	546,795(97.83%)
7	114,077	37(0.03%)	1,677(1.47%)	26(0.02%)	112,337(98.47%)
8	2,954,230	5,052(0.17%)	72,822(2.46%)	1,074(2.4%)	2,875,282(97.32%)
9	2,753,884	179,880(6.5%)	43,340(1.57%)	5,099(0.18%)	2,525,565(91.7%)
10	1,309,791	106,315(8.11%)	15,847(1.2%)	37(0.002%)	1,187,592(90.67%)
11	107,251	8,161(7.6%)	2,718(2.53%)	3(0.002%)	96,369(89.85%)
12	325,471	2,143(0.65%)	7,628(2.34%)	25(0.007%)	315,675(96.99%)
13	1,925,149	38,791(2.01%)	31,939(1.65%)	1,202(0.06%)	1,853,217(96.26%)

2.1.4.2 CSE-CIC-IDS2018 Dataset

A program developed formed between the Canadian Institute for Cybersecurity (CIC) and the Communication Security Establishment (CSE) is the CSE-CIC-IDS2018.

This dataset was intended to examine, test, and analyze intrusion detection systems, namely network-based anomaly detectors. The CSE CICDS2018 intrusion dataset is based on actual network behavior and includes

a variety of intrusion states. Furthermore, the payloads for data packets are calculated across the entire network, spanning all traces. This dataset includes several intrusion profiles covering a broad range of networking protocols and topologies that are relevant to the security industry. There are now seven intrusion methods and two profiles in the IDS2018 public data collection. The raw data were regularly adjusted, and the data were collected in multiple states (IDS 2018 | Datasets | Research | Canadian Institute for Cybersecurity | University of New Brunswick, n.d.).

Brute-force DOS attacks, DDOS attacks, Brute-force SSH attacks, Infiltration, Heartbleed, Web attacks, and Botnet attacks are among the seven different types of attacks found in the CSE CICDS2018 (IDS 2018 | Datasets | Research | Canadian Institute for Cybersecurity | UNB, n.d.).

Table 2.4 List of conducted attacks and duration (IDS 2018 | Datasets | Research | Canadian Institute for Cybersecurity | UNB, n.d.)

Attack	Tools	Duration	Attacker	Victim
Bruteforce attack	FTP – Patator SSH – Patator	One day	Kali linux	Ubuntu 16.4 (Web Server)
DoS attack	Hulk, GoldenEye, Slowloris, Slowhttptest	One day	Kali linux	Ubuntu 16.4 (Apache)
DoS attack	Heartleech	One day	Kali linux	Ubuntu 12.04 (Open SSL)

Web attack	<ul style="list-style-type: none"> • Damn Vulnerable Web App (DVWA) • In-house selenium framework (XSS and Brute-force) 	Two days	Kali linux	Ubuntu 16.4 (Web Server)
Infiltration attack	<ul style="list-style-type: none"> • First level: Dropbox download in a windows machine • Second Level: Nmap and portscan 	Two days	Kali linux	Windows Vista and Macintosh
Botnet attack	<ul style="list-style-type: none"> • Ares (developed by Python): remote shell, file upload/download, capturing • screenshots and key logging 	One day	Kali linux	Windows Vista, 7, 8.1, 10 (32-bit) and 10 (64-bit)
DDoS+ PortScan	Low Orbit Ion Canon (LOIC) for UDP, TCP, or HTTP requests	Two days	Kali linux	Windows Vista, 7, 8.1, 10 (32-bit) and 10 (64-bit)

Table 2.5 Overview of the extracted features of the CSE-CIC IDS2018 dataset
 (IDS 2018 | Datasets | Research | Canadian Institute for Cybersecurity | UNB, n.d.)

Feature Name	Description
fl_dur	Flow duration
tot_fw_pk	Total packets in the forward direction
tot_bw_pk	Total packets in the backward direction
tot_l_fw_pkt	Total size of packet in forward direction

fw_pkt_l_max	Maximum size of packet in forward direction
fw_pkt_l_min	Minimum size of packet in forward direction
fw_pkt_l_avg	Average size of packet in forward direction
fw_pkt_l_std	Standard deviation size of packet in forward direction
Bw_pkt_l_max	Maximum size of packet in backward direction
Bw_pkt_l_min	Minimum size of packet in backward direction
Bw_pkt_l_avg	Mean size of packet in backward direction
Bw_pkt_l_std	Standard deviation size of packet in backward direction
fl_byt_s	Flow byte rate that is number of packets transferred per second
fl_pkt_s	Flow packets rate that is number of packets transferred per second
fl_iat_avg	Average time between two flows
fw_iat_tot	Total time between two packets sent in the forward direction
bw_iat_tot	Total time between two packets sent in the backward direction

The CIC-IDS-2017 and CSE-CIC-IDS-2018 datasets are covered in a review paper by Thakkar and Lohiya that summarizes the Data mining (DM) and Machine learning (ML) methods used in intrusion detection systems (IDS). These datasets are up to date and contain both the attributes of network attacks and new attack categories. The paper explores the latest progress in IDS datasets, emphasizing their usefulness for different research communities. It advocates for the adoption of these new IDS datasets as a foundation for creating improved ML and DM-based IDS solutions (Thakkar & Lohiya, 2020).

2.1.4.2.1 Limitations of Datasets

The network flow analysis generates data samples that are saved in files, which need a lot of work to process because each file contains many data instances (Thakkar & Lohiya, 2020).

Table 2.6 Comparison to previous version of CSE-CIC IDS2018 dataset

Dataset Name	CIC-IDS-2017	CSE-CIC-IDS-2018
Dataset Type	Multi-class	Multi-class
Year of formation	2017	2018
Duration of Capture	5 days	10 Days
Attack Infrastructure	4 PCs, 1 router, 1 switch	50 PCs
Victim Infrastructure	3 servers, 1 firewall, 2 switches, 10 PCs	420 PCs, 30 servers
Features	80	80
Number of Class	15	18

2.1.5 Machine Learning Algorithms

2.1.5.1 SVM

Support Vector Machine is a supervised machine learning method. SVM is employed to address classification and regression issues. It seeks to identify the optimum hyperplane in a feature space with high dimensions that bestows the greatest margin of separation between the data points of various classes (Cortes, C. et al., 1995). One application for SVM is used in Intrusion Detection Systems (IDS) to distinguish between legitimate and malicious network data. SVMs are capable of extracting patterns from network data to identify attacks, such as DoS (Denial-of-Service), DDoS (Distributed Denial-of-Service), and intrusion attempts, from legal network activity (Gharib, A. et al., 2015)

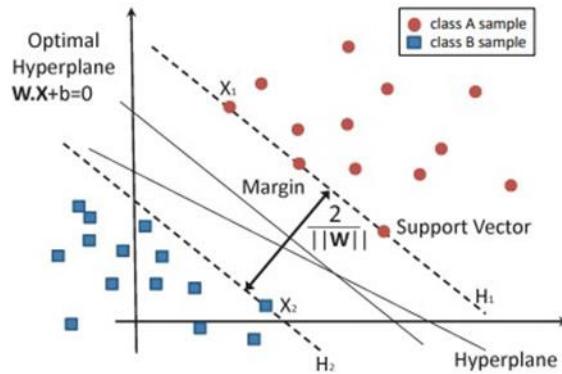


Figure 2.1 Classification of Data by Support Vector Machines (García, E. et al., 2016)

2.1.5.2 Decision Tree

A decision tree is a kind of tree that is utilized to categorize datasets based on the values of their characteristics. A node in a decision tree displays a feature along with any relevant edges. Every edge links a node to a leaf or to another node. A leaf that is explained by a decision result defines the type of input data (Meng, 2011).

In a decision tree, each internal (non-leaf) node selects a test for a given characteristic; each branch reveals the test's outcome; and each exterior (leaf) node displays a class prediction. The method selects the most basic feature at each node to divide data into distinct classes. A dataset with pre-classified data is used to build the decision tree. They employ a top-down methodology in which the branch is followed the root (Kumari & Mehta, 2020).

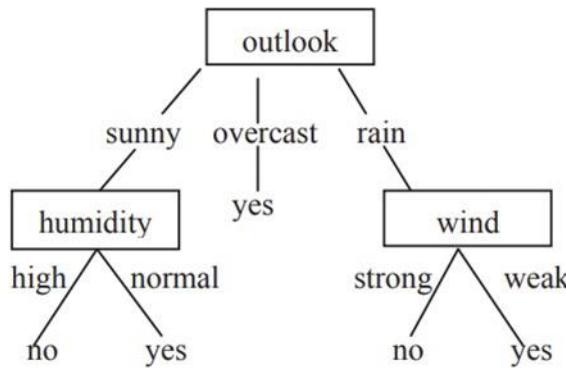


Figure 2.2. Decision Tree (Cortes & Vapnik, 1995)

2.1.5.3 Naive Bayes

The "Bayes Theorem" is the foundation of the Naive Bayes approach, a supervised learning approach that operates under the erroneous assumption that every feature is independent of every other feature (Zwane et al., 2019). In a more formal context, let's consider the task of classifying a vector $X = x_1, \dots, x_n$ into m classes, C_1, \dots, C_m . The initial step involves calculating the probabilities for each possible class given X . This calculation enables us to assign X the label of the class with the highest probability. The Bayes Theorem is used in the calculating process to determine the probability:

$$P(C_i|X) = \frac{P(X|C_i)P(C_i)}{P(X)}$$

$P(C_i)$ is the prior probability of being an element of class i . Normalizing constant $P(X)$ is used, and the conditional probability of observing the input vector X , given the information that the class is C_i , is represented as $P(X|C_i)$. After that, the final prediction model is defined as follows:

$$C(X) = \operatorname{argmax}_{i \in \text{classes}(t)} \frac{P(X|Ci)P(Ci)}{P(X)}$$

Where C(X) represents the prediction that is returned for the input X.

With training data, the classifier determines the likelihood of each attribute A_i based on the class label C. Using the specific values of A₁, ..., A_n, the probability of the class C is calculated using the Bayes rule to classify fresh cases. The final classification is then expected to be the class with the highest resultant probability.

2.1.5.4 XG Boost

Performance and speed were the main goals in the development of XG Boost, which employs gradient boosted decision trees. It talks about a technique called machine boosting, or applying boosting to machines, which was developed by Tianqi Chen and is still used by a lot of developers. The Distributed Machine Learning Community (DMLC) is the source of this technology. Xtreme Gradient Boosting, or XGBoost for short, aids in optimizing memory and hardware use for tree boosting algorithms. It offers the benefits of process improvement, model refinement, and computing environment applications. The three primary gradient boosting techniques that XGBoost supports are Gradient Boosting, Regularized Boosting, and Stochastic Boosting (Dhaliwal et al., 2018).

2.1.5.5 Ensemble Learning

Ensemble learning is a machine learning approach that creates a more robust and reliable prediction model by combining several discrete models, often referred to as "base models" or "weak learners." The idea behind ensemble learning is that by merging the predictions of multiple models, a model can outperform a single model.

Homogeneous and heterogeneous ensembles are the two basic types of ensembles learning techniques (Polikar, R., 2006).

1. Homogeneous Ensembles have identical base models but were trained using various subsets of the training data or using various hyperparameters. As illustrations of homogenous ensembles, consider bagging and random forest.
2. Heterogeneous Ensembles' basis types might be various algorithms or architectural designs. Each model may have distinct advantages and disadvantages, but by merging them, the ensemble can gain from their varied viewpoints. A few instances of heterogeneous ensembles include boosting and stacking.

Several machines learning tasks, including classification, regression, and Anomaly detection, among others, have effectively used ensemble learning. It has been demonstrated to enhance generalization, lessen overfitting, and handle noisy or imperfect data more skillfully.

2.1.6 Web Application

A web application is a software program that operates over the Internet or an intranet, accessible through a web browser. It is designed to provide interactive functionality and services to users, utilizing web-based programming languages like HTML, JavaScript, Java, or others (Yik Ern, 2019). A web application's fundamental structure comprises several key components: web browsers, a network, and a web server (Conallen, 1999). Users can access web applications through a web browser, which acts as a client, rendering the user interface and executing the underlying code.

Web applications offer advantages such as cross-platform compatibility, easy deployment and updates, and centralized data storage, making them versatile solutions for various tasks and industries.

2.1.6.1 GUI

The introduction of Graphical User Interface (GUI) has significantly enhanced the user-friendliness of PCs, making them more accessible and intuitive to operate. “GUI is a means of enabling user interaction with electronic devices such as computers or hand-held devices” (Closa et al., 2010). GUI is a program interface that leverages the graphical capabilities of a computer to enhance the usability of software applications. By utilizing graphics, GUIs provide users with a comprehensive and intuitive method of interacting with the software, offering a wide range of possibilities for user engagement (Bastanford & Tabibi, 2016).

2.1.7 Intrusion Detection System

In the past few decades, the potential damage caused by internet threats has increased significantly. This has led to a greater need for systems that can defend against these threats and protect users' data. Intrusion Detection Systems (IDSs) are one such system that can help to reduce the severity of attacks (Guo et al., 2016).

An intrusion is an attempt to access a networking or computer resource without authorization. Confidentiality, availability, or integrity of the resource can be damaged by intrusions. In essence, intrusion detection systems generate warnings by spotting threats, attacks, and other malicious activity. IDSs are only capable in detecting and monitoring and cannot resolve network attacks which makes it different to the concept of Intrusion prevention systems (IPSs). IPSs can identify malicious attacks and respond to threats and intrusions found across the network (Ashoor and Gore, 2011).

There are a lot of types of IDS today, which are also characterized on different bases. There are differences in the advantages and disadvantages of each approach. In addition, the general process model of IDS can be described for all approaches. Three basic functional components can be used to characterize many IDSs (Scarfone and Mell, 2007).

The first one is Information sources. Information sources are different sources where event information is gathered and examined to see if there has been an intrusion. Although these sources might come from different system levels, network, host, and application monitoring are the most often used ones (Scarfone and Mell, 2007).

The analysis is the second component. As a component of the intrusion detection system, analysis groups and reflects events acquired from information sources, identifying when they indicate the presence of intrusions or their impending arrival. The two most utilized analytical techniques are anomaly and misuse detection (Scarfone and Mell, 2007).

The response component comes last. It consists of the actions that the system needs to take when it detects an intrusion. Usually, these can be separated into two groups: active measures and passive measures. While passive measures include informing humans of IDS findings so they can take appropriate action, active measures involve some automated system involvement (Scarfone and Mell, 2007).

2.1.7.1 IDS based on Detection

There are 2 kinds of intrusion detection systems: Anomaly-based and Signature-based. (Pietro et al., 2008).

The SD makes use of methods for matching patterns. It looks for matches between the examined data and a database of identified attack signatures. When the match is discovered, an alarm will ring (Pietro et al., 2008).

Misuse Detection can assist the security manager in setting priorities for remedial actions by quickly and accurately determining whether a particular attack tool or technique is being used, as well as by effectively detecting attacks without generating numerous false alarms. Because it can only identify assaults that it is aware of—it cannot recognize versions of well-known attacks—it needs to be updated on a regular basis with the signatures of new threats (Scarfone & Mell, 2007).

On the other hand, an anomaly-based detection (AD) exists. Anomaly-based detection looks for unusual or anomalous behavior on a host or network. They operate under the premise that assaults may be distinguished from "normal" legal acts and can thus be recognized by systems designed to do so. Anomaly detector profiles show normal host, user, or network connection activity. The profiles are constructed using previous data that has been collected over the course of ongoing operations. The detectors will then collect event data and use various metrics to find deviations from the average activity that is captured (Scarfone & Mell, 2007).

2.1.7.2 IDS based on Application

IDSs can also be categorized according on the locations in which they are installed. Host-based IDS (HIDS), Network-based IDS (NIDS), Wireless-based IDS (WIDS), Network Behavior Analysis (NBA), and Mixed IDS (MIDS) are the five categories into which they belong (Liao et al., 2016).

The HIDS monitors and analyzes the activities of a single host's internal computer system or system level (Othman et al., 2018). This means that host-based intrusion detection systems (IDSs) can accurately and reliably track down the exact users and processes that are a part of an operating system attack. Moreover, host-based intrusion detection systems (IDSs) have the advantage over network-based IDSs in that they are able to access and track system processes and data files that are frequently the target of attacks, enabling them to "see" the outcomes of an attempted intrusion (Scarfone and Mell, 2007).

The majority of commercial intrusion detection systems operate via networks. By monitoring and analyzing network traffic, these IDSs can identify threats. One network-based intrusion detection system (IDS) can defend several hosts linked to a network segment by monitoring network traffic and listening on a network segment or switch (Scarfone and Mell, 2007).

In order to identify any attacks, WIDS tracks and examines wireless traffic. Wireless traffic includes Ad hoc networks, wireless sensor networks, and wireless mesh networks. It is not possible to fully use IDSs designed for wired networks due to the various characteristics of wireless networks, including their existence in an open environment and the limitations placed on sensor, battery life, and memory computing capability (Mohammed et al., 2018).

A technique called Network Behavior Analysis (NBA) passively monitors incoming and outgoing network traffic for a predefined period of time, creating a baseline for typical traffic flow. Future behavior is compared to this benchmark to identify all typical actions inside a network. Every new or unexpected movement needs to be recognized as an intrusion or a threat. The NBA-based IDS is incredibly successful (Kakuru, 2011).

The last category is MIDS. To take advantage of the advantages of IDS, MIDS consists of two types or more and can provide a precise detection. However, it takes a long time for MIDS to analyze the data (Othman et al., 2018).

2.2 Related Studies

2.2.1. Internetwork Systems

2.2.1.1. A low-cost embedded IDS to monitor and prevent Man-in-the-Middle attacks on wired LAN environments

The researchers in this study highlight the deficiencies of current Intrusion Detection Systems (IDSs) in identifying ARP-based Man-in-the-Middle (MitM) attacks in switched LAN environments. They provide evidence of the substantial security risks that arise when no preventive measures are taken. In order to address this problem, the researchers present an embedded intrusion detection system (IDS) that is both affordable and successful in identifying MitM attacks and fixing compromised ARP caches on hosts. The researchers created two different prototype variations: proactive and reactive. These variations have varied specifications and performance levels in addition to offering unique capabilities. The usefulness and limitations of the suggested prototype were illustrated using an experimental testbed. It was found that these restrictions were directly related to the hardware assets that were available. As to the researchers, a regular use and usage of cost-effective devices, like the one recommended in this paper, in switched LANs will aid in enhancing the privacy of companies and organizations with limited resources.

In this study, the researchers also examine the specific LAN environment and the utilization of cost-effective IDS solutions. By considering the LAN context, they aim to provide insights into how the proposed IDS can effectively operate within this setting. Additionally, the emphasis on cost-effectiveness

highlights the researchers' efforts to make security solutions more accessible to organizations with limited budgets. By addressing these aspects, the study aims to offer practical and applicable solutions to mitigate the security risks of ARP-based MitM attacks in switched LANs.

2.2.2 Cyber Threats

2.2.2.1 Botnet Attack Detection using Machine Learning

The Decision tree, Naïve Bayes, K-Nearest Neighbor, and Support Vector Machines were the four machine learning models created utilizing the Bot-IoT and UNSW datasets. Each model is based on a different classifier. This study aims to mitigate the increasing security threats posed by botnets through the application of machine learning techniques. The Decision Trees model, which was trained using the UNSW-NB15 dataset, 82,000 records, displays the most appealing results. It detects botnet attacks with ideal precision, recall, and an F-score of 100% and reaches a testing accuracy of 99.89%. These results demonstrate the potential of machine learning for botnet detection and offer insightful information for further study in this field. (Information Technology Innovations Conference (IIT'20), n.d.).

2.2.3 Raspberry Pi

2.2.3.1 Snort IDPS using Raspberry Pi 4

Based on the research, an intrusion detection system's strength depends on how appropriate it is to the network it is intended to protect. Researchers have developed and implemented a global system for detecting and preventing

intrusions or IDPS with the Snort engine and an inexpensive Raspberry Pi 4. Utilizing TALOS/VRT rules, the system is portable and can identify known network intrusions. To evaluate the system's security, the researchers staged a few attacks. Varma et al. (n.d.) stated that model B of Raspberry Pi is a feasible choice for an affordable IDPS.

2.2.3.2 Raspberry Pi as an Intrusion Detection System, a Honeypot and a Packet Analyzer

The Raspberry Pi Foundation is responsible for developing the mini single-board computers in the Raspberry Pi series. It is a cheap computer with a sizeable credit card with many uses. These boards have all the essential parts of a computer, such as memory, an input/output interface, a processor, and several connectivity choices. The primary objective of its creation was to provide a good deal tool that could improve knowledge of hardware and programming, especially among young individuals. Although the processing on a Raspberry Pi capability is significantly lower than modern computers, it still serves as a portable and affordable Linux-based computer. It can run various programs while consuming minimal power (Tripathi & Kumar, 2018).

2.2.3.3 RpiDS: Raspberry Pi IDS A Fruitful Intrusion Detection System for IoT

In the context of RpiDs, extensive tests have demonstrated that Raspberry Pi can be operated as a tracking node for examination different network traffic. The Raspberry Pi has the capability to function as a system for detecting or IDS

within a dispersed network such as the Internet of Things (IoT) (Sforzin et al., 2016).

2.2.3.4 IDS on Raspberry Pi: A Performance Evaluation

The purpose of this study is to assess the effectiveness of two unique Raspberry Pi models as an intrusion detection system (IDS) and how well they handled the network traffic with particular focus. Additionally, it looked into the effects of using a Raspberry Pi as an IDS on network performance. Testing the network performance and tracking each Raspberry Pi device's CPU and memory utilization were both part of the investigation. Model B Raspberry Pi 2 and Model B+ Raspberry Pi, both running the Arch Linux ARM operating system, were the devices used in the study (Aspernäs & Simonsson, 2015).

2.2.3.5 Pi-IDS: Evaluation of Open-source intrusion detection systems on Raspberry Pi 2

The Raspberry Pi is a small, multifunctional, inexpensive device with an ARM CPU that can be utilized in computer networks for intrusion detection. This study contrasts Snort IDS and Bro IDS, two open-source intrusion detection systems (IDS), and the model used to assess the level of performance of two IDS is Raspberry Pi. The aim of this study is to review the performance and efficacy of utilizing Raspberry Pi devices in settings involving computer networks, with cost being a crucial factor in the evaluation process. Based on the result, Snort IDS performed superior to Bro IDS on a Raspberry Pi 2 (Ar Kar Kyaw et al., 2015).

2.2.4 Dataset

2.2.4.1 Deep learning-based botnet detection using the CTU-13 dataset

A study by Chen et al. (2019) developed a new method for detecting botnets. The study used deep learning models and found that the accuracy of detecting botnet traffic using the new botnet detection method gave promising results. Even though there is noise, the study achieves high accuracy. Moreover, the study used the CTU-13 dataset and found that it was an excellent dataset to train the deep learning models because of its large and diverse data. With the CTU-13 dataset, the trained deep-learning models could generalize well to new botnet traffic. It shows that the CTU-13 dataset can be valuable for developing detection methods like an Intrusion Detection system.

2.2.4.2 HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System

In a study by Khan in 2021, created the hybrid identification framework, which can identify and categorize network cyberattacks, DL convolutional recurrent neural networks based on CNRN are used. Convolutional neural networks (CNN) use convolution in the HCRNNIDS to gather regional data. In contrast, recurrent neural networks (RNNs) in the system obtain temporal characteristics to enhance the ID system's functionality and accuracy. Experiments were conducted using publicly accessible ID features, especially the realistic and recent CSE-CIC-IDS2018 data, in order to evaluate the effectiveness within the system of hybrid convolutional recurrent neural networks for monitoring intrusions (HCRNNIDS) (Muhammad Ashfaq Khan, 2021).

Khan also compared CSE-CIC-IDS2018 and CICIDS2017 Table 2.8. displays the outcomes. Compared to the CICIDS 2017 ID dataset, the CSE-CIC-IDS2018 sample size was much larger, especially in the areas of attacks using botnets and infiltration, which rose by 4497 and 143, in that order. Nevertheless, very few web attacks are available in CSE-CICIDS2018 (Muhammad Ashfaq Khan, 2021).

Table 2.7 Comparison of the CSE-CIC 2018 ID dataset with CICIDS-2017
(Muhammad Ashfaq Khan, 2021)

Dataset	Normal	DDoS	Dos	Botnet	Brute Force	Infiltration	Web Attacks	Port Scan
CICIDS-2017	1,743,179	128,027	252,661	1966	13,835	36	2180	158,930
CSE-CICIDS2018	6,112,151	687,742	654,301	286,191	380,949	161,934	928	-

Results of the simulation show that the HCRNNIDS that is being suggested greatly exceeds existing ID techniques, with a high accuracy of up to 97.75% in the detection of malicious attacks using CSE-CIC-IDS2018 data and 10-fold cross-validation (Muhammad Ashfaq Khan, 2021).

2.2.4.3 FastTrafficAnalyzer: An Efficient Method for Intrusion Detection Systems to Analyze Network Traffic

According to Arslan (2021), the CSE-CIC-IDS2018 dataset is tested. The algorithm ExtraTree demonstrated a 99.00% binary classification probability of detection and an 82.96% decrease in time spent processing for each sample shown in the experimental findings. From the case of multiclass detection (15 classes), the Random Forest algorithm achieved a detection rate of 98.5%, accompanied by a reduction of 64.43% in the processing duration per sample.

Tests using the suggested model showed classification rates that were equivalent to those of previous studies while requiring a significant reduction in processing time. This implies that classification might be completed efficiently.

2.2.5 Machine Learning Algorithms

2.2.5.1 Intrusion detection system using XGBoost algorithm on CICIDS 2017 dataset

In the study from Bansal and Kaur (2020), an intrusion detection system was trained using the XGBoost algorithm and the purpose of the IDS is to assess the network behaviour. The normal and attack traffic is included in the dataset they used, CICIDS 2017. Testing proved that the XGBoost algorithm had a successful accuracy rate of 99.3% in identifying attack traffic. The created intrusion detection system detected different kinds of attacks, namely, DosS, DDoS, and malware. In training network behaviour analysis intrusion detection systems, the XGBoost algorithm produces positive results. However, in this paper only the CICIDS dataset is used and not the other datasets. Despite this, the results showed that XGBoost could potentially be used efficiently for intrusion detection systems.

2.2.6 Web Application

2.2.6.1 Web application testing: A systematic literature review

The Internet has a significant influence on every facet of the community. Given the increasing reliance of society on the internet, the reliability of web applications has become progressively crucial. In this research, the proponents suggested a number of methods for testing web-based software to enhance the

reliability of these applications. The researchers yielded a total of 193 articles focusing on web application testing that were published from 2000 to 2013. Furthermore, the researchers thoroughly examined the existing knowledge on testing web applications' functionality by conducting a systematic literature review or SLR study. This study discussed the new developments in testing of new developments when testing web applications and explored the consequences for practitioners and researchers in this field. The structured literature review (SLR) findings offer insightful information to academics, offering a summary of current methodologies, tools, measurements, fault models, and empirical data related to web application testing. (Serdar Doğan et al., 2014).

2.2.6.2 A Graphical User Interface Framework for detecting Intrusions using Bro IDS

The internet has changed business operations for the better, but it has also brought about new threats that corporations need to protect against. To secure their networks, corporations require network security, which involves implementing an Intrusion Detection System. In this research, the proponents discussed that numerous open-source programs are available for spotting network breaches., namely Snort and Bro. The research is mainly emphasized and explored in Bro. They also discussed Bro's largest deficit, which Is that the only reports lack a Graphical User Interface (GUI) and use information to log files. Until now, users have had to manually capture traffic by typing commands, which can be burdensome. Therefore, there is a need for a GUI structure that can get traffic in a more efficient and user-friendly manner. Additionally, a

framework is required to automate the creation of policy scripts and execute them for capturing and filtering network traffic. The researchers designed a Bro GUI Framework, a graphical user interface that automates the construction and running of scripts for policies. (Gupta & Goel, 2012)

2.2.7 Intrusion Detection System

2.2.7.1 Efficient detection of botnet traffic by features selection and decision trees

In the study of Velasco-Mata et al., 2021, the proponents have been focusing on enhancing botnet traffic classification by using more powerful features to detect them. They selected the most relevant attributes by applying the Gini importance criterion and information acquisition standards. They suggested three subsets utilizing the chosen features, assessing each one's usefulness for botnet identification employing Decision trees (DT), Random Forests (RF), and K-Nearest Neighbors (k-NN). The proponents produced the QB-CTU13 and EQB-CTU13 datasets. to be used for the experiments. This was founded on the database CTU 13, which had been developed to get around its disadvantages regarding class differences. In addition, three additional classes of botnets have been added to EQB-CTU13, which are Bunitu, Miuref and NotPetya, for comparing their ideal model to other models. Considering the outcomes of the tests, the researchers have determined that the best option for a multiple-class botnet analyzer that prioritizes performance is to employ D with the five features they have chosen (Velasco-Mata et al., 2021).

2.2.7.2 An Ensemble Approach for Intrusion Detection system using Machine Learning Algorithms

Gautam and Doegar, in 2018, used high-quality KDD Cup 99 data to conduct thorough examinations of anomalies in the network. In this research. Three trial configurations are used in this study. Frameworks based on all forty features are developed in the primary analysis. Feature selection is carried out based on Information Gain's application to select the most appropriate components instead of using all 41 included items and playing this study with Naïve Bayes, PART (Partial Decision Tree) or Adaptive Boost in order to analyze results. In the third analysis, an Ensemble Method used the Bagging approach because it reduces feature variance and imbalance by representing the distribution based on feature similarity in the form of distribution. The ensemble model was then evaluated using the accuracy, precision, and recall metrics (Ravindra et al., 2018).

Table 2.8 Efficiency Analysis with Making use of Ensemble Approach using Bagging for KDDcup99 Data Set (Ravindra Kumar Gautam & Amit Doegar, 2018)

Classifier	Accuracy	Precision	Recall
<i>Naïve Bayes</i>	91.9818	98.90	92.00
<i>PART</i>	99.9589	99.90	99.60
<i>Adaptive Boost</i>	97.8597	96.20	97.90
<i>Ensemble Approach</i>	99.9732	99.99	99.98

2.2.7.3 An efficient XGBoost–DNN-based classification model for network intrusion detection system

A successful classification structure for XGBoost-DNN-based intrusion detection systems in networks was proposed by Devan and Khare (2020). Normalization, feature selection, and classification are the three stages that make up the model. Network intrusions are classified using softmax classifiers and learning rate optimization is performed with the Adam optimizer during DNN training. The experiments have been properly performed on a reference NSL-KDD dataset. Using cross-validation against current basic methods for machine learning, including SVM and logistic regression and uncomprehending Bayes, the proposal model has been validated. In comparison with the existing shallow methods, the assessment metrics for classification are calculated, including F1 score, recall, accuracy, and precision. Compared with the current flimsy techniques applied to the data, the suggested model has performed better (Devan & Khare, 2020).

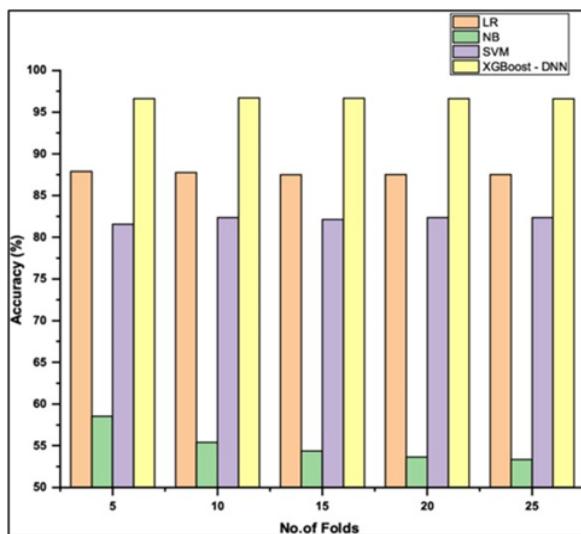


Figure 2.3 Comparative analysis of the proposed model and the existing models with different K-folds (Devan & Khare, 2020)

Table 2.9 Comparative analysis of the proposed model and the existing models based on accuracy (Devan & Khare, 2020)

Population size	Accuracy			
	XGBoost-DNN	LR	NB	SVM
1000	0.953	0.91	0.85	0.73
2000	0.963	0.88	0.83	0.78
3000	0.967	0.88	0.55	0.82
4000	0.969	0.87	0.53	0.88
5000	0.971	0.86	0.52	0.89
6000	0.974	0.87	0.52	0.89
7000	0.976	0.87	0.52	0.90

CHAPTER 3

METHODOLOGY

3.1 Theoretical Framework

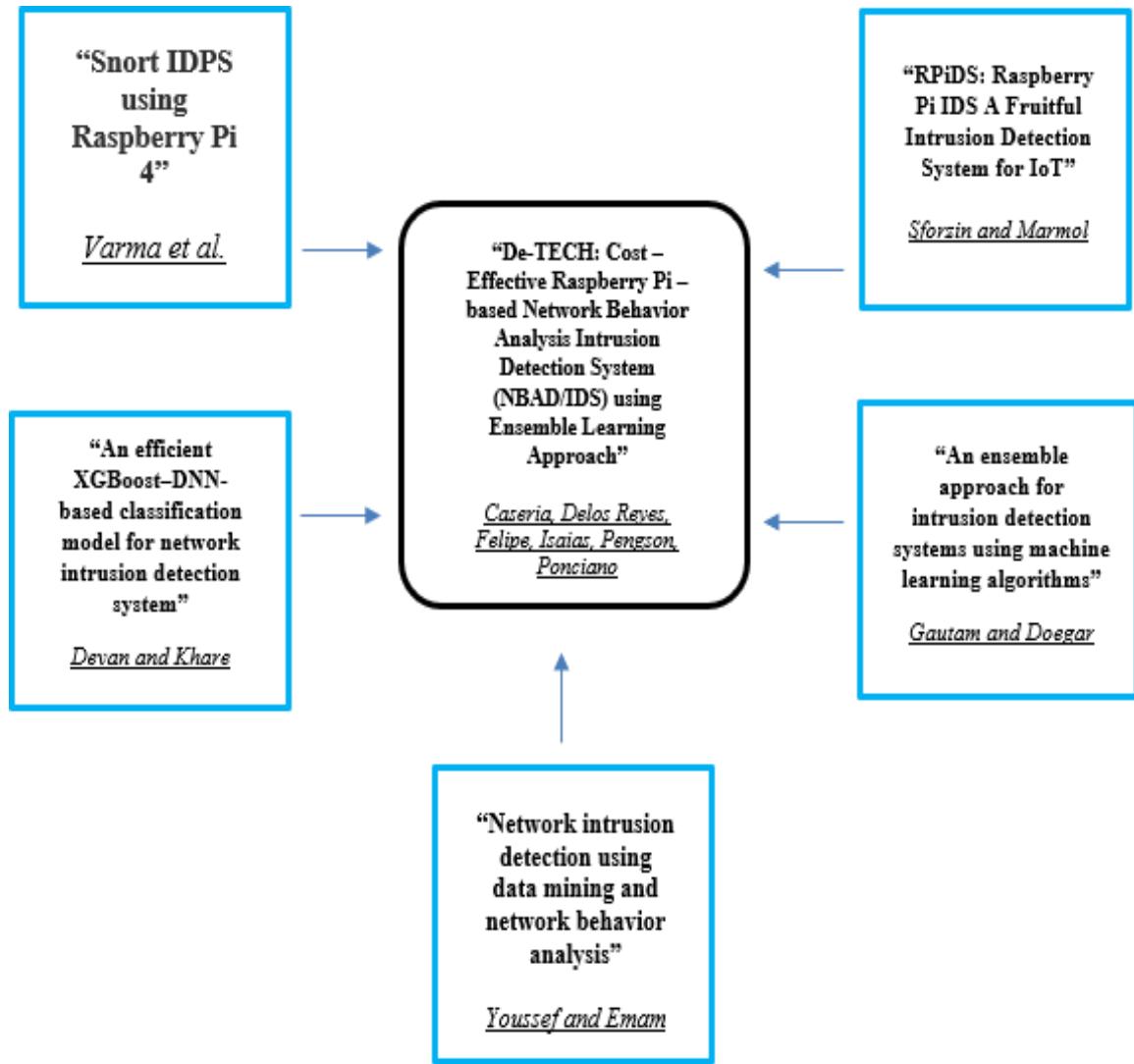


Figure 3.1 Theoretical Framework

The figure above shows the relevant studies that supported this research study. It highlighted the utilization of Raspberry Pi 4 as a cost-effective IDPS and the open-source IDS, Snort. The Raspberry Pi 4 model B could be an option for an economical IDPS. The study by Sforzin and Marmol (2016) designed a portable device pre-packaged with an IDS consisting of Raspberry Pi equipped with Snort. They tested their model with smart home

applications in mind and concluded that the Raspberry Pi could host Snort, making it a feasible solution for RPiDS.

A study by Gautam and Doegar (2018) designed an ensemble model using Naive Bayes, Adaptive Boost, and Partial Decision Tree (PART) for the ensemble approach. The ensemble model was evaluated using accuracy, precision, and recall metrics. About the ensemble approach, Devan and Khare compared the XG-Boost-DNN-based classification model to existing shallow methods and found that the suggested model performed better. In the study by Youssef and Emam (2011), they proposed a model that used data mining (DM) and network behavior analysis (NBA). The researchers discussed how the combination of DM and NBA could overcome limitations in current IDS.

3.2 Conceptual Framework

3.2.1 IPO Diagram

An input-process-output, or IPO, diagram is a graphic representation of the information flow inside a system or process. The project involved the development of a Raspberry Pi-based Intrusion Detection System (IDS) utilizing an Ensemble Learning approach and featuring a Graphical User Interface (GUI). In the input stage, the project required proficiency in Python programming, Packet and NetFlow analysis expertise, and familiarity with two malware databases: CTU-13 and CSE-CIC-IDS2018. Hardware requirements encompassed various laptop/PC configurations. They emphasized the pivotal role of a Raspberry Pi 4 Model B. Software requirements included Python 3, a Python IDE, and the PythonAnywhere web hosting platform. The process stage involved software development through Python programming, flowcharting, and web application development.

Table 3.1. Input-Process-Output Diagram

INPUT	PROCESS	OUTPUT
<p>Knowledge Requirements:</p> <ul style="list-style-type: none"> • Python Programming • Packet and NetFlow Analysis • Malware Database (CTU-13 and CSE-CIC-IDS2018) <p>Hardware Requirements:</p> <ul style="list-style-type: none"> • Laptop/PC <ol style="list-style-type: none"> 1. (12th Gen Intel® Core™ i5-12500H 3.10GHz, 8GB RAM, NVIDIA GeForce RTX 3050 Laptop GPU) 2. AMD Ryzen 5 3550H with Radeon Vega Mobile Gfx 2.10 GH1z 6.0 GB RAM 3. Intel® Core™ i5-6200U CPU @ 2.30GHz 2.40 GHz 4.00 GB RAM • Raspberry Pi 4 <p>Software Requirements:</p> <ul style="list-style-type: none"> • Python 3 • Python IDE • PythonAnywhere Web Hosting Platform 	<p>Software Development</p> <ul style="list-style-type: none"> • Flowcharting • Python Programming • Web App Programming <p>Simulation:</p> <ul style="list-style-type: none"> • Datasets partition (Training and Testing Datasets) • Feature Extraction and Data • Creation of binary Decision Tree • SVM modelling • Naïve Bayes Algorithm • Boosting • Ensemble Modelling and Training • Testing • Cross Validation 	Raspberry Pi-based Intrusion Detection System using Ensemble Learning approach with GUI

The simulation encompassed tasks related to datasets, feature extraction, and implementing various machine learning algorithms such as binary decision trees, SVM modeling, Naïve Bayes, boosting, ensemble modeling, and training, followed by testing

and cross-validation. The project's main output was a Raspberry Pi-based IDS using an Ensemble Learning Approach, determined by a GUI for enhanced user interaction and usability.

3.2.2 Block Diagram

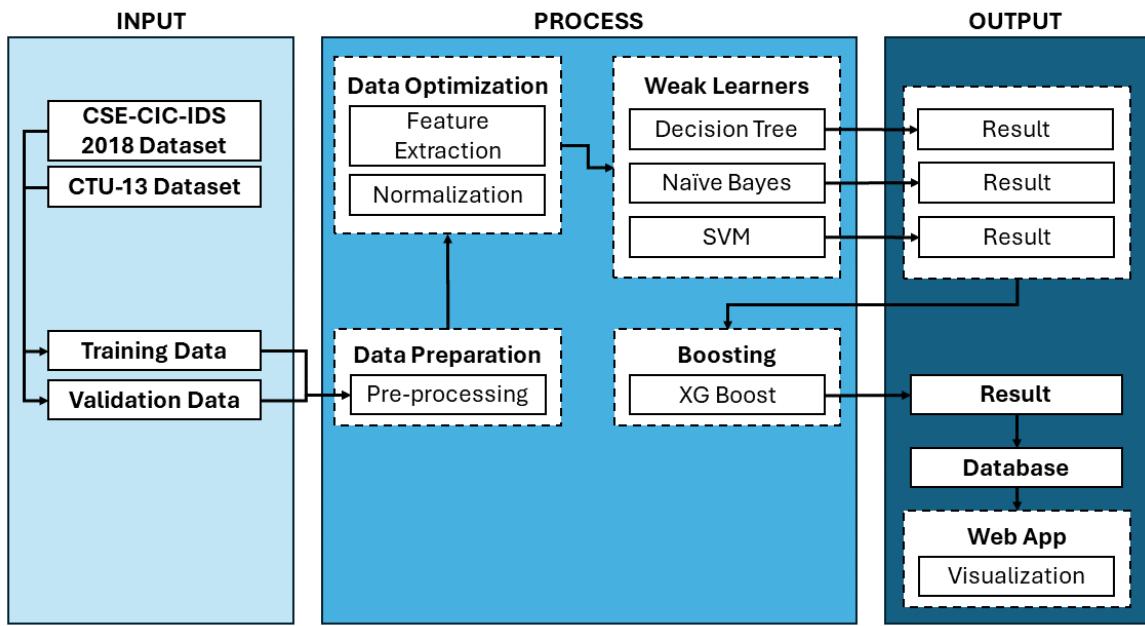


Figure 3.2 Block Diagram of Intrusion Detection System using Ensemble Learning Approach

The Block Diagram of the Intrusion Detection System (IDS) System using the Ensemble Learning Approach follows a clear Input-Process-Output (IPO) structure. Input utilizes two malware databases, CTU-13 and CSE-CIC-IDS2018, as training and testing data. In the process stage, the data undergoes Pre-Processing, followed by Feature Extraction and Normalization in Data Optimization. The subsequent step involves training the data using three weak learners – SVM, Decision Tree, and Naïve Bayes. The Output phase integrates the results through XG Boosting and stores them in a database. Finally, these results are visualized in a web application, ensuring a comprehensive and user-friendly presentation of the IDS's analysis.

3.2.3 Network Diagram

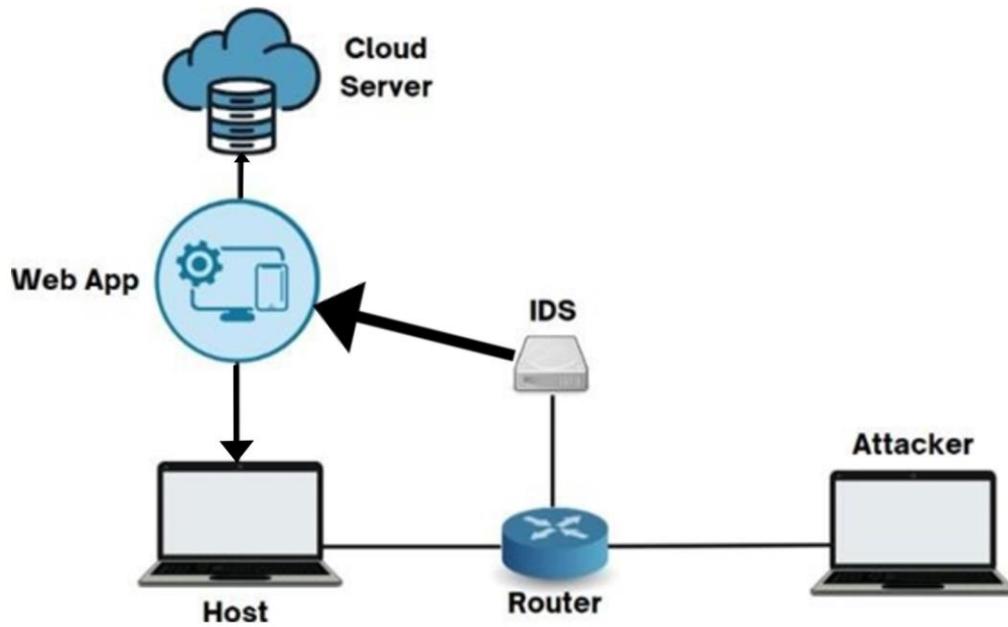


Figure 3.3. Network Diagram

The network diagram presents an architecture with a host and attacker connected to a central router, which, in turn, is connected to a Raspberry Pi-based Intrusion Detection System (IDS). The intended inclusion of an attacker system indicates a focus on security testing. The host's connection to a web application is a visualization tool for displaying results, specifically detected malicious and network attacks by the IDS. At the same time, the web application connects to a cloud server, indicating a decentralized approach for efficient data storage and analysis. This setup qualifies for thorough security testing, user-friendly visualization of results, and comprehensive analysis of intrusion data in a cloud environment, reflecting a thoughtful and adaptable network configuration.

3.2.4 One-Line Diagram

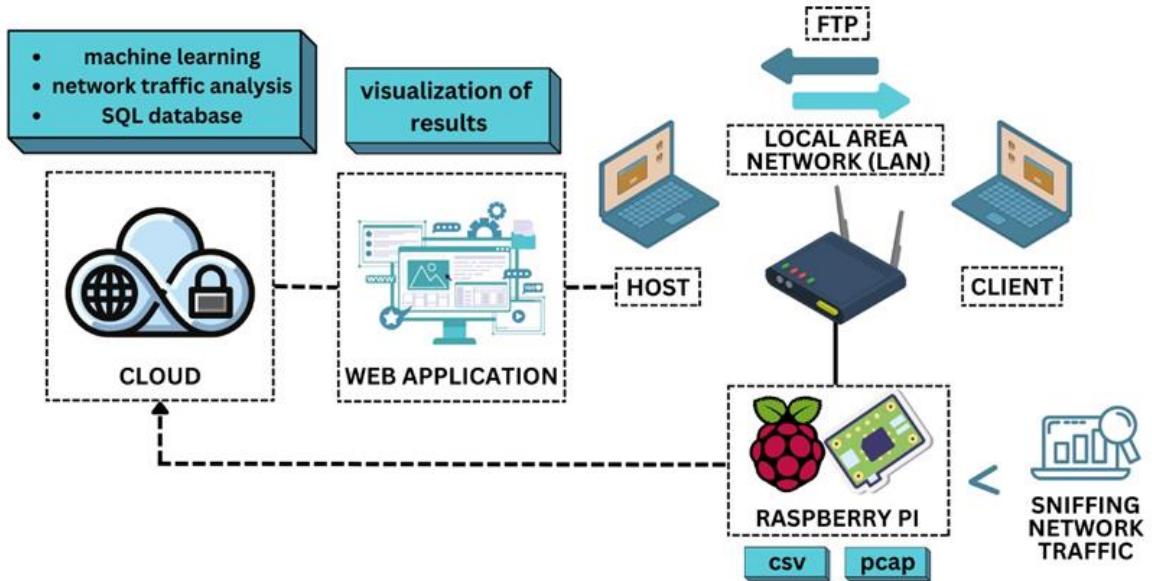


Figure 3.4 One-Line Diagram

The one-line diagram illustrates a Raspberry Pi integrated into a Local Area Network (LAN), functioning as a network sniffer. Within this LAN, two machines, a host and a client, are involved in File Transfer Protocol (FTP) communication. The Raspberry Pi actively captures and records the network traffic, storing the data in CSV or PCAP files. Subsequently, these files are transmitted to a cloud infrastructure equipped with machine learning-trained models, a database, and network traffic analysis tools. The cloud processes the data, applies analytical models, and conducts traffic analysis. Finally, the cloud sends the processed data to a web application connected to the host. This web application provides a user-friendly interface for visualizing results, offering insights into the analyzed network traffic data.

3.2.5 System Architecture

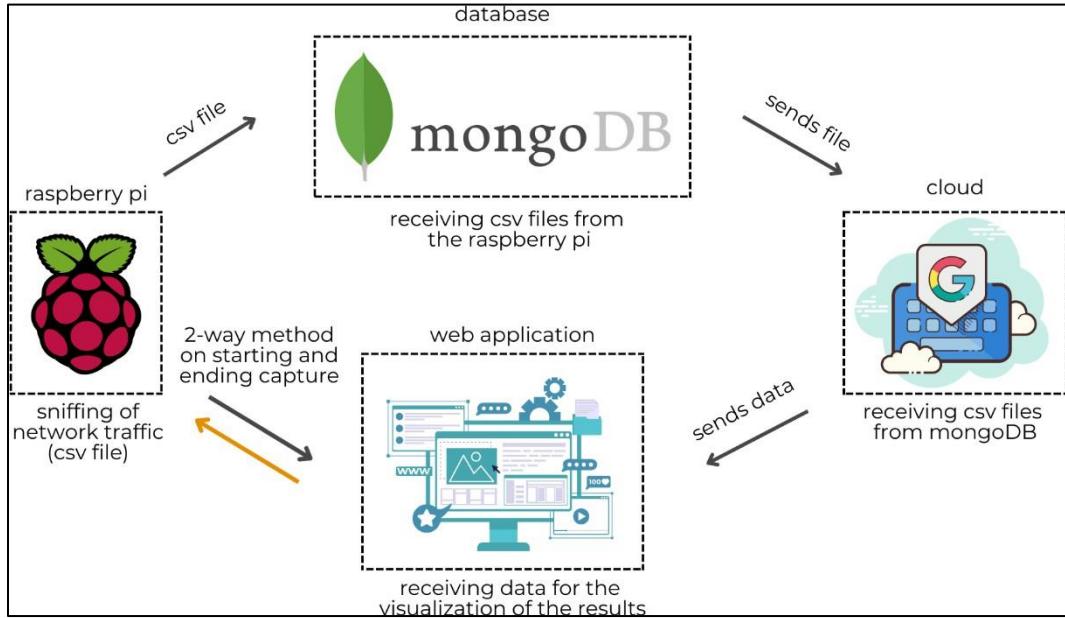


Figure 3.5 System Architecture Diagram

Figure 3.5 illustrates a system architecture involving a Raspberry Pi device, a MongoDB database, a cloud service, and a web application. The key components and their interactions are as follows:

1. Raspberry Pi: It is responsible for capturing network traffic and sending the captured CSV files to the MongoDB database using a 2-way method for sending and receiving data.
2. MongoDB: This is the central database that receives CSV files from the Raspberry Pi. It stores and manages the data.
3. Cloud: The cloud service receives CSV files from the MongoDB database, indicating that the data can be further processed or analyzed in the cloud environment.
4. Web Application: The web application receives data from the cloud, which is used to visualize the data.

The diagram shows the flow of data between these components, with the Raspberry Pi capturing network traffic and sending it to the MongoDB database, which then distributes the data to the cloud for further processing or analysis and the web application for visualization.

3.3 Research Locale

The Raspberry Pi-based Network Behavior Analysis Intrusion Detection System (NBAIDS) deployment location using an Ensemble Learning Approach will be the Valenzuela City Academic Center for Excellence (ValACE) in Valenzuela, Metro Manila. The ValACE is an excellent testing ground for the device, as it offers free Wi-Fi access to diverse users, including students, professionals, and casual internet surfers. This variety generates a rich mix of network traffic, testing the NBAIDS's ability to detect anomalies. Additionally, the library's wide range of users mirrors the challenges public Wi-Fi networks face, making the results applicable to real-world scenarios. The ValACE permits researchers to conduct studies within its premises, and there is potential for collaboration with the library's IT department, which could provide deeper insights into the network's intricacies.

3.4 Research Design

3.4.1 Hardware Design

The Raspberry Pi 4 model B has specifications such as Broadcom BCM2711, Quad-core Cortex-A72 (ARM v8) 64-bit SoC @ 1.8GHz, 2.4 GHz and 5.0 GHz IEEE 802.11ac wireless, Bluetooth 5.0, BLE, Gigabit Ethernet, 2 USB 3.0 ports; 2 USB 2.0 ports, 2 × micro-HDMI® ports (up to 4kp60 supported), 2-lane MIPI DSI display port, 2-lane MIPI CSI camera port, 4-pole stereo audio and composite video port, H.265

(4kp60 decode), H264 (1080p60 decode, 1080p30 encode), OpenGL ES 3.1, Vulkan 1.0, Micro-SD card slot for loading operating system and data storage, 5V DC via USB-C connector (minimum 3A*), 5V DC via GPIO header (minimum 3A*), Power over Ethernet (PoE) enabled (requires separate PoE HAT), Operating temperature: 0 – 50 degrees C ambient, and it is a good quality 2.5A power supply that can be used if downstream USB peripherals consume less than 500mA in total.

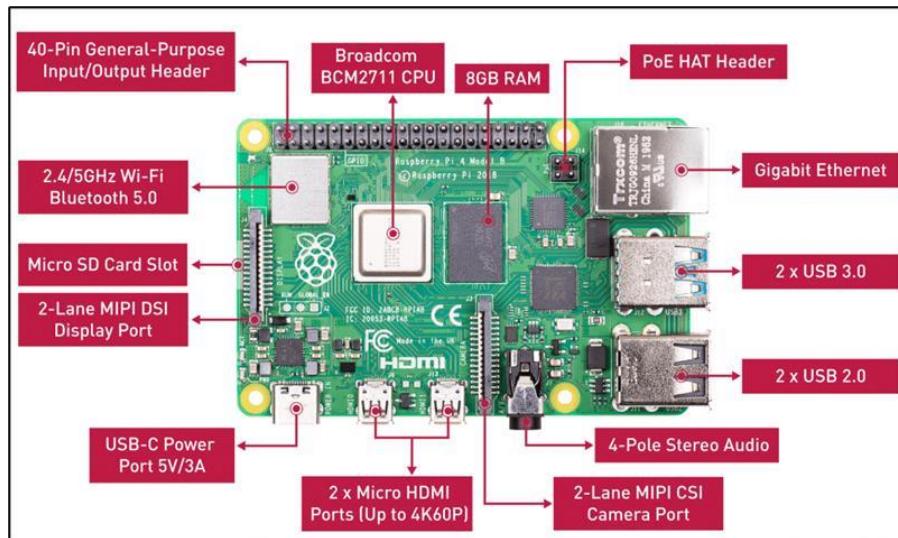


Figure 3.6 Hardware Specifications

Figure 3.6 shows the schematic of the prerequisites needed to build an Intrusion Detection System (IDS). The first requirement is the CPU, which is the Raspberry Pi's key microprocessor and central component. The CPU and the victim's device are connected via the Ethernet connection. The Raspberry Pi's button, LED light, and cooling fan are all connected to the 40-pin GPIO header. The Raspberry Pi's cooling fan is connected explicitly to pins 4 and 6. Furthermore, Pins 11, 12, and 14 are designated for attaching the Raspberry Pi's button and LED light, giving the user control over the network traffic sniffing feature. The data needed for Linux is stored in the Memory Card slot or microSD card. The USB-C power port powers the Raspberry

Pi, and the USB port allows the Pi to be powered in addition to facilitating USB device connectivity.

The function of this microprocessor is to capture and analyze network traffic, converting the data into a CSV file. Subsequently, the information is transmitted to the cloud for analysis by machine learning algorithms. The experimental setup connected a Raspberry Pi 4 Model B to the router. The Raspberry Pi could sniff network traffic from all devices connected to the router through this configuration.

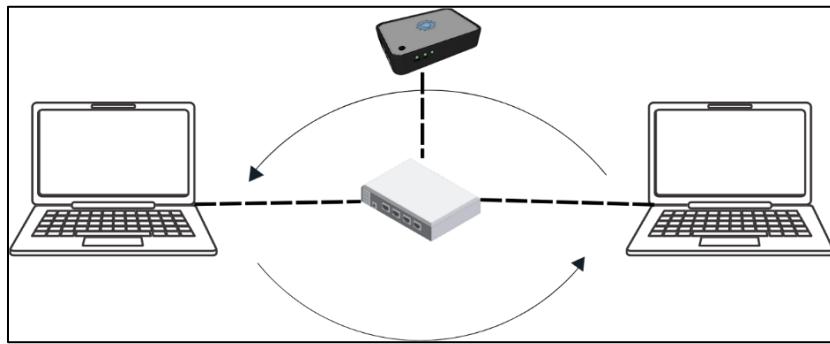


Figure 3.7 RPi-based IDS Attached to the Point-to-point Connected Devices

3.4.2 Software Design

3.4.2.1 Algorithm Selection

The machine learning algorithm employed by the researchers for the Intrusion Detection System (IDS) was the Ensemble Learning Approach. The learned weak machine learning algorithms, such as Decision Tree, Support Vector Machine (SVM), and Naive Bayes, are sources of the ensemble learning. The ensemble learning algorithm is produced by combining and optimizing the output of the weak learning methods using XGBoost.

Numerous studies demonstrate that ensemble learning outperforms alternative classifiers regarding accuracy for an intrusion detection system. Based on the findings of the study on the Intrusion Detection Model Using Ensemble Learning Methods (Wang et al., 2016), the ensemble learning model outperformed the Bayesian network and RandomTree in terms of accuracy per attack class. Among various classifiers like Naive Bayes, PART, and Adaptive Boost, the ensemble technique exhibits the highest accuracy, precision, and recall in a different study on an Ensemble technique for IDS using Machine Learning Algorithms (Kumar & Doegar, 2018). It demonstrates that, in comparison to alternative classifiers, the ensemble learning strategy can yield more promising results.

3.4.2.2 Flow Chart of Processes

Figure 3.8 shows the flowchart of the intrusion detection system using ensemble learning. The input of the system is the network traffic captured using the IDS. The network traffic, which may contain malicious or normal activity, is preprocessed to remove noise and extract important features. Once the preprocessing is complete, relevant features such as packet size, source and destination IP addresses, ports, and protocols are extracted. These extracted features are essential for the analysis of the captured network traffic. The preprocessed data then undergoes training with an ensemble learning algorithm to detect any unusual behavior within the traffic. If anomalies arise, the user receives an alert via a web-based application from the system. In addition, the results are shown by the web application, which highlights the significant characteristics that

were extracted from the traffic. This data provides facts that verify the traffic that the IDS was able to capture.

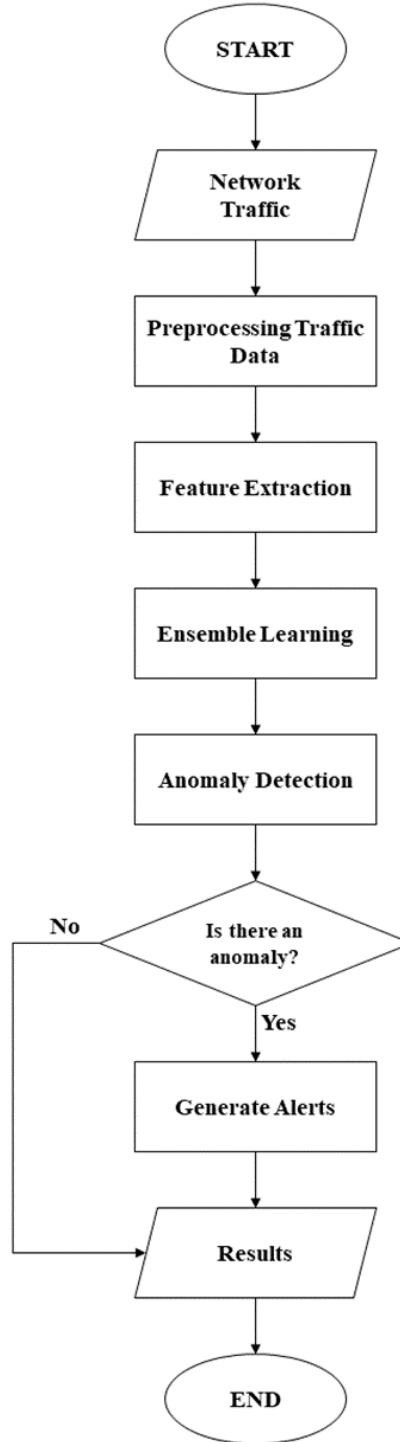


Figure 3.8 Flow Chart of Intrusion Detection System using Ensemble Learning

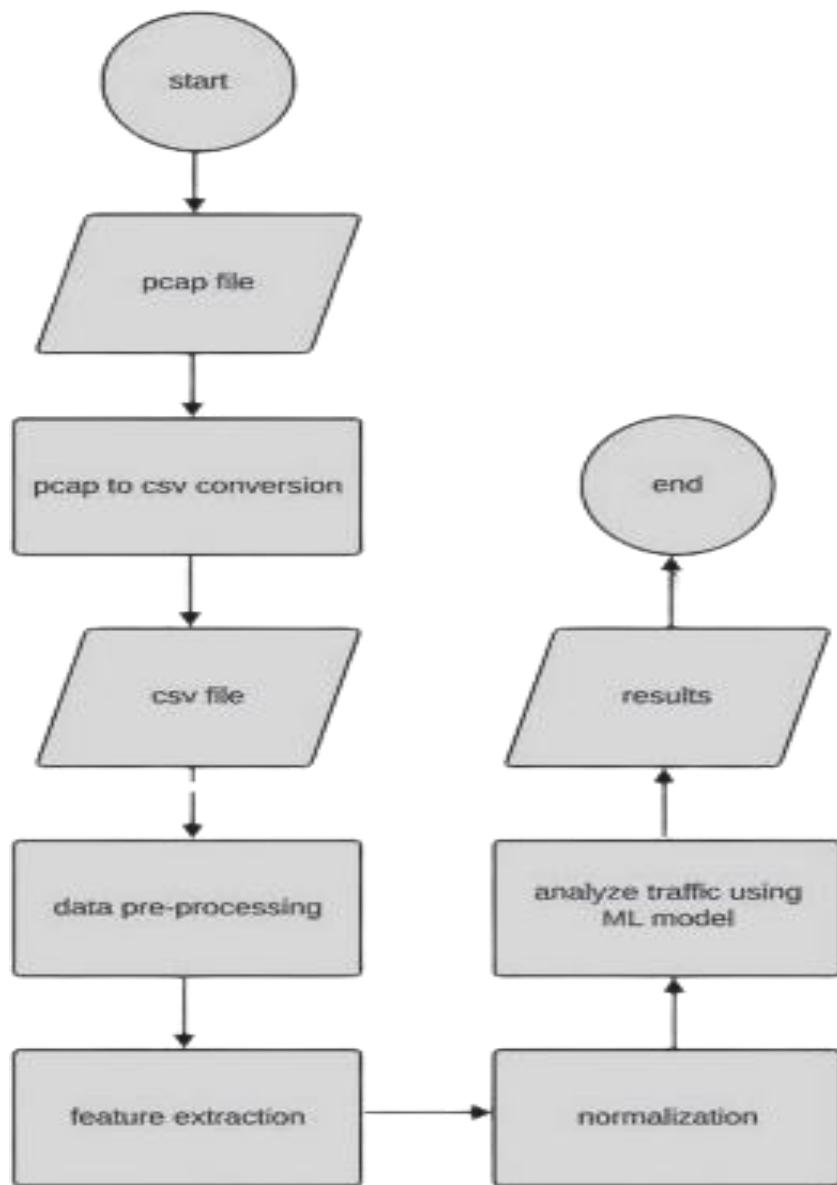


Figure 3.9 Flow Chart of Data Flow of NBAIDS

The flowchart in Figure 3.9 above shows the critical processes in managing network traffic data for a machine learning-based intrusion detection system. The process begins by obtaining a pcap file, a specialized format for capturing packet information on a network. This file is then transformed into CSV, a format that is better suited for data manipulation. To ensure accuracy and consistency, the data undergoes pre-processing to remove errors and standardize its structure. Next, key

features were identified and normalized to preserve measurement uniformity — which is essential for optimizing the effectiveness of diverse machine learning techniques. Once the machine learning model is applied, it thoroughly examines the traffic using normalized features to identify any irregularities or possible security risks. The results provided valuable insights into the nature of network traffic, completing the entire process.

Figure 3.10 shows the inner workings of a web application specifically created to handle network traffic information. The process starts with user authentication and then seamlessly moves on to capturing the data and generating a pcap file. Next, the file is converted to binary form and sent to a NoSQL Database, which will be later sent to the cloud, where it undergoes preparations before delving into the analysis phase. It likely involves converting the file to CSV format and applying other necessary pre-processing steps. Once ready, the CSV file is fed into a cloud-based machine learning model, producing valuable insights and effectively marking the end of cloud-based data processing.



Figure 3.10 Flow Chart of the Backend of the Web Application of NBAIDS

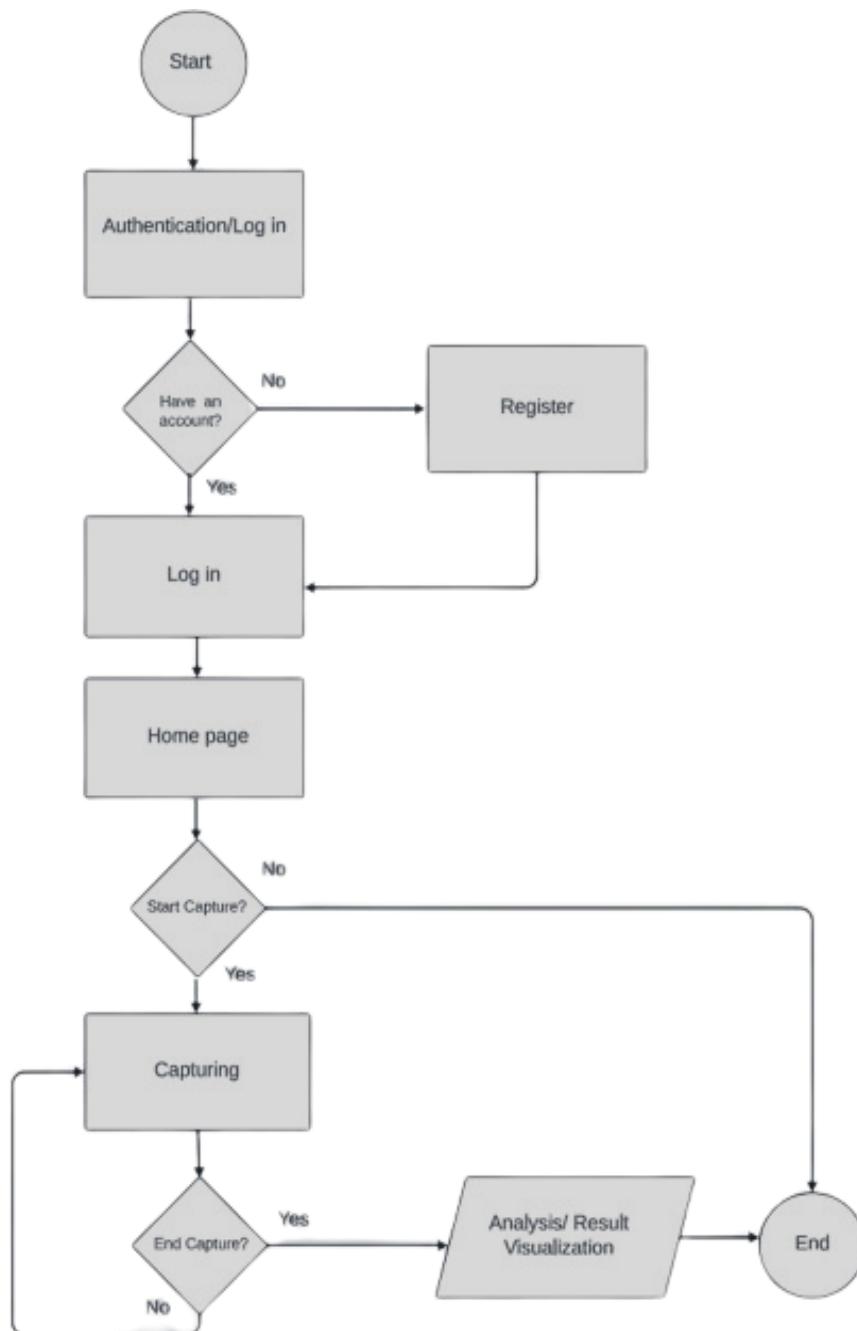


Figure 3.11 Flow Chart of the Frontend of the Web Application of NBAIDS

Figure 3.11 shows the user's journey within the web application, introducing an immersive interactive experience. It commences with the user being prompted to authenticate or log in. Without an existing account, the user is seamlessly directed to the registration process, while those with existing accounts can

effortlessly log in. After a successful login, the user is directed to the dynamic home page, where they can initiate network data capture. Upon selecting this option, the system automatically starts gathering network data until the user chooses to terminate it. Once the capture is complete, the gathered data is analyzed and transformed into visually appealing results for the user, providing valuable insights into the network traffic.

3.4.2.3 Web Application Design

1. “Access Page”. This page is the initial landing page or entry point for users to access the application. It contains Login/Registration Forms, Forgot Password/Account Recovery, and App Information and Features.

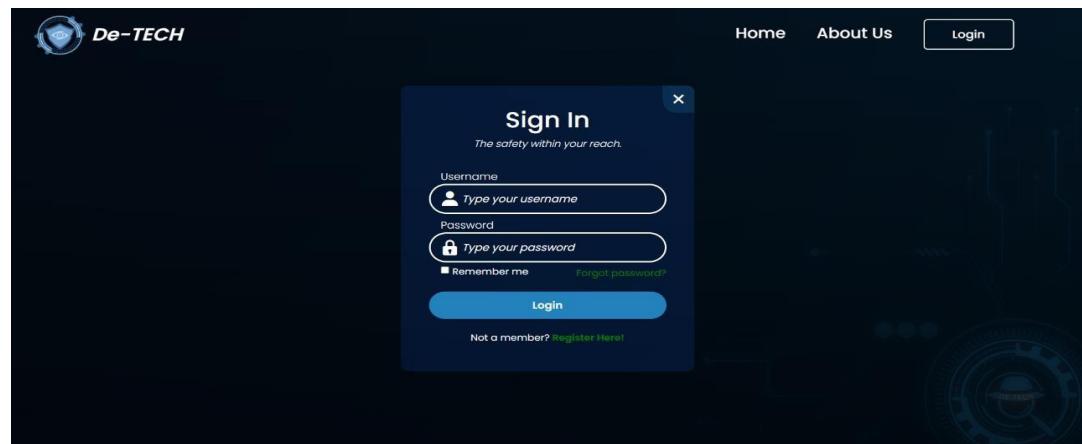


Figure 3.12 Access Page of De-TECH Web Application

2. “Home Page”. This page is the primary landing page users see after logging in or accessing the web application. It is the central hub where users can access the application's numerous sections and functions. It contains information about Intrusion Detection Systems and what type De-TECH is.



Figure 3.13 Home Page of De-TECH Web Application

3. “Detect”. This feature contains buttons for starting capture, ending capture, and analysis. It is a dedicated feature designed to test the project itself. It will serve as the means to start and end the capture or sniffing of network traffic, followed by analyzing the results.

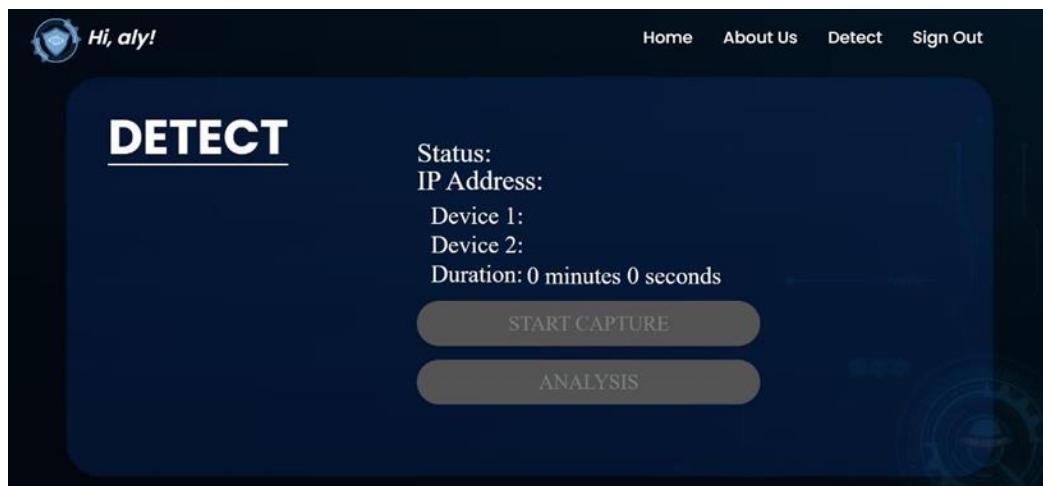


Figure 3.14 Detect Feature of De-TECH Web Application

4. “Analysis”. This feature contains the analyzed information data after sniffing the desired network traffic. It includes notable attributes from the CTU-13 Dataset. It also indicates whether the network traffic is normal or malicious and identifies the type of attack it belongs to.

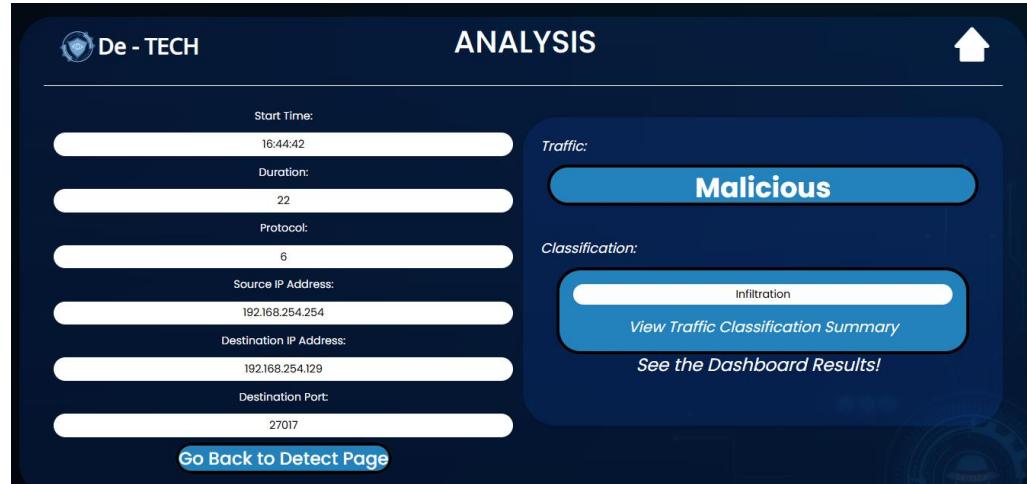


Figure 3.15 Analysis Feature of De-TECH Web Application

5. “Dashboard”. This feature contains a visual interface that presents essential information and data in a consolidated and easy-to-understand format. Various widgets or modules display charts, graphs, tables, and other visual elements representing data.



Figure 3.16a Dashboard Feature of De-TECH Web Application

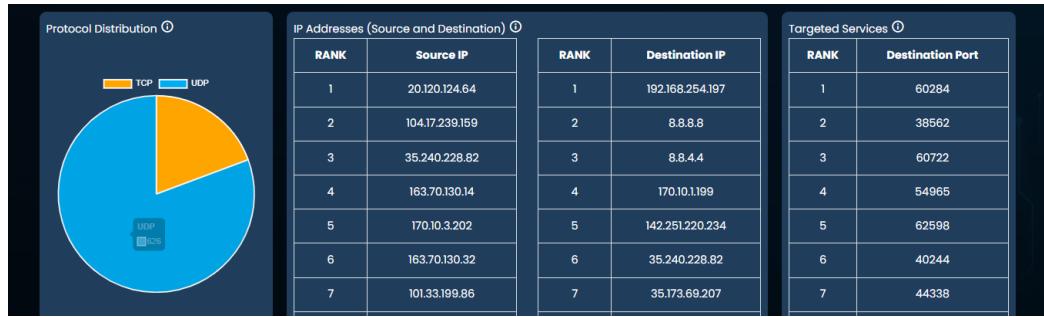


Figure 3.16b Dashboard Feature of De-TECH Web Application

3.5 Testing Procedure

The testing procedure begins by using the CTU-13 and CICIDS2018 data sets, which include the malicious traffic class consisting of Botnet, DDoS/Dos, Bruteforce, and Infiltration traffic. The objective is to find unique patterns and behaviors in malicious traffic to improve the accuracy and detection rate of the system and reduce false alarms. Based on network flow information, the attributes sourced serve as a valuable reference for the anomaly-based aspect of the IDS. Table 3.2 displays specific characteristics or qualities that will be considered essential factors from the datasets.

After extracting essential features, the training datasets are fed into the weak learning models using different algorithms like Support Vector Machines, Decision Trees, and Naive Bayes. The system will determine if incoming data is malicious or normal. Support Vector Machine (SVM) is a learning method that helps us classify things, predict values, and find unusual data. It is like a tool that learns from examples to make decisions about new information. Decision tree learning model is a way to make predictions by organizing information in a tree-like structure. It takes what we observe as input and figures out what we want to know as output. It is like following a map with different paths to reach a destination. Lastly, the Naïve Bayes algorithm predicts things by using the Bayes

Theorem, which is a way to calculate probabilities. It is like using a formula to make educated guesses based on the likelihood of different outcomes.

Table 3.2 Notable Attributes from CTU-13 Dataset (Kasimov, 2018)

Attributes	Description
StartTime	the time, when the first packet was forwarded
Dur	duration of the communication
Proto	protocol of the transport level
srcAddr	source IP address
dstAddr	destination IP address
dstPort	destination port
Flag	which flags were seen during the communication
SrcPackets	the number of packets that were sent from the source IP to the destination IP during the communication
DstPackets	the number of packets that were sent from the destination IP to the source IP during the communication
srcAppBytes	the number of application bytes that were sent from the source IP to the destination IP during the communication
dstAppBytes	the number of application bytes that were sent from the destination IP to the source IP during the communication
srcBytes	the number of all bytes that were sent from the source IP to the destination IP during the communication
dstBytes	the number of all bytes that were sent from the destination IP to the source IP during the communication

Once the testing is done, the results from each algorithm will be combined using the XG Boost algorithm to achieve the ultimate output for the ensemble learning model.

3.5.1 Cross-validation Procedure

This section will describe the procedure for validating the proposed detection system through cross-validation. The researchers aim to create a controlled and isolated environment by utilizing a virtual environment to simulate and identify real network traffic. The network configuration will be kept simple within this virtual environment, consisting of two machines. In this setup, one machine will generate malicious traffic

while the other will simulate normal traffic. The Intrusion Detection System (IDS) device and the web application will be connected via a router. One machine will access the web application to simulate the detection process.

3.5.1.1 Malicious Traffic Scenario

Because datasets with harmful computer programs are out there for researchers, it is important to keep them separate and safe so they do not spread to other computers. To imitate an attack, the infected computer will only communicate with the target computer directly, and it will only be done in a virtual environment.

Here is what will be done to simulate the attack:

A computer will be targeted and infected to create a virtual computer on the main computer using Windows 10 as its operating system. In this situation, various cyber-attacks mentioned in the information will be activated on the infected computer. All the given results can be seen on the web application that will be used. The traffic simulation for each cyber-attack will be documented and found in Table 3.3.

Table 3.3 Table of Detection Result for Different Malicious Traffic

Attack	Results	Classification	Percentage				
			Normal	DoS	Bruteforce	Botnet	Infiltration
Botnet							
DoS							
Bruteforce							
Infiltration							

3.5.1.2 Normal Traffic Scenario

To test the regular network traffic, we will use a virtual that is not infected. This machine will represent a typical network device and help us observe the normal flow of network activity.

To create a virtual computer on the main computer using Windows 10 as their operating system, a computer that will be targeted will act as a normal machine. In this scenario, typical traffic activities such as FTP and p2p ping response and the traffic simulation for each activity will be documented and found in Table 3.4.

Table 3.4 Table of Detection Result for Different Normal Traffic

Traffic Activity	Results	Classification	Percentage				
			Normal	DoS	Bruteforce	Botnet	Infiltration
FTP							
P2P Ping Response							

Below is an explanation of each column in the table:

- Attack/Traffic Activity – This category represents the specific type of malicious activity that the IDS is designed to identify.
- Results – This category represents the results of the binary detection if it is malicious or normal.
- Classification – This category represents the results of the multi-classification detection. It classifies the specific traffic type it detected.
- Percentage (Normal, DoS, Brutefroce, Botnet, Infiltration) – This category represents the percentage of the prediction of model for each traffic type.

Once we create pcap files for the various scenarios, we will use a separate table to link the results of the detection and classification performed by our system. This table will provide a comprehensive summary, showcasing the effectiveness of each machine learning model in detecting and classifying traffic as either malicious or normal. The Intrusion Detection System (IDS) results will be presented in a user-friendly web application, allowing users to view and analyze them conveniently based on specific time intervals.

3.6 Functionality Testing

Researchers conducted functionality testing to assess the functionality of the Raspberry Pi-based Network Behavior Analysis Intrusion Detection System (NBAIDS), employing an ensemble learning approach before deployment. The testing aimed to evaluate the system's performance and capabilities. The testing process commenced with data collection and preprocessing, ensuring the system could effectively handle the CTU-13 and CSE- CIC-IDS2018 dataset, encompassing diverse network traffic scenarios. Utilizing the CTU- 13 and CSE-CIC-IDS2018 dataset, the ensemble learning model underwent training and evaluation to gauge its effectiveness in detecting and classifying network intrusions. To assess the effectiveness of NBAIDS, various performance metrics, including accuracy, precision, recall, F1-score, True Positive, False Positive, True Negative, and False Negative, were evaluated. Additionally, CPU and memory usage were monitored during testing to ensure the system operated effectively on the Raspberry Pi platform. The CTU-13 and CSE-CIC-IDS2018 dataset responses from the NIDS to different types of intrusion were examined to measure the system's accuracy in identifying potential threats. The Raspberry Pi-based NIDS could be assessed and optimized through

thorough functionality testing to provide effective network intrusion detection using ensemble learning approaches.

3.7 ISO 9126 Standard Testing

An evaluation form will be provided to test if the product meets the ISO/IEC 9126 software evaluation. The evaluation form was based on the characteristics and sub-characteristics of the ISO/IEC 9126 software evaluation. The IT experts and users will complete the form with a background in web applications. An analysis will be done based on the evaluation results.

3.8 Statistical Treatment

3.8.1 Percentage Frequency Distribution

The percentage frequency distribution is used to determine the effectiveness of the Raspberry Pi-based Network Behavior Analysis Intrusion Detection System based on the ISO/IEC 9216 software produce evaluation.

The formula is as follows:

$$P = \frac{f}{n} \times 100$$

P = the percentage

f = the number of response

n = the number of respondents

3.8.2 Confusion Matrix

Metrics for intrusion detection help with evaluating the performance of an intrusion detection system. Accuracy, Precision, Recall, and F1-score are the evaluation metrics frequently employed concerning intrusion detection.

All these evaluation measures result from the four essential features of the confusion matrix that show the actual and expected classes, as depicted in Table 3.5. The confusion matrix has the following components:

1. True Positive (TP): The method accurately detected and classified malicious attempts across numerous samples.
2. True Negative (TN): The algorithm correctly identified and categorized normal samples.
3. False Positive (FP): The method incorrectly detected and classified normal samples as malicious attempts.
4. False Negative (FN): The algorithm failed to identify and categorize malicious attempts, mistakenly classifying them as normal samples.

Table 3.5 Confusion Matrix

	Predicted as Normal	Predicted as Attack
Actual Labeling as Normal	T _{Positive}	F _{Negative}
Actual Labeling as Attack	F _{Positive}	T _{Negative}

These parameters will then be used to calculate the accuracy, precision, recall, and f1 score to measure the overall performance and adaptability of the Intrusion Detection System.

Accuracy

It is described as the system's capacity to correctly recognize attacks as "attacks" and normal traffic as "normal flows." It provides information on the proportion of accurate predictions across all samples (Hussain et al., 2020). It is mathematically expressed as follows in equation 1:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FN} + \text{TN} + \text{FP}} \times 100$$

Precision

It indicates the proportion of correctly predicted attacks. It is a proportion between the correctly predicted attacks (i.e., TP) and the actual results (i.e., TP+FP) (Hussain et al., 2020). It is mathematically expressed as follows in equation 2:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \times 100$$

Recall

It is described as the system's capacity to identify the attack when a security breach occurs accurately. Another name for it is sensitivity (Hussain et al., 2020). It is mathematically expressed as follows in equation:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \times 100$$

F1 – Score

The weighted harmonic mean of recall and precision is how it is defined. It provides information on the test set's correct prediction ratio (Hussain et al., 2020). It is mathematically expressed as follows in equation:

$$\text{F1 – Score} = 2 \times \frac{\text{Recall} * \text{Precision}}{\text{Recall} + \text{Precision}}$$

The summary parameters for each machine learning model that will be recorded for the setup are shown in Table 3.6.

Table 3.6 Summary Performance Results of the Supervised Model

Evaluation	Learning Model			
	Decision Tree	Naïve Bayes Gaussian	SVM	Ensemble Learning
Performance Results	Accuracy			
	Precision			
	Recall			
	F1 – Score			
	False Positive Rate			

Chapter 4

RESULTS AND DISCUSSION

This chapter presents the project structure, interprets the data, and analyzes the findings in relation to the tests conducted.

4.1 Project Technical Description

The project study consists of three major parts: the packet capturing tool, the machine learning model, and the web application. The Raspberry Pi 4 Model B microprocessor is used as the packet capturing tool for the Intrusion Detection System and operates with a 5.1V power supply. It must be connected to the local area network to capture network traffic. After capturing the traffic, it will be sent to a cloud-based web application. There, it will be processed using an ensemble learning model, which combines weak learners such as SVM, Naive Bayes, and Decision Tree. The datasets used to train the model are CTU-13 and CSE-CIC-IDS 2018. The model will undergo a detection and classification process. For detection, the outputs are “Malicious” or “Normal.” For classification, the outputs will be “Normal,” “Botnet,” “Bruteforce,” “Denial of Service,” or “Infiltration.” The results will be displayed in the web application, which also features a dashboard and a history tab providing additional information about the network during monitoring.

4.2 Project Structural Organization

4.2.1 Packet Capturing Tool

Figure 4.1 shows the packet capturing tool of De-TECH. It is enclosed in a 3D-printed white casing, customized to fit all the parts. Inside the case is the Raspberry Pi 4 Model B, which runs the program for sniffing or capturing network traffic. Also

shown in Figure 4.1 are an LED light and a button. The button is used to start and stop the capture process but is only needed if an error occurs in the web app and human intervention is required. The red LED light serves as an indicator of the device's status. When the device is idle, the LED light is steady. When the device is capturing traffic, the LED light blinks.



Figure 4.1 De-TECH Hardware

Moreover, Figure 4.2 shows the actual setup of how De-TECH is used. The black cord is the power cord, supplying the device with the required 7.6 watts of power. The white wire is the LAN cable, which connects the device to the entire network.



Figure 4.2 De-TECH connected in the switch using LAN cable

4.2.2 Device Limitations

The researchers use the command “nmap” in the terminal of the Raspberry Pi to see all the connected devices in the network. After viewing the list of IP addresses, these addresses are manually entered into the device’s code to sniff the network of the chosen IP addresses.

During the deployment, the researchers identified nearly 200 IP addresses. They attempted to enter all the IP addresses into the code, but the system couldn’t handle the traffic volume when monitoring all the devices using De-TECH. Therefore, the researchers reduced the list to around 100 IP addresses. The table 4.1 shows the duration the Raspberry Pi ran before encountering an error during the deployment at the Valenzuela City Academic Center for Excellence and at the UITC, connected to the CAFA building network at the Technological University of the Philippines – Manila.

Table 4.1 Durating the Raspberry Pi ran in the Deployment Sites

Deployment Site	Model	No. of files Processed	Duration
Valenzuela City Academic Center for Excellence (ValACE)	Day 1 – M20	44	6hrs and 25mins
	Day 2 – M20	56	4hrs and 14mins
	Day 2 – M39	130	8hrs
	Day 3 – M39	161	11hrs and 2mins
	Day 4 – M39	243	16hrs
	Day 5 – M39	170	12hrs
	Day 6 – M39	203	10hrs and 30mins
	Day 6 – M20	46	6hrs
	Day 7 – M26	156	9hrs
	Day 8 – M26	217	11hrs and 12mins
UITC (CAFA Bldg)	Day 9 – M26	277	14hrs and 30mins

In the “Model” column of Table 4.1, “Day” represents when the device is used, “M” represents the ensemble model, and the number indicates the number of features used to train the model. Based on the results shown, the device can run for up to 16 hours without human intervention. This implies that it can operate autonomously without needing a restart, even if an error occurs, which may be due to heavy traffic or an unstable internet connection.

4.3 Experimental and Data Analysis

4.3.1 Using Validation Data

To achieve the optimal model for the Intrusion Detection System, the researchers used trial and error to select the best set of features for training the model. Some features were derived from the paper by Fitni and Ibraheem, others were based on suggestions from cybersecurity experts, and some were selected based on correlation using linear regression, Random Forest, and Chi-square tests. Some models were not yet hyper-tuned. Based on the performance results, hyper-tuned models showed better outcomes compared to those that were not. However, these models were only tested using validation data. Furthermore, as shown in Table 1.1, the best model was Model 33, which achieved an accuracy of 96.40%, a precision of 95.83%, a recall of 96.40%, and an F1-score of 95.70%.

Table 4.2 Performance Results of different Ensemble Models using Validation Data

Model	Accuracy	Precision	Recall	F1-score
1. Model 33 (Ibraheem, reduced 50-50, Hypertuned)	96.40%	95.83%	96.40%	95.70%
2. Model 26 (hypertuned)	96.39%	95.82%	96.39%	95.66%
3. Model 39 (50-50, Linear Regression-Hypertuned)	96.29%	95.70%	96.29%	95.57%
4. Model 39 (Linear Regression-Hypertuned)	93.62%	93.90%	93.62%	93.08%
5. Model 23 (Fitni, Spearman-Hypertuned)	93.35%	93.77%	93.35%	92.71%
6. Model 39 (reduced 50-50, Linear Regression-Hypertuned)	92.94%	93.46%	92.94%	92.37%
7. Model Fitni 23 (Chi Square-Hypertuned)	92.57%	93.05%	92.57%	91.73%
8. Model 20 (Ibraheem, Hypertuned)	89.16%	89.71%	89.16%	87.84%
9. Model 55	68.68%	74.99%	68.67%	69.35%
10. Model 39	67.36%	77.15%	67.36%	64.49%
11. Model 44	67.91%	68.64%	67.91%	64.99%
12. Model 20	60.38%	74.66%	60.38%	62.74%
13. Model 19	65.29%	63.30%	65.29%	62.62%
14. Model 42	57.72%	72.68%	57.72%	49.35%
15. Model 26	55.10%	59.54%	55.10%	52.47%
16. Model 38	46.32%	71.35%	46.32%	42.17%
17. Model 33	47.42%	67.28%	47.42%	42.75%
18. Model 30	39.69%	54.64%	39.69%	31.75%

4.3.2 Using Generated Traffic

Using the same models from Table 1.1, all of them were tested using the saved traffic generated by one of the researchers, and some were tested using pcap files from a GitHub repository. Upon testing each ensemble model, the rankings changed. In Table 1.2, the best model when tested using generated traffic is Model 20, which features are based on the paper by Ibraheem and is also hyper-tuned. It has an accuracy of 66.00%, a precision of 48.00%, a recall of 100%, and an F1-score of 65.00%.

Additionally, observations show that Model 26 remained in the second rank for both testing methods.

Table 4.3 Performance Results of different Ensemble Models using Generated Traffic

Model	Accuracy	Precision	Recall	F1-score
1. Model 20 (Ibraheem, Hypertuned)	66.00%	48.00%	100.00%	65.00%
2. Model 26	60.94%	44.44%	100.00%	61.54%
3. Model 39 (reduced 50-50, Linear Regression-Hypertuned)	70.31%	52.63%	50.00%	51.28%
4. Model 42	45.00%	27.78%	50.00%	35.71%
5. Model 55	40.00%	11.54%	85.00%	20.32%
6. Model 30	64.00%	17.65%	40.00%	24.49%
7. Model 33	53.33%	30.00%	30.00%	30.00%
8. Model 20	33.33%	22.22%	40.00%	28.57%
9. Model 23 (Fitni, Spearman-Hypertuned)	76.00%	19.57%	10.00%	13.24%
10. Model 39 (Linear Regression-Hypertuned)	75.00%	25.00%	0.00%	0.00%
11. Model 38	80.00%	20.00%	0.00%	0.00%
12. Model 19	30.00%	17.65%	30.00%	22.22%
13. Model 39	83.33%	11.76%	0.00%	0.00%
14. Model 44	82.22%	11.90%	0.00%	0.00%
15. Model 39 (50-50, Linear Regression-Hypertuned)	54.00%	14.00%	10.00%	12.00%
16. Model 33 (Ibraheem, reduced 50-50, Hypertuned)	46.00%	4.00%	5.00%	4.00%

4.3.3 Using Traffic from Deployment Sites

The top three Ensemble models based on Table 1.2 was used for testing during deployment in Valenzuela City Academic Excellence (ValACE) namely Model-20, Model-39, and Model-26 and in the network of CAFA Building in Technological University of the Philippines – Manila. Even though three different models were used, all of them shows that most of the traffic detected were Malicious.

Table 4.4 Results from Deployment Sites

Model	No. of files Processed	Duration	Normal	Malicious
Day 1 – M20	44	6hrs and 25mins	2.27 %	97.73 %
Day 2 – M20	56	4hrs and 14mins	8.93 %	91.07%
Day 2 – M39	130	8hrs	9.23 %	90.77 %
Day 3 – M39	161	11hrs and 2mins	8.07 %	91.93 %
Day 4 – M39	243	16hrs	7.82 %	92.18 %
Day 5 – M39	170	12hrs	15.29 %	84.71 %
Day 6 – M39	203	10hrs and 30mins	14.29 %	85.71 %
Day 6 – M20	46	6hrs	100 %	0
Day 7 – M26	156	9hrs	12.82 %	87.18 %
Day 8 – M26	217	11hrs and 12mins	23.96 %	76.04 %
Day 9 – M26	277	14hrs and 30mins	13.72 %	86.28%

4.3.4 Chosen Ensemble Model

Based on observations, it seems that the performance of the models weakened as the traffic became less filtered. The researchers consulted the results with cybersecurity expert Engr. Julius Erick Evangelista, a SOC Analyst at Nexus Technologies. Engr. Evangelista stated that the generated traffic is less filtered compared to the traffic in the dataset used for training the model, which explains the lower performance results in Table 4.3. Moreover, the performance of the models decreased further in Table 4.4. Engr. Evangelista agreed with the statement that the Raspberry Pi is used for monitoring traffic in a network, which includes random traffic from different sources as users access the internet. Therefore, the researchers chose the model that ranked highest in both Table 4.2 and Table 4.3. The chosen model is Model 26.

Table 4.5 Summary Performance Results of the Model 26

Evaluation	Learning Model				
	Decision Tree	Naïve Bayes Gaussian	SVM	Ensemble Learning	
Performance Results	Accuracy	96.39%	55.70%	90.71%	96.39%
	Precision	95.82%	56.41%	89.97%	95.82%
	Recall	96.39%	55.70%	90.71%	96.39%
	F1 – Score	95.66%	49.32%	89.00%	95.66%

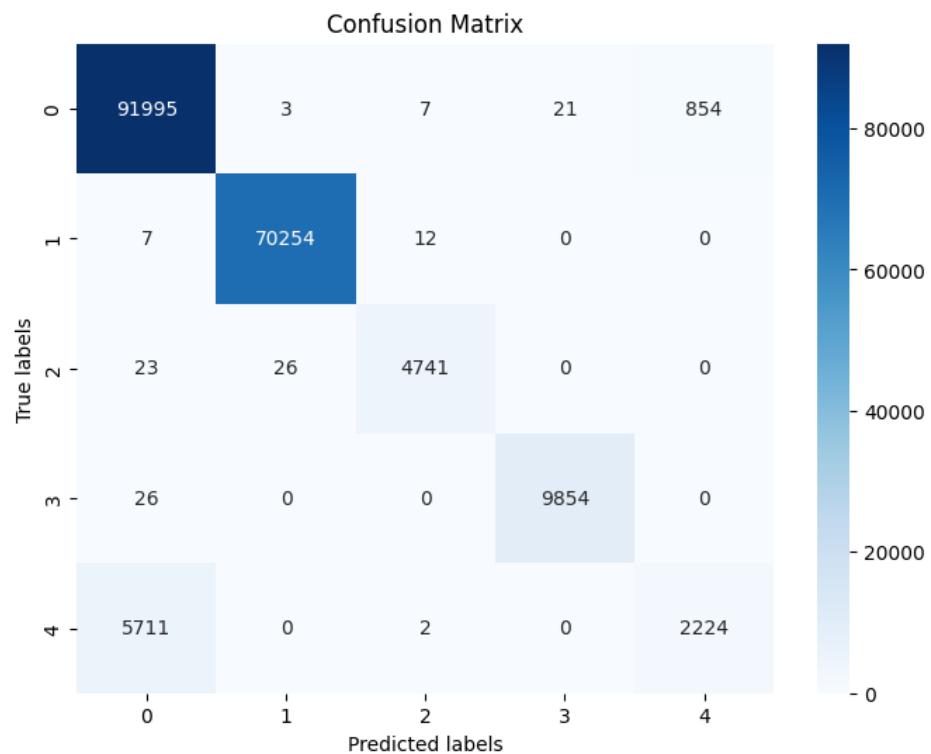


Figure 4.3 Confusion Matrix of Decision Tree Model

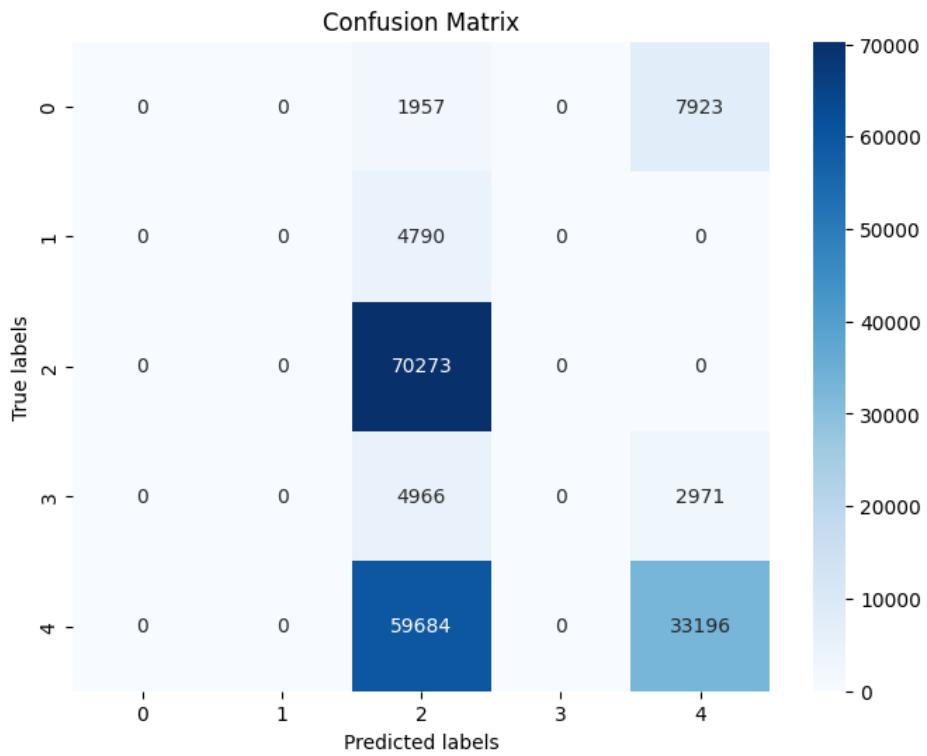


Figure 4.4 Confusion Matrix of Naïve Bayes Model

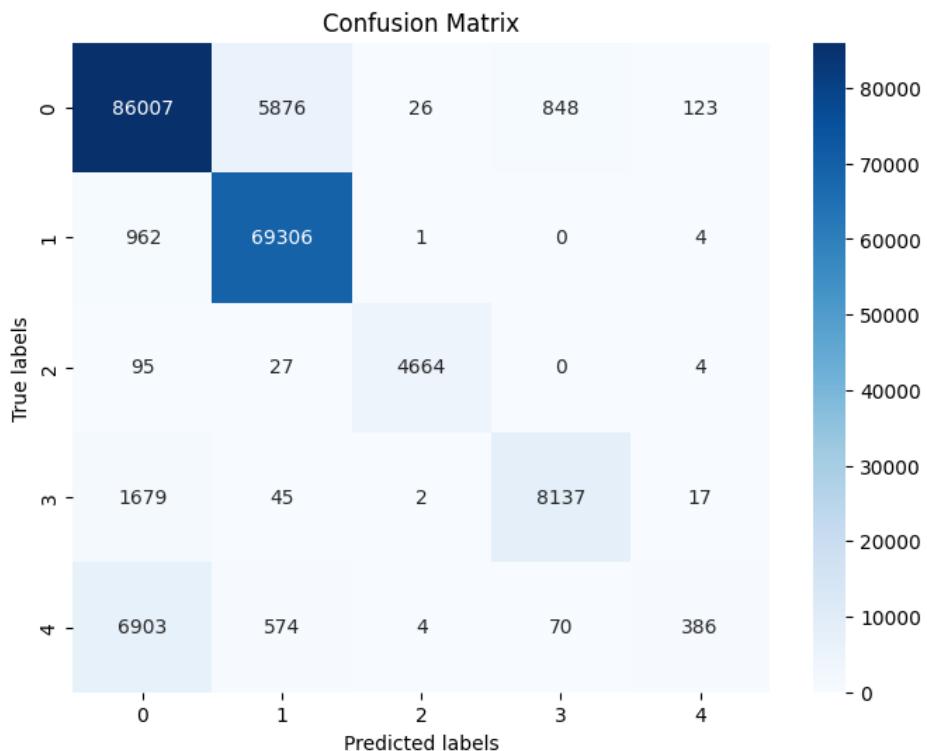


Figure 4.5 Confusion Matrix of SVM Model

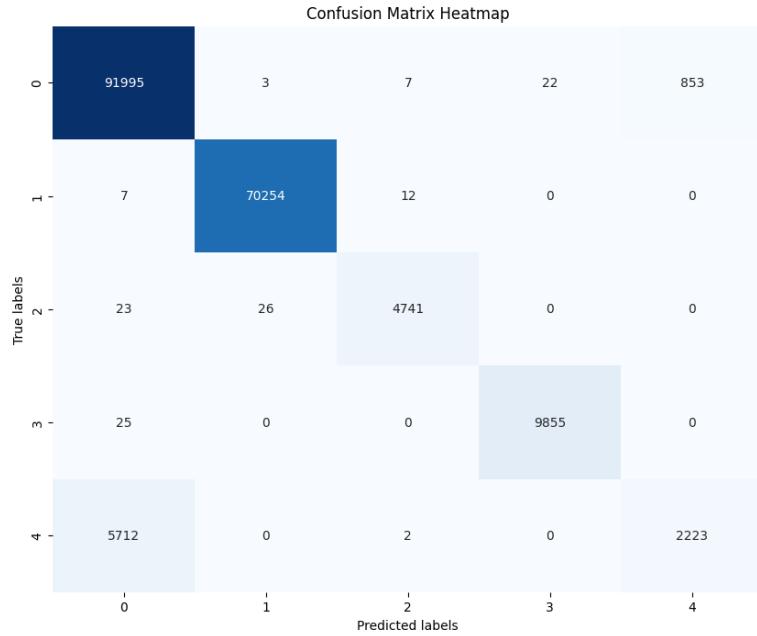


Figure 4.6 Confusion Matrix of Ensemble Model

Table 4.5 shows the summary of the performance of Model 26. Among the three weak learners—Decision Tree, Naïve Bayes, and SVM—the Decision Tree has the highest accuracy. It can be observed that when these models are combined into an ensemble model, the ensemble’s performance aligns closely with that of the Decision Tree model.

4.3.5 Web Application Evaluation

The ISO 9126 standard is used to evaluate the Web Application of the research project. It is an international standard for the evaluation of software quality, and it categorizes software quality attributes into six main characteristics, each of which is further subdivided into sub-characteristics.

The project evaluation is conducted using Google Forms. The evaluation utilized feedback from both IT professionals with web development backgrounds from various companies and student learners from various universities, as indicated in Table

4.6. These participants tested and explored our web application, providing valuable feedback and recommendations.

Table 4.6. Project Evaluators

Evaluator	Role	Expertise
Project Evaluator No. 1	IT Professional	System Analyst
Project Evaluator No. 2	IT Professional	Jr. PHP Developer
Project Evaluator No. 3	IT Professional	Net Core Developer
Project Evaluator No. 4	IT Graduate	Learner
Project Evaluator No. 5	Student	Student Learner
Project Evaluator No. 6	Student	Student Learner
Project Evaluator No. 7	Student	Student Learner

The project evaluation is divided into the six main characteristics of the ISO 9126 standard, and it summarizes the feedback from the various respondents. Table 4.7 shows the frequency-percentage distribution table of the respondedesnts' answer using the Questionnaire De-Tech Web Application Questionnaire. Most of the respondents answered Agree on each sub-characteristic. As shown in Table 4.8, all the sub-characteristics have an above average score.

Moreover, the respondents' feedback is about enhancing the security of the web application by implementing reCAPTCHA and defending against common web attacks such as SQL injection, Cross-Site Scripting (XSS), session management vulnerabilities, and password encryption issues. They also suggested using popular Bootstrap-based web layouts like Metronic, AdminLTE, or CoreUI to improve design and functionality. The basic operation of the system was praised for being easy and user-friendly, and a recommendation was made to simplify the color combination to enhance readability. Finally, they extended their best wishes for the project's success.

Table 4.7 Frequency-Percentage Distribution Table of the Web App Evaluation using Questionnaire De-Tech Web Application Questionnaire

Characteristics	Sub-Characteristics	Strongly Agree (5)		Agree (4)		Neutral (3)		Disagree (2)		Strongly Disagree (1)	
		F	P	F	P	F	P	F	P	F	P
Functionality	Suitability	1	14.29%	6	85.71%	0	0.00%	0	0.00%	0	0.00%
	Accurateness	1	14.29%	6	85.71%	0	0.00%	0	0.00%	0	0.00%
	Interoperability	2	28.57%	5	71.43%	0	0.00%	0	0.00%	0	0.00%
	Security	1	14.29%	3	42.86%	3	42.86%	0	0.00%	0	0.00%
Reliability	Maturity	2	28.57%	5	71.43%	0	0.00%	0	0.00%	0	0.00%
	Fault Tolerance	0	0.00%	5	71.43%	2	28.57%	0	0.00%	0	0.00%
	Recoverability	1	14.29%	4	57.14%	2	28.57%	0	0.00%	0	0.00%
Usability	Understandability	0	0.00%	4	57.14%	1	14.29%	1	14.29%	0	0.00%
	Learnability	2	28.57%	2	28.57%	2	28.57%	1	14.29%	0	0.00%
	Operability	2	28.57%	5	71.43%	0	0.00%	0	0.00%	0	0.00%
	Attractiveness	2	28.57%	2	28.57%	3	42.86%	0	0.00%	0	0.00%
Efficiency	Time Behaviour	1	14.29%	6	85.71%	0	0.00%	0	0.00%	0	0.00%
	Resource Utilisation	2	28.57%	5	71.43%	0	0.00%	0	0.00%	0	0.00%
Maintainability	Analysability	0	0.00%	5	71.43%	2	28.57%	0	0.00%	0	0.00%
	Changeability	1	14.29%	2	28.57%	4	57.14%	0	0.00%	0	0.00%
	Stability	1	14.29%	4	57.14%	2	28.57%	0	0.00%	0	0.00%
	Testability	1	14.29%	3	42.86%	3	42.86%	0	0.00%	0	0.00%
Portability	Adaptability	1	14.29%	1	14.29%	5	71.43%	0	0.00%	0	0.00%
	Installability	3	42.86%	2	28.57%	2	28.57%	0	0.00%	0	0.00%
	Conformance	0	0.00%	5	71.43%	2	28.57%	0	0.00%	0	0.00%
	Replaceability	1	14.29%	2	28.57%	4	57.14%	0	0.00%	0	0.00%
All Characteristics	Compliance	1	14.29%	3	42.86%	3	42.86%	0	0.00%	0	0.00%

Table 4.8 Weighted Score and Average Table of the Web App Evaluation using Questionnaire De-Tech Web Application Questionnaire

Characteristics	Sub-Characteristics	Weighted Score	Weighted Average	Average
Functionality	Suitability	29	4.1	4.1
	Accurateness	29	4.1	
	Interoperability	30	4.3	
	Security	26	3.7	
Reliability	Maturity	30	4.3	4.0
	Fault Tolerance	26	3.7	
	Recoverability	27	3.9	
Usability	Understandability	21	3.0	3.7
	Learnability	26	3.7	
	Operability	30	4.3	
	Attractiveness	27	3.9	
Efficiency	Time Behaviour	29	4.1	4.2
	Resource Utilisation	30	4.3	
Maintainability	Analysability	26	3.7	3.7
	Changeability	25	3.6	
	Stability	27	3.9	
	Testability	26	3.7	
Portability	Adaptability	24	3.4	3.7
	Installability	29	4.1	
	Conformance	26	3.7	
	Replaceability	25	3.6	
All Characteristics	Compliance	26	3.7	3.7
OVERALL AVERAGE				3.9

Chapter 5

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

This chapter presents the summary of findings, conclusions, and recommendations relative to the results conducted on the duration of this research.

5.1 Summary of findings

The researchers successfully developed and tested De-TECH, a Raspberry Pi-based device capable of capturing and analyzing network traffic using machine learning models to classify it as normal or malicious. Through an extensive process of training and evaluating different ensemble models, Model 26, a hypertuned ensemble model, emerged as the top performer. On validation data, Model 26 achieved an impressive accuracy of 96.39%, precision of 95.82%, recall of 96.39%, and F1-score of 95.66%. However, when tested on generated traffic, its performance declined, with an accuracy of 60.94%, precision of 44.44%, recall of 100%, and F1-score of 61.54%. During deployment at Valenzuela City Academic Center for Excellence and TUP-Manila, Model 26 detected 76.04% to 92.18% of the traffic as malicious. Additionally, the web application developed for the project underwent evaluation using the ISO 9126 standard, with feedback collected from IT professionals and students. The respondents gave an above average score for the web application.

5.2 Conclusions

Based on the results and findings of the research, the following conclusions were inferred:

1. The researchers successfully developed an Intrusion Detection System (IDS) using the Raspberry Pi 4 Model B. The device demonstrated its capability to capture and analyze network traffic in semi-realtime. The device can monitor traffic up to 16 hours with stable internet connection.

2. The ensemble model, Model 26, demonstrated an accuracy of 96.39%. The Decision Tree Model, Naïve Bayes Model, and SVM Model with the same 26 features as ensemble model has an accuracy of 96.39%, 55.70%, and 90.71%, respectively. This shows that the ensemble learning model, combining Naïve Bayes, Support Vector Machine (SVM), and Decision Tree, generally outperformed the individual algorithms. However, the performance of these models varied depending on the nature and complexity of the network traffic being analyzed.
3. An adaptive web application was developed to display the results of the IDS based on specified start and end times of the captured data. The web application met the required standards for functionality, reliability, usability, efficiency, maintainability, and portability. The dashboard and history tab effectively provided additional information about the network, enhancing the monitoring process. Some areas for improvement were identified, but overall, the application scores 3.9 which is above the average score.
4. The evaluation of the Network Behavior Analysis Intrusion Detection System (NBAIDS) using the ISO 9126 standard showed that the system met the required benchmarks for quality. The IDS demonstrated acceptable levels of functionality, reliability, usability, efficiency, maintainability, and portability with scores of 4.1, 4.0, 3.7, 4.2, 3.7, 3.7, and 3.7, respectively. This evaluation confirms that the developed system is effective, although continuous improvements are necessary to address any identified shortcomings.

5.3 Recommendations

The researchers recommend continuously updating and retraining the machine learning models with new network traffic data to improve their accuracy and adaptability. The researchers also recommend using deep learning for creating a model for detection and classification of network traffic types.

Moreover, for the web application, they suggest implementing recommended security measures, such as reCAPTCHA and protection against common web attacks, to enhance the security of the web application. Considering popular Bootstrap-based web layouts could improve the design and functionality of the web application. Also, simplifying the color combination of the web application could enhance readability.

Exploring further optimization techniques could improve the performance of the De-TECH device, allowing it to handle higher volumes of network traffic. Finally, conducting more extensive testing and deployment in various network environments would validate the system's performance and identify potential areas for improvement.

REFERENCES

- Almutairi, S., Aborokbah, M. M., Chilamkurti, N., Ganesan, S., & Patan, R. (2020). Effective Attack Detection in Internet of Medical Things Smart-Environment using a Deep Belief Neural Network. *IEEE Access*, 1–1.
- Doi:10.1109/access.2020.2986013.
- Alrowaily, M., Alenezi, F. N., & Lu, Z. (2019). Effectiveness of machine learning based intrusion detection systems. In *Lecture Notes in Computer Science* (pp. 277–288). https://doi.org/10.1007/978-3-030-24907-6_21
- Alshamkhany, M., et al., (2020)“Botnet Attack Detection using Machine Learning,” 2020 14th International Conference on Innovations in Information Technology (IIT), Al Ain, United Arab Emirates, 2020, pp. 203-208, doi: 10.1109/IIT50501.2020.9299061.
- Anderson., B. and Tracey, K. (2001). “Digital Living,” *American Behavioral Scientist*, vol. 45, no. 3, pp. 456–475,” 2001. [Online]. Available: doi:10.1177/00027640121957295.
- Ashoor, A. S. and Gore, S. (2011). “Difference between intrusion detection system (IDS) and Intrusion Prevention System (IPS),” *Advances in Network Security and Applications*, pp. 497–501, 2011. Doi:10.1007/978-3-642-22540-6_48
- Aslan, Ö., et. al. (2023). “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions,” 11 March 2023. [Online]. Available: <https://doi.org/10.3390/electronics12061333>.
- O. S. Mohammed, N. T. Alsohybe, F. M. Ba-Alwi, and A. T. Zahary, rep., 2018
- Aspernäs, A. and Simonsson, T. (2015). “IDS on Raspberry Pi: A Performance Evaluation”.

Available:

<http://www.diva portal.org/smash/record.jsf?pid=diva2%3A819555&dswid=8450>.

Arslan, R. S. (2021). “FastTrafficAnalyzer: An efficient method for intrusion detection systems to analyze network traffic,” DÜMF Mühendislik Dergisi, pp. 565–572, 2021. Doi:10.24012/dumf.1001881

Australian (2017), “Australian cyber security center threat report 2017.”

[Online].Available:

https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf.

Azap, B. (2022). “What is a Point-to-Point Connection? | phoenixNAP IT Glossary,” phoenixNAP IT Glossary,” 28 June 2022. [Online]. Available: <https://phoenixnap.com/glossary/point-to-point-connection>.

Bansal, S., & Kaur, P. (2020). Intrusion detection system using XGBoost algorithm on CICIDS 2017 dataset. International Journal of Computer Applications, 176(13), 1-10. Doi:10.5120/ijca2020935610

Bansal, A. and Mahapatra, S. (2017). “A comparative analysis of Machine Learning Techniques for Botnet detection,” Proceedings of the 10th International Conference on Security of Information and Networks. Doi:10.1145/3136825.3136874.

Bastanford, A. & Tabibi, T. (2016). “A Critical Review of Graphical User Interface Recent Articles.” ResearchGate.

https://www.researchgate.net/publication/335813138_A_Critical_Review_of_Graphical_User_Interface_Recent_Articles

BasuMallick, C. (2022). “Raspberry Pi Models and Features,” Spiceworks, Aug. 26, 2022.

Available: <https://www.spiceworks.com/tech/networking/articles/what-is->

raspberry-pi/.

Belenguer, J. and Calafate, C. T. (2007). “A low-cost embedded IDS to monitor and prevent Man-in-the-Middle attacks on wired LAN environments,” The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007), Valencia, Spain, 2007, pp. 122-127, doi: 10.1109/SECUREWARE.2007.4385321.

Berners-Lee, T., et. al. (1994). “The world-wide web,” Communications of the ACM, vol. 37, no. 8, pp. 76–82,” 1994. [Online]. Available: doi:10.1145/179606.179671.

Bhardwaj, R. (2020) “Local Area Network Explained (What is LAN?) – IP With Ease,” IP With Ease,” 6 July 2020. [Online]. Available: <https://ipwitthease.com/what-is-local-area-network/>.

Chen, C.-Y., Chen, L.-A., Cai, Y.-Z., & Tsai, M.-H. (2020). RNN-based DDoS Detection in IoT Scenario. 2020 International Computer Symposium (ICS), 448-453. <https://doi.org/10.1109/ICS51289.2020.00094>

Chen, S.-C., et. al. (2018). “Effective botnet detection through neural networks on convolutional features,” 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018. Doi:10.1109/trustcom/bigdatase.2018.00062.

Chen, X., Zhang, L., & Wang, H. (2019). Deep learning-based botnet detection using CTU-13 dataset. Security and Privacy, IEEE Transactions on, 17(2), 406-420. Doi:10.1109/TSEC.2018.2881658

Closa, D. .et. al. (2010). “Patent law for computer scientists”, 2010. Doi:10.1007/978-3-642-05078-7

Conallen, J. (1999). “Modeling web application architectures with UML,” Communications of the ACM, vol. 42, no. 10, pp. 63–70, 1999. Doi:10.1145/317665.317677

Cortes, C. and Vapnik, V. (1995). “Support-Vector Networks,” Machine Learning, vol. 20, no. 3, pp. 273–297, 1995. Doi:10.1007/bf00994018

CPX 360 (2023). “Check Point Software Releases its 2023 Security Report Highlighting Rise in Cyberattacks and Disruptive Malware,” Check Point Software.
<https://www.checkpoint.com/press-releases/check-point-software-releases-its-2023-security-report-highlighting-rise-in-cyberattacks-and-disruptive-malware/>

Devan, P. and Khare, N. (2020). “An efficient xgboost–DNN-based classification model for network Intrusion Detection System,” Neural Computing and Applications, vol. 32, no. 16, pp. 12499–12514, 2020. Doi:10.1007/s00521-020-04708-x

Dhaliwal, S., et. al. (2018). “Effective intrusion detection system using XGBoost,” Information, vol. 9, no. 7, p. 149, 2018. Doi:10.3390/info9070149

Doğan, S., Betin-Can, A. and Garousi, V. (2014). “Web application testing: A systematic literature review,” Journal of Systems and Software, vol. 91, pp. 174–201.
Doi: 10.1016/j.jss.2014.01.010

Ern, A. Y. (2019). “Web Applications,” ResearchGate. DOI: 10.13140/RG.2.2.16545.15207

Feily, M., et. al. (2009). “A Survey of Botnet and Botnet Detection,” 2009. [Online]. Available: <https://doi.org/10.1109/securware.2009.48>.

Flynn, J. (2023). "How Many People Use The Internet? [2023]: 35 Facts About Internet Usage In America And The World." [Online]. Available: <https://www.zippia.com/advice/how-many-people-use-the-internet/#:~:text=There%20are%204.9%20billion%20active,Americans%20currently%20use%20the%20internet>.

Forouzan, B. A. (2007) "Data Communications and Networking. New York: McGraw-Hill Higher Education," in Data Communications and Networking, New York, McGraw-Hill Higher Education. <https://dpviprcollege.in/wp-content/uploads/2023/01/Data-Communications-and-Networking-By-Behrouz-A.Forouzan.pdf>

García-Gonzalo, E., et. al. (2016). "Hard-rock stability analysis for span design in entry-type excavations with learning classifiers," Materials, vol. 9, no. 7, p. 531, 2016. Doi:10.3390/ma9070531

García, S., et. al. (2014). "An empirical comparison of botnet detection methods," Computers & Security, vol. 45, pp. 100–123, 2014. Doi: 10.1016/j.cose.2014.05.011

Gautam, R. and Doegar, E. A. (2018). "An ensemble approach for Intrusion Detection System using machine learning algorithms," 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence). Doi:10.1109/confluence.2018.8442693

Gharib, A. and Ghorbani, A. A. (2015). "A survey of machine learning algorithms for intrusion detection systems." Computers & Security, 49, 60-83.

Gupta, P. (2020). "An efficient classifier for U2R, R2L, Dos Attack," International Journal

- of Recent Technology and Engineering (IJRTE), vol. 9, no. 1, pp. 644–647. Doi:10.35940/ijrte.a1942.059120
- Gupta, S. and Goel, R. (2012). “A graphical user interface framework for detecting intrusions using Bro Ids,” International Journal of Computer Applications, vol. 55, no. 13, pp. 7–12. Doi:10.5120/8813-2409
- Hagar, A. A., & Gawali, D. W. (2022). Deep Learning for Improving Attack Detection System using CSE-CICIDS2018. ResearchGate. DOI:10.14704/nq.2022.20.7.NQ33385
- Haq, S., & Singh, Y. (2018). Botnet detection using machine learning. 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC). <https://doi.org/10.1109/pdgc.2018.8745912>
- Hirsch, P. M. (1995). “Exercise the power of the World Wide Web,” IEEE Computer Applications in Power, vol. 8, no. 3, pp. 25–29,” 1995. [Online]. Available: doi:10.1109/67.392022.
- Ibrahim, N. J. (2023). “IMPROVING THE EFFICIENCY OF BRUTE-FORCE ATTACK DETECTION USING DECISION TREES: AN ANALYSIS STUDY”. Researchgate.net. https://www.researchgate.net/publication/375834787_IMPROVING_THE_EFFICIENCY_OF_BRUTE-FORCE_ATTACK_DETECTION_USING_DECISION TREES_AN_ANALYSIS_STUDY
- Johnson, C. N. et. al. (2016) “Guide to Cyber Threat Information Sharing,” 2016. [Online]. Available: <https://doi.org/10.6028/nist.sp.800-150>.

Kakuru, S. (2011). "Behavior based network traffic analysis tool," 2011 IEEE 3rd International Conference on Communication Software and Networks, 2011.
Doi:10.1109/iccsn.2011.6014810

Kasimov, Y. (2018). " Anomaly detection of host roles in computer networks. Diploma Thesis, Open Informatics, Czech Technical University.," 2018. [Online]. Available: <https://www.stratosphereips.org/thesis-projects-list/2020/4/22/anomaly-detection- of-host-roles-in-computer-networks>.

Khan, M. (2021). "HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system," Processes, vol. 9, no. 5, p. 834.
Doi:10.3390/pr9050834

Kozik, R. (2018). "Distributing Extreme Learning Machines with apache spark for NetFlow- based malware activity detection," Pattern Recognition Letters, vol. 101, pp. 14– 20, 2018. Doi:10.1016/j.patrec.2017.11.004

Kumari, A. and Mehta, A. K. (2020). "A hybrid intrusion detection system based on decision tree and support vector machine," 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA).
Doi:10.1109/iccca49541.2020.9250753

Kyaw, A. K., Chen, Y., and Joseph, J. (2015). "Pi-IDS: evaluation of open-source intrusion detection systems on Raspberry Pi 2," ResearchGate. Available: https://www.researchgate.net/publication/304256574_Pi- IDS_evaluation_of_open-source_intrusion_detection_systems_on_Raspberry_Pi_2.

Liao, H.-J., et. al. (2013). "Intrusion detection system: A comprehensive review," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16–24, 2013. Doi:

10.1016/j.jnca.2012.09.004

Malwarebytes, “Malwarebytes Labs 2020 State of Malware Report,” 2020. [Online].

Available: <https://www.malwarebytes.com/resource/2020-state-of-malware-report>.

Mathews, J., Chatterjee, P., & Banik, S. (2022). CoAP-DoS: An IoT Network Intrusion Data Set. 2022 6th International Conference on Cryptography, Security and Privacy (CSP), 91-95. <https://doi.org/10.1109/CSP55486.2022.00025>

Meng, Y.-X. (2011). “The practice on using machine learning for network anomaly intrusion detection,” 2011 International Conference on Machine Learning and Cybernetics, 2011. Doi:10.1109/icmlc.2011.6016798

Mohammed Salim, M., Rathore, S., & Park, J. (2019). Distributed denial of service attacks and its defenses in IoT: a survey. *The Journal of Supercomputing*, 76, 5320-5363. <https://doi.org/10.1007/s11227-019-02945-z>

Nuttall, B. (2021). “What is a Raspberry Pi?,” Opensource.com. Available: <https://opensource.com/resources/raspberry-pi>.

Olanrewaju, R. F., et. al. (2018). “Snort-based smart and swift intrusion detection system,” Indian Journal of Science and Technology, vol. 11, no. 4, pp. 1–9, 2018. Doi:10.17485/ijst/2018/v11i4/120917

Park, S., et. al (2012). “A Scheme of Access Network Management in Convergence Networks,” Journal of The Korea Society of Computer and Information, vol. 17, no. 11, pp. 93–99,” November 2012. [Online]. Available: <http://journal.kci.go.kr/jksci/archive/articleView?artId=ART001714812>.

- Petrosyan, A. (2023). “Number of internet and social media users worldwide as of April 2023,” 22 May 2023. [Online]. Available: <https://www.statista.com/statistics/617136/digital-population-worldwide/>.
- Pietro, R. D. and Mancini, L. V. (2008). “Intrusion Detection Systems”. New York, New York: Springer Science+Business Media. <https://download.e-bookshelf.de/download/0000/0024/78/L-G-0000002478-0002340950.pdf>
- Piñon, J. C. (2016). “Virtualization | Solutions.” [Online]. Available: [https://www.ids-sl.com/en/solutions/virtualization#:~:text=Virtualization%20is%20the%20technology%20that,same%20machine%20\(physical%20server\).](https://www.ids-sl.com/en/solutions/virtualization#:~:text=Virtualization%20is%20the%20technology%20that,same%20machine%20(physical%20server).)
- Polikar, R. (2006). “Ensemble based systems in decision making,” IEEE Circuits and Systems Magazine, vol. 6, no. 3, pp. 21–45, 2006. Doi:10.1109/mcas.2006.1688199
- Rodda, S. and Shankar, U. (2016). “Class imbalance problem in the Network Intrusion Detection Systems. ResearchGate,” 2016. [Online]. Available: https://www.researchgate.net/publication/311251995_Class_imbalance_problem_in_the_Network_Intrusion_Detection_Systems.
- Rudder, C. (2020). “7 ways to use Raspberry Pi in enterprise IT,” The Enterprisers Project, 2020. Available: <https://enterprisersproject.com/article/2020/11/raspberry-pi-7-enterprise-it-uses>.
- Sachidananda, V., Bhairav, S., & Elovici, Y. (2019). Spill the Beans: Extrospection of Internet of Things by Exploiting Denial of Service. EAI Endorsed Transactions on Security and Safety, 6, e1. <https://doi.org/10.4108/EAI.13-7-2018.159803>

- Scarfone, K. A. and Mell, P. M. (2007). “Guide to intrusion detection and prevention systems (idps),” 2007. Doi:10.6028/nist.sp.800-94
- Shah, Z., Ullah, I., Li, H., Levula, A., & Khurshid, K. (2022). Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. Sensors (Basel, Switzerland), 22, 1094. <https://doi.org/10.3390/s22031094>
- Sharafaldin, I., Lashkari, A. H. and Ghorbani, A. (2018). “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal. <https://api.semanticscholar.org/CorpusID:4707749>
- Sforzin, A., et. al. (2016). “RpiDS: Raspberry Pi IDS — A Fruitful Intrusion Detection System for IoT”. doi: <https://doi.org/10.1109/uic-atc-scalcom-cbdcom-iop-smartworld.2016.0080>. Available: <https://ieeexplore.ieee.org/document/7816876>.
- Stein, M. (2022). “What is a LAN cable? Easily explained,” PATCHBOX – Simplify IT,” 6 July 2022. [Online]. Available: <https://patchbox.com/what-is-a-lan-cable/#:~:text=A%20LAN%20cable%20is%20a>.
- Thakkar, A. and Lohiya, R. (2020). “A Review of the Advancement in Intrusion Detection Datasets,” vol. 167, pp. 636–645, Jan. 2020.
doi: <https://doi.org/10.1016/j.procs.2020.03.330>.
- Tripathi, S. and Kumar, R, (2018). “Raspberry Pi as an Intrusion Detection System, a Honeypot and a Packet Analyzer”,
doi: <https://doi.org/10.1109/ctems.2018.8769135>.

UNB. “CSE-CIC-IDS2018 on AWS”, University of New Brunswick est.1785,
<https://www.unb.ca/cic/datasets/ids-2018.html>

Varma, P., Siddiqui, A., Vadher, P., and Baloda, V., (202). “Snort IDPS using Raspberry Pi 4.” Available: <https://www.ijert.org/research/snort-idps-using-raspberry-pi-4-IJERTV9IS070099.pdf>

Velasco-Mata, J., Gonzalez-Castro, V., Fernandez, E. F., and Alegre, E. (2021). “Efficient detection of botnet traffic by features selection and decision trees,” IEEE Access, vol. 9, pp. 120567–120579. Doi:10.1109/access.2021.3108222

Wang, Y., et. al, (2016). “Research on intrusion detection model using Ensemble Learning Methods,” 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), 2016. Doi:10.1109/icsess.2016.7883100

Wyle, M. F. (1991). “A wide area network information filter,” Proceedings First International Conference on Artificial Intelligence Applications on Wall Street,” [Online]. Available: doi:10.1109/aiaws.1991.236580.

Youssef, A. & Emam, A. (2011). Network Intrusion Detection Using Data Mining and Network Behaviour Analysis. International Journal of Computer Science and Information Technology. 3. 10.5121/ijcsit.2011.3607.

Zwane, S., et. al (2019). “Ensemble learning approach for FLOW-based Intrusion Detection System,” 2019 IEEE AFRICON, 2019. Doi:10.1109/africon46755.2019.9133979

.

APPENDICES

A. Bill of Materials

Table 6.1 Billing of Materials

Item #	Unit	Item Description	Qty	Unit Cost	Total Cost
1	mth.	PythonAnywhere Web Hosting Platform	1	₱ 732	₱ 732
2	pcs	Raspberry Pi 4 model B Package	3	₱ 8,000	₱ 24,000
2	pcs.	Ethernet cable (4 meter per cable)	3	₱ 60	₱ 180
TOTAL AMOUNT					₱ 24,912

B. Codes

a) Raspberry Pi

```

import subprocess
import time
import pandas as pd
from pymongo import MongoClient
import RPi.GPIO as GPIO
import threading
from http.server import BaseHTTPRequestHandler, HTTPServer
from urllib.parse import parse_qs
import os
from bson import ObjectId
import requests
import webbrowser

# GPIO setup
BUTTON_PIN = 17 # GPIO pin for the button
LED_PIN = 18    # GPIO pin for the LED

GPIO.setmode(GPIO.BCM)
GPIO.setup(BUTTON_PIN, GPIO.IN, pull_up_down=GPIO.PUD_UP)
GPIO.setup(LED_PIN, GPIO.OUT)
GPIO.output(LED_PIN, GPIO.HIGH) # Turn on the LED initially

# MongoDB connection setup
mongo_client = MongoClient("mongodb+srv://detech322:mamamg2023@detech.tuz0ow4.mongodb.net/?retryWrites=true&w=majority")
db = mongo_client["De-TECH"] # Replace with your actual database name
collection = db["Raw CSV"] # Replace with your actual collection name

# Event for capturing state
capture_event = threading.Event()

```

```

# Define the initial capturing state
capturing = False

# Specify parameters
network_interface = "eth0"
duration = 180 # seconds

# Function to handle button press
def button_callback(channel):
    global capturing
    if capture_event.is_set():
        print("Stopping packet capture.")
        capturing = False
        capture_event.clear()
        GPIO.output(LED_PIN, GPIO.HIGH) # Turn on the LED (steady state)
    else:
        print("Starting packet capture.")

    capturing = True
    capture_event.set()
    GPIO.output(LED_PIN, GPIO.LOW) # Turn off the LED (blinking)
    # Start capturing and uploading packets in a separate thread
    capture_thread = threading.Thread(target=capture_traffic_and_upload)
    capture_thread.start()

# Set up button callback
GPIO.add_event_detect(BUTTON_PIN, GPIO.FALLING, callback=button_callback, bouncetime=300)

# Function to start or stop packet capture on the Raspberry Pi
def control_capture(start_capture):
    global capturing
    if start_capture:
        if not capture_event.is_set():
            print("Starting packet capture.")
            capturing = True
            capture_event.set()
            GPIO.output(LED_PIN, GPIO.LOW) # Turn off the LED (blinking)

            # Start capturing and uploading packets in a separate thread
            capture_thread = threading.Thread(target=capture_traffic_and_upload)
            capture_thread.start()
    else:
        if capture_event.is_set():
            print("Stopping packet capture.")
            capturing = False
            capture_event.clear()
            GPIO.output(LED_PIN, GPIO.HIGH) # Turn on the LED (steady state)

# Function to handle button press from the web server
def web_button_callback(action):
    if action == 'start':
        control_capture(True)
    elif action == 'stop':
        control_capture(False)

```

```

def upload_to_mongodb(csv_file_path):
    # Read the CSV content
    df = pd.read_csv(csv_file_path)

    # Generate a unique hexadecimal ObjectId
    counter_value = collection.count_documents({})
    unique_id = '2' + format(counter_value, '023x').zfill(23) # Zero-fill to ensure it's 24 characters

    # Insert the CSV data into MongoDB with the unique ObjectId
    result = collection.insert_one({"_id": ObjectId(unique_id), "csv_data": df.to_dict(orient='records')})
        # Call detech Web API to insert file name
    api_url = 'https://detech.pythonanywhere.com/api/saveLatestFileName/' + str(result.inserted_id) + '/33'
    response = requests.get(api_url)

    # Print the inserted _id
    print("Inserted document with _id:", result.inserted_id)

# Function to capture traffic and upload to MongoDB
def capture_traffic_and_upload():
    try:
        while capture_event.is_set():
            # Specify parameters
            current_time = time.localtime()
            csv_filename = f"captured_traffic_{current_time.tm_hour}_{current_time.tm_min}.csv"
            pcap_filename = "captured_traffic.pcap"
            target_ip = ["192.168.1.2", "192.168.1.3", "192.168.1.4"] # Replace with the target IP address

            # Start capturing traffic using tcpdump
            tcpdump_command = f"sudo tcpdump -i {network_interface} -w {pcap_filename} host {' or host 'join(target_ip)}"
            subprocess.Popen(tcpdump_command, shell=True)

            # Blink the LED while capturing
            blink_start_time = time.time()
            while capture_event.is_set() and time.time() - blink_start_time < duration: # Adjust duration as needed
                GPIO.output(LED_PIN, not GPIO.input(LED_PIN)) # Toggle the LED state
                time.sleep(0.5) # Blink interval

            # Stop ettercap
            subprocess.run("sudo pkill -2 ettercap", shell=True)

            # Introduce a delay to allow the pcap file to be finalized
            time.sleep(2)

            # Convert the captured traffic to CSV using cicflowmeter
            cicflowmeter_command = f"cicflowmeter -f {pcap_filename} -c {csv_filename}"
            subprocess.run(cicflowmeter_command, shell=True)

            # Modify CSV header to replace underscores with spaces and capitalize each word
            df = pd.read_csv(csv_filename)

```

```

df.columns = [col.replace('_', ' ') for col in df.columns]
df.to_csv(csv_filename, index=False)

# Upload the CSV file to MongoDB
upload_to_mongodb(csv_filename)

except KeyboardInterrupt:
    print("Capture stopped by user.")
finally:
    GPIO.output(LED_PIN, GPIO.HIGH) # Turn on the LED (steady state)

# Web server setup
host_name = '192.168.1.100' # IP Address of Raspberry Pi
host_port = 8000

class MyServer(BaseHTTPRequestHandler):

    def do_HEAD(self):
        self.send_response(200)
        self.send_header('Content-type', 'text/html')
        self.end_headers()

    def _redirect(self, path):
        self.send_response(303)
        self.send_header('Content-type', 'text/html')
        self.send_header('Location', path)
        self.end_headers()

    def do_GET(self):
        state = "Capturing" if capturing else "Not Capturing"
        html_content = """
<html>
<head>
<link href="https://fonts.googleapis.com/css2?family=Poppins:wght@400;700&display=swap" rel="stylesheet">
<script src="https://code.jquery.com/jquery-3.6.4.min.js"></script>
</head>
<body style="background-color: #162938; color: #fff; font-family: 'Poppins', sans-serif; display: flex; flex-direction: column; align-items: center; justify-content: center; width: 100%; height: 100vh;">
<h1 style="font-size: 5em;">De-TECH</h1>
<p id="remoteState"></p>
<p>Capturing State: </p><p id="capturingState">"" + str(capturing) + "</p>
<form action="/" method="POST" style="display: flex; flex-direction: column; align-items: center; width: 50%;">
    <input type="submit" name="submit" id="btnStartCapture" value="Start Capture" style="background-color: #2382BC; color: #fff; padding: 20px; border: 2px solid black; cursor: pointer; border-radius: 10px; margin-bottom: 10px; width: 100%; font-size: 1.5em; font-weight: bold;">
        <input type="submit" name="submit" id="btnStopCapture" value="Stop Capture" disabled style="background-color: #01C063; color: #fff; padding: 20px; border: 2px solid black; cursor: not-allowed; border-radius: 10px; margin-bottom: 10px; width: 100%; font-size: 1.5em; font-weight: bold;">
</form>
"""
        self.end_headers()
        self.wfile.write(html_content.encode())

```

```

<script>
    console.log("test123");
    $(document).ready(function() {
        var timerInterval = setInterval(function() {
            getDataCapture();
        }, 1000);
    });

    let getDataCapture = function () {
        $.ajax({
            url: "https://detech.pythonanywhere.com/api/getCaptureState/33",
            type: "GET",
            async: false,
            success: function (response)
            {
                $("#remoteState").html("Current State: " + (response.switchid == 1 ? "ON" : "OFF"));

                let capturing = $("#capturingState").html();

                if(capturing == "False") {
                    $("#btnStartCapture").prop("disabled", false);
                    $("#btnStopCapture").prop("disabled", true);

                    if(response.switchid == 1)
                    {
                        $("#capturingState").html("True");
                        $("#btnStartCapture").click();
                    }
                }
                else
                {
                    $("#btnStartCapture").prop("disabled", true);
                    $("#btnStopCapture").prop("disabled", false);

                    if(response.switchid == 0)
                    {
                        $("#capturingState").html("False");
                        $("#btnStopCapture").click();
                    }
                }
            },
            error: function (error)
            {
                console.log(error);
            }
        });
    }
</script>
</body>
</html>
"""

```

```

        self.do_HEAD()
        self.wfile.write(html_content.encode('utf-8'))

    def do_POST(self):
        content_length = int(self.headers['Content-Length'])
        post_data = self.rfile.read(content_length).decode("utf-8")
        post_data = parse_qs(post_data)['submit'][0]

        if post_data == 'Start Capture':
            web_button_callback('start')
        elif post_data == 'Stop Capture':
            web_button_callback('stop')

        self._redirect('/')

    if __name__ == '__main__':
        try:
            print("Waiting for button press to start/stop packet capture.")

            # Open the default web browser with the specified URL
            url_to_open = f"http://{{host_name}}:{{host_port}}"
            webbrowser.open(url_to_open)

            # Web server setup
            http_server = HTTPServer((host_name, host_port), MyServer)
            print(f"Web server Starts - {{host_name}}:{{host_port}}")

            while True:
                http_server.handle_request() # Handle web server requests
                time.sleep(1) # Keep the main script running

            except KeyboardInterrupt:
                print("Script stopped by user.")
                GPIO.cleanup() # Clean up GPIO on KeyboardInterrupt

```

b) Machine Learning Model Training

```

import os
import pandas as pd
import seaborn as sns
import matplotlib.pyplot as plt
from sklearn.preprocessing import StandardScaler
from sklearn.tree import DecisionTreeClassifier
from sklearn.metrics import precision_recall_fscore_support, classification_report, confusion_matrix
from sklearn.preprocessing import LabelEncoder
from sklearn import tree
import joblib
import pickle
from sklearn.naive_bayes import GaussianNB
from joblib import load
import numpy as np
from tensorflow.keras.models import load_model
import tensorflow as tf

```

```

# Preparation
import pandas as pd

def data_preparation(csv, file_name):
    # Read the CSV file into a pandas DataFrame
    df = pd.read_csv(csv)

    # Check for NaN values
    nan_counts = df.isnull().sum().sum()

    if nan_counts > 0:
        print(f"File '{file_name}' has {nan_counts} NaN values. Filling with 0 and saving...")
        # Fill NaN values with 0
        df_filled = df.fillna(0)
    else:
        df_filled = df # If no NaN values, keep original DataFrame

    # Check for NaN values again
    nan_counts = df_filled.isnull().sum().sum()
    if nan_counts > 0:
        print(f"File '{file_name}' still has {nan_counts} NaN values.")
    else:
        print(f"File '{file_name}' has no NaN values.")

    df = df_filled

    # Identify duplicate rows, keeping the first occurrence
    duplicate_mask = df.duplicated(keep='first')
    duplicate_count = duplicate_mask.sum()
    print(f"Number of duplicate rows (excluding the first occurrence): {duplicate_count}")

    # Filter and keep only unique rows
    df = df[~duplicate_mask]
    print("Preprocessed data")

    # Define your label mappings
    label_mappings = {
        'Normal': 0,
        'Denial of Service': 1,
        'Bruteforce': 2,
        'Botnet': 3,
        'Botnet_ctu': 3,
        'Infiltration': 4,
    }

    # Relabel the 'label' column
    df['label_no'] = df['label'].map(label_mappings)
    print('Label encoded')

    label_counts = df['label_no'].value_counts()
    print(label_counts)

```

```

return df

# Normalization
def normalize_for_detection(prepped_csv):
    df = prepped_csv.copy()

    # Define the list of important features
    important_features_list = ['dst port','tot fwd pkts','tot bwd pkts','totlen fwd pkts','totlen bwd pkts','fwd pkt len mean','bwd pkt len max','fwd iat mean','flow iat max','flow iat min','fwd iat std','bwd iat mean','bwd iat std','bwd iat max','bwd iat min','fwd header len','bwd header len','fwd pkts s','bwd pkts s','pkt len mean','pkt len var','fwd seg size avg','bwd seg size avg','init fwd win byts','init bwd win byts','label_no']

    # Select the important features
    csv_data = df[important_features_list]

    # Convert columns to numeric (coerce errors to NaN)
    csv_data = csv_data.apply(pd.to_numeric, errors='coerce')

    # Replace NaN values with 0
    csv_data.fillna(0, inplace=True)

    # Replace infinite values with a very large finite number
    csv_data.replace([np.inf, -np.inf], np.nan, inplace=True)
    csv_data.fillna(1e9, inplace=True)

    # Separate categorical columns
    categorical_cols = ['dst port','label_no']
    df_categorical = csv_data[categorical_cols]
    df_numerical = csv_data.drop(columns=categorical_cols)

    # Normalize the numerical features using StandardScaler
    scaler = StandardScaler()
    df_numerical_scaled = pd.DataFrame(scaler.fit_transform(df_numerical),
                                         columns=df_numerical.columns)

    # Concatenate the numerical and categorical features
    df_normalized = pd.concat([df_numerical_scaled, df_categorical.reset_index(drop=True)], axis=1)
    df_normalized = df_normalized[important_features_list]

    return df_normalized

# Training and Testing Data
# TRAIN DATA
csv1 = '/content/drive/MyDrive/A5_De-TECH/50:50/Training Data/5050_reduced_training-file.csv'
file_name1 = 'Train Data'
# TEST DATA
csv2 = '/content/drive/MyDrive/A5_De-TECH/50:50/Training Data/5050_Train Data_14.csv'
file_name2 = 'Validation Data'
# Load the CSV file into a pandas DataFrame
df = pd.read_csv(csv1)
print(df.head())

```

```

train_df_prep = data_preparation(csv1,file_name1)
normalized_train_df = normalize_for_detection(train_df_prep)
val_df_prep = data_preparation(csv2,file_name2)
normalized_val_df = normalize_for_detection(val_df_prep)

X = normalized_train_df
Y = normalized_val_df

label_counts = normalized_train_df['label_no'].value_counts()
label_counts
X_counts = X['label_no'].value_counts()
X_counts

# Training data
X_train_2 = X.drop(columns='label_no', axis=1).values
y_train_2 = X['label_no'].values.ravel()
print("X_train=",X_train_2)
print("y_train=",y_train_2)

# Testing data
X_test_2 = Y.drop(columns='label_no', axis=1).values
y_test_2 = Y['label_no'].values.ravel()
print("X_test=",X_test_2)
print("y_test=",y_test_2)

# Decision Tree
dt_2 = tree.DecisionTreeClassifier(criterion='entropy', random_state=0)

dt_2.fit(X_train_2, y_train_2)

# Specify the path in Google Drive where you want to save the model
model_path_2 = '/content/drive/My Drive/A5_De-TECH/new26-DT_model.pkl'

joblib.dump(dt_2, model_path_2)

print(f'Model saved to {model_path_2}')

accuracy = accuracy_score(y_test_2, y_predict)
precision = precision_score(y_test_2, y_predict, average='weighted') # Use 'weighted' for multiclass
recall = recall_score(y_test_2, y_predict, average='weighted') # Use 'weighted' for multiclass
f1 = f1_score(y_test_2, y_predict, average='weighted') # Use 'weighted' for multiclass

# Generate confusion matrix
cm = confusion_matrix(y_test_2, y_predict)

# Extract TP, FP, FN, TN from confusion matrix
tp, fp, fn, tn = cm[1, 1], cm[0, 1], cm[1, 0], cm[0, 0]

# Print metrics
print("Metrics:")

```

```

print(f"Accuracy: {accuracy:.4f}")
print(f"Precision: {precision:.4f}")
print(f"Recall: {recall:.4f}")
print(f"F1 Score: {f1:.4f}")
print(f"True Positive (TP): {tp}")
print(f"True Negative (TN): {tn}")
print(f"False Positive (FP): {fp}")
print(f"False Negative (FN): {fn}")

# Create a DataFrame for the heatmap
heatmap_data = pd.DataFrame([[tp, fp], [fn, tn]], index=['Actual Positive', 'Actual Negative'],
columns=['Predicted Positive', 'Predicted Negative'])

# Plot the heatmap for TP, FP, FN, TN
plt.figure(figsize=(8, 6))
sns.heatmap(heatmap_data, annot=True, fmt="d", cmap="Blues", cbar=False)
plt.title('Decision Tree Confusion Matrix Heatmap')
plt.show()

# Naïve Bayes
nb_2 = GaussianNB()

nb_2.fit(X_train_2, y_train_2)

# Specify the path in Google Drive where you want to save the model
model_path_2 = '/content/drive/My Drive/A5_De-TECH/new26-NB_model.pkl'

joblib.dump(nb_2, model_path_2)

print(f'Model saved to {model_path_2}')

y_predict_2 = nb_2.predict(X_test_2)

accuracy_2 = accuracy_score(y_test_2, y_predict_2)
precision_2 = precision_score(y_test_2, y_predict_2, average='weighted') # Use 'weighted' for multiclass
recall_2 = recall_score(y_test_2, y_predict_2, average='weighted') # Use 'weighted' for multiclass
f1_2 = f1_score(y_test_2, y_predict_2, average='weighted') # Use 'weighted' for multiclass

# Generate confusion matrix
cm_2 = confusion_matrix(y_test_2, y_predict_2)

# Extract TP, FP, FN, TN from confusion matrix
tp_2, fp_2, fn_2, tn_2 = cm_2[1, 1], cm_2[0, 1], cm_2[1, 0], cm_2[0, 0]

# Print metrics
print("Metrics:")
print(f"Accuracy: {accuracy_2:.4f}")
print(f"Precision: {precision_2:.4f}")
print(f"Recall: {recall_2:.4f}")
print(f"F1 Score: {f1_2:.4f}")
print(f"True Positive (TP): {tp_2}")
print(f"True Negative (TN): {tn_2}")

```

```

print(f"False Positive (FP): {fp_2}")
print(f"False Negative (FN): {fn_2}")

# Create a DataFrame for the heatmap
heatmap_data = pd.DataFrame([[tp_2, fp_2], [fn_2, tn_2]], index=['Actual Positive', 'Actual Negative'],
columns=['Predicted Positive', 'Predicted Negative'])

# Plot the heatmap for TP, FP, FN, TN
plt.figure(figsize=(8, 6))
sns.heatmap(heatmap_data, annot=True, fmt="d", cmap="Blues", cbar=False)
plt.title('Naive Bayes Confusion Matrix Heatmap')
plt.show()

# SVM

# Assuming X_train_2 and y_train_2 are your features and labels respectively
X = X_train_2
y = y_train_2

# Convert numpy arrays to TensorFlow tensors
X_tensor = tf.convert_to_tensor(X, dtype=tf.float32)
y_encoded_tensor = tf.convert_to_tensor(y, dtype=tf.int32)

# Check GPU availability
physical_devices = tf.config.list_physical_devices('GPU')
if not physical_devices:
    print("GPU not available. Make sure you have selected GPU as the hardware accelerator in Colab.")
else:
    print("GPU is available. Training on GPU.")

# Adjust the Sequential model for multi-class classification
svm_model = tf.keras.Sequential([
    tf.keras.layers.Input(shape=(X.shape[1],)),
    tf.keras.layers.Dense(5, activation='softmax') # Output layer for 5 classes
])

# Compile the model for multi-class classification
svm_model.compile(optimizer='adam',
                   loss='sparse_categorical_crossentropy', # Suitable for integer-encoded targets
                   metrics=['accuracy'])

# Train the model
svm_model.fit(X_tensor, y_encoded_tensor, epochs=10, batch_size=32)

# Save the trained model
svm_model.save('new26_svm_model.h5')

X_test = X_test_2
y_test = y_test_2

# Make predictions on the test data

```

```

svm_predictions = svm_model.predict(X_test)
svm_predictions = np.argmax(svm_predictions, axis=1)

# Evaluate the performance using scikit-learn metrics
accuracy = accuracy_score(y_test, svm_predictions)
precision = precision_score(y_test, svm_predictions, average='weighted')
recall = recall_score(y_test, svm_predictions, average='weighted')
f1 = f1_score(y_test, svm_predictions, average='weighted')

# Generate confusion matrix
cm = confusion_matrix(y_test, svm_predictions)

# Extract TP, FP, FN, TN from confusion matrix
tp, fp, fn, tn = cm[1, 1], cm[0, 1], cm[1, 0], cm[0, 0]

# Print metrics
print("Metrics:")
print(f"Accuracy: {accuracy:.4f}")
print(f"Precision: {precision:.4f}")
print(f"Recall: {recall:.4f}")
print(f"F1 Score: {f1:.4f}")
print(f"True Positive (TP): {tp}")
print(f"True Negative (TN): {tn}")
print(f"False Positive (FP): {fp}")
print(f"False Negative (FN): {fn}")

# Create a DataFrame for the heatmap
heatmap_data = pd.DataFrame([[tp, fp], [fn, tn]], index=['Actual Positive', 'Actual Negative'],
columns=['Predicted Positive', 'Predicted Negative'])

# Plot the heatmap for TP, FP, FN, TN
plt.figure(figsize=(8, 6))
sns.heatmap(heatmap_data, annot=True, fmt="d", cmap="Blues", cbar=False)
plt.title('SVM Confusion Matrix Heatmap')
plt.show()

# Ensemble (XGBoost)
def svm_predict(csv_data_detect):

    data = csv_data_detect

    #current_directory = os.path.dirname(os.path.abspath(__file__))
    #svm_model_path = os.path.join(current_directory, "binary_svmmmodel.h5")
    #svm_model = tf.keras.models.load_model(svm_model_path)
    #svm_model = tf.keras.models.load_model('new26_svm_model.h5')

    svm_predictions_raw = svm_model.predict(data)
    svm_threshold = 0.5 # Set your desired threshold
    svm_predictions = np.where(svm_predictions_raw >= svm_threshold, 1, 0)

    return svm_predictions

```

```

def nb_predict(csv_data_detect):
    data = csv_data_detect

    #current_directory = os.path.dirname(os.path.abspath(__file__))
    #nb_model_path = os.path.join(current_directory, "binary_nbmodel.pkl")
    #nb_model = joblib.load(nb_model_path)
    nb_model = joblib.load('/content/drive/MyDrive/A5_De-TECH/new26-NB_model.pkl')

    nb_predictions = nb_model.predict(data)

    label_encoder = LabelEncoder()
    nb_predictions_numeric = label_encoder.fit_transform(nb_predictions)

    return nb_predictions_numeric

def dt_predict(csv_data_detect):
    data = csv_data_detect

    #current_directory = os.path.dirname(os.path.abspath(__file__))
    #dt_model_path = os.path.join(current_directory, "binary_dtmodel.pkl")
    #dt_model = joblib.load(dt_model_path)
    dt_model = joblib.load('/content/drive/MyDrive/A5_De-TECH/new26-DT_model.pkl')

    dt_predictions = dt_model.predict(data)

    return dt_predictions

csv_data_detect = X_train_2
svm_data = svm_predict(csv_data_detect)
nb_data = nb_predict(csv_data_detect)
dt_data = dt_predict(csv_data_detect)

stacked_predictions_1 = np.column_stack((svm_data, nb_data, dt_data))

import xgboost as xgb
import joblib

# Assuming y_test_svm contains integer labels for multiple classes
num_classes = 5 # Determine the number of unique classes

xgb_model = xgb.XGBClassifier(objective="multi:softmax", # Use multi:softmax for multi-class
                                classification
                                num_class=num_classes, # Specify the number of classes
                                random_state=42)

# Train the XGBoost model on the stacked predictions
xgb_model.fit(stacked_predictions_1, y_train_2) # Use y_test_svm as the target

# Ensure feature names consistency (This step is usually not necessary for XGBoost models trained with
numpy arrays)

```

```

feature_names = [str(i) for i in range(stacked_predictions_1.shape[1])]
xgb_model.feature_names = feature_names

# Make predictions using the ensemble model
ensemble_predictions = xgb_model.predict(stacked_predictions_1)

# Save the trained ensemble model
ensemble_model_path = 'new26-Ensemble_model_multi_class.pkl'
joblib.dump(xgb_model, ensemble_model_path)

print("Multi-class ensemble model saved successfully.")

def ensemble_predict(svm_predict, nb_predict, dt_predict):

    xgb_model = joblib.load('/content/drive/MyDrive/A5_De-TECH/35-Ensemble_model.pkl')

    stacked_predictions = np.column_stack((svm_predict, nb_predict, dt_predict))

    predictions = xgb_model.predict(stacked_predictions)

    return predictions

csv_data_test = X_test_2
svm_data = svm_predict(csv_data_test)
nb_data = nb_predict(csv_data_test)
dt_data = dt_predict(csv_data_test)

stacked_predictions_2 = np.column_stack((svm_data, nb_data, dt_data))

ensemble_prediction = xgb_model.predict(stacked_predictions_2)

print("Shape of stacked_predictions_1:", stacked_predictions_1.shape)
print("Shape of y_test_2:", y_test_2.shape)

stacked_predictions_2

# Evaluate the performance of the ensemble model
accuracy = accuracy_score(y_test_2, ensemble_prediction)
precision = precision_score(y_test_2, ensemble_prediction, average='weighted')
recall = recall_score(y_test_2, ensemble_prediction, average='weighted')
f1 = f1_score(y_test_2, ensemble_prediction, average='weighted')

print(f'Ensemble Model Metrics:')
print(f'Accuracy: {accuracy}')
print(f'Precision: {precision}')
print(f'Recall: {recall}')
print(f'F1 Score: {f1}')

# Confusion Matrix
conf_matrix = confusion_matrix(y_test_2, ensemble_prediction)
print('\nConfusion Matrix:')
print(conf_matrix)

```

```

# Create a heatmap for the confusion matrix
plt.figure(figsize=(10, 8))
sns.heatmap(conf_matrix, annot=True, fmt='d', cmap='Blues', cbar=False)
plt.xlabel('Predicted labels')
plt.ylabel('True labels')
plt.title('Confusion Matrix Heatmap')
plt.show()

# MODEL TRAINING (HYPERTUNED)
# Decision Tree
import pandas as pd
import numpy as np
from sklearn.preprocessing import LabelEncoder, StandardScaler
from sklearn.tree import DecisionTreeClassifier
from sklearn.metrics import accuracy_score, classification_report, confusion_matrix
from skopt import gp_minimize
from skopt.space import Integer
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score, confusion_matrix
import seaborn as sns
import matplotlib.pyplot as plt

# Define label renaming mappings
label_renaming = {
    'Malicious': 'Denial of Service',
    'SQL Injection': 'Infiltration'
}

# Define your label mappings
label_mappings = {
    'Normal': 0,
    'Denial of Service': 1,
    'Bruteforce': 2,
    'Botnet': 3,
    'Botnet_ctu': 3,
    'Infiltration': 4,
}

# Load training dataset
train_df = pd.read_csv('/content/drive/MyDrive/A5_De-TECH/50:50/Training Data/5050_reduced_training-file.csv')

# Load validation dataset
valid_df = pd.read_csv('/content/drive/MyDrive/A5_De-TECH/50:50/Training Data/5050_Train Data_14.csv')

# Define selected features
selected_features = ['dst port', 'tot fwd pkts', 'tot bwd pkts', 'totlen fwd pkts', 'totlen bwd pkts', 'fwd pkt len mean', 'bwd pkt len max', 'fwd iat mean', 'flow iat max', 'flow iat min', 'fwd iat std', 'bwd iat mean', 'bwd iat std', 'bwd iat max', 'bwd iat min', 'fwd header len', 'bwd header len', 'fwd pkts s', 'bwd pkts s', 'pkt len mean', 'pkt len var', 'fwd seg size avg', 'bwd seg size avg', 'init fwd win byts', 'init bwd win byts']

```

```

# Select only the desired features
train_df = train_df[selected_features + ['label']]
valid_df = valid_df[selected_features + ['label']]

# Define features and target variables
X_train = train_df[selected_features]
y_train = train_df['label']

X_valid = valid_df[selected_features]
y_valid = valid_df['label']

# Replace infinite values with a very large finite number
X_train.replace([np.inf, -np.inf], np.nan, inplace=True)
X_valid.replace([np.inf, -np.inf], np.nan, inplace=True)
X_train.fillna(1e9, inplace=True)
X_valid.fillna(1e9, inplace=True)

# Rename labels under the 'label_2' column
y_train = y_train.replace(label_renaming)
y_valid = y_valid.replace(label_renaming)

# Convert string labels to integers using LabelEncoder
label_encoder = LabelEncoder()
y_train_encoded = label_encoder.fit_transform(y_train)
y_valid_encoded = label_encoder.transform(y_valid)

# Map string labels to numerical values using label mappings
y_train_encoded = [label_mappings.get(label, -1) for label in y_train]
y_valid_encoded = [label_mappings.get(label, -1) for label in y_valid]

# Normalize the numerical features excluding 'dst port' and 'protocol' using StandardScaler
scaler = StandardScaler()

# Exclude 'dst port' and 'protocol' from both training and validation data
X_train_for_scaling = X_train.drop(['dst port'], axis=1)
X_valid_for_scaling = X_valid.drop(['dst port'], axis=1)

# Fit StandardScaler only on the training data
scaler.fit(X_train_for_scaling)

# Transform both training and validation data using the fitted scaler
X_train_normalized = X_train.copy()
X_train_normalized[X_train_for_scaling.columns] = scaler.transform(X_train_for_scaling)

X_valid_normalized = X_valid.copy()
X_valid_normalized[X_valid_for_scaling.columns] = scaler.transform(X_valid_for_scaling)

# Define the parameter space
space = [Integer(3, 20, name='max_depth'),
         Integer(2, 100, name='min_samples_split'),
         Integer(1, 100, name='min_samples_leaf')]

```

```

# Define the evaluation function
def evaluate_model(params):
    max_depth, min_samples_split, min_samples_leaf = params

    # Create and train the decision tree model
    model = DecisionTreeClassifier(max_depth=max_depth, min_samples_split=min_samples_split,
                                    min_samples_leaf=min_samples_leaf)
    model.fit(X_train_normalized, y_train_encoded)

    # Predict on the validation set and calculate metrics
    y_pred = model.predict(X_valid_normalized)
    accuracy = accuracy_score(y_valid_encoded, y_pred)
    precision = precision_score(y_valid_encoded, y_pred, average='weighted')
    recall = recall_score(y_valid_encoded, y_pred, average='weighted')
    f1 = f1_score(y_valid_encoded, y_pred, average='weighted')

    # Return negative accuracy (to minimize)
    return -accuracy

# Run optimization
res = gp_minimize(evaluate_model, space, n_calls=20, random_state=42)

# Retrieve best hyperparameters
best_params = res.x
print("Best hyperparameters:", best_params)

# Fit the model with the best hyperparameters on the entire dataset
best_model = DecisionTreeClassifier(max_depth=best_params[0], min_samples_split=best_params[1],
                                    min_samples_leaf=best_params[2])
best_model.fit(X_train_normalized, y_train_encoded)

# Evaluate performance on the validation set
y_pred = best_model.predict(X_valid_normalized)
accuracy = accuracy_score(y_valid_encoded, y_pred)
precision = precision_score(y_valid_encoded, y_pred, average='weighted')
recall = recall_score(y_valid_encoded, y_pred, average='weighted')
f1 = f1_score(y_valid_encoded, y_pred, average='weighted')

print("Final Evaluation Metrics:")
print("Validation Accuracy:", accuracy)
print("Precision:", precision)
print("Recall:", recall)
print("F1 Score:", f1)

# Plot confusion matrix
conf_matrix = confusion_matrix(y_valid_encoded, y_pred)
plt.figure(figsize=(8, 6))
sns.heatmap(conf_matrix, annot=True, fmt='d', cmap="Blues")
plt.xlabel('Predicted labels')
plt.ylabel('True labels')
plt.title('Confusion Matrix')

```

```

plt.show()

from joblib import dump

# Specify the path in Google Drive where you want to save the model
model_path = '/content/drive/My Drive/A5_De-TECH/new26-model-hypertuned-DT_model.pkl'

# Save the trained model to the specified path
dump(best_model, model_path)

print(f'Model saved to {model_path}')

# Naïve Bayes
import pandas as pd
import numpy as np
from sklearn.preprocessing import LabelEncoder, StandardScaler
from sklearn.naive_bayes import GaussianNB
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score, classification_report, confusion_matrix
from skopt import gp_minimize
from skopt.space import Real
import seaborn as sns
import matplotlib.pyplot as plt

# Define label renaming mappings
label_renaming = {
    'Malicious': 'Denial of Service',
    'SQL Injection': 'Infiltration'
}

# Define your label mappings
label_mappings = {
    'Normal': 0,
    'Denial of Service': 1,
    'Bruteforce': 2,
    'Botnet': 3,
    'Botnet_ctu': 3,
    'Infiltration': 4,
}

# Load training dataset
train_df = pd.read_csv('/content/drive/MyDrive/A5_De-TECH/50:50/Training Data/5050_reduced_training-file.csv')

# Load validation dataset
valid_df = pd.read_csv('/content/drive/MyDrive/A5_De-TECH/50:50/Training Data/5050_Train Data_14.csv')

# Apply label renaming to the training and validation datasets
train_df['label'] = train_df['label'].map(label_renaming).fillna(train_df['label'])
valid_df['label'] = valid_df['label'].map(label_renaming).fillna(valid_df['label'])

```

```

# Define selected features
selected_features = ['dst port','tot fwd pkts','tot bwd pkts','totlen fwd pkts','totlen bwd pkts','fwd pkt len mean','bwd pkt len max','fwd iat mean','flow iat max','flow iat min','fwd iat std','bwd iat mean','bwd iat std','bwd iat max','bwd iat min','fwd header len','bwd header len','fwd pkts s','bwd pkts s','pkt len mean','pkt len var','fwd seg size avg','bwd seg size avg','init fwd win byts','init bwd win byts']

# Select only the desired features
train_df = train_df[selected_features + ['label']]
valid_df = valid_df[selected_features + ['label']]

# Define features and target variables
X_train = train_df[selected_features]
y_train = train_df['label']

X_valid = valid_df[selected_features]
y_valid = valid_df['label']

# Replace infinite values with a very large finite number
X_train.replace([np.inf, -np.inf], np.nan, inplace=True)
X_valid.replace([np.inf, -np.inf], np.nan, inplace=True)
X_train.fillna(1e9, inplace=True)
X_valid.fillna(1e9, inplace=True)

# Convert string labels to integers using LabelEncoder
label_encoder = LabelEncoder()
y_train_encoded = label_encoder.fit_transform(y_train)
y_valid_encoded = label_encoder.transform(y_valid)

# Normalize the numerical features excluding 'dst port' and 'protocol' using StandardScaler
scaler = StandardScaler()

# Exclude 'dst port' and 'protocol' from both training and validation data
X_train_for_scaling = X_train.drop(['dst port'], axis=1)
X_valid_for_scaling = X_valid.drop(['dst port'], axis=1)

# Fit StandardScaler only on the training data
scaler.fit(X_train_for_scaling)

# Transform both training and validation data using the fitted scaler
X_train_normalized = X_train.copy()
X_train_normalized[X_train_for_scaling.columns] = scaler.transform(X_train_for_scaling)

X_valid_normalized = X_valid.copy()
X_valid_normalized[X_valid_for_scaling.columns] = scaler.transform(X_valid_for_scaling)

# Define the parameter space for Naive Bayes
space = [Real(1e-9, 1e-1, name='var_smoothing')] # var_smoothing is a parameter of GaussianNB

# Define the evaluation function
def evaluate_model(params):
    var_smoothing = params[0]

```

```

# Create and train the Gaussian Naive Bayes model
model = GaussianNB(var_smoothing=var_smoothing)
model.fit(X_train_normalized, y_train_encoded)

# Predict on the validation set and calculate accuracy
y_pred = model.predict(X_valid_normalized)
accuracy = accuracy_score(y_valid_encoded, y_pred)

# Return negative accuracy (to minimize)
return -accuracy

# Run optimization
res = gp_minimize(evaluate_model, space, n_calls=20, random_state=42)

# Retrieve best hyperparameters
best_params = res.x
print("Best hyperparameters:", best_params)

# Create and train the final model using the best hyperparameters
final_model = GaussianNB(var_smoothing=best_params[0])
final_model.fit(X_train_normalized, y_train_encoded)

# Evaluate performance on the validation set
y_pred = final_model.predict(X_valid_normalized)
accuracy = accuracy_score(y_valid_encoded, y_pred)
precision = precision_score(y_valid_encoded, y_pred, average='weighted')
recall = recall_score(y_valid_encoded, y_pred, average='weighted')
f1 = f1_score(y_valid_encoded, y_pred, average='weighted')

print("Final Evaluation Metrics:")
print("Validation Accuracy:", accuracy)
print("Precision:", precision)
print("Recall:", recall)
print("F1 Score:", f1)

# Plot confusion matrix
conf_matrix = confusion_matrix(y_valid_encoded, y_pred)
plt.figure(figsize=(8, 6))
sns.heatmap(conf_matrix, annot=True, fmt='d', cmap="Blues")
plt.xlabel('Predicted labels')
plt.ylabel('True labels')
plt.title('Confusion Matrix')
plt.show()

from joblib import dump

# Specify the path where you want to save the model
model_path = '/content/drive/My Drive/A5_De-TECH/new26-model-hypertuned-NB_model.pkl'

# Save the trained model to the specified path
dump(final_model, model_path)

```

```

print(f'Model saved to {model_path}')

# SVM
import pandas as pd
import numpy as np
from sklearn.preprocessing import LabelEncoder, StandardScaler
import tensorflow as tf

# Define label renaming mappings
label_renaming = {
    'Malicious': 'Denial of Service',
    'SQL Injection': 'Infiltration'
}

# Define your label mappings
label_mappings = {
    'Normal': 0,
    'Denial of Service': 1,
    'Bruteforce': 2,
    'Botnet': 3,
    'Botnet_ctu': 3,
    'Infiltration': 4,
}

# Read the training CSV file
train_file_path = '/content/drive/MyDrive/A5_De-TECH/50:50/Training Data/5050_reduced_training-file.csv'
train_df = pd.read_csv(train_file_path)

# Apply label renaming to the training dataset
train_df['label'] = train_df['label'].map(label_renaming).fillna(train_df['label'])

# Read the validation CSV file
valid_file_path = '/content/drive/MyDrive/A5_De-TECH/50:50/Training Data/5050_Train Data_14.csv'
valid_df = pd.read_csv(valid_file_path)

# Apply label renaming to the validation dataset
valid_df['label'] = valid_df['label'].map(label_renaming).fillna(valid_df['label'])

# Define selected features
selected_features = ['dst port','tot fwd pkts','tot bwd pkts','totlen fwd pkts','totlen bwd pkts','fwd pkt len mean','bwd pkt len max','fwd iat mean','flow iat max','flow iat min','fwd iat std','bwd iat mean','bwd iat std','bwd iat max','bwd iat min','fwd header len','bwd header len','fwd pkts s','bwd pkts s','pkt len mean','pkt len var','fwd seg size avg','bwd seg size avg','init fwd win byts','init bwd win byts']

# Select features and target variables for training and validation datasets
X_train = train_df[selected_features]
y_train = train_df['label']
X_valid = valid_df[selected_features]
y_valid = valid_df['label']

# Replace infinite values with a very large finite number

```

```

X_train.replace([np.inf, -np.inf], np.nan, inplace=True)
X_valid.replace([np.inf, -np.inf], np.nan, inplace=True)
X_train.fillna(1e9, inplace=True)
X_valid.fillna(1e9, inplace=True)

# Convert string labels to integers using LabelEncoder
label_encoder = LabelEncoder()
y_train_encoded = label_encoder.fit_transform(y_train)
y_valid_encoded = label_encoder.transform(y_valid)

# Transform integer labels based on label mappings
y_train_encoded_mapped = np.array([label_mappings[label] for label in y_train])
y_valid_encoded_mapped = np.array([label_mappings[label] for label in y_valid])

# Get the number of classes
num_classes = len(set(label_mappings.values()))
print("Number of classes:", num_classes)

# Normalize the numerical features excluding 'dst port' and 'protocol' using StandardScaler
scaler = StandardScaler()
scaler.fit(X_train)
X_train_normalized = scaler.transform(X_train)
X_valid_normalized = scaler.transform(X_valid)

# Create TensorFlow datasets
train_dataset = tf.data.Dataset.from_tensor_slices((X_train_normalized, y_train_encoded_mapped))
valid_dataset = tf.data.Dataset.from_tensor_slices((X_valid_normalized, y_valid_encoded_mapped))

# Shuffle and batch the datasets
BATCH_SIZE = 32
train_dataset = train_dataset.shuffle(buffer_size=len(X_train_normalized)).batch(BATCH_SIZE)
valid_dataset = valid_dataset.batch(BATCH_SIZE)

# Check GPU availability
physical_devices = tf.config.list_physical_devices('GPU')
if not physical_devices:
    print("GPU not available. Make sure you have selected GPU as the hardware accelerator in Colab.")
else:
    print("GPU is available. Training on GPU.")

# Adjust the Sequential model for multi-class classification
svm_model = tf.keras.Sequential([
    tf.keras.layers.Input(shape=(len(selected_features),)),
    tf.keras.layers.Dense(num_classes, activation='softmax') # Output layer for the number of classes
])

# Compile the model for multi-class classification
svm_model.compile(optimizer='adam',
                   loss='sparse_categorical_crossentropy', # Suitable for integer-encoded targets
                   metrics=['accuracy'])

```

```

# Train the model
history = svm_model.fit(train_dataset, epochs=10, validation_data=valid_dataset)

import numpy as np
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score, confusion_matrix
import matplotlib.pyplot as plt
import seaborn as sns

# Evaluate the model on the validation set
y_valid_pred = np.argmax(svm_model.predict(X_valid_normalized), axis=-1)

# Compute evaluation metrics
accuracy = accuracy_score(y_valid_encoded_mapped, y_valid_pred)
precision = precision_score(y_valid_encoded_mapped, y_valid_pred, average='weighted')
recall = recall_score(y_valid_encoded_mapped, y_valid_pred, average='weighted')
f1 = f1_score(y_valid_encoded_mapped, y_valid_pred, average='weighted')
conf_matrix = confusion_matrix(y_valid_encoded_mapped, y_valid_pred)

print("Accuracy:", accuracy)
print("Precision:", precision)
print("Recall:", recall)
print("F1-score:", f1)
print("Confusion Matrix:\n", conf_matrix)

# Plot confusion matrix
plt.figure(figsize=(8, 6))
sns.heatmap(conf_matrix, annot=True, fmt='d', cmap="Blues", xticklabels=range(num_classes),
            yticklabels=range(num_classes))
plt.xlabel('Predicted labels')
plt.ylabel('True labels')
plt.title('Confusion Matrix')
plt.show()

# Save the trained model
svm_model.save('new26-model-hypertuned-SVM_model.h5')

Ensemble (XGBoost)
import pandas as pd
import numpy as np
import xgboost as xgb
from sklearn.preprocessing import LabelEncoder, StandardScaler
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score, confusion_matrix
import joblib
import seaborn as sns
import matplotlib.pyplot as plt
import tensorflow as tf

# Define label renaming mappings
label_renaming = {
    'Malicious': 'Denial of Service',
    'SQL Injection': 'Infiltration'
}

```

```

# Define your label mappings
label_mappings = {
    'Normal': 0,
    'Denial of Service': 1,
    'Bruteforce': 2,
    'Botnet': 3,
    'Botnet_ctu': 3,
    'Infiltration': 4,
}

# Load training dataset
train_df = pd.read_csv('/content/drive/MyDrive/A5_De-TECH/50:50/Training Data/5050_reduced_training-file.csv')

# Load validation dataset
valid_df = pd.read_csv('/content/drive/MyDrive/A5_De-TECH/50:50/Training Data/5050_Train Data_14.csv')

# Replace 'SQL Injection' with 'Infiltration' in validation dataset
valid_df['label'] = valid_df['label'].replace('SQL Injection', 'Infiltration')

# Define selected features
selected_features = ['dst port','tot fwd pkts','tot bwd pkts','totlen fwd pkts','totlen bwd pkts','fwd pkt len mean','bwd pkt len max','fwd iat mean','flow iat max','flow iat min','fwd iat std','bwd iat mean','bwd iat std','bwd iat max','bwd iat min','fwd header len','bwd header len','fwd pkts s','bwd pkts s','pkt len mean','pkt len var','fwd seg size avg','bwd seg size avg','init fwd win byts','init bwd win byts']

# Define features and target variables for training and validation
X_train = train_df[selected_features]
y_train = train_df['label']

X_valid = valid_df[selected_features]
y_valid = valid_df['label']

# Replace infinite values with a very large finite number
X_train = X_train.replace([np.inf, -np.inf], np.nan).fillna(1e9)
X_valid = X_valid.replace([np.inf, -np.inf], np.nan).fillna(1e9)

# Convert string labels to integers using LabelEncoder
label_encoder = LabelEncoder()
y_train_encoded = label_encoder.fit_transform(y_train)
y_valid_encoded = label_encoder.transform(y_valid)

# Map labels using the defined mappings
y_train_mapped = [label_renaming[label] if label in label_renaming else label for label in y_train]
y_train_encoded_mapped = np.array([label_mappings[label] for label in y_train_mapped])

y_valid_mapped = [label_renaming[label] if label in label_renaming else label for label in y_valid]
y_valid_encoded_mapped = np.array([label_mappings[label] for label in y_valid_mapped])

# Normalize the numerical features excluding 'dst port' and 'protocol' using StandardScaler

```

```

scaler = StandardScaler()

# Exclude 'dst port' and 'protocol' from both training and validation data
X_train_for_scaling = X_train.drop(['dst port'], axis=1)
X_valid_for_scaling = X_valid.drop(['dst port'], axis=1)

# Fit StandardScaler only on the training data
scaler.fit(X_train_for_scaling)

# Transform both training and validation data using the fitted scaler
X_train_normalized = X_train.copy()
X_train_normalized[X_train_for_scaling.columns] = scaler.transform(X_train_for_scaling)

X_valid_normalized = X_valid.copy()
X_valid_normalized[X_valid_for_scaling.columns] = scaler.transform(X_valid_for_scaling)

# SVM prediction function
def svm_predict(csv_data_detect):
    data = csv_data_detect
    svm_model = tf.keras.models.load_model('/content/drive/MyDrive/A5_De-TECH/new26-model-hypertuned-SVM_model.h5')
    svm_predictions_raw = svm_model.predict(data)
    svm_threshold = 0.5 # Set your desired threshold
    svm_predictions = np.where(svm_predictions_raw >= svm_threshold, 1, 0)
    return svm_predictions

# Naive Bayes prediction function
def nb_predict(csv_data_detect):
    data = csv_data_detect
    nb_model = joblib.load('/content/drive/MyDrive/A5_De-TECH/new26-model-hypertuned-NB_model.pkl')
    nb_predictions = nb_model.predict(data)
    label_encoder = LabelEncoder()
    nb_predictions_numeric = label_encoder.fit_transform(nb_predictions)
    return nb_predictions_numeric

# Decision Tree prediction function
def dt_predict(csv_data_detect):
    data = csv_data_detect
    dt_model = joblib.load('/content/drive/MyDrive/A5_De-TECH/new26-model-hypertuned-DT_model.pkl')
    dt_predictions = dt_model.predict(data)
    return dt_predictions

# Obtain predictions for SVM, Naive Bayes, and Decision Tree models
csv_data_test = X_valid_normalized
svm_data = svm_predict(csv_data_test)
nb_data = nb_predict(csv_data_test)
dt_data = dt_predict(csv_data_test)

# Stack the predictions
stacked_predictions_1 = np.column_stack((svm_data, nb_data, dt_data))

```

```

# Initialize XGBoost Classifier
num_classes = len(label_mappings) # Determine the number of unique classes
xgb_model = xgb.XGBClassifier(objective="multi:softmax", num_class=num_classes, random_state=42)

# Train the XGBoost model on the stacked predictions
xgb_model.fit(stacked_predictions_1, y_valid_encoded_mapped)

# Make predictions using the ensemble model
ensemble_predictions = xgb_model.predict(stacked_predictions_1)

# Evaluate the performance of the ensemble model
accuracy = accuracy_score(y_valid_encoded_mapped, ensemble_predictions)
precision = precision_score(y_valid_encoded_mapped, ensemble_predictions, average='weighted')
recall = recall_score(y_valid_encoded_mapped, ensemble_predictions, average='weighted')
f1 = f1_score(y_valid_encoded_mapped, ensemble_predictions, average='weighted')

print(f'Ensemble Model Metrics:')
print(f'Accuracy: {accuracy}')
print(f'Precision: {precision}')
print(f'Recall: {recall}')
print(f'F1 Score: {f1}')

# Confusion Matrix
conf_matrix = confusion_matrix(y_valid_encoded_mapped, ensemble_predictions)
print('\nConfusion Matrix:')
print(conf_matrix)

# Create a heatmap for the confusion matrix
plt.figure(figsize=(10, 8))
sns.heatmap(conf_matrix, annot=True, fmt='d', cmap='Blues', cbar=False)
plt.xlabel('Predicted labels')
plt.ylabel('True labels')
plt.title('Confusion Matrix Heatmap')
plt.show()

# Save the trained ensemble model
ensemble_model_path = '/content/drive/MyDrive/A5_De-TECH/new26-model-hypertuned-newEnsemble_model.pkl'
joblib.dump(xgb_model, ensemble_model_path)

print("Multi-class ensemble model saved successfully.")

```

c) Web App (Frontend)

About HTML code:

```
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>De-TECH About</title>
    <link rel="icon" href="../static/images/favicon16.png" sizes="16x16" type="image/png">
    <link rel="icon" href="../static/images/favicon32.png" sizes="32x32" type="image/png">
    <link rel="icon" href="../static/images/favicon192.png" sizes="192x192" type="image/png">
    <link rel="icon" href="../static/images/favicon512.png" sizes="512x512" type="image/png">
    <link rel="apple-touch-icon" href="../static/images/faviconapple.png" sizes="180x180">
    <link href='https://unpkg.com/boxicons@2.1.4/css/boxicons.min.css' rel='stylesheet'>
    <script src="../static/scripts/jquery-1.10.2.js"></script>
    <script src="../static/scripts/js/abs.js"></script>
    <script src="../static/scripts/js/script1.js"></script>

    <link href="../static/content/style2abt.css" rel="stylesheet" />

    <!-- APPLY ALL PAGE START -->
    <link rel="stylesheet"
        href="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/css/bootstrap.min.css"
        integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T"
        crossorigin="anonymous">
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/js/bootstrap.min.js"
        integrity="sha384-JjSmVgyd0p3pXB1rRibZUAYoIl6OrQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM"
        crossorigin="anonymous"></script>
    <script src="https://code.jquery.com/jquery-3.6.4.min.js"></script>
    <!-- APPLY ALL PAGE END -->
</head>

<body>

    <!-- HEADER START -->
    <div class="row-header">
        <div class="col-sm-6 col-12">
            
            <h2>De-TECH</h2>
        </div>
        <div class="col-sm-6 col-12">
            <nav class="navigation">
                <a href="/home">Home</a>
                <a href="/about">About Us</a>
                <a href="/detect" id="btnDetect">Detect</a>
                <a href="/" id="loginLogOutMethod">Sign Out</a>
            </nav>
        </div>
    </div>
</body>
```

```

<!-- HEADER END -->

<!-- CONTENT -->
<div class="col-12 wrapper" style="text-align: center">
    <h1>ABOUT US</h1>
    <div class="col-12" style="margin-top: 70px;">
        <button onclick="goToAbstract()" class="btn">ABSTRACT</button>
    </div>
    <div class="col-12" style="margin-top: 20px;">
        <button onclick="goToMembers()" class="bttn">MEMBERS</button>
    </div>
</div>

<script>
    // Check if an alert message is provided and display it
    const userLoggedIn = "{{ userLoggedIn }}"; // Injected from Flask
    if (userLoggedIn != "") {
        $("#loggedInUserDescription").html("Hi, " + userLoggedIn + "!");
        $("#loginLogOutMethod").html("Sign Out");
    } else {
        $("#loggedInUserDescription").html("");
        $("#loginLogOutMethod").html("Log In");
        $("#btnDetect").css("display", "none");
    }
</script>

</body>
</html>

```

About CSS code:

```

@import
url("https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;500;600;700;800;900&display=swa
p");

* {
margin: 0;
padding: 0;
box-sizing: border-box;
font-family: "Poppins", sans-serif;
}

body {
min-height: 100vh;
background: url(..../images/bbackground.png);
background-repeat: no-repeat;
background-size: cover;
background-attachment: fixed;
}

.row-header {
display: flex;

```

```
justify-content: space-between;
align-items: center;
padding: 20px 40px;
background-color: transparent;
color: #fff;
height: 15%;
margin-right: auto;
}
```

```
.row-header .navigation {
  display: flex;
  justify-content: flex-end;
  margin-top: 10px;
}
```

```
.row-header .navigation a {
  font-size: 25px;
  color: #fff;
  text-decoration: none;
  margin-left: 20px;
}
```

```
.row-header .navigation a:hover {
  text-decoration: underline;
}
```

```
.navigation .btnlogin-popup {
  width: 130px;
  height: 50px;
  background: transparent;
  border: 2px solid #fff;
  outline: none;
  border-radius: 6px;
  cursor: pointer;
  font-size: 1.1em;
  color: #fff;
  font-weight: 500;
  transition: .5s;
}
```

```
.navigation .btnlogin-popup:hover {
  background: #fff;
  color: #162938;
}
```

```
.col-sm-6 h2 {
  position: fixed;
  top: 5px;
  left: 5px;
  margin-left: 120px;
  color: #ffffff;
  font-style: italic;
```

```
margin-top: 25px;
}

.Dlogo {
    position: fixed;
    left: 20px;
    top: 1px;
    width: 110px;
}

.col-12.wrapper {
    position: relative;
    width: 90%;
    margin: 80px auto;
    background-color: rgba(14, 70, 178, .20);
    border: none;
    backdrop-filter: blur(-2px);
    box-shadow: 0 0 10px rgba(0, 0, 0, .1);
    color: #fff;
    border-radius: 50px;
    padding: 30px 40px;
    text-align: center;
}

.col-12.wrapper::before {
    content: "";
    position: absolute;
    border: 3px solid #2382BC;
    border-radius: 60px;
    top: -5%;
    left: -1.5%;
    right: -1.5%;
    bottom: -5%;
}

.col-12.wrapper .col-12 {
    display: flex;
    flex-direction: column;
    justify-content: center;
    align-items: center;
}

.col-12.wrapper button {
    width: 55%;
    height: 70px;
    margin: 10px 0;
    text-align: center;
    background: #2382BC;
    border-radius: 40px;
    box-shadow: 0 0 10px rgba(0, 0, 0, .1);
    cursor: pointer;
    font-size: 50px;
}
```

```

font-family: 'Times New Roman';
color: #fff;
display: flex;
justify-content: center;
align-items: center;
}

.col-12.wrapper button.active, .col-12.wrapper button:hover {
background-color: #fff;
color: #000000;
box-shadow: 0 0 26px 1px #fff;
border: 1px solid #2382BC;
}

.col-12.wrapper h1 {
position: relative;
font-size: 5rem;
font-weight: 700;
}

.col-12.wrapper h1::after {
content: "";
position: absolute;
bottom: -5px;
left: 50%;
transform: translateX(-50%);
width: 40%;
height: 3px;
background-color: #fff;
}

@media only screen and (max-width: 768px) {
.row-header {
flex-direction: column;
align-items: center;
height: auto;
}

.row-header .navigation {
margin-top: 20px;
justify-content: center;
}

.col-sm-6 h2 {
position: static;
margin-top: 20px;
margin-left: 0;
text-align: center;
}

.Dlogo {
position: static;
}

```

```
    margin-top: 10px;  
}  
}  
}
```

```
@media only screen and (max-width: 576px) {  
.row-header {  
    padding: 10px;  
}  
  
.row-header .navigation {  
    flex-direction: column;  
    align-items: center;  
}  
  
.row-header .navigation a {  
    margin-left: 0;  
    margin-top: 10px;  
}  
  
.col-12.wrapper button {  
    width: 80%;  
    height: 50px;  
    font-size: 20px;  
    margin: 10px 0;  
}  
}
```

Abstract HTML code:

```
<html lang="en">  
  <head>  
    <meta charset="UTF-8">  
    <meta http-equiv="X-UA-Compatible" content="IE=edge">  
    <meta name="viewport" content="width=device-width, initial-scale=1.0">  
    <title> De-TECH Abstract </title>  
    <link rel="icon" href="../static/images/favicon16.png" sizes="16x16" type="image/png">  
    <link rel="icon" href="../static/images/favicon32.png" sizes="32x32" type="image/png">  
    <link rel="icon" href="../static/images/favicon192.png" sizes="192x192" type="image/png">  
    <link rel="icon" href="../static/images/favicon512.png" sizes="512x512" type="image/png">  
    <link rel="apple-touch-icon" href="../static/images/faviconapple.png" sizes="180x180">  
    <link href="https://unpkg.com/boxicons@2.1.4/css/boxicons.min.css" rel='stylesheet'>  
    <link href="../static/content/indexstyle.css" rel="stylesheet" />  
    <script src="../static/scripts/jquery-1.10.2.js"></script>  
    <script src="../static/scripts/js/abs.js"></script>  
    <script src="../static/scripts/js/script1.js"></script>  
  
    <!-- APPLY ALL PAGE START -->  
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/css/bootstrap.min.css" integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
```

```

<script src="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/js/bootstrap.min.js" integrity="sha384-JjSmVgyd0p3pXB1rRibZUAYoIly6OrQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM"
crossorigin="anonymous"></script>
<script src="https://code.jquery.com/jquery-3.6.4.min.js"></script>
<!-- APPLY ALL PAGE END -->
</head>
<body>

<!-- HEADER START -->
<div class="row-header">
<div class="col-sm-6 col-12">

<h2>De-TECH</h2>
</div>
<div class="col-sm-6 col-12">
<nav class="navigation">
<a href="/home">Home</a>
<a href="/about">About Us</a>
<a href="/detect" id="btnDetect">Detect</a>
<a href="/" id="loginLogOutMethod">Sign Out</a>
</nav>
</div>
</div>
<!-- HEADER END -->

<!-- CONTENT -->
<div class="col-12 wrapper" style="text-align: center">
<h1>ABSTRACT</h1>
<div class="col-12" style="margin-top: 30px;">
<p class="abstract-text">
As technology rapidly advances, the threat landscape evolves, necessitating stronger network infrastructure. This research introduces a Raspberry Pi-based Network Behavior Analysis

```

Intrusion Detection System (NBAIDS) using Ensemble Learning Approach. The system analyzes traffic through network behavior analysis with the help of the datasets, such as CTU-13 and CSE-CIC-IDS2018, that are trained using Ensemble Learning Approach. It distinguishes normal or malicious activities such as Denial of Service, Botnet, Bruteforce, SQL Injection, and Infiltration. Visualizations of the results are presented via a Web Application that helps in real-time monitoring. This study contributes to the growing development of cybersecurity in the country by detecting previously unseen threats, thereby enhancing network security. Recognizing the continuous growth and development of technology, the research addresses the need to handle evolving threats, offering solutions to cybersecurity-related problems.

```

</p>
</div>
</div>

```

```

<script>
    // Check if an alert message is provided and display it
    const userLoggedIn = "{{ userLoggedIn }}"; // Injected from Flask
    if (userLoggedIn != "") {
        $("#loggedInUserDescription").html("Hi, " + userLoggedIn + "!");
        $("#loginLogOutMethod").html("Sign Out");
    } else {
        $("#loggedInUserDescription").html("");
        $("#loginLogOutMethod").html("Log In");
        $("#btnDetect").css("display", "none");
    }
</script>

</body>
</html>

```

Abstract CSS code:

```

@import
url("https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;500;600;700;800;900&display=swa
p");

* {
margin: 0;
padding: 0;
box-sizing: border-box;
font-family: "Poppins", sans-serif;
}

body {
min-height: 100vh;
background: url(..images/bbackground.png);
background-repeat: no-repeat;
background-size: cover;
background-attachment: fixed;
}

.row-header {
display: flex;
justify-content: space-between;
align-items: center;
padding: 20px 40px; /* Adjust padding for left and right sides */
background-color: transparent;
color: #fff;
height: 15%;
margin-right: auto; /* Set right margin to auto */
}

.row-header .navigation {
display: flex;
justify-content: flex-end;
}

```

```
.row-header .navigation a {  
    font-size: 25px;  
    color: #fff;  
    text-decoration: none;  
    margin-left: 20px;  
}  
  
.row-header .navigation a:hover {  
    text-decoration: underline;  
}  
  
.navigation .btnlogin-popup {  
    width: 130px;  
    height: 50px;  
    background: transparent;  
    border: 2px solid #fff;  
    outline: none;  
    border-radius: 6px;  
    cursor: pointer;  
    font-size: 1.1em;  
    color: #fff;  
    font-weight: 500;  
    transition: .5s;  
}  
  
.navigation .btnlogin-popup:hover {  
    background: #fff;  
    color: #162938;  
}  
  
.col-sm-6 h2 {  
    position: fixed;  
    top: 5px;  
    left: 5px;  
    margin-left: 120px;  
    color: #ffffff;  
    font-style: italic;  
    margin-top: 25px;  
}  
  
.Dlogo {  
    position: fixed;  
    left: 20px;  
    top: 1px;  
    width: 110px;  
}  
  
.col-12.wrapper {  
    position: relative;  
    width: 90%;  
    margin: 80px auto;  
    background-color: rgba(14, 70, 178, .20);
```

```
border: none;
backdrop-filter: blur(-2px);
box-shadow: 0 0 10px rgba(0, 0, 0, .1);
color: #fff;
border-radius: 50px;
padding: 30px 40px;
text-align: center; /* Center align text */
}
```

```
.col-12.wrapper::before {
  content: "";
  position: absolute;
  border: 3px solid #2382BC;
  border-radius: 60px;
  top: -30px;
  left: -1.5%;
  right: -1.5%;
  bottom: -30px;
}
```

```
.col-12.wrapper h1 {
  position: relative;
  font-size: 60px;
  font-weight: 700;
}
```

```
.col-12.wrapper h1::after {
  content: "";
  position: absolute;
  bottom: -5px;
  left: 50%;
  transform: translateX(-50%);
  width: 30%;
  height: 3px;
  background-color: #fff;
}
```

```
.col-12.wrapper .col-12 {
  display: flex;
  flex-direction: column;
  justify-content: center;
}
```

```
.col-12.wrapper p {
  font-size: 20px;
  margin-top: 0;
  margin-bottom: 1rem;
  text-align: justify;
}
```

```
@media only screen and (max-width: 768px) {
```

```

.row-header {
  flex-direction: column;
  align-items: center;
  height: auto;
}

.row-header .navigation {
  margin-top: 20px;
  justify-content: center;
}

.col-sm-6 h2 {
  position: static;
  margin-top: 20px;
  margin-left: 0;
  text-align: center;
}

.Dlogo {
  position: static;
  margin-top: 10px;
}

@media only screen and (max-width: 576px) {
  .row-header {
    padding: 10px;
    flex-direction: column;
    align-items: center;
  }

  .row-header .navigation {
    margin-top: 20px;
    flex-direction: column;
    align-items: center;
  }

  .row-header .navigation a {
    margin-left: 0;
    margin-top: 10px;
  }

  .col-12.wrapper {
    padding: 20px;
  }

  .col-12.wrapper h1 {
    font-size: 40px;
  }
}

```

Analysis HTML code:

```

<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>De-TECH</title>
    <link rel="icon" href="../static/images/favicon16.png" sizes="16x16" type="image/png">
    <link rel="icon" href="../static/images/favicon32.png" sizes="32x32" type="image/png">
    <link rel="icon" href="../static/images/favicon192.png" sizes="192x192" type="image/png">
    <link rel="icon" href="../static/images/favicon512.png" sizes="512x512" type="image/png">
    <link rel="apple-touch-icon" href="../static/images/faviconapple.png" sizes="180x180">
    <link href='https://unpkg.com/boxicons@2.1.4/css/boxicons.min.css' rel='stylesheet'>
    <link rel="stylesheet" href="../static/content/style3a.css">
    <script src="../static/scripts/jquery-1.10.2.js"></script>

    <!-- APPLY ALL PAGE START -->
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/css/bootstrap.min.css" integrity="sha384-gOYR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
        <script src="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/js/bootstrap.min.js" integrity="sha384-JjSmVgyd0p3pXB1rRibZUAYoIly6OrQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymous"></script>
        <script src="https://code.jquery.com/jquery-3.6.4.min.js"></script>
    <!-- APPLY ALL PAGE END -->
</head>

<body>

    <!-- PARENT WRAPPER -->
    <div class="wrapper-card">

        <!-- HEADER -->
        <div class="row wrapper-header">
            <div class="col-sm-5 col-12" style="text-align: left; margin-top: -10px;">
                <span class="logo-container">
                    
                    <span class="logo-description">De - TECH</span>
                </span>
            </div>

            <div class="col-sm-4 col-12" style="text-align: left;">
                <h1 class="sis">
                    ANALYSIS
                </h1>
            </div>

            <div class="col-sm-3 col-12" style="text-align: right;">
                <a href="/home"><i class="bx bxs-home-alt-2"></i></a>
            </div>
        </div>
    </div>

```

```

</div>
<!-- HEADER END -->

<!-- CONTENT -->
<div class="row">
    <div class="col-sm-6 col-12">
        <table class="table">
            <tr>
                <td class="td2">Start Time:</td>
            </tr>
            <tr>
                <td class="td1" id="analysisstarttime"></td>
            </tr>
            <tr>
                <td class="td2">Duration:</td>
            </tr>
            <tr>
                <td class="td1" id="analysisdur"></td>
            </tr>
            <tr>
                <td class="td2">Protocol:</td>
            </tr>
            <tr>
                <td class="td1" id="analysisprotocol"></td>
            </tr>
            <tr>
                <td class="td2">Source IP Address:</td>
            </tr>
            <tr>
                <td class="td1" id="analysissourceip"></td>
            </tr>
            <tr>
                <td class="td2">Destination IP Address:</td>
            </tr>
            <tr>
                <td class="td1" id="analysisdestip"></td>
            </tr>
            <tr>
                <td class="td2">Destination Port:</td>
            </tr>
            <tr>
                <td class="td1" id="analysisdestport"></td>
            </tr>
        </table>
    <div class="col-12" style="text-align: center">
        <a class="h3" href="/detect">Go Back to Detect Page</a>
    </div>
</div>

<div class="col-sm-6 col-12 container">
    <div class="h4">
        <p>Traffic:</p>

```

```

</div>
<div class="container2" id="analysistraffic"></div>
<div class="h5">
    <p>Classification:</p>
</div>
<div class="container1" style="text-align: center;">
    <table class="table3" id="table3">
        <tr>
            <td class="td3" id="analysisclassify"></td>
        </tr>
    </table>
    <a class="h6" id="toggleLink">View Traffic Classification Summary</a>
</div>
<div class="col-12" style="text-align: right; margin-top: 0px;">
    <a class="h2" href="/dashboard">See the Dashboard Results!</a>
</div>
</div>

<!-- MODAL -->
<div class="modal" id="termsModal">
    <div class="modal-content">
        <span class="close">&times;</span>
        <table class="table4" id="table4">
            <tr>
                <td class="td6">NORMAL</td>
            </tr>
            <tr>
                <td class="td5" id="analysisnormal"></td>
            </tr>
            <tr>
                <td class="td6">BOTNET</td>
            </tr>
            <tr>
                <td class="td5" id="analysisbotnet"></td>
            </tr>
            <tr>
                <td class="td6">BRUTEFORCE</td>
            </tr>
            <tr>
                <td class="td5" id="analysisbrutef"></td>
            </tr>
            <tr>
                <td class="td6">DENIAL OF SERVICE (DoS)</td>
            </tr>
            <tr>
                <td class="td5" id="analysisdos"></td>
            </tr>
            <tr>
                <td class="td6">INFILTRATION</td>
            </tr>
            <tr>
                <td class="td5" id="analysisinf"></td>
            </tr>
        </table>
    </div>
</div>

```

```

        </tr>
    </table>
</div>
</div>
</div>
</div>

</body>
</html>

<script>
// Check if an alert message is provided and display it
const userLoggedIn = "{{ userLoggedIn }}"; // Injected from Flask
const userIdLoggedIn = "{{ userIdLoggedIn }}"; // Injected from Flask
const recordExists = "{{ recordExists }}";

if (recordExists == "1") {
    $("#analysisstarttime").html("{{ starttime }}");
    $("#analysisdur").html("{{ dur }}");
    $("#analysisprotocol").html("{{ protocol }}");
    $("#analysissourceip").html("{{ sourceip }}");
    $("#analysisdestip").html("{{ destip }}");
    $("#analysisdestport").html("{{ destport }}");
    $("#analysistraffic").html("{{ traffic }}");
    $("#analysisnormal").html("{{ normal }}");
    $("#analysisbrutef").html("{{ brutef }}");
    $("#analysisbotnet").html("{{ botnet }}");
    $("#analysisdos").html("{{ dos }}");
    $("#analysisinf").html("{{ inf }}");
    $("#analysisclassify").html("{{ classify }}");
}

// Get the modal
var modal = document.getElementById("termsModal");

// Get the link that opens the modal
var link = document.getElementById("toggleLink");

// Get the <span> element that closes the modal
var span = document.getElementsByClassName("close")[0];

// When the user clicks the link, open the modal
link.onclick = function() {
    modal.style.display = "block";
}

// When the user clicks on <span> (x), close the modal
span.onclick = function() {
    modal.style.display = "none";
}

```

```
// When the user clicks anywhere outside of the modal, close it
window.onclick = function(event) {
  if (event.target == modal) {
    modal.style.display = "none";
  }
}
</script>
```

Analysis CSS code:

```
@import
url("https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;500;600;700;800;900&display=swap");
@import
url('https://fonts.googleapis.com/css2?family=Open+Sans:ital,wght@0,400;1,300&display=swap');

* {
  margin: 0;
  padding: 0;
  box-sizing: border-box;
  font-family: 'Poppins', sans-serif;
}

body {
  background: url('../images/bbackground.png') no-repeat;
  background-size: cover;
  background-attachment: fixed;
}

.wrapper-card {
  width: 100%;
  margin: 0 auto;
  padding: 20px;
  background-color: rgba(14, 70, 178, 0.2);
  border: none;
  box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
  color: #fff;
  border-radius: 50px;
}

.wrapper-container {
  position: relative;
}

.wrapper-header {
  border-bottom: 2px solid #fff;
  margin-bottom: 20px;
  padding-bottom: 10px;
}

.wrapper-header h1 {
  color: white;
```

```
font-size: 45px;
font-weight: 500;
margin-top: -10px;
}

.wrapper-header i {
  font-size: 60px;
  color: #fff;
  margin-top: -10px;
}

.row {
  margin-bottom: 20px;
}

.col-12 {
  text-align: center;
}

.logo-container img {
  margin-bottom: 10px;
}

.logo-description {
  font-size: 32px;
  font-weight: bold;
  color: white;
  margin-left: -10px;
  font-family: 'Open Sans', sans-serif;
}

.table .td1,
.table .td2 {
  border-top: none;
}

.td1 {
  background: white;
  color: black;
  border-radius: 20px;
  width: 650px;
  text-align: center;
  line-height: 10px;
}

.td2 {
  color: white;
  width: 430px;
}

.a.h3 {
```

```
color: white;
font-size: 26px;
text-align: center;
text-decoration: none;
background-color: #2382BC;
box-sizing: border-box;
border: 5px solid black;
border-radius: 40px;
}

.container {
height: 450px;
float: right;
background-color: rgba(14, 70, 178, .20);
border: none;
box-shadow: 0 0 10px rgba(0, 0, 0, .1);
text-align: center;
border-radius: 50px;
margin-top: 25px;
width: 80%;
}

.container .h4 {
color: white;
font-size: 20px;
font-style: italic;
font-weight: 400;
text-align: left;
padding-top: 30px;
margin-left: 10px;
}

.container .h5 {
color: white;
font-size: 20px;
font-style: italic;
font-weight: 400;
text-align: left;
margin-left: 10px;
padding-top: 50px;
}

.container .col-12 a.h2 {
color: white;
font-size: 26px;
font-weight: 400;
font-style: italic;
margin-right: 150px;
margin-top: 20px;
}

.container1 {
```

```
max-width: 100%;  
background-color: #2382BC;  
box-sizing: border-box;  
text-align: center;  
border-radius: 35px;  
border: 5px solid black;  
padding-bottom: 20px;  
height: auto;  
margin-top: 2%;  
margin-left: 5%;  
margin-right: 5%;  
}  
  
.container2 {  
width: 98%;  
height: 60px;  
margin: 0 auto;  
background-color: #2382BC;  
box-sizing: border-box;  
text-align: center;  
border-radius: 40px;  
margin-top: 5px;  
border: 5px solid black;  
font-size: 40px;  
font-weight: bold;  
margin-left: auto;  
margin-right: auto;  
max-width: calc(100% - 40px);  
}  
  
.table3 {  
width: 98%;  
max-width: calc(100% - 40px);  
margin-top: 20px;  
margin-left: auto;  
margin-right: auto;  
margin-bottom: 20px;  
}  
  
.td3 {  
background-color: white;  
color: black;  
border-radius: 20px;  
padding: 1px;  
height: 30px;  
width: 41.5vw;  
}  
  
.h6 {  
color: white;  
font-size: 22px;  
font-weight: 400;
```

```

        font-style: italic;
        cursor: pointer;
    }

.a.h6:hover {
    text-decoration: underline;
}

.col-12 a.h2 {
    color: white;
    font-size: 26px;
    font-weight: 400;
    font-style: italic;
    margin-right: 3%; /* Adjust the percentage as needed */
    margin-top: 2%; /* Adjust the percentage as needed */
}

#termsModal {
    display: none;
    position: fixed;
    z-index: 1;
    left: 0;
    top: 0;
    width: 100vw; /* Full width */
    height: 100vh; /* Full height */
    overflow: auto;
    background-color: rgba(0,0,0,0.4);
}

#termsModal .modal-content {
    position: absolute;
    top: 50%;
    left: 50%;
    transform: translate(-50%, -50%);
    background-color: #2382BC;
    box-sizing: border-box;
    border-radius: 40px;
    border: 5px solid black;
    padding: 20px;
    max-width: 80%;
    max-height: 80%;
    overflow: auto;
}

.close {
    color: #aaa;
    float: right;
    font-size: 28px;
    font-weight: bold;
}

.close:hover,

```

```
.close:focus {
    color: black;
    text-decoration: none;
    cursor: pointer;
}

.table4 {
    width: 100%;
    max-width: 100%;
    margin: 0 auto;
    border: none;
}

.td6 {
    border: none;
    font-style: italic;
    font-size: 14px;
    padding: 5px;
    color: white;
}

#termsModal .modal-content .td6 {
    border: none;
}

#termsModal .modal-content .td5 {
    background-color: #fff;
    color: #000;
    padding: 5px;
    font-size: 14px;
    margin-top: 5px;
    text-align: center;
}

#termsModal .modal-content .table4 .td5 {
    border-radius: 20px;
    border: none;
}

.table4 td {
    border: 1px solid #ddd;
    padding: 8px;
}

.table4 tr:nth-child(even) {
    background-color: #f2f2f2;
}

.table4 tr:hover {
    background-color: transparent;
}
```

```

.table4 td.td6:hover {
    background-color: transparent;
}

@media screen and (max-width: 840px) {
    a.h3 {
        font-size: 18px;
    }
}

@media screen and (max-width: 761px) {
    .container .col-12 a.h2 {
        font-size: 18px;
    }
}

@media screen and (min-width: 576px) {
    .wrapper-card {
        width: 98%;
        padding-top: 20px;
        padding-bottom: 20px;
        padding-left: 50px;
        padding-right: 50px;
        margin-top: 20px;
        margin-bottom: 20px;
    }
}

@media screen and (max-width: 576px) {
    .wrapper-card {
        width: 97%;
        padding-top: 15px;
        padding-left: 31px;
        padding-right: 30px;
        margin-top: 20px;
    }

    .wrapper-header {
        margin-bottom: 10px;
    }

    .container1 {
        max-width: 85%;
        margin-left: auto;
        margin-right: auto;
        overflow: hidden;
    }

    .container2 {
        width: 85%;
        margin-right: auto;
        margin-left: auto;
    }
}

```

```

        overflow: hidden;
    }

    .container .col-12 a.h2 {
        font-size: 26px;
    }
}

@media screen and (max-width: 646px) {
    a.h3 {
        font-size: 17px;
    }
}

@media screen and (max-width: 622px) {
    a.h3 {
        font-size: 15px;
    }
}

```

Dashboard HTML code:

```

<!doctype html>
<html lang="en">
    <head>
        <!-- Required meta tags -->
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
        <title> De-TECH Dashboard </title>
        <link rel="icon" href="../static/images/favicon16.png" sizes="16x16" type="image/png">
        <link rel="icon" href="../static/images/favicon32.png" sizes="32x32" type="image/png">
        <link rel="icon" href="../static/images/favicon192.png" sizes="192x192" type="image/png">
        <link rel="icon" href="../static/images/favicon512.png" sizes="512x512" type="image/png">
        <link rel="apple-touch-icon" href="../static/images/faviconapple.png" sizes="180x180">
        <link href="https://unpkg.com/boxicons@2.1.4/css/boxicons.min.css" rel='stylesheet'>
        <!-- Bootstrap CSS -->
        <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/css/bootstrap.min.css" integrity="sha384-gOyR0iXCbMQu3Xipma34MD+dH/1fQ784/j6cY/iJTQUhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
        <link rel="stylesheet" href="../static/content/dstyle.css">
        <script src="../static/scripts/jquery-1.10.2.js"></script>
        <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.0.0-beta3/css/all.min.css" integrity="sha384-4ulTu00CY7euGzHI1S2goWFEbRtA/GIMlw8LF5zVS9Iw+M0R2AI3J6zCkQw0A2ej" crossorigin="anonymous">
    </head>
    <body>
        <!-- Optional JavaScript -->
        <!-- jQuery first, then Popper.js, then Bootstrap JS -->
        <script src="https://cdn.jsdelivr.net/npm/popper.js@1.14.7/dist/umd/popper.min.js" integrity="sha384-"

```

```

UO2eT0CpHqdSJQ6hJty5KVphtPhzWj9WO1clHTMGa3JDZwrnQq4sF86dIHNDz0W1"
crossorigin="anonymous">></script>
<script src="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/js/bootstrap.min.js" integrity="sha384-JjSmVgyd0p3pXB1rRibZUAYoIy6OrQ6VrjIEaFf/nGzIxFDsf4x0xIM+B07jRM"
crossorigin="anonymous">></script>
<script src="https://code.jquery.com/jquery-3.6.4.min.js"></script>
<script src="https://cdn.jsdelivr.net/npm/chart.js"></script>
<!-- PARENT WRAPPER -->
<div class="wrapper-card">
    <!-- HEADER START -->
<div class="row-header">
<div class="col-sm-4 col-12">
    
    <h2>De-TECH</h2>
</div>
<div class="col-sm-4 col-12">
    <div class="container" style="text-align: center;">
        <p>DASHBOARD</p>
    </div>
</div>
<div class="col-sm-4 col-12">
    <nav class="navigation">
        <a href="/home">Home</a>
        <a href="/analysis">Analysis</a>
        <a href="/history">History</a>
    </nav>
</div>
</div>
<!-- HEADER END -->

    <!-- CONTENT -->
<div class="row">
<div class="col-sm-5 col-12" style="min-height:100px; padding:10px;">
    <div class="chart-wrapper"> Malicious Activity Trend
        <span class="icon-circle" data-toggle="modal" data-target="#maliciousActivityModal">
            <i class='bx bx-info-circle'></i>
        </span>
        <canvas id="lineChart" width="300" height="170"></canvas>
    </div>
    <p>
        <span id="dashboardtime"></span>
    </p>
</div>
<div class="col-sm-7 col-12" style="min-height:100px">
    <div class="row">
        <div class="col-12" style="min-height:50px; padding:10px;">
            <div class="chart_wrapper" style="text-align:left;"> Number of Alerts:
                <div class="col-12" style="min-height:50px; padding:10px; text-align: center;">
                    <span id="dashboardnumalerts" style="font-size: 42px;"></span>
                </div>
            </div>
        </div>
    </div>

```

```

        </div>
    </div>
    <div class="row">
        <div class="col-sm-6 col-12" style="min-height:100px; padding:10px">
            <div class="chart-wrapper"> Traffic Patterns
                <span class="icon-circle" data-toggle="modal" data-target="#trafficPatternsModal">
                    <i class='bx bx-info-circle'></i>
                </span>
                <canvas id="lineChart1" width="100" height="50"></canvas>
            </div>
            <p>
                <span id="dashboardaveflowbytsrate"></span>
            </p>
        </div>
        <div class="col-sm-6 col-12" style="min-height:100px; padding:10px">
            <div class="chart-wrapper"> Packet Capture
                <span class="icon-circle" data-toggle="modal" data-target="#packetCaptureModal">
                    <i class='bx bx-info-circle'></i>
                </span>
                <canvas id="lineChart2" width="100" height="50"></canvas>
            </div>
            <p>
                <span id="dashboardaveflowpktsrate"></span>
            </p>
        </div>
        </div>
    </div>
    <div class="row">
        <div class="col-lg-3 col-12 align-items-center justify-content-center" style="min-height:100px; padding:10px; content:center;">
            <div class="chart-wrapper"> Protocol Distribution
                <span class="icon-circle" data-toggle="modal" data-target="#protocolDistributionModal">
                    <i class='bx bx-info-circle'></i>
                </span>
                <canvas id="pieChart" width="100" height="50" style="margin-top: 50px;"></canvas>
            </div>
        </div>
        <div class="col-lg-6 col-12" style="min-height:100px; padding:10px;">
            <div class="chart-wrapper"> IP Addresses (Source and Destination)
                <span class="icon-circle" data-toggle="modal" data-target="#ipAddressesModal">
                    <i class='bx bx-info-circle'></i>
                </span>
                <div style="text-align:center; center; min-width: 100%;">
                    <div class="row">
                        <div class="col-6">
                            <table id="ipTableSource" class="table table-bordered" style="width: 100%; color: white;">
                                <thead>
                                    <tr>
                                        <th style="color: white;">RANK</th>
                                        <th style="color: white;">Source IP</th>

```

```

</tr>
</thead>
<tbody>
    <!-- Table data will be populated dynamically using JavaScript -->
</tbody>
</table>
</div>
<div class="col-6">
    <table id="ipTableDestination" class="table table-bordered" style="width: 100%; color: white;">
        <thead>
            <tr>
                <th style="color: white;">RANK</th>
                <th style="color: white;">Destination IP</th>
            </tr>
        </thead>
        <tbody>
            <!-- Table data will be populated dynamically using JavaScript -->
        </tbody>
    </table>
</div>
</div>
</div>
</div>
</div>
<div class="col-lg-3 col-12 " style="min-height:100px; padding:10px">
    <div class="chart-wrapper"> Targeted Services
        <span class="icon-circle" data-toggle="modal" data-target="#targetedServicesModal">
            <i class='bx bx-info-circle'></i>
        </span>
        <div class="table-responsive" style="text-align:center;">
            <table id="ipPortTable" class="table table-bordered">
                <thead>
                    <tr>
                        <th style="color: white;">RANK</th>
                        <th style="color: white;">Destination Port</th>
                    </tr>
                </thead>
                <tbody>
                    <!-- This will be populated with JavaScript -->
                </tbody>
            </table>
        </div>
    </div>
</div>
</div>
</div>
</div>

```

```

<div class="modal-content">
  <div class="modal-header">
    <h5 class="modal-title" id="maliciousActivityModalLabel">Malicious Activity Trend Information</h5>
    <button type="button" class="close" data-dismiss="modal" aria-label="Close">
      <span aria-hidden="true">&times;</span>
    </button>
  </div>
  <div class="modal-body">
    <!-- Your pop-up message content goes here -->
    The malicious activity trend indicates when malicious traffic appeared.
  </div>
  <div class="modal-footer">
    <button type="button" class="btn btn-secondary" data-dismiss="modal">Close</button>
  </div>
</div>
</div>

<!-- Modal for Traffic Patterns pop-up message -->
<div class="modal fade" id="trafficPatternsModal" tabindex="-1" role="dialog" aria-labelledby="trafficPatternsModalLabel" aria-hidden="true">
  <div class="modal-dialog" role="document">
    <div class="modal-content">
      <div class="modal-header">
        <h5 class="modal-title" id="trafficPatternsModalLabel">Traffic Patterns Information</h5>
        <button type="button" class="close" data-dismiss="modal" aria-label="Close">
          <span aria-hidden="true">&times;</span>
        </button>
      </div>
      <div class="modal-body">
        <!-- Your pop-up message content goes here -->
        This graph displays the number of analyzed bytes over time. The y-axis represents the average flow speed of bytes, while the x-axis represents each captured traffic instance.
      </div>
      <div class="modal-footer">
        <button type="button" class="btn btn-secondary" data-dismiss="modal">Close</button>
      </div>
    </div>
  </div>
</div>

<!-- Modal for Packet Capture pop-up message -->
<div class="modal fade" id="packetCaptureModal" tabindex="-1" role="dialog" aria-labelledby="packetCaptureModalLabel" aria-hidden="true">
  <div class="modal-dialog" role="document">
    <div class="modal-content">
      <div class="modal-header">
        <h5 class="modal-title" id="packetCaptureModalLabel">Packet Capture Information</h5>
        <button type="button" class="close" data-dismiss="modal" aria-label="Close">
          <span aria-hidden="true">&times;</span>
        </button>
      </div>

```

```

        </button>
    </div>
    <div class="modal-body">
        <!-- Your pop-up message content goes here -->
        This graph displays the number of analyzed packets over time. The y-axis
        represents the average flow speed of packets, while the x-axis represents each captured traffic
        instance.
    </div>
    <div class="modal-footer">
        <button type="button" class="btn btn-secondary" data-dismiss="modal">Close</button>
    </div>
</div>
</div>
</div>

<!-- Modal for Protocol Distribution pop-up message -->
<div class="modal fade" id="protocolDistributionModal" tabindex="-1" role="dialog" aria-
labelledby="protocolDistributionModalLabel" aria-hidden="true">
    <div class="modal-dialog" role="document">
        <div class="modal-content">
            <div class="modal-header">
                <h5 class="modal-title" id="protocolDistributionModalLabel">Protocol Distribution
                Information</h5>
                <button type="button" class="close" data-dismiss="modal" aria-label="Close">
                    <span aria-hidden="true">&times;</span>
                </button>
            </div>
            <div class="modal-body">
                <!-- Your pop-up message content goes here -->
                This graph displays the frequency of protocols used in the network.
            </div>
            <div class="modal-footer">
                <button type="button" class="btn btn-secondary" data-dismiss="modal">Close</button>
            </div>
        </div>
    </div>
</div>

<!-- Modal for IP Addresses pop-up message -->
<div class="modal fade" id="ipAddressesModal" tabindex="-1" role="dialog" aria-
labelledby="ipAddressesModalLabel" aria-hidden="true">
    <div class="modal-dialog" role="document">
        <div class="modal-content">
            <div class="modal-header">
                <h5 class="modal-title" id="ipAddressesModalLabel">IP Addresses Information</h5>
                <button type="button" class="close" data-dismiss="modal" aria-label="Close">
                    <span aria-hidden="true">&times;</span>
                </button>
            </div>
            <div class="modal-body">
                <!-- Your pop-up message content goes here -->
                <strong>Source IP Address Rank:</strong>
            </div>
        </div>
    </div>
</div>

```

The ranking of source IP addresses represents which IP address has the highest number of forwarded packets in the network. This is measured by the sum of 'forward packets/second' for each respective source IP address.

```
<br><br>

<strong>Destination IP Address Rank:</strong>
The ranking of destination IP addresses represents which IP address has the highest number of received packets in the network. This is measured by the sum of 'backward packets/second' for each respective destination IP address.
</div>
<div class="modal-footer">
    <button type="button" class="btn btn-secondary" data-dismiss="modal">Close</button>
</div>
</div>
</div>
</div>

<!-- Modal for Targeted Services pop-up message -->
<div class="modal fade" id="targetedServicesModal" tabindex="-1" role="dialog" aria-labelledby="targetedServicesModalLabel" aria-hidden="true">
    <div class="modal-dialog" role="document">
        <div class="modal-content">
            <div class="modal-header">
                <h5 class="modal-title" id="targetedServicesModalLabel">Targeted Services Information</h5>
                <button type="button" class="close" data-dismiss="modal" aria-label="Close">
                    <span aria-hidden="true">&times;</span>
                </button>
            </div>
            <div class="modal-body">
                <!-- Your pop-up message content goes here -->
                This ranking represents which ports are often used. It is measured by the sum of 'flow bytes/second' for each respective port.
            </div>
        </div>
    </div>
</div>

To find out more about the given ports/services, refer to the Service Name and Transport Protocol Port Number Registry of the
Internet Assigned Numbers Authority (IANA): https://tinyurl.com/IANAPortNumbers
</div>
<div class="modal-footer">
    <button type="button" class="btn btn-secondary" data-dismiss="modal">Close</button>
</div>
</div>
</div>

</body>
<script src="https://cdn.jsdelivr.net/npm/chart.js"></script>
</html>
<script>
    // Check if an alert message is provided and display it

```

```

const userLoggedIn = "{{ userLoggedIn }}"; // Injected from Flask
const userIdLoggedIn = "{{ userIdLoggedIn }}"; // Injected from Flask
const totalTCPCount = "{{ total_tcp_count }}"; // Injected from Flask
const totalUDPCount = "{{ total_udp_count }}"; // Injected from Flask
const resultExists = "{{ resultExists }}";

var resultLscSortByDestinationIp = [];
var resultLscSortByPort = [];
var resultLscSortBySourceIp = [];

if (resultExists == "1") {
    $("#dashboardtime").html("{{ time }}");
    $("#dashboardaveflowpktsrate").html("{{ aveflowpktsrate }}");
    $("#dashboardaveflowbytsrate").html("{{ aveflowbytsrate }}");
    $("#dashboardnumalerts").html("{{ numalerts }}");
    // $("#dashboardprotocol").html("{{ protocol }}");
}
// Check if an alert message is provided and display it
var chartDay = $.parseJSON('{{ chartDay | toJSON | safe }}'); // Injected from Flask
var chartPackets = $.parseJSON('{{ chartPackets | toJSON | safe }}'); // Injected from Flask
var chartHours = $.parseJSON('{{ chartHours | toJSON | safe }}'); // Injected from Flask
var chartTraffic = $.parseJSON('{{ chartTraffic | toJSON | safe }}'); // Injected from Flask
var chartWeek = $.parseJSON('{{ chartWeek | toJSON | safe }}'); // Injected from Flask
var chartNPackets = $.parseJSON('{{ chartNPackets | toJSON | safe }}'); // Injected from Flask
var chartHUT = $.parseJSON('{{ chartHUT | toJSON | safe }}'); // Injected from Flask
var chartDt = $.parseJSON('{{ chartDt | toJSON | safe }}'); // Injected from Flask
var chartColors = ["#56A6DF", "#FF3131", "#00BF63"];
var pieColors = ['#FFA500', '#00ADEF'];

// get and clean tblrankings data - start
var latestranking = '{{ latestranking | toJSON | safe }}'; // Injected from Flask
var latestrankingclean =
$.parseJSON(latestranking).replaceAll("[{,[").replaceAll('}],')].replaceAll('},{,{}');

var jsonData = [];

for(x=0; x< latestrankingclean.length; x++){
    for(x2=1; x2<= Object.keys(latestrankingclean[x]).length; x2++){
        let topdstip = Object.keys(latestrankingclean[x]['Rank ' + x2]['top_dst_ip'])[0].trim();
        let topdstipvalue = Object.values(latestrankingclean[x]['Rank ' + x2]['top_dst_ip'])[0];
        let topports = Object.keys(latestrankingclean[x]['Rank ' + x2]['top_ports'])[0].trim();
        let topportsvalue = Object.values(latestrankingclean[x]['Rank ' + x2]['top_ports'])[0];
        let topsrcip = Object.keys(latestrankingclean[x]['Rank ' + x2]['top_src_ip'])[0].trim();
        let topsrcipvalue = Object.values(latestrankingclean[x]['Rank ' + x2]['top_src_ip'])[0];

        jsonData.push([
            {'top_dst_ip': topdstip, 'value': topdstipvalue },
            {'top_ports': topports, 'value': topportsvalue},
            {'top_src_ip': topsrcip, 'value': topsrcipvalue }]);
    }
}

var lsc = [];

```

```

$.each(jsonData, function(index, array) {
    let matchCount = 0;
    let arraytop_dst_ip = array[0].top_dst_ip;
    let arraytop_dst_ipvalue = array[0].value;
    let arraytop_ports = array[1].top_ports;
    let arraytop_portsvalue = array[1].value;
    let arraytop_src_ip = array[2].top_src_ip;
    let arraytop_src_ipvalue = array[2].value;

    for(a = 0; a < lsc.length; a++) {
        if (lsc[a][0].top_dst_ip == arraytop_dst_ip && lsc[a][1].top_ports == arraytop_ports &&
            lsc[a][2].top_src_ip == arraytop_src_ip) {
            matchCount++;

            lsc[a][0].top_dst_ip_value = lsc[a][0].top_dst_ip_value + arraytop_dst_ipvalue;
            lsc[a][1].top_ports_value = lsc[a][1].top_ports_value + arraytop_portsvalue;
            lsc[a][2].top_src_ip_value = lsc[a][2].top_src_ip_value + arraytop_src_ipvalue;
        }
    }

    if (matchCount == 0) {
        lsc.push([{'top_dst_ip': arraytop_dst_ip, 'top_dst_ip_value': arraytop_dst_ipvalue },
                  {'top_ports': arraytop_ports, 'top_ports_value': arraytop_portsvalue},
                  {'top_src_ip': arraytop_src_ip, 'top_src_ip_value': arraytop_src_ipvalue }]);
    }
});

//DESTINATION P
var lscSortByDestinationIp = [];
for(m = 0; m < lsc.length; m++) {
    lscSortByDestinationIp.push(lsc[m][0]);
}

var sumMaplscSortByDestinationIp = {};
lscSortByDestinationIp.forEach(function(obj) {
    if (!sumMaplscSortByDestinationIp[obj.top_dst_ip]) {
        sumMaplscSortByDestinationIp[obj.top_dst_ip] = obj.top_dst_ip_value;
    } else {
        sumMaplscSortByDestinationIp[obj.top_dst_ip] += obj.top_dst_ip_value;
    }
});

resultlscSortByDestinationIp = [];
for (var key in sumMaplscSortByDestinationIp) {
    resultlscSortByDestinationIp.push({ top_dst_ip: key, top_dst_ip_value:
        sumMaplscSortByDestinationIp[key] });
}

```

```

resultlscSortByDestinationIp.sort((a, b) => b.top_dst_ip_value - a.top_dst_ip_value);

// PORT
var lscSortByPort = [];
for(m = 0; m < lsc.length; m++) {
    lscSortByPort.push(lsc[m][1]);
}

var sumMaplscSortByPort = { };
lscSortByPort.forEach(function(obj) {
    if (!sumMaplscSortByPort[obj.top_ports]) {
        sumMaplscSortByPort[obj.top_ports] = obj.top_ports_value;
    } else {
        sumMaplscSortByPort[obj.top_ports] += obj.top_ports_value;
    }
});

resultlscSortByPort = [];
for (var key in sumMaplscSortByPort) {
    resultlscSortByPort.push({ top_ports: key, top_ports_value: sumMaplscSortByPort[key] });
}

resultlscSortByPort.sort((a, b) => b.top_ports_value - a.top_ports_value);

// SOURCE IP
var lscSortBySourceIp = [];
for(m = 0; m < lsc.length; m++) {
    lscSortBySourceIp.push(lsc[m][2]);
}

var sumMaplscSortBySourceIp = { };
lscSortBySourceIp.forEach(function(obj) {
    if (!sumMaplscSortBySourceIp[obj.top_src_ip]) {
        sumMaplscSortBySourceIp[obj.top_src_ip] = obj.top_src_ip_value;
    } else {
        sumMaplscSortBySourceIp[obj.top_src_ip] += obj.top_src_ip_value;
    }
});

resultlscSortBySourceIp = [];
for (var key in sumMaplscSortBySourceIp) {
    resultlscSortBySourceIp.push({ top_src_ip: key, top_src_ip_value: sumMaplscSortBySourceIp[key] });
}

resultlscSortBySourceIp.sort((a, b) => b.top_src_ip_value - a.top_src_ip_value);

// get and clean tblrankings data - end

```

```

console.log(chartDay);
console.log(chartPackets);
console.log(chartHours);
console.log(chartTraffic);
console.log(chartWeek);
console.log(chartNPackets);
console.log(chartHUT);
console.log(chartDt);
$(document).ready(function() {
    createLineChart(chartDay, chartPackets, 'lineChart', 'Number of Alerts', chartColors[0]);
    createLineChart(chartHours, chartTraffic, 'lineChart1', 'Traffic Patterns', chartColors[1]);
    createLineChart(chartWeek, chartNPackets, 'lineChart2', 'Packet Capture', chartColors[2]);
    createPieChart(['TCP', 'UDP'], [totalTCPCount, totalUDPCount], 'pieChart', 'Protocol Distribution',
    ['#FFA500', '#00ADEF', '#FF9B00']);
    populateSourceIpTable(resultlscSortBySourceIp);
    populateDestinationIpTable(resultlscSortByDestinationIp);
    populatePortTable(resultlscSortByPort);
});
let createLineChart = function(chartLabel, chartData, chartElement, chartLabelName, chartColors) {
    // Example chart data for a line chart
    var linechartData = {
        type: 'line',
        data: {
            labels: chartLabel,
            datasets: [{
                label: chartLabelName,
                data: chartData,
                fill: false,
                borderColor: chartColors,
                borderWidth: 2,
                pointRadius: 5,
                pointBackgroundColor: chartColors,
                pointBorderColor: chartColors,
                pointHoverRadius: 7,
                pointHoverBackgroundColor: 'rgba(32,61,91)',
                pointHoverBorderColor: chartColors,
                backgroundColor: 'rgba(32,61,91)'
            }]
        },
        options: {
            plugins: {
                legend: {
                    labels: {
                        color: "white"
                    }
                }
            },
            scales: {
                x: {
                    ticks: {

```

```

        color: 'white' // Set the color of X-axis labels to white
    }
},
y: {
    ticks: {
        color: 'white', // Set the color of Y-axis labels to white
        stepSize: 1 // Display only integer values on the y-axis
    }
}
};

var ctx = document.getElementById(chartElement).getContext('2d');
// Initialize Chart.js line chart
var lineChart = new Chart(ctx, linechartData);
};

let createBarChart = function(barLabel, barData, barElement) {
// Example chart data for a bar chart
var barchartData = {
    type: 'bar',
    data: {
        labels: barLabel,
        datasets: [{
            label: 'Malicious Activity Trends',
            data: barData,
            backgroundColor: ['rgba(255, 99, 132, 0.5)', 'rgba(54, 162, 235, 0.5)', 'rgba(255, 206, 86, 0.5)',
            'rgba(75, 192, 192, 0.5)', 'rgba(153, 102, 255, 0.5)'],
            borderColor: ['rgba(255, 99, 132, 1)', 'rgba(54, 162, 235, 1)', 'rgba(255, 206, 86, 1)', 'rgba(75,
            192, 192, 1)', 'rgba(153, 102, 255, 1)'],
            borderWidth: 1
        }]
    },
    options: {
        plugins: {
            legend: {
                labels: {
                    color: "white"
                }
            }
        },
        scales: {
            x: {
                ticks: {
                    color: 'white' // Set the color of X-axis labels to white
                }
            },
            y: {
                ticks: {
                    color: 'white', // Set the color of Y-axis labels to white
                    stepSize: 1 // Display only integer values on the y-axis
                }
            }
        }
    }
};

```

```

        }
    }
};

var ctx = document.getElementById(barElement).getContext('2d');
// Initialize Chart.js bar chart
var barChart = new Chart(ctx, barchartData);
};

let createPieChart = function(labels, data, element, labelName) {
    var pieChartData = {
        type: 'pie',
        data: {
            labels: labels,
            datasets: [{
                data: data,
                backgroundColor: ['#FFA500', '#00ADEF'],
            }]
        },
        options: {
            plugins: {
                legend: {
                    labels: {
                        color: 'white' // Customize legend text color
                    }
                }
            }
        }
    };
    var ctx = document.getElementById(element).getContext('2d');
    var pieChart = new Chart(ctx, pieChartData);
};

let populateSourceIpTable = function(data) {
    var tableBody = document.getElementById('ipTableSource').getElementsByTagName('tbody')[0];
    // Clear any existing rows
    tableBody.innerHTML = "";
    // Create 6 empty rows with 3 columns each
    for (var i = 0; i < data.length; i++) {
        var newRow = tableBody.insertRow();
        for (var j = 0; j < 2; j++) {
            var newCell = newRow.insertCell(j);
            // Set the cells to be empty or with a placeholder if needed
            newCell.style.color = 'white';
        }

        newRow.cells[0].innerText = i + 1;
        newRow.cells[1].innerText = data[i].top_src_ip;
    }
};

let populateDestinationIpTable = function(data) {
    var tableBody = document.getElementById('ipTableDestination').getElementsByTagName('tbody')[0];

```

```

// Clear any existing rows
tableBody.innerHTML = "";
// Create 6 empty rows with 3 columns each
for (var i = 0; i < data.length; i++) {
    var newRow = tableBody.insertRow();
    for (var j = 0; j < 2; j++) {
        var newCell = newRow.insertCell(j);
        // Set the cells to be empty or with a placeholder if needed
        newCell.style.color = 'white';
    }

    newRow.cells[0].innerText = i + 1;
    newRow.cells[1].innerText = data[i].top_dst_ip;
}
};

let populatePortTable = function(data) {
    var tableBody = document.getElementById('ipPortTable').getElementsByTagName('tbody')[0];
    // Clear any existing rows
    tableBody.innerHTML = "";
    // Create 6 empty rows with 3 columns each
    for (var i = 0; i < data.length; i++) {
        var newRow = tableBody.insertRow();
        for (var j = 0; j < 2; j++) {
            var newCell = newRow.insertCell(j);
            // Set the cells to be empty or with a placeholder if needed
            newCell.style.color = 'white';
        }

        newRow.cells[0].innerText = i + 1;
        newRow.cells[1].innerText = data[i].top_ports;
    }
};

```

src="https://cdn.jsdelivr.net/npm/chart.js"
</script>

Dashboard CSS code:

```

@import
url("https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;500;600;700;800;900&display=swa
p");

* {
margin: 0;
padding: 0;
box-sizing: border-box;
font-family: "Poppins", sans-serif;
}

header {
position: fixed;
top: 0;

```

```
        left: 0;
        width: 100%;
        padding: 20px 100px;
        background: transparent;
        display: flex;
        justify-content: space-between;
        align-items: center;
        z-index: 99;

    }

body {
    display: flex;
    justify-content: center;
    align-items: center;
    min-height: 100vh;
    background-image: url('../images/bbackground.png');
    background-repeat: no-repeat;
    background-size: cover;
    background-position: center;
    background-attachment: fixed;
    margin: 0;
}

.logo {
    font-size: 1.8em;
    color: #fff;
    user-select: none;
    font-weight: 600;
    font-style: italic;
}

.wrapper {
    width: 1200px;
    height: 900px;
    background-color: rgba(14, 70, 178, .20);
    border: none;
    backdrop-filter: blur(-2px);
    box-shadow: 0 0 10px rgba(0, 0, 0, .1);
    color: #fff;
    border-radius: 10px;
    padding: 30px 40px;
    overflow: hidden;
    margin-top: 50px;
    margin: 0 auto;
    text-align: center;
}
```

```
.wrapper-header {  
    max-height: 100px !important;  
}  
  
.wrapper-card {  
    position: absolute !important;  
    top: 0 !important;  
}  
  
.chart-wrapper {  
    background-color: rgb(32,61,91);  
    color: #fff;  
    border-radius: 10px;  
    padding: 10px;  
    height:100%;  
}  
  
}  
  
.chart_wrapper {  
    background-color: rgb(32,61,91);  
    color: #fff;  
    border-radius: 10px;  
    padding: 10px;  
    padding-bottom: 20px;  
    height:100%;  
}  
  
}  
  
.floatingImage {  
    position: absolute;  
    bottom: 100%; /* Adjust the top position as needed */  
    left: 50px; /* Adjust the left position as needed */  
    z-index: 2; /* Ensure the image is on top of other elements */  
}  
  
  
.container p {  
    margin-top: 0;  
    margin-bottom: 1rem;  
    font-weight: 500;  
    font-family: 'Poppins';  
    font-size: 30px;  
    background-color: rgb(33,129,187);  
    border-radius: 40px;  
    width: fit-content;  
    padding: 10px 20px;  
  
    max-width: 100%;  
    white-space: nowrap;  
    overflow: hidden;  
    text-overflow: ellipsis;  
}
```

```
}

.wrapper p{
    font-style:italic;
    font-family:'Times New Roman', Times, serif;
    font-size: 20px;
    text-align: left;
    margin-left: 20px;
}

.navigation1 {
    color: #ffffff;
    margin-top: 30px;
    margin-left: 350px;
    font-size: 22px;
    display: inline;
}

.navigation1 a{
    color: #ffffff;
    margin-left: 650px;
    font-style:italic;
}

.row-header {
    display: flex;
    justify-content: space-between;
    align-items: center;
    padding: 20px 40px;
    background-color: transparent;
    color: #fff;
    height: 15%;
    margin-right: auto;
}

.row-header .navigation {
    display: flex;
    justify-content: flex-end;
    margin-top: 10px;
}

.row-header .navigation a {
    font-size: 25px;
    color: #fff;
    text-decoration: none;
    margin-left: 20px;
}

.row-header .navigation a:hover {
    text-decoration: underline;
```

```
}
```

```
.navigation .btnlogin-popup {
```

```
    width: 130px;
```

```
    height: 50px;
```

```
    background: transparent;
```

```
    border: 2px solid #fff;
```

```
    outline: none;
```

```
    border-radius: 6px;
```

```
    cursor: pointer;
```

```
    font-size: 1.1em;
```

```
    color: #fff;
```

```
    font-weight: 500;
```

```
    transition: .5s;
```

```
}
```

```
.navigation .btnlogin-popup:hover {
```

```
    background: #fff;
```

```
    color: #162938;
```

```
}
```

```
.col-sm-4 h2 {
```

```
    top: 5px;
```

```
    left: 5px;
```

```
    /* right: 1px; */
```

```
    margin-left: 40px;
```

```
    color: #ffffff;
```

```
    font-style: italic;
```

```
    margin-top: 25px;
```

```
    position: absolute;
```

```
    /* margin-right: 50px; */
```

```
}
```

```
.Dlogo {
```

```
    position: relative;
```

```
    right: 70px;
```

```
    top: 1px
```

```
    width: 110px;
```

```
}
```

```
.dashboardnumalerts {
```

```
    padding-left: 300px;
```

```
}
```

```
.icon-circle {
```

```
    display: inline-block;
```

```
    width: 15px;
```

```
    height: 15px;
```

```
    color: #fff;
```

```
    border-radius: 50%;
```

```
    text-align: center;
```

```
    line-height: 30px;
```

```

        cursor: pointer;
    }

.icon-circle i {
    font-size: 20px;
}

.question-mark {
    font-size: 18px;
}

@media screen and (min-width: 576px) /* IF PAGE WIDTH IS GREATER THAN 576px */
{
    .wrapper-card {
        width: 100% !important;
        padding-left: 50px !important;
        padding-right: 50px !important;
    }
}

@media screen and (max-width: 576px) /* IF PAGE WIDTH IS LESS THAN 576px */
{
    .wrapper-card {
        width: 100% !important;
        padding-left: 30px !important;
        padding-right: 30px !important;
    }
}

@media screen and (max-width: 576px)
{
    .navigation {
        margin-left: 0; /* Adjust as needed */
        text-align: right; /* Align to the right for smaller screens */
    }
}

.row-header {
    padding: 10px;
}

.row-header .navigation {
    flex-direction: column;
    align-items: center;
}

.row-header .navigation a {
    margin-left: 0;
    margin-top: 10px;
}

```

```

.col-sm-10 h4 {
  margin-right: 0;
  font-size: 20px;
}

.col-sm-4 h2 {
  top: 5px;
  left: 5px;
  margin-left: 105px;
  color: #ffffff;
  font-style: italic;
  margin-top: 30px;
}

.dashboardnumeralerts {
  padding-left: 300px;
}

.col-6 {
  flex: 0 0 50%;
  max-width: 60%;
}

@media only screen and (max-width: 768px) {
  .row-header {
    flex-direction: column;
    align-items: center;
    height: auto;
  }

  .row-header .navigation {
    margin-top: 20px;
    justify-content: center;
  }

  .col-sm-6 h2 {
    position: static;
    margin-top: 20px;
    margin-left: 0;
    text-align: center;
  }

  .Dlogo {
    position: static;
    margin-top: 10px;
  }
}

@media only screen and (max-width: 576px) {

```

```

.row-header {
  padding: 10px;
}

.row-header .navigation {
  flex-direction: column;
  align-items: center;
}

.row-header .navigation a {
  margin-left: 0;
  margin-top: 10px;
}

.col-12.wrapper button {
  width: 80%;
  height: 50px;
  font-size: 20px;
  margin: 10px 0;
}
}

Detect HTML code:
<!DOCTYPE html>
<html lang="en">

<head>

<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title> De-TECH </title>
<link rel="icon" href="../static/images/favicon16.png" sizes="16x16" type="image/png">
<link rel="icon" href="../static/images/favicon32.png" sizes="32x32" type="image/png">
<link rel="icon" href="../static/images/favicon192.png" sizes="192x192" type="image/png">
<link rel="icon" href="../static/images/favicon512.png" sizes="512x512" type="image/png">
<link rel="apple-touch-icon" href="../static/images/faviconapple.png" sizes="180x180">

<link href="../static/content/style1dtch.css" rel="stylesheet" />

<link href="https://unpkg.com/boxicons@2.1.4/css/boxicons.min.css" rel='stylesheet'>
<script src="https://momentjs.com/downloads/moment.min.js"></script>
<script src="../static/scripts/jquery-1.10.2.js"></script>
<script src="../static/scripts/detechSwitch.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/luxon/2.1.2/luxon.min.js"></script>

<!-- APPLY ALL PAGE START -->
<link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/css/bootstrap.min.css" integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">

```

```

<script src="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/js/bootstrap.min.js" integrity="sha384-JjSmVgyd0p3pXB1rRibZUAYoIly6OrQ6VrjIEaFf/nJGzIxDSf4x0xIM+B07jRM"
crossorigin="anonymous"></script>
<script src="https://code.jquery.com/jquery-3.6.4.min.js"></script>
<!-- APPLY ALL PAGE END -->

</head>

<body>

<!-- HEADER START -->
<div class="row-header">
<div class="col-sm-6 col-12">

<h2>De-TECH</h2>
</div>
<div class="col-sm-6 col-12">
<nav class="navigation">
<a href="/home">Home</a>
<a href="/about">About Us</a>
<a href="/detect" id="btnDetect">Detect</a>
<a href="/" id="loginLogOutMethod">Sign Out</a>
</nav>
</div>
</div>
<!-- HEADER END -->

<!-- CONTENT -->
<div class="col-12 wrapper">
<h1>DETECT</h1>
<div class="col-sm-10 col-12">
<h3>Status: <span id="captureStatus">Not Capturing</span></h3>
<h4>Duration: <span id="duration">0 minutes 0 seconds</span></h4>
</div>

<div class="col-12" style="margin-top: 40px;">
<button type="button" id="btn" class="btn">START CAPTURE</button>
<button type="button" id="btnnn" class="bttnn" style="display: none;">END CAPTURE</button>
</div>

<div class="col-12" style="margin-top: 20px;">
<a href="/analysis" class="bttn link-style" id="bttn" disabled>ANALYSIS</a>
<input type="hidden" id="userIdLoggedIn" />
</div>
</div>

<script src="https://momentjs.com/downloads/moment.min.js"></script>
<script src="../static/scripts/jquery-1.10.2.js"></script>
<script src="../static/scripts/detectSwitch.js"></script>

```

```

<script>
    // Check if the status is stored in localStorage and display it
    const status = localStorage.getItem('captureStatus');
    if (status) {
        $('#captureStatus').text(status);
    }

    $('#btn').click(function() {
        // Change the status message when the button is clicked
        $('#captureStatus').text('Capturing Packets');

        // Store the status in localStorage
        localStorage.setItem('captureStatus', 'Capturing Packets');

        // Optionally, change the status back when "END CAPTURE" is clicked or capturing is done
        $('#bttnn').click(function() {
            $('#captureStatus').text('Capturing Stopped');
            localStorage.setItem('captureStatus', 'Capturing Stopped');
        });
    });

    // Check if an alert message is provided and display it
    const userLoggedIn = "{{ userLoggedIn }}"; // Injected from Flask
    const userIdLoggedIn = "{{ userIdLoggedIn }}"; // Injected from Flask

    if (userLoggedIn != "") {
        $("#loggedInUserDescription").html("Hi, " + userLoggedIn + "!");
        $("#loginLogOutMethod").html("Sign Out");
        $("#userIdLoggedIn").val(userIdLoggedIn);
    } else {
        $("#loggedInUserDescription").html("");
        $("#loginLogOutMethod").html("Log In");
        $("#btnDetect").css("display", "none");
    }
</script>

</body>
</html>

```

Detect CSS code:

```

@import
url("https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;500;600;700;800;900&display=swa
p");

* {
margin: 0;
padding: 0;
box-sizing: border-box;
font-family: "Poppins", sans-serif;
}

```

```
body {
    min-height: 100vh;
    background: url(..../images/bbackground.png);
    background-repeat: no-repeat;
    background-size: cover;
    background-attachment: fixed;
}

.row-header {
    display: flex;
    justify-content: space-between;
    align-items: center;
    padding: 20px 40px;
    background-color: transparent;
    color: #fff;
    height: 15%;
    margin-right: auto;
}

.row-header .navigation {
    display: flex;
    justify-content: flex-end;
    margin-top: 10px;
}

.row-header .navigation a {
    font-size: 25px;
    color: #fff;
    text-decoration: none;
    margin-left: 20px;
}

.row-header .navigation a:hover {
    text-decoration: underline;
}

.navigation .btnlogin-popup {
    width: 130px;
    height: 50px;
    background: transparent;
    border: 2px solid #fff;
    outline: none;
    border-radius: 6px;
    cursor: pointer;
    font-size: 1.1em;
    color: #fff;
    font-weight: 500;
    transition: .5s;
}

.navigation .btnlogin-popup:hover {
    background: #fff;
```

```
color: #162938;
}

.col-sm-6 h2 {
    position: fixed;
    top: 5px;
    left: 5px;
    margin-left: 120px;
    color: #ffffff;
    font-style: italic;
    margin-top: 25px;
}

.Dlogo {
    position: fixed;
    left: 20px;
    top: 1px;
    width: 110px;
}

.col-12.wrapper {
    position: relative;
    width: 90%;
    margin: 50px auto;
    background-color: rgba(14, 70, 178, .20);
    border: none;
    backdrop-filter: blur(-2px);
    box-shadow: 0 0 10px rgba(0, 0, 0, .1);
    color: #fff;
    border-radius: 50px;
    padding: 30px 40px;
}

.col-12.wrapper::before {
    content: "";
    position: absolute;
    border: 3px solid #2382BC;
    border-radius: 60px;
    top: -5%;
    left: -1.5%;
    right: -1.5%;
    bottom: -5%;
}

.col-12.wrapper .col-12 {
    display: flex;
    flex-direction: column;
    justify-content: center;
    align-items: center;
    margin-top: auto;
}
```

```
.col-12.wrapper button {  
    width: 55%;  
    height: 70px;  
    margin: 10px 0;  
    text-align: center;  
    background: #808080;  
    border-radius: 40px;  
    box-shadow: 0 0 10px rgba(0, 0, 0, .1);  
    cursor: pointer;  
    font-size: 50px;  
    font-family: 'Times New Roman';  
    color: #fff;  
    display: flex;  
    justify-content: center;  
    align-items: center;  
}  
  
.col-12.wrapper button:active {  
    margin-top: 35px; /* Adjust the margin-top value as needed */  
}  
  
.col-12.wrapper button.active, .col-12.wrapper button:hover {  
    background-color: #01C063;  
    color: #fff;  
    box-shadow: 0 0 26px 1px #01C063;  
    border: 1px solid #01C063;  
}  
  
.col-12.wrapper .bttnnn.active,  
.col-12.wrapper .bttnnn:hover {  
    background-color: #f44336;  
    box-shadow: 0 0 26px 1px #f44336;  
    border: 1px solid #f44336;  
}  
  
.link-style {  
    width: 55%;  
    height: 70px;  
    margin: 10px 0;  
    text-align: center;  
    background: #808080;  
    border-radius: 40px;  
    box-shadow: 0 0 10px rgba(0, 0, 0, .1);  
    cursor: pointer;  
    font-size: 50px;  
    font-family: 'Times New Roman';  
    color: #fff;  
    display: flex;  
    justify-content: center;  
    align-items: center;  
}
```

```

.link-style.active, .link-style:hover {
    background-color:#2382BC;
    color: #fff;
    box-shadow: 0 0 26px 1px #2382BC;
    border: 1px solid #2382BC;
    text-decoration: none;
}

.col-12.wrapper h1 {
    position: relative;
    font-size: 5rem;
    font-weight: 700;
    text-align: left;
    max-width: calc(100% - 30px);
    white-space: nowrap;
    overflow: hidden;
    text-overflow: ellipsis;
}

#captureStatus {
    font-weight: bold;
    color: #007BFF;
    font-family: 'Times New Roman';
    font-style: normal;
}

.col-sm-10.col-12 {
    max-width: 100%;
}

.col-sm-10 h3,
.col-sm-10 h4 {
    font-size: 35px;
    text-align: center;
}

.col-sm-10 h4 {
    font-size: 35px;
    text-align: center;
    margin: 10px auto;
}

.col-sm-10 h4 span {
    font-weight: normal;
}

@media screen and (max-width: 576px) /* IF PAGE WIDTH IS LESS THAN 576px */
{
    .row-header {
        padding: 10px;
    }
}

```

```
.row-header .navigation {  
    flex-direction: column;  
    align-items: center;  
}  
  
.row-header .navigation a {  
    margin-left: 0;  
    margin-top: 10px;  
}  
  
.col-sm-10 h4 {  
    margin-right: 0;  
    font-size: 20px;  
}  
}  
  
@media screen and (max-width: 768px) {  
    .row-header {  
        flex-direction: column;  
        align-items: center;  
        height: auto;  
    }  
  
.row-header .navigation {  
    margin-top: 20px;  
    justify-content: center;  
}  
  
.col-sm-6 h2 {  
    position: static;  
    margin-top: 20px;  
    margin-left: 0;  
    text-align: center;  
}  
  
.Dlogo {  
    position: static;  
    margin-top: 10px;  
}  
  
.col-12.wrapper button {  
    width: 100%;  
    max-width: 300px;  
    margin: 10px auto;  
    padding: 10px;  
    font-size: 18px;  
}  
  
.col-12.wrapper button.bttn {  
    margin-top: 20px;  
}
```

```

.link-style {
    width: 100%;
    max-width: 300px;
    margin: 10px auto;
    padding: 10px;
    font-size: 18px;
}

.link-style {
    margin-top: 20px;
}

.col-sm-10 h4 {
    font-size: 25px; /* Adjust font size for smaller screens */
}

@media only screen and (max-width: 956px) {
    .col-12.wrapper button {
        width: 100%;
        max-width: 300px;
        margin: 10px auto;
        padding: 10px;
        font-size: 18px;
    }

    .col-12.wrapper button.bn {
        margin-top: 20px;
    }

    .link-style {
        width: 100%;
        max-width: 300px;
        margin: 10px auto;
        padding: 10px;
        font-size: 18px;
    }

    .link-style {
        margin-top: 20px;
    }
}

```

History HTML code:

```

<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="UTF-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <title> De-TECH </title>
        <link rel="icon" href="../static/images/favicon16.png" sizes="16x16" type="image/png">

```

```

<link rel="icon" href="../static/images/favicon32.png" sizes="32x32" type="image/png">
<link rel="icon" href="../static/images/favicon192.png" sizes="192x192" type="image/png">
<link rel="icon" href="../static/images/favicon512.png" sizes="512x512" type="image/png">
<link rel="apple-touch-icon" href="../static/images/faviconapple.png" sizes="180x180">
<link rel="stylesheet" href="../static/content/hstyle.css">
<link href='https://unpkg.com/boxicons@2.1.4/css/boxicons.min.css' rel='stylesheet'>
<script src="../static/scripts/jquery-1.10.2.js"></script>
<style>
    .scrollable-table {
        max-height: 500px;
        /* Set the max height of the table */
        overflow-y: auto;
        /* Enable vertical scrolling */
    }
</style>
</head>
<body>

<!-- PARENT WRAPPER -->
<div class="wrapper-card">

    <!-- HEADER START -->
    <div class="row-header">
        <div class="col-sm-5 col-12">
            
            <h2>De-TECH</h2>
        </div>
        <div class="col-sm-3 col-12" style="text-align: right;">
            <div class="container01" style="text-align: right;">
                <p>HISTORY</p>
            </div>
        </div>
        <div class="col-sm-4 col-12">
            <nav class="navigation">
                <a href="/home">Home</a>
                <a href="/analysis">Analysis</a>
                <a href="/dashboard">Dashboard</a>
            </nav>
        </div>
    </div>
    <!-- HEADER END -->

    <!-- CONTENT -->

    <div class="col-12" style="min-height:100px; padding:10px;">
        <div class="wrapper-m" style="align-items: center;">
            <div class="row">
                <div class="scrollable-table">
                    <table class="data-table">

```

```

<thead>
  <tr>
    <th>DATE</th>
    <th>TIME</th>
    <th>Src IP Address</th>
    <th>Dst IP Address</th>
    <th>TRAFFIC</th>
    <th>CLASSIFICATION</th>
  </tr>
</thead>
<tbody id='tblHistoryBody'></tbody>
</table>
</div>
</div>
</div>
</div>
</div>
</script>
const userLoggedIn = "{{ userLoggedIn }}"; // Injected from Flask
const userIdLoggedIn = "{{ userIdLoggedIn }}"; // Injected from Flask
let historyJSONdata = "{{ historyJSONdata }}";
let historyData = JSON.parse(historyJSONdata.replace(/\\"/g, ""));
let tblHistoryRow = 1;
let tblHistoryBody = "";
$.each(historyData, function(index, item) {
  // Access individual properties for each item
  var historyDataDate = new Date(item.date);
  // Format date
  var monthNames = ["January", "February", "March", "April", "May", "June", "July", "August",
"September", "October", "November", "December"];
  var formattedDate = monthNames[historyDataDate.getMonth()] + ' ' + historyDataDate.getDate() + ', '
+ historyDataDate.getFullYear();
  // Format time
  var timeParts = item.time.split(":");
  var hours = parseInt(timeParts[0], 10);
  var minutes = parseInt(timeParts[1], 10);
  var seconds = parseInt(timeParts[2], 10);
  var ampm = hours >= 12 ? "PM" : "AM";
  hours = hours % 12;
  hours = hours ? hours : 12; // Handle midnight (00:00:00) as 12 AM
  var formattedTime = hours + ":" + minutes + ":" + seconds + " " + ampm;
  var historyDataTime = formattedTime;
  var historyDataSourceip = item.sourceip;
  var historyDataDestip = item.destip;
  var historyDataTraffic = item.traffic;
  var historyDataClassification = item.classification;
  let historyTableRow =
<tr>
  <td class="td${tblHistoryRow}" id="historydate${tblHistoryRow}">${formattedDate}</td>
  <td class="td${tblHistoryRow}" id="historystarttime${tblHistoryRow}">${historyDataTime}</td>

```

```

<td class="td${tblHistoryRow}"  

id="historysourceip${tblHistoryRow}">${historyDataSourceip}</td>  

<td class="td${tblHistoryRow}" id="historydestip${tblHistoryRow}">${historyDataDestip}</td>  

<td class="td${tblHistoryRow}" id="historytraffic${tblHistoryRow}">${historyDataTraffic}</td>  

<td class="td${tblHistoryRow}"  

id="historyclassification${tblHistoryRow}">${historyDataClassification}</td>  

</tr>`;  
  

tblHistoryBody = tblHistoryBody + historyTableRow;  

tblHistoryRow++;  

});  

// Append additional continuous rows  

const startIdx = tblHistoryRow; // Index to start continuous rows  

const numRowsToAdd = 5; // Number of continuous rows to add  

for (let i = 0; i < numRowsToAdd; i++) {  

let continuousHistoryTableRow = `  

<tr>  

<td>New Date ${startIdx + i}</td>  

<td>New Time ${startIdx + i}</td>  

<td>New Sourceip ${startIdx + i}</td>  

<td>New Destip ${startIdx + i}</td>  

<td>New Traffic ${startIdx + i}</td>  

<td>New Classification ${startIdx + i}</td>  

</tr>`;  

tblHistoryBody += continuousHistoryTableRow;  

}  

$("#tblHistoryBody").html(tblHistoryBody);  

</script>  
  

</body>  

</html>

```

History CSS code:

```

@import  

url("https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;500;600;700;800;900&display=swa  

p");  
  

* {  

margin: 0;  

padding: 0;  

box-sizing: border-box;  

font-family: "Poppins", sans-serif;  

}  
  

header {  

position: fixed;

```

```
    top: 0;
    left: 0;
    width: 100%;
    padding: 20px 100px;
    background: transparent;
    display: flex;
    justify-content: space-between;
    align-items: center;
    z-index: 99;

}

body {
    display: flex;
    justify-content: center;
    align-items: center;
    min-height: 100vh;
    background-image: url('../images/bbackground.png');
    background-repeat: no-repeat;
    background-size: cover;
    background-position: center;
    background-attachment: fixed;
    margin: 0;
}

.col-md-8 {
    display: flex;
    align-items: center;
}

.logo {
    font-size: 1.8em;
    color: #fff;
    user-select: none;
    font-weight: 600;
    font-style: italic;
}

.navigation {
    margin-top: 30px;
}

.header-right {
    text-align: right;
    font-size: 26px;
    text-decoration: none;
    font-weight: 500;
    font-style: italic;
}
```

```

.btn-dashboard {
    font-size: 25px;
    color: #fff;
    text-decoration: none;
    font-weight: 500;
    margin: 20px;
    font-style: italic;
    position: absolute;
    top: 10px;
    right: 20px;
    z-index: 999;
    display: block;
}

.btn-dashboard::after {
    content: attr(data-text);
    position: absolute;
    left: 0;
    bottom: -6px;
    width: 100%;
    height: 3px;
    background: #fff;
    border-radius: 5px;
    transform-origin: right;
    transform: scaleX(0);
    transition: transform .5s, width .5s;
}

.btn-dashboard:hover::after {
    transform: scaleX(1);
    width: 100%; /* Expand width on hover */
}

.container01 p {
    font-family: 'Poppins';
    font-size: 30px;
    font-weight: 500;
    background-color: rgb(33,129,187);
    width: fit-content;
    border-radius: 40px;
    padding: 10px 20px;

    margin-bottom: 15px;

    color: #fff;
}

.wrapper-m {
    min-height: 600px; /* Changed from height to min-height */
    background-color: rgba(14, 70, 178, .20);
    border: none;
}

```

```

        box-shadow: 0 0 10px rgba(0, 0, 0, .1);
        color: #fff;
        border-radius: 50px;
        padding: 30px 40px;
        justify-content: center;
        display: flex;
        margin-left: 30px;
        overflow-x: auto;
    }

.wrapper-m-container {
    position: relative; /* Required for absolute positioning of pseudo-element */
}

.wrapper-m p{
    font-style:italic;
    font-family:"Times New Roman', Times, serif;
    font-size: 20px;
    text-align: left;
    margin-left: 20px;
}

.navigation1 {
    color: #ffffff;
    margin-left: 300px;
    font-size: 22px;
    display: inline;
    position: relative;
    z-index: 1000;
}

.table.data-table {
    width: 5px; /* Set the width as desired */
    margin: 0 auto; /* Center the table */
    border-collapse: collapse;
    margin-top: 20px;
    text-align: center;
}

.table.data-table th, table.data-table td {
    border: 1px solid #ddd;
    padding: 8px;
    text-align: center;
    border-radius: 5px;
    background-color: #35648F;
    color: #ffffff;
    font-size: 20px;
    min-width: 170px;
    height: 50px;
    text-align: center;
}

```

```

        border: 3px solid #BEDAEF
    }

.table.data-table th {
    background-color: #f2f2f2;
    font-family:'Times New Roman', Times, serif;
}

.data-table thead tr {
    background-color: #2181BB;
    color: #ffffff;
    text-align: Center;
    font-family:'Times New Roman', Times, serif;
    font-size: 20px;
}

.scrollable-table {
    max-height: 400px;
    width: 100%;
    overflow-y: auto;
    overflow-x: auto;
    margin-left: 25px;
    margin-right: 25px;
    margin-top: 20px;
    margin-bottom: 20px;
}

.table.data-table th:nth-child(1),
.table.data-table td:nth-child(1) {
    width: 10%; /* Adjust the width of the first column */
}

.table.data-table th:nth-child(2),
.table.data-table td:nth-child(2) {
    width: 15%; /* Adjust the width of the second column */
}

.row-header {
    display: flex;
    justify-content: space-between;
    align-items: center;
    padding: 20px 40px;
    background-color: transparent;
    color: #fff;
    height: 15%;
    margin-right: auto;
}

.row-header .navigation {
    display: flex;
    justify-content: flex-end;
}

```

```
    margin-top: 10px;  
}
```

```
.row-header .navigation a {  
    font-size: 25px;  
    color: #fff;  
    text-decoration: none;  
    margin-left: 20px;  
}
```

```
.row-header .navigation a:hover {  
    text-decoration: underline;  
}
```

```
.navigation .btnlogin-popup {  
    width: 130px;  
    height: 50px;  
    background: transparent;  
    border: 2px solid #fff;  
    outline: none;  
    border-radius: 6px;  
    cursor: pointer;  
    font-size: 1.1em;  
    color: #fff;  
    font-weight: 500;  
    transition: .5s;  
}
```

```
.navigation .btnlogin-popup:hover {  
    background: #fff;  
    color: #162938;  
}
```

```
.col-sm-5 h2 {  
    top: 5px;  
    left: 5px;  
    /* right: 1px; */  
    margin-left: 180px;  
    color: #fffff;  
    font-style: italic;  
    margin-top: 60px;  
    position: absolute;  
    /* margin-right: 50px; */  
    font-weight: 500;  
    font-size: 32px;  
}
```

```
.Dlogo {  
    position: relative;  
  
    top: 1px  
    width: 110px;
```

```

}

.col-sm-3 p {
    margin-left: 200px;
}

@media screen and (min-width: 576px) /* IF PAGE WIDTH IS GREATER THAN 576px */
{
    .wrapper-card {
        width: 100% !important;
        padding-left: 50px !important;
        padding-right: 50px !important;
    }

    .logo {
        font-size: 1.8em;
        color: #fff;
        user-select: none;
        font-weight: 600;
        font-style: italic;
    }

    .col-sm-5 h2 {
        top: 15px;
        left: 9px;
        /* right: 1px; */
        margin-left: 180px;
        color: #ffffff;
        font-style: italic;
        margin-top: 60px;
        position: absolute;
        /* margin-right: 50px; */
        font-weight: 500;
        font-size: 32px;
    }

    .Dlogo {
        position: relative;

        top: 1px
        width: 110px;
    }
}

@media screen and (max-width: 650px) /* IF PAGE WIDTH IS LESS THAN 576px */
{
}

```

```

.wrapper-card {
  width: 100% !important;
  padding-left: 30px !important;
  padding-right: 30px !important;
}

.col-md-8 {
  justify-content: center;
}

.navigation {
  order: -1; /* Move the navigation to the top */
  margin-top: 10px; /* Adjust the margin as needed */
  text-align: center; /* Center the navigation */
}

.btn-dashboard {
  position: static; /* Reset the position to static */
  margin-top: 20px; /* Adjust the margin as needed */
}

.row-header {
  padding: 10px;
}

.row-header .navigation {
  flex-direction: column;
  align-items: center;
}

.row-header .navigation a {
  margin-left: 0;
  margin-top: 10px;
}

.col-sm-10 h4 {
  margin-right: 0;
  font-size: 20px;
}

.scrollable-table {
  max-height: 500px;
  /* Set the max height of the table */
  overflow-y: auto;
  /* Enable vertical scrolling */
}

.col-sm-5 h2 {
  margin-left: 130px;
  margin-top: 60px;
  text-align: right;
}

```

```

}

.col-sm-3 p {
margin-left: 1px;

}

.data-table {
max-width: 50%;

}

.table.data-table th, table.data-table td {
border: 1px solid #ddd;
padding: 8px;
text-align: center;
border-radius: 5px;
background-color: #35648F;
color: #ffffff;
font-size: 5px;
min-width: 5px;
height: 50px;
text-align: center;
border: 1px solid #BEDAEF
}

.data-table thead tr {
background-color: #2181BB;
color: #ffffff;
text-align: Center;
font-family:'Times New Roman', Times, serif;
font-size: 5px;
}

}

@media only screen and (max-width: 768px) {

.row-header {
flex-direction: column;
align-items: center;
height: auto;
}

.row-header .navigation {
margin-top: 20px;
justify-content: center;
}

.col-sm-6 h2 {
position: static;
margin-top: 20px;
margin-left: 0;
text-align: center;
}

```

```

}

.Dlogo {
  position: static;
  margin-top: 10px;
  margin-right: 200px;
}

.col-sm-5 h2 {
  margin-left: 130px;
  margin-top: 60px;
  text-align: right;
}

.col-sm-3 p {
  margin-left: 1px;
}

.scrollable-table {
  max-height: 500px;
  /* Set the max height of the table */
  overflow-y: auto;
  /* Enable vertical scrolling */
}
}

@media only screen and (max-width: 576px) {
  .row-header {
    padding: 10px;
  }

  .row-header .navigation {
    flex-direction: column;
    align-items: center;
  }

  .row-header .navigation a {
    margin-left: 0;
    margin-top: 10px;
  }

  .col-12.wrapper button {
    width: 80%;
    height: 50px;
    font-size: 20px;
    margin: 10px 0;
  }

  .scrollable-table {
    max-height: 500px;
    /* Set the max height of the table */
  }
}

```

```

        overflow-y: auto;
        /* Enable vertical scrolling */
    }
}

Home page HTML code:
/* Global styles */

@import
url("https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;500;600;700;800;900&display=swa
p");

* {
    padding: 0;
    margin: 0;
    font-family: 'Poppins', sans-serif;
    text-decoration: none;
    list-style: none;
}

body {
    display: inline;
    justify-content: center;
    align-items: center;
    min-height: 100vh;
    background-image: url('../images/bbackground.png');
    background-size: cover;
    background-position: center;
    background-repeat: no-repeat;
    background-attachment: fixed;
}

header {
    width: 100%;
    top: 0;
    right: 0;
    z-index: 1000;
    align-items: center;
    transition: all .50s ease;
}

.logo {
    position: relative;
    font-size: 1.8em;
    color: #fff;
    user-select: none;
    font-weight: 600;
    font-style: italic;
    margin-left: 15px;
}

.Dlogo {

```

```
position: absolute;
height: 100px;
left: 20px;
top: -5px;
width: 100px;
}

.user-greeting {
margin-top: 30px;
color: #ffffff;
font-style: italic;
font-size: 28px;
font-weight: 600;
}

.navigation a {
font-size: 30px;
color: #fff;
text-decoration: none;
font-weight: 500;
margin: 20px;
}

.navigation a::after {
content: "";
position: absolute;
left: 0;
bottom: -6px;
width: 100%;
height: 3px;
background: #fff;
border-radius: 5px;
transform-origin: right;
transform: scaleX(0);
transition: transform .5s;
}

.navigation .btnlogin-popup {
width: 130px;
height: 50px;
background: transparent;
border: 2px solid #fff;
outline: none;
border-radius: 6px;
font-size: 1.1em;
color: #fff;
font-weight: 500;
transition: .5s;
}

.navigation .btnlogin-popup:hover {
background: #fff;
```

```
    color: #162938;
}

.user {
    position: relative;
    color: #2382BC;
    align-items: center;
    font-size: 75px;
}

.dropdown {
    position: relative;
    display: inline-block;
}

.dropdown-content {
    display: none;
    position: absolute;
    background-color: rgba(22, 86, 212, 0.2);
    border: none;
    backdrop-filter: blur(20px);
    box-shadow: 0 0 10px rgba(0, 0, 0, 10);
    border-radius: 5px;
    z-index: 1;
    top: 100%;
    left: 0;
    width: 150px;
}

.dropdown:hover .dropdown-content {
    display: block;
}

.dropdown-content a {
    color: #fff;
    padding: 10px 15px;
    display: block;
    text-decoration: none;
    transition: all .50s ease;
    font-size: 20px;
}

.dropdown-content a:hover {
    background-color: rgba(255, 255, 255, 0.1);
}

#menu-icon {
    font-size: 35px;
    color: var(--text-color);
    cursor: pointer;
    z-index: 10001;
    display: none;
}
```

```
}

.col-12-content {
    display: flex;
    justify-content: left;
    flex-wrap: wrap;
    align-items: center;
}

.col-12-content h1.detect {
    font-size: 3.5vw;
    color: #fff;
    margin-right: 20px;
    font-weight: 600;
}

.intrusion {
    display: flex;
    flex-direction: column;
}

.intrusion h2,
.intrusion h3 {
    color: #fff;
    margin: 0;
    margin-top: 5px;
}

.intrusion h2 {
    font-size: 2.2rem;
    font-weight: 800;
}

.intrusion h3 {
    font-size: 1.5rem;
    text-align: center;
}

.col-12-image {
    margin-top: 20px;
}

.col-12-image img {
    width: 100%;
    height: 500px;
}

.chart-wrapper {
    background-color: rgb(32,61,91);
    color: #fff;
    border-radius: 10px;
    padding: 10px;
```

```

}

@media (min-width: 576px) {
  .user-greeting {
    margin-top: 0;
    margin-left: 0;
  }
}

@media (min-width: 768px) {
  .user-greeting {
    margin-top: 30px;
    margin-left: 130px;
  }
}

@media (max-width: 768px) {
  .col-12-content h1.detect {
    font-size: 5vw;
    font-weight: 600;
  }

  .intrusion h2,
  .intrusion h3,
  .col-12-content h1.detect {
    font-size: 2em;
  }

  .intrusion h2 {
    font-size: 2.2rem;
    font-weight: 800;
    text-align: center;
  }
}

@media (max-width: 1090px) {
  #menu-icon {
    display: block;
  }

  .wrapper h1,
  .wrapper h2,
  .wrapper h3,
  .img,
  .logodt {
    position: static;
    margin: 0;
  }
}

@media (min-width: 1200px) {
  .col-12-content {
    font-size: 3.5vw; /* Set font size based on viewport width */
  }
}

```

```
}
```

Login page HTML code:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>De-TECH</title>
    <!-- Link to your CSS file -->
    <link rel="stylesheet" href="../static/content/stylemain1.css">
    <!-- Link to Bootstrap CSS -->
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/css/bootstrap.min.css"
integrity="sha384-
ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T"
crossorigin="anonymous">
    <link href='https://unpkg.com/boxicons@2.1.4/css/boxicons.min.css' rel='stylesheet'>
</head>
<body>
    <!-- HEADER START -->
    <div class="container-fluid">
        <div class="row align-items-center">
            <div class="col-md-6 d-flex align-items-center">
                <div class="col-md-6 text-right">
                    <nav class="navigation" style="font-size: 1.5rem;">
                        <div class="dropdown d-sm-none">
                            <button class="btn btn-secondary dropdown-toggle" type="button"
id="dropdownMenuButton" data-toggle="dropdown" aria-haspopup="true" aria-expanded="false">
                                Menu
                            </button>
                            <div class="dropdown-menu dropdown-menu-right" aria-
labelledby="dropdownMenuButton">
                                <a class="dropdown-item" href="/home">Home</a>
                                <a class="dropdown-item" href="/about">About Us</a>
                                <button class="btnlogin-popup dropdown-item">Login</button>
                            </div>
                        </div>
                    <div class="d-none d-sm-block">
                        <a href="/home" class="text-white">Home</a>
                        <a href="/about" class="text-white">About Us</a>
                        <button class="btn btn-outline-light btnlogin-popup">Login</button>
                    </div>
                </nav>
            </div>
        </div>
    </div>
    <!-- HEADER END -->
```

```

<!-- Your existing content -->
<div class="row-content">
    <span class="icon-close" onclick="closeForm()">
        <i class='bx bx-x'></i>
    </span>

    <form method="post" action="/">
        <div class="form login_form" id="loginForm">

            <h1>Sign In</h1>
            <i><h5>The safety within your reach.</h5></i>

            <div class="input-box">
                <label for="usr"><b>Username</b></label>
                <input type="username" placeholder="Type your username" id="loginPageUsername" name="loginPageUsername" required>
                    <i class="bx bxs-user"></i>
            </div>

            <div class="input-box">
                <label for="psw"><b>Password</b></label>
                <input type="password" placeholder="Type your password" id="loginPagePassword" name="loginPagePassword" required>
                    <i class="bx bxs-lock"></i>
            </div>

            <div class="remember-forgot">
                <label><input type="checkbox" /> Remember me</label>
                <a href="#">Forgot password?</a>
            </div>

            <button type="submit" class="btn">Login</button>

            <div class="register-link">
                <p>Not a member? <a href="register" class="loginLink"> Register Here!</a></p>
            </div>
        </div>
    </form>
</div>

<script>
    // Check if an alert message is provided and display it
    const alert_message = "{{ alert_message }}"; // Injected from Flask

    if (alert_message) {
        alert(alert_message);
    }
</script>

<!-- Link to Bootstrap JS and jQuery -->

```

```

<script src="https://code.jquery.com/jquery-3.6.4.min.js"></script>
<script src="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/js/bootstrap.min.js" integrity="sha384-JjSmVgyd0p3pXB1rRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM"
crossorigin="anonymous"></script>
</body>
</html>

```

Login page CSS code:

```

/* Global Styles */
@import
url("https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;500;600;700;800;900&display=swa
p");

* {
    margin: 0;
    padding: 0;
    box-sizing: border-box;
    font-family: "Poppins", sans-serif;
}

body {
    min-height: 100vh;
    background: url(..//images/bbackground.png);
    background-repeat: no-repeat;
    background-size: cover;
    background-attachment: fixed;
    overflow: hidden; /* Prevent scrolling */
}

/* Header Styles */
.container-fluid {
    background-color: transparent;
    padding: 10px;
}

.Dlogo {
    max-height: 110px;
    margin-right: 10px;
}

.navigation a {
    font-size: 1.5em;
    color: #fff;
    text-decoration: none;
    margin-left: 40px;
    margin-right: 20px;
    position: relative;
}

.navigation a::after {
    content: "";
    background: #fff;
}

```

```
border-radius: 5px;
transform-origin: right;
transform: scaleX(0);
transition: transform 0.5s;
position: absolute;
bottom: -5px;
left: 0;
right: 0;
margin: 0 auto;
}

.navigation a:hover::after {
    transform: scaleX(1);
}

.navigation .btnlogin-popup {
    width: 130px;
    height: 50px;
    background: transparent;
    border: 2px solid #fff;
    border-radius: 6px;
    cursor: pointer;
    font-size: 1.1em;
    color: #fff;
    font-weight: 500;
    margin-left: 40px;
    transition: background 0.5s, color 0.5s;
}

.navigation .btnlogin-popup:hover {
    background: #fff;
    color: #162938;
}

/* Content Styles */
.row-content {
    width: 420px;
    background-color: rgba(14, 70, 178, 0.2);
    border: none;
    backdrop-filter: blur(-2px);
    box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
    color: #fff;
    border-radius: 10px;
    padding: 30px 40px;
    text-align: center;
    overflow: hidden;
    transition: transform 0.5s ease;
    margin: 0 auto;
    position: relative;
}

.row-content.active-popup {
```

```
        transform: scale(1);
    }

.row-content .icon-close {
    position: absolute;
    top: 0;
    right: 0;
    width: 45px;
    height: 45px;
    background-color: rgba(31, 125, 174, 0.2);
    font-size: 2em;
    color: #fff;
    display: flex;
    justify-content: center;
    align-items: center;
    border-bottom-left-radius: 20px;
    cursor: pointer;
    z-index: 1;
}

.row-content h1 {
    font-size: 36px;
    text-align: center;
    font-weight: 500;
}

.row-content h5 {
    font-size: 15px;
    text-align: center;
    font-weight: 100;
}

.row-content .input-box {
    position: relative;
    width: 100%;
    height: 50px;
    margin: 30px 0;
    text-align: left;
}

.input-box b {
    margin-left: 17px;
    font-weight: 100;
}

.input-box input {
    width: 100%;
    height: 100%;
    background: transparent;
    border: none;
    outline: none;
    border: 3px solid;
```

```
border-color: #fff;
border-radius: 40px;
font-size: 16px;
color: #fff;
padding: 20px 0px 20px 45px;
}

.input-box input::placeholder {
  color: white;
  font-style: italic;
}

.input-box i {
  position: absolute;
  left: 15px;
  top: 110%;
  transform: translateY(-50%);
  font-size: 30px;
}

.row-content .remember-forgot {
  display: flex;
  justify-content: space-between;
  font-size: 14.5px;
  margin: -20px 0 5px;
}

.remember-forgot label input {
  accent-color: #fff;
  margin-left: 17px;
  margin-top: 25px;
}

.remember-forgot a {
  color: green;
  text-decoration: none;
  margin-top: 25px;
}

.remember-forgot a:hover {
  text-decoration: underline;
}

.row-content .btn {
  width: 100%;
  height: 45px;
  background: #2382BC;
  border: none;
  outline: none;
  border-radius: 40px;
  box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
  cursor: pointer;
}
```

```

font-size: 16px;
color: #fff;
font-weight: 600;
}

/* Media Queries */
@media screen and (min-width: 576px) {
    /* Adjustments for larger screens */
    .container-fluid {
        padding: 20px;
    }

    .row-content {
        width: 500px;
    }
}

@media screen and (max-width: 576px) {
    /* Adjustments for smaller screens */
    .container-fluid {
        padding: 10px;
    }

    .row-content {
        width: 100%;
        margin-top: 10px;
    }
}

```

De-TECH Members page HTML code:

```

<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="UTF-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <title> De-TECH Members </title>
        <link rel="icon" href="../static/images/favicon16.png" sizes="16x16" type="image/png">
        <link rel="icon" href="../static/images/favicon32.png" sizes="32x32" type="image/png">
        <link rel="icon" href="../static/images/favicon192.png" sizes="192x192" type="image/png">
        <link rel="icon" href="../static/images/favicon512.png" sizes="512x512" type="image/png">
        <link rel="apple-touch-icon" href="../static/images/faviconapple.png" sizes="180x180">
        <link href='https://unpkg.com/boxicons@2.1.4/css/boxicons.min.css' rel='stylesheet'>
        <link href="../static/content/style5m.css" rel="stylesheet" />
        <script src="../static/scripts/jquery-1.10.2.js"></script>
        <script src="../static/scripts/js/abs.js"></script>
        <script src="../static/scripts/js/script1.js"></script>
        <!-- APPLY ALL PAGE START -->
        <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/css/bootstrap.min.css" integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">

```

```

<script src="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/js/bootstrap.min.js" integrity="sha384-JjSmVgyd0p3pXB1rRibZUAYoIlly6OrQ6VrjIEaFf/nJGzIxDSf4x0xIM+B07jRM"
crossorigin="anonymous"></script>
<script src="https://code.jquery.com/jquery-3.6.4.min.js"></script>
<!-- APPLY ALL PAGE END -->
</head>
<body>

<!-- HEADER START -->
<div class="row-header">
    <div class="col-sm-6 col-12">
        
        <h2>De-TECH</h2>
    </div>
    <div class="col-sm-6 col-12">
        <nav class="navigation">
            <a href="/home">Home</a>
            <a href="/about">About Us</a>
            <a href="/detect" id="btnDetect">Detect</a>
            <a href="/" id="loginLogOutMethod">Sign Out</a>
        </nav>
    </div>
</div>
<!-- HEADER END -->

<!-- CONTENT -->
<div class="col-12 wrapper" style="text-align: center">
    <h1>MEMBERS</h1>

    <div class="col-12" style="margin-top: 80px;">
        
        
        
    </div>

    <div class="Word">
        <span class="name1">Aila Marie S. Pengson</span>
        <span class="name2">Aliah Fhae A. Felipe</span>
        <span class="name3">Judiel A. Isaias</span>
    </div>

    <div class="col-12" style="margin-top: 60px;">
        
        
        
    </div>

    <div class="Word1">
        <span class="name4">Khylla Krizel S. Delos Reyes</span>
    </div>

```

```

<span class="name5">Mary Grace C. Ponciano</span>
<span class="name6">Ranah Mae M. Caseria</span>
</div>
</div>

<script>
$(document).ready(function() {
    // Check if an alert message is provided and display it
    const userLoggedIn = "{{ userLoggedIn }}"; // Injected from Flask
    if (userLoggedIn != "") {
        $("#loggedInUserDescription").html("Hi, " + userLoggedIn + "!");
        $("#loginLogOutMethod").html("Sign Out");
    } else {
        $("#loggedInUserDescription").html("");
        $("#loginLogOutMethod").html("Log In");
        $("#btnDetect").css("display", "none");
    }
});
</script>

</body>
</html>

```

De-TECH Members page CSS code:

```

@import
url("https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;500;600;700;800;900&display=swa
p");

* {
margin: 0;
padding: 0;
box-sizing: border-box;
font-family: "Poppins", sans-serif;
}

body {
min-height: 100vh;
background: url(..//images/bbackground.png);
background-repeat: no-repeat;
background-size: cover;
background-attachment: fixed;
}

.row-header {
display: flex;
justify-content: space-between;
align-items: center;
padding: 20px 40px;
background-color: transparent;
color: #fff;
}

```

```
height: 15%;  
margin-right: auto;  
}  
  
.row-header .navigation {  
    display: flex;  
    justify-content: flex-end;  
    margin-top: 10px;  
}  
  
.row-header .navigation a {  
    font-size: 25px;  
    color: #fff;  
    text-decoration: none;  
    margin-left: 20px;  
}  
  
.row-header .navigation a:hover {  
    text-decoration: underline;  
}  
  
.navigation .btnlogin-popup {  
    width: 130px;  
    height: 50px;  
    background: transparent;  
    border: 2px solid #fff;  
    outline: none;  
    border-radius: 6px;  
    cursor: pointer;  
    font-size: 1.1em;  
    color: #fff;  
    font-weight: 500;  
    transition: .5s;  
}  
  
.navigation .btnlogin-popup:hover {  
    background: #fff;  
    color: #162938;  
}  
  
.col-sm-6 h2 {  
    position: fixed;  
    top: 5px;  
    left: 5px;  
    margin-left: 120px;  
    color: #ffffff;  
    font-style: italic;  
    margin-top: 25px;  
}  
  
.Dlogo {  
    position: fixed;
```

```
    left: 20px;
    top: 1px;
    width: 110px;
}

.col-12.wrapper {
    position: relative;
    width: 90%;
    margin: 35px auto;
    background-color: rgba(14, 70, 178, .20);
    border: none;
    backdrop-filter: blur(-2px);
    box-shadow: 0 0 10px rgba(0, 0, 0, .1);
    color: #fff;
    border-radius: 50px;
    padding: 30px 40px;
    text-align: center;
}

.col-12.wrapper::before {
    content: "";
    position: absolute;
    border: 3px solid #2382BC;
    border-radius: 60px;
    top: -30px;
    left: -1.5%;
    right: -1.5%;
    bottom: -30px;
}

.col-12.wrapper .col-12 {
    display: flex;
    justify-content: center;
    align-items: center;
    flex-wrap: wrap;
}

.col-12.wrapper .col-12 img {
    margin: 100px;
    margin-top: -40px;
}

.col-12.wrapper h1 {
    position: relative;
    font-size: 5rem;
    font-weight: 700;
    max-width: 90%;
    white-space: nowrap;
    overflow: hidden;
    text-overflow: ellipsis;
    margin: 0 auto;
}
```

```
.col-12.wrapper h1::after {
    content: "";
    position: absolute;
    bottom: -5px;
    left: 50%;
    transform: translateX(-50%);
    width: 40%;
    height: 3px;
    background-color: #fff;
}

.member1 {
    max-width: 200px;
    height: 130px;
    border-radius: 100px;
}

.member2 {
    max-width: 200px;
    height: 130px;
    border-radius: 100px;
}

.member3 {
    max-width: 200px;
    height: 130px;
    border-radius: 100px;
}

.member4 {
    max-width: 200px;
    height: 130px;
    border-radius: 100px;
}

.member5 {
    max-width: 200px;
    height: 130px;
    border-radius: 100px;
}

.member6 {
    max-width: 200px;
    height: 130px;
    border-radius: 100px;
}

.Word {
    display: flex;
    justify-content: center;
    align-items: flex-start;
}
```

```

flex-wrap: wrap;
margin-top: -90px;
}

.Word1 {
  display: flex;
  justify-content: center;
  align-items: flex-start;
  flex-wrap: wrap;
  margin-top: -90px;
}

.Word span {
  margin: 0 95px;
  font-size: 18px;
  font-weight: 300;
  font-family: 'Times New Roman', Times, serif;
  color: #ffffff;
}

.Word1 span {
  margin: 0 70px;
  font-size: 18px;
  font-weight: 300;
  font-family: 'Times New Roman', Times, serif;
  color: #ffffff;
}

@media only screen and (max-width: 768px) {
  .row-header {
    flex-direction: column;
    align-items: center;
    height: auto;
  }

  .row-header .navigation {
    margin-top: 20px;
    justify-content: center;
  }

  .col-sm-6 h2 {
    position: static;
    margin-top: 20px;
    margin-left: 0;
    text-align: center;
  }

  .Dlogo {
    position: static;
    margin-top: 10px;
  }
}

```

```

@media only screen and (max-width: 576px) {
    .row-header {
        padding: 10px;
        flex-direction: column;
        align-items: center;
    }

    .row-header .navigation {
        margin-top: 20px;
        flex-direction: column;
        align-items: center;
    }

    .row-header .navigation a {
        margin-left: 0;
        margin-top: 10px;
    }
}

```

Register page HTML code:

```

<!DOCTYPE html>
<html lang="en">

    <head>
        <meta charset="UTF-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <title> De-TECH </title>
        <link rel="icon" href="../static/images/favicon16.png" sizes="16x16" type="image/png">
        <link rel="icon" href="../static/images/favicon32.png" sizes="32x32" type="image/png">
        <link rel="icon" href="../static/images/favicon192.png" sizes="192x192" type="image/png">
        <link rel="icon" href="../static/images/favicon512.png" sizes="512x512" type="image/png">
        <link rel="apple-touch-icon" href="../static/images/faviconapple.png" sizes="180x180">
        <link href='https://unpkg.com/boxicons@2.1.4/css/boxicons.min.css' rel='stylesheet'>
        <link href="../static/content/stylemain.css" rel="stylesheet" />
        <script src="../static/scripts/jquery-1.10.2.js"></script>

    </head>

    <body>

        <!-- HEADER START -->
        <div class="row">
            <div class="col-6" style="display: flex; align-items: center;">
                
                <span style="font-size: 2rem; color: #fff; margin-left: 130px; margin-top: 30px;">De-TECH</span>
            </div>
            <div class="col-6" style="text-align: right; margin-top: -51px; padding-right: 40px;">
                <nav class="navigation" style="font-size: 1.5rem;">
                    <a href="/home">Home</a>

```

```

        <a href="/about">About Us</a>
        <button class="btnlogin-popup">Login</button>
    </nav>
</div>
</div>
<!-- HEADER END -->

<div class="wrapper">
    <form method="post" action="/register" id="registerForm">
        <span class="icon-close" onclick="closeForm()" style="cursor: pointer;">
            <i class='bx bx-x'></i>
        </span>

        <h1>Register</h1>
        <i>
            <h5>The safety within your reach.</h5>
        </i>

        <div class="input-box">
            <label for="registerPageUsername"><b>Username</b></label>
            <input type="username" placeholder="Type your username" id="registerPageUsername" name="registerPageUsername" required>
                <i class='bx bxs-user'></i>
            </div>

        <div class="input-box">
            <label for="registerPageEmail"><b>Email</b></label>
            <input type="email" placeholder="Type your email" id="registerPageEmail" name="registerPageEmail" required>
                <i class='bx bxs-envelope'></i>
            </div>

        <div class="input-box">
            <label for="registerPagePassword"><b>Password</b></label>
            <input type="password" placeholder="Type your password" id="registerPagePassword" name="registerPagePassword" required>
                <i class='bx bxs-lock'></i>
            </div>

        <div class="remember-forgot">
            <label><input type="checkbox" id="termsCheckbox" checked=""> I agree to the terms & conditions</label>
        </div>

        <button type="submit" class="btn">Register</button>

        <div class="register-link">
            <p>Already have an account? <a href="/" class="loginLink"> Login</a></p>
        </div>
    </form>
</div>

```

```

<div id="termsModal" class="modal">
    <div class="modal-content">
        <span class="close" onclick="closeModal()">&times;</span>

        <div class="terms-section" id="section1">
            <h2>Terms and Conditions for De-TECH</h2>
            <section>
                <h3>1. Acceptance of Terms</h3>
                <p>1.1. By accessing and using [Your Web Application], you agree to comply with and be bound by these terms and conditions. If you do not agree with any part of these terms, please do not use the application.</p>
            </section>
        </div>

        <div class="terms-section" id="section2">
            <section>
                <h3>2. Use of the Application</h3>
                <p>2.1. You must be at least 18 years old to use De-TECH.</p>
                <p>2.2. You are responsible for maintaining the confidentiality of your account and password. You agree to accept responsibility for all activities that occur under your account.</p>
            </section>
        </div>

        <div class="terms-section" id="section3">
            <section>
                <h3>3. User Content</h3>
                <p>3.1. Users are solely responsible for the content they post or share on De-TECH.</p>
                <p>3.2. By posting content, you grant [Your Company] a worldwide, non-exclusive, royalty-free license to use, reproduce, modify, publish, distribute, and display the content.</p>
            </section>
        </div>

        <div class="terms-section" id="section4">
            <section>
                <h3>4. Privacy Policy</h3>
                <p>4.1. The application's privacy policy outlines the collection, use, and disclosure of personal information. By using the application, you consent to the practices described in the privacy policy.</p>
            </section>
        </div>

        <div class="terms-section" id="section5">
            <section>
                <h3>5. Intellectual Property</h3>
                <p>5.1. All content and materials available on [Your Web Application], including but not limited to text, graphics, logos, and images, are the property of [Your Company] and are protected by applicable intellectual property laws.</p>
            </section>
        </div>
    </div>

```

```

        </div>

        <div class="terms-section" id="section6">
            <section>
                <h3>6. Disclaimers and Limitation of Liability</h3>
                <p>6.1. De-TECH is provided "as is" without any warranties, express or implied.</p>
                <p>6.2. De-TECH shall not be liable for any indirect, incidental, special, consequential, or punitive damages, or any loss of profits or revenues.</p>
            </section>
        </div>

        <div class="terms-section" id="section7">
            <section>
                <h3>7. Changes to Terms</h3>
                <p>7.1. De-TECH reserves the right to update or modify these terms and conditions at any time without prior notice.</p>
            </section>
        </div>

        <div class="terms-section" id="section8">
            <section>
                <h3>8. Governing Law</h3>
                <p>8.1. These terms and conditions are governed by and construed in accordance with the laws of [Your Jurisdiction].</p>
            </section>
        </div>

        <button onclick="agreeTerms()">Agree</button>
    </div>
</body>

</html>

```

```

<script>
    // Check if an alert message is provided and display it
    const alert_message = "{{ alert_message }}"; // Injected from Flask

    if (alert_message) {
        alert(alert_message);
    }
</script>

```

<script src="../static/scripts/js/script.js"></script>

Register page CSS code:

```

@import
url("https://fonts.googleapis.com/css2?family=Poppins:wght@300;400;500;600;700;800;900&display=swap");

```

* {

```

margin: 0;
padding: 0;
box-sizing: border-box;
font-family: "Poppins", sans-serif;
}

body {
  min-height: 100vh;
  background: url(..../images/bbackground.png);
  background-repeat: no-repeat;
  background-size: cover;
  background-attachment: fixed;
  overflow: hidden; /* Prevent scrolling */
}

.row-content {
  align-items: center;
  background: transparent;
}

.Dlogo {
  position: fixed;
  left: 20px;
  top: 1px;
}

.navigation a {
  font-size: 1.5em;
  color: #fff;
  text-decoration: none;
  margin-left: 40px;
  margin-right: 20px;
}

.navigation a::after {
  content: "";
  background: #fff;
  border-radius: 5px;
  transform-origin: right;
  transform: scaleX(0);
  transition: transform .5s;
}

.navigation a:hover::after {
  transform: scaleX(1);
}

.navigation .btnlogin-popup {
  width: 130px;
  height: 50px;
  background: transparent;
  border: 2px solid #fff;
}

```

```
outline: none;
border-radius: 6px;
cursor: pointer;
font-size: 1.1em;
color: #fff;
font-weight: 500;
margin-left: 40px;
transition: .5s;
}

.navigation .btnlogin-popup:hover {
background: #fff;
color: #162938;
}
.wrapper {
width: 420px;
background-color: rgba(14, 70, 178, .20);
border: none;
backdrop-filter: blur(-2px);
box-shadow: 0 0 10px rgba(0, 0, 0, .1);
color: #fff;
border-radius: 10px;
padding: 30px 40px;
text-align: center;
overflow: hidden;
transition: transform .5s ease;
margin: 10px auto;
position: relative;
}

.wrapper.active-popup {
transform: scale(1);
}

.wrapper .icon-close {
position: absolute;
top: 0;
right: 0;
width: 45px;
height: 45px;
background-color: rgba(31, 125, 174, .20);
font-size: 2em;
color: #fff;
display: flex;
justify-content: center;
align-items: center;
border-bottom-left-radius: 20px;
cursor: pointer;
z-index: 1;
}

.wrapper h1 {
```

```
font-size: 36px;
text-align: center;
font-weight: 500;
}

.wrapper h5 {
font-size: 15px;
text-align: center;
font-weight: 100;
}

.wrapper .input-box {
position: relative;
width: 100%;
height: 50px;
margin: 30px 0;
text-align: left;
}

.input-box b {
margin-left: 17px;
font-weight: 100;
}

.input-box input {
width: 100%;
height: 100%;
background: transparent;
border: none;
outline: none;
border: 3px solid;
border-color: #fff;
border-radius: 40px;
font-size: 16px;
color: #fff;
padding: 20px 0px 20px 45px;
}

.input-box input::placeholder {
color: white;
font-style: italic;
}

.input-box i {
position: absolute;
left: 15px;
top: 100%;
transform: translateY(-50%);
font-size: 30px;
}
```

```
.wrapper .remember-forgot {  
    display: flex;  
    justify-content: space-between;  
    font-size: 14.5px;  
    margin: -25px 0 20px;  
}  
  
.remember-forgot label input {  
    accent-color: #fff;  
    margin-left: 17px;  
    margin-top: 25px;  
}  
  
.remember-forgot a {  
    color: green;  
    text-decoration: none;  
    margin-top: 25px;  
}  
  
.remember-forgot a:hover {  
    text-decoration: underline;  
}  
  
.wrapper .btn {  
    width: 100%;  
    height: 45px;  
    background: #2382BC;  
    border: none;  
    outline: none;  
    border-radius: 40px;  
    box-shadow: 0 0 10px rgba(0, 0, 0, .1);  
    cursor: pointer;  
    font-size: 16px;  
    color: #fff;  
    font-weight: 600;  
}  
  
.wrapper .register-link {  
    font-size: 14.5px;  
    text-align: center;  
    margin-top: 20px;  
    margin: 20px 0 15px;  
}  
  
.register-link p a {  
    color: green;  
    text-decoration: none;  
    font-weight: 600;  
}  
  
.wrapper p a:hover {  
    text-decoration: underline;
```

```

}

body.modal-open {
  overflow: hidden;
}

.modal {
  display: none;
  position: fixed;
  z-index: 1;
  left: 0;
  top: 0;
  width: 100%;
  height: 100%;
  overflow: auto;
  background-color: rgba(0, 0, 0, 0.5);
}

.modal-content {
  max-height: 80vh;
  overflow-y: auto;
  background-color: rgba(14, 70, 178, .20);
  border: none;
  backdrop-filter: blur(20px);
  box-shadow: 0 0 20px rgba(0, 0, 0, .1);
  color: #fff;
  border-radius: 20px;
  margin: 10% auto;
  padding: 20px;
  width: 50%;
  display: flex;
  flex-direction: column;
  align-items: center;
  position: relative; /* Added relative positioning */
}

/* Style for the scrollbar */
.modal-content::-webkit-scrollbar {
  width: 10px;
}

.modal-content::-webkit-scrollbar-thumb {
  background-color: #2382BC; /* Same as the modal background color */
  border-radius: 10px;
}

.modal-content::-webkit-scrollbar-track {
  background-color: rgba(14, 70, 178, .20);
  border-radius: 10px;
}

/* Style for the button */

```

```

.modal-content button {
    background-color: #2382BC; /* Change this color as needed */
    color: #fff;
    border: none;
    padding: 10px 20px;
    border-radius: 5px;
    cursor: pointer;
    font-size: 16px;
    font-weight: 600;
    transition: background-color 0.3s;
    margin-top: 20px;
}

/* Hover effect for the button */
.modal-content button:hover {
    background-color: #185A87; /* Change this color as needed */
}

/* Style for the close button */
.modal-content .close {
    color: #aaa;
    font-size: 28px;
    font-weight: bold;
    cursor: pointer;
    position: absolute;
    top: 10px;
    right: 10px;
}

.close {
    color: #aaa;
    float: right;
    font-size: 28px;
    font-weight: bold;
}

.close:hover,
.close:focus {
    color: black;
    text-decoration: none;
    cursor: pointer;
}

bootstrap.js
/* NUGET: BEGIN LICENSE TEXT
*
* Microsoft grants you the right to use these script files for the sole
* purpose of either: (i) interacting through your browser with the Microsoft
* website or online service, subject to the applicable licensing or use
* terms; or (ii) using the files as included with a Microsoft product subject
* to that product's license terms. Microsoft reserves all other rights to the
* files not expressly granted by Microsoft, whether by implication, estoppel

```

```

* or otherwise. Insofar as a script file is dual licensed under GPL,
* Microsoft neither took the code under GPL nor distributes it thereunder but
* under the terms set out in this paragraph. All notices and licenses
* below are for informational purposes only.
*
* NUGET: END LICENSE TEXT */

/**
* bootstrap.js v3.0.0 by @fat and @mdo
* Copyright 2013 Twitter Inc.
* http://www.apache.org/licenses/LICENSE-2.0
*/
if (!jQuery) { throw new Error("Bootstrap requires jQuery") }

/*
=====
* Bootstrap: transition.js v3.0.0
* http://twbs.github.com/bootstrap/javascript.html#transitions
* =====
* Copyright 2013 Twitter, Inc.
*
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
* You may obtain a copy of the License at
*
* http://www.apache.org/licenses/LICENSE-2.0
*
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
* See the License for the specific language governing permissions and
* limitations under the License.
* ===== */
*/



+function ($) { "use strict";

// CSS TRANSITION SUPPORT (Shoutout: http://www.modernizr.com/)
// =====

function transitionEnd() {
    var el = document.createElement('bootstrap')

    var transEndEventNames = {
        'WebkitTransition' : 'webkitTransitionEnd',
        'MozTransition'   : 'transitionend',
        'OTransition'    : 'oTransitionEnd otransitionend',
        'transition'     : 'transitionend'
    }

    for (var name in transEndEventNames) {
        if (el.style[name] !== undefined) {
            return { end: transEndEventNames[name] }
        }
    }
}

```

```

        }
    }
}

// http://blog.alexmaccaaw.com/css-transitions
$.fn.emulateTransitionEnd = function (duration) {
    var called = false, $el = this
    $(this).one($.support.transition.end, function () { called = true })
    var callback = function () { if (!called) $($el).trigger($.support.transition.end) }
    setTimeout(callback, duration)
    return this
}

$(function () {
    $.support.transition = transitionEnd()
})

})(window.jQuery);

/*
 * Bootstrap: alert.js v3.0.0
 * http://twbs.github.com/bootstrap/javascript.html#alerts
 *
 * Copyright 2013 Twitter, Inc.
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 * http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 */

```

```

+function ($) { "use strict";

// ALERT CLASS DEFINITION
// =====

var dismiss = '[data-dismiss="alert"]'
var Alert = function (el) {
    $(el).on('click', dismiss, this.close)
}

Alert.prototype.close = function (e) {
    var $this = $(this)
    var selector = $this.attr('data-target')

```

```

if (!selector) {
  selector = $this.attr('href')
  selector = selector && selector.replace(/.*(?=#[^\s]*$/), "") // strip for ie7
}

var $parent = $(selector)

if (e) e.preventDefault()

if (!$parent.length) {
  $parent = $this.hasClass('alert') ? $this : $this.parent()
}

$parent.trigger(e = $.Event('close.bs.alert'))

if (e.isDefaultPrevented()) return

$parent.removeClass('in')

function removeElement() {
  $parent.trigger('closed.bs.alert').remove()
}

$.support.transition && $parent.hasClass('fade') ?
$parent
  .one($.support.transition.end, removeElement)
  .emulateTransitionEnd(150) :
  removeElement()
}

// ALERT PLUGIN DEFINITION
// =====

var old = $.fn.alert

$.fn.alert = function (option) {
  return this.each(function () {
    var $this = $(this)
    var data = $this.data('bs.alert')

    if (!data) $this.data('bs.alert', (data = new Alert(this)))
    if (typeof option === 'string') data[option].call($this)
  })
}

$.fn.alert.Constructor = Alert

// ALERT NO CONFLICT
// =====

```

```

$.fn.alert.noConflict = function () {
  $.fn.alert = old
  return this
}

// ALERT DATA-API
// =====

$(document).on('click.bs.alert.data-api', dismiss, Alert.prototype.close)

}(window.jQuery);

/*
=====
* Bootstrap: button.js v3.0.0
* http://twbs.github.com/bootstrap/javascript.html#buttons
* =====
* Copyright 2013 Twitter, Inc.
*
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
* You may obtain a copy of the License at
*
* http://www.apache.org/licenses/LICENSE-2.0
*
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
* See the License for the specific language governing permissions and
* limitations under the License.
* ===== */

```

```

+function ($) { "use strict";

// BUTTON PUBLIC CLASS DEFINITION
// =====

var Button = function (element, options) {
  this.$element = $(element)
  this.options = $.extend({}, Button.DEFAULTS, options)
}

Button.DEFAULTS = {
  loadingText: 'loading...'
}

Button.prototype.setState = function (state) {
  var d = 'disabled'
  var $el = this.$element
  var val = $el.is('input') ? 'val' : 'html'

```

```

var data = $el.data()

state = state + 'Text'

if (!data.resetText) $el.data('resetText', $el[val]())

$el[val](data[state] || this.options[state])

// push to event loop to allow forms to submit
setTimeout(function () {
  state == 'loadingText' ?
    $el.addClass(d).attr(d, d) :
    $el.removeClass(d).removeAttr(d);
}, 0)
}

Button.prototype.toggle = function () {
  var $parent = this.$element.closest('[data-toggle="buttons"]')

  if ($parent.length) {
    var $input = this.$element.find('input')
      .prop('checked', !this.$element.hasClass('active'))
      .trigger('change')
    if ($input.prop('type') === 'radio') $parent.find('.active').removeClass('active')
  }

  this.$element.toggleClass('active')
}

// BUTTON PLUGIN DEFINITION
// =====

var old = $.fn.button

$.fn.button = function (option) {
  return this.each(function () {
    var $this = $(this)
    var data = $this.data('bs.button')
    var options = typeof option === 'object' && option

    if (!data) $this.data('bs.button', (data = new Button(this, options)))

    if (option === 'toggle') data.toggle()
    else if (option) data.setState(option)
  })
}

$.fn.button.Constructor = Button

// BUTTON NO CONFLICT

```

```

// =====

$.fn.button.noConflict = function () {
    $.fn.button = old
    return this
}

// BUTTON DATA-API
// =====

$(document).on('click.bs.button.data-api', '[data-toggle^=button]', function (e) {
    var $btn = $(e.target)
    if (!$btn.hasClass('btn')) $btn = $btn.closest('.btn')
    $btn.button('toggle')
    e.preventDefault()
})

}(window.jQuery);

/*
=====
* Bootstrap: carousel.js v3.0.0
* http://twbs.github.com/bootstrap/javascript.html#carousel
* =====
* Copyright 2012 Twitter, Inc.
*
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
* You may obtain a copy of the License at
*
* http://www.apache.org/licenses/LICENSE-2.0
*
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
* See the License for the specific language governing permissions and
* limitations under the License.
* ===== */

```

```

+function ($) { "use strict";

// CAROUSEL CLASS DEFINITION
// =====

var Carousel = function (element, options) {
    this.$element = $(element)
    this.$indicators = this.$element.find('.carousel-indicators')
    this.options = options
    this.paused = false
    this.sliding = false
    this.interval = null
}

```

```

this.$active    =
this.$items     = null

this.options.pause === 'hover' && this.$element
  .on('mouseenter', $.proxy(this.pause, this))
  .on('mouseleave', $.proxy(this.cycle, this))
}

Carousel.DEFAULTS = {
  interval: 5000
, pause: 'hover'
, wrap: true
}

Carousel.prototype.cycle = function (e) {
  e || (this.paused = false)

  this.interval && clearInterval(this.interval)

  this.options.interval
  &&& !this.paused
  &&& (this.interval = setInterval($.proxy(this.next, this), this.options.interval))

  return this
}

Carousel.prototype.getActiveIndex = function () {
  this.$active = this.$element.find('.item.active')
  this.$items = this.$active.parent().children()

  return this.$items.index(this.$active)
}

Carousel.prototype.to = function (pos) {
  var that = this
  var activeIndex = this.getActiveIndex()

  if (pos > (this.$items.length - 1) || pos < 0) return

  if (this.sliding) return this.$element.one('slid', function () { that.to(pos) })
  if (activeIndex == pos) return this.pause().cycle()

  return this.slide(pos > activeIndex ? 'next' : 'prev', $(this.$items[pos]))
}

Carousel.prototype.pause = function (e) {
  e || (this.paused = true)

  if (this.$element.find('.next, .prev').length && $.support.transition.end) {
    this.$element.trigger($.support.transition.end)
    this.cycle(true)
  }
}

```

```

this.interval = clearInterval(this.interval)

return this
}

Carousel.prototype.next = function () {
  if (this.sliding) return
  return this.slide('next')
}

Carousel.prototype.prev = function () {
  if (this.sliding) return
  return this.slide('prev')
}

Carousel.prototype.slide = function (type, next) {
  var $active = this.$element.find('.item.active')
  var $next = next || $active[type]()
  var isCycling = this.interval
  var direction = type === 'next' ? 'left' : 'right'
  var fallback = type === 'next' ? 'first' : 'last'
  var that = this

  if (!$next.length) {
    if (!this.options.wrap) return
    $next = this.$element.find('.item')[fallback]()
  }

  this.sliding = true

  isCycling && this.pause()

  var e = $.Event('slide.bs.carousel', { relatedTarget: $next[0], direction: direction })
  if ($next.hasClass('active')) return

  if (this.$indicators.length) {
    this.$indicators.find('.active').removeClass('active')
    this.$element.one('slid', function () {
      var $nextIndicator = $(that.$indicators.children()[that.getActiveIndex()])
      $nextIndicator && $nextIndicator.addClass('active')
    })
  }

  if ($.support.transition && this.$element.hasClass('slide')) {
    this.$element.trigger(e)
    if (e.isDefaultPrevented()) return
    $next.addClass(type)
    $next[0].offsetWidth // force reflow
    $active.addClass(direction)
    $next.addClass(direction)
  }
}

```

```

$active
.one($.support.transition.end, function () {
$next.removeClass([type, direction].join(' ')).addClass('active')
$active.removeClass(['active', direction].join(' '))
that.sliding = false
setTimeout(function () { that.$element.trigger('slid') }, 0)
})
.emulateTransitionEnd(600)
} else {
this.$element.trigger(e)
if (e.isDefaultPrevented()) return
$active.removeClass('active')
$next.addClass('active')
this.sliding = false
this.$element.trigger('slid')
}

isCycling && this.cycle()

return this
}

// CAROUSEL PLUGIN DEFINITION
// =====

var old = $.fn.carousel

$.fn.carousel = function (option) {
return this.each(function () {
var $this = $(this)
var data = $this.data('bs.carousel')
var options = $.extend({}, Carousel.DEFAULTS, $this.data(), typeof option == 'object' && option)
var action = typeof option == 'string' ? option : options.slide

if (!data) $this.data('bs.carousel', (data = new Carousel(this, options)))
if (typeof option == 'number') data.to(option)
else if (action) data[action]()
else if (options.interval) data.pause().cycle()
})
}

$.fn.carousel.Constructor = Carousel

// CAROUSEL NO CONFLICT
// =====

$.fn.carousel.noConflict = function () {
$.fn.carousel = old
return this
}

```

```

// CAROUSEL DATA-API
// =====

$(document).on('click.bs.carousel.data-api', '[data-slide]', [data-slide-to]', function (e) {
  var $this = $(this), href
  var $target = $($this.attr('data-target') || (href = $this.attr('href')) && href.replace(/>.*(?=#[^\s]+$/,'"))
  //strip for ie7
  var options = $.extend({}, $target.data(), $this.data())
  var slideIndex = $this.attr('data-slide-to')
  if (slideIndex) options.interval = false

  $target.carousel(options)

  if (slideIndex = $this.attr('data-slide-to')) {
    $target.data('bs.carousel').to(slideIndex)
  }

  e.preventDefault()
})

$(window).on('load', function () {
  $('[data-ride="carousel"]').each(function () {
    var $carousel = $(this)
    $carousel.carousel($carousel.data())
  })
})

}(window.jQuery);

/*
=====
* Bootstrap: collapse.js v3.0.0
* http://twbs.github.com/bootstrap/javascript.html#collapse
* =====
* Copyright 2012 Twitter, Inc.
*
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
* You may obtain a copy of the License at
*
* http://www.apache.org/licenses/LICENSE-2.0
*
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
* See the License for the specific language governing permissions and
* limitations under the License.
* ===== */
+function ($) { "use strict";

```

```

// COLLAPSE PUBLIC CLASS DEFINITION
// =====

var Collapse = function (element, options) {
  this.$element = $(element)
  this.options = $.extend({}, Collapse.DEFAULTS, options)
  this.transitioning = null

  if (this.options.parent) this.$parent = $(this.options.parent)
  if (this.options.toggle) this.toggle()
}

Collapse.DEFAULTS = {
  toggle: true
}

Collapse.prototype.dimension = function () {
  var hasWidth = this.$element.hasClass('width')
  return hasWidth ? 'width' : 'height'
}

Collapse.prototype.show = function () {
  if (this.transitioning || this.$element.hasClass('in')) return

  var startEvent = $.Event('show.bs.collapse')
  this.$element.trigger(startEvent)
  if (startEvent.isDefaultPrevented()) return

  var actives = this.$parent && this.$parent.find('> .panel > .in')

  if (actives && actives.length) {
    var hasData = actives.data('bs.collapse')
    if (hasData && hasData.transitioning) return
    actives.collapse('hide')
    hasData || actives.data('bs.collapse', null)
  }

  var dimension = this.dimension()

  this.$element
    .removeClass('collapse')
    .addClass('collapsing')
    [dimension](0)

  this.transitioning = 1

  var complete = function () {
    this.$element
      .removeClass('collapsing')
      .addClass('in')
      [dimension]('auto')
  }
}

```

```

this.transitioning = 0
this.$element.trigger('shown.bs.collapse')
}

if (!$.support.transition) return complete.call(this)

var scrollSize = $.camelCase(['scroll', dimension].join('-'))

this.$element
.one($.support.transition.end, $.proxy(complete, this))
.emulateTransitionEnd(350)
[dimension](this.$element[0][scrollSize])
}

Collapse.prototype.hide = function () {
if (this.transitioning || !this.$element.hasClass('in')) return

var startEvent = $.Event('hide.bs.collapse')
this.$element.trigger(startEvent)
if (startEvent.isDefaultPrevented()) return

var dimension = this.dimension()

this.$element
[dimension](this.$element[dimension]())
[0].offsetHeight

this.$element
.addClass('collapsing')
.removeClass('collapse')
.removeClass('in')

this.transitioning = 1

var complete = function () {
this.transitioning = 0
this.$element
.trigger('hidden.bs.collapse')
.removeClass('collapsing')
.addClass('collapse')
}

if (!$.support.transition) return complete.call(this)

this.$element
[dimension](0)
.one($.support.transition.end, $.proxy(complete, this))
.emulateTransitionEnd(350)
}

Collapse.prototype.toggle = function () {
this[this.$element.hasClass('in') ? 'hide' : 'show']()
}

```

```

}

// COLLAPSE PLUGIN DEFINITION
// =====

var old = $.fn.collapse

$.fn.collapse = function (option) {
  return this.each(function () {
    var $this = $(this)
    var data = $this.data('bs.collapse')
    var options = $.extend({}, Collapse.DEFAULTS, $this.data(), typeof option == 'object' && option)

    if (!data) $this.data('bs.collapse', (data = new Collapse(this, options)))
    if (typeof option == 'string') data[option]()
  })
}

$.fn.collapse.Constructor = Collapse


// COLLAPSE NO CONFLICT
// =====

$.fn.collapse.noConflict = function () {
  $.fn.collapse = old
  return this
}

// COLLAPSE DATA-API
// =====

$(document).on('click.bs.collapse.data-api', '[data-toggle=collapse]', function (e) {
  var $this = $(this), href
  var target = $this.attr('data-target')
    || e.preventDefault()
    || (href = $this.attr('href')) && href.replace(/.*(?=#[^\s]+$/)/, "") //strip for ie7
  var $target = $(target)
  var data = $target.data('bs.collapse')
  var option = data ? 'toggle' : $this.data()
  var parent = $this.attr('data-parent')
  var $parent = parent && $(parent)

  if (!data || !data.transitioning) {
    if ($parent) $parent.find('[data-toggle=collapse][data-parent=' + parent +
    "']").not($this).addClass('collapsed')
    $this[$target.hasClass('in') ? 'addClass' : 'removeClass']('collapsed')
  }

  $target.collapse(option)
})

```

```

        })
    })(window.jQuery);

/*
=====
* Bootstrap: dropdown.js v3.0.0
* http://twbs.github.com/bootstrap/javascript.html#dropdowns
* =====
* Copyright 2012 Twitter, Inc.
*
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
* You may obtain a copy of the License at
*
* http://www.apache.org/licenses/LICENSE-2.0
*
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
* See the License for the specific language governing permissions and
* limitations under the License.
* ===== */

```

```

+function ($) { "use strict";

// DROPODOWN CLASS DEFINITION
// =====

var backdrop = '.dropdown-backdrop'
var toggle = '[data-toggle=dropdown]'
var Dropdown = function (element) {
  var $el = $(element).on('click.bs.dropdown', this.toggle)
}

Dropdown.prototype.toggle = function (e) {
  var $this = $(this)

  if ($this.is('.disabled, :disabled')) return

  var $parent = getParent($this)
  var isActive = $parent.hasClass('open')

  clearMenus()

  if (!isActive) {
    if ('ontouchstart' in document.documentElement && !$parent.closest('.navbar-nav').length) {
      // if mobile we we use a backdrop because click events don't delegate
      $('<div class="dropdown-backdrop"/>').insertAfter($(this)).on('click', clearMenus)
    }
  }

  $parent.trigger(e = $.Event('show.bs.dropdown'))
}

```

```

if (e.isDefaultPrevented()) return

$parent
.toggleClass('open')
.trigger('shown.bs.dropdown')

$this.focus()
}

return false
}

Dropdown.prototype.keydown = function (e) {
if (!(38|40|27).test(e.keyCode)) return

var $this = $(this)

e.preventDefault()
e.stopPropagation()

if ($this.is('.disabled, :disabled')) return

var $parent = getParent($this)
var isActive = $parent.hasClass('open')

if (!isActive || (isActive && e.keyCode == 27)) {
if (e.which == 27) $parent.find(toggle).focus()
return $this.click()
}

var $items = $('[role=menu] li:not(.divider):visible a', $parent)

if (!$items.length) return

var index = $items.index($items.filter(':focus'))

if (e.keyCode == 38 && index > 0)           index--          // up
if (e.keyCode == 40 && index < $items.length - 1) index++        // down
if (!~index)                                index=0

$items.eq(index).focus()
}

function clearMenus() {
$(backdrop).remove()
$(toggle).each(function (e) {
var $parent = getParent($(this))
if (!$parent.hasClass('open')) return
$parent.trigger(e = $.Event('hide.bs.dropdown'))
if (e.isDefaultPrevented()) return
$parent.removeClass('open').trigger('hidden.bs.dropdown')
})
}

```

```

        })
    }

function getParent($this) {
    var selector = $this.attr('data-target')

    if (!selector) {
        selector = $this.attr('href')
        selector = selector && /#/.test(selector) && selector.replace(/>.*(?=[^\s]*$/), " ) //strip for ie7
    }

    var $parent = selector && $(selector)

    return $parent && $parent.length ? $parent : $this.parent()
}

// DROPODOWN PLUGIN DEFINITION
// =====

var old = $.fn.dropdown

$.fn.dropdown = function (option) {
    return this.each(function () {
        var $this = $(this)
        var data = $this.data('dropdown')

        if (!data) $this.data('dropdown', (data = new Dropdown(this)))
        if (typeof option == 'string') data[option].call($this)
    })
}

$.fn.dropdown.Constructor = Dropdown

// DROPODOWN NO CONFLICT
// =====

$.fn.dropdown.noConflict = function () {
    $.fn.dropdown = old
    return this
}

// APPLY TO STANDARD DROPODOWN ELEMENTS
// =====

$(document)
    .on('click.bs.dropdown.data-api', clearMenus)
    .on('click.bs.dropdown.data-api', '.dropdown form', function (e) { e.stopPropagation() })
    .on('click.bs.dropdown.data-api' , toggle, Dropdown.prototype.toggle)
    .on('keydown.bs.dropdown.data-api', toggle + '[role=menu]' , Dropdown.prototype.keydown)

```

```

}(window.jQuery);

/*
=====
* Bootstrap: modal.js v3.0.0
* http://twbs.github.com/bootstrap/javascript.html#modals
=====
* Copyright 2012 Twitter, Inc.
*
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
* You may obtain a copy of the License at
*
* http://www.apache.org/licenses/LICENSE-2.0
*
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
* See the License for the specific language governing permissions and
* limitations under the License.
=====
*/

```

```

+function ($) { "use strict";

// MODAL CLASS DEFINITION
// =====

var Modal = function (element, options) {
    this.options = options
    this.$element = $(element)
    this.$backdrop =
    this.isHidden = null

    if (this.options.remote) this.$element.load(this.options.remote)
}

Modal.DEFAULTS = {
    backdrop: true
    , keyboard: true
    , show: true
}

Modal.prototype.toggle = function (_relatedTarget) {
    return this[!this.isHidden ? 'show' : 'hide'](_relatedTarget)
}

Modal.prototype.show = function (_relatedTarget) {
    var that = this
    var e = $.Event('show.bs.modal', { relatedTarget: _relatedTarget })

    this.$element.trigger(e)
}

```

```

if (this.isHidden || e.isDefaultPrevented()) return

this.isHidden = true

this.escape()

this.$element.on('click.dismiss.modal', '[data-dismiss="modal"]', $.proxy(this.hide, this))

this.backdrop(function () {
  var transition = $.support.transition && that.$element.hasClass('fade')

  if (!that.$element.parent().length) {
    that.$element.appendTo(document.body) // don't move modals dom position
  }

  that.$element.show()

  if (transition) {
    that.$element[0].offsetWidth // force reflow
  }

  that.$element
    .addClass('in')
    .attr('aria-hidden', false)

  that.enforceFocus()

  var e = $.Event('shown.bs.modal', { relatedTarget: _relatedTarget })

  transition ?
    that.$element.find('.modal-dialog') // wait for modal to slide in
    .one($.support.transition.end, function () {
      that.$element.focus().trigger(e)
    })
    .emulateTransitionEnd(300) :
    that.$element.focus().trigger(e)
  )
}
}

Modal.prototype.hide = function (e) {
  if (e) e.preventDefault()

  e = $.Event('hide.bs.modal')

  this.$element.trigger(e)

  if (!this.isHidden || e.isDefaultPrevented()) return

  this.isHidden = false

  this.escape()
}

```

```

$(document).off('focusin.bs.modal')

this.$element
  .removeClass('in')
  .attr('aria-hidden', true)
  .off('click.dismiss.modal')

$.support.transition && this.$element.hasClass('fade') ?
  this.$element
    .one($.support.transition.end, $.proxy(this.hideModal, this))
    .emulateTransitionEnd(300) :
  this.hideModal()
}

Modal.prototype.enforceFocus = function () {
  $(document)
    .off('focusin.bs.modal') // guard against infinite focus loop
    .on('focusin.bs.modal', $.proxy(function (e) {
      if (this.$element[0] !== e.target && !this.$element.has(e.target).length) {
        this.$element.focus()
      }
    }, this))
}

Modal.prototype.escape = function () {
  if (this.isShown && this.options.keyboard) {
    this.$element.on('keyup.dismiss.bs.modal', $.proxy(function (e) {
      e.which == 27 && this.hide()
    }, this)))
  } else if (!this.isShown) {
    this.$element.off('keyup.dismiss.bs.modal')
  }
}

Modal.prototype.hideModal = function () {
  var that = this
  this.$element.hide()
  this.backdrop(function () {
    that.removeBackdrop()
    that.$element.trigger('hidden.bs.modal')
  })
}
}

Modal.prototype.removeBackdrop = function () {
  this.$backdrop && this.$backdrop.remove()
  this.$backdrop = null
}

Modal.prototype.backdrop = function (callback) {
  var that = this
  var animate = this.$element.hasClass('fade') ? 'fade' : "

```

```

if (this.isShown && this.options.backdrop) {
  var doAnimate = $.support.transition && animate

  this.$backdrop = $('<div class="modal-backdrop ' + animate + '" />')
    .appendTo(document.body)

  this.$element.on('click.dismiss.modal', $.proxy(function (e) {
    if (e.target !== e.currentTarget) return
    this.options.backdrop == 'static'
      ? this.$element[0].focus.call(this.$element[0])
      : this.hide.call(this)
  }, this))

  if (doAnimate) this.$backdrop[0].offsetWidth // force reflow

  this.$backdrop.addClass('in')

  if (!callback) return

  doAnimate ?
    this.$backdrop
      .one($.support.transition.end, callback)
      .emulateTransitionEnd(150) :
    callback()

} else if (!this.isShown && this.$backdrop) {
  this.$backdrop.removeClass('in')

  $.support.transition && this.$element.hasClass('fade')?
    this.$backdrop
      .one($.support.transition.end, callback)
      .emulateTransitionEnd(150) :
    callback()

} else if (callback) {
  callback()
}

}

// MODAL PLUGIN DEFINITION
// =====

var old = $.fn.modal

$.fn.modal = function (option, _relatedTarget) {
  return this.each(function () {
    var $this = $(this)
    var data = $this.data('bs.modal')
    var options = $.extend({}, Modal.DEFAULTS, $this.data(), typeof option == 'object' && option)

```

```

if (!data) $this.data('bs.modal', (data = new Modal(this, options)))
if (typeof option == 'string') data[option](_relatedTarget)
else if (options.show) data.show(_relatedTarget)
})
}

$.fn.modal.Constructor = Modal

// MODAL NO CONFLICT
// =====

$.fn.modal.noConflict = function () {
  $.fn.modal = old
  return this
}

// MODAL DATA-API
// =====

$(document).on('click.bs.modal.data-api', '[data-toggle="modal"]', function (e) {
  var $this = $(this)
  var href = $this.attr('href')
  var $target = $($this.attr('data-target') || (href && href.replace(.*(?=[^\s]+$/), ''))) //strip for ie7
  var option = $target.data('modal') ? 'toggle' : $.extend({ remote: !/#/.test(href) && href }, $target.data(),
  $this.data())
  e.preventDefault()

  $target
    .modal(option, this)
    .one('hide', function () {
      $this.is(':visible') && $this.focus()
    })
  }

  $(document)
    .on('show.bs.modal', '.modal', function () { $(document.body).addClass('modal-open') })
    .on('hidden.bs.modal', '.modal', function () { $(document.body).removeClass('modal-open') })

})(window.jQuery);

/*
=====
* Bootstrap: tooltip.js v3.0.0
* http://twbs.github.com/bootstrap/javascript.html#tooltip
* Inspired by the original jQuery.tipsy by Jason Frame
=====
* Copyright 2012 Twitter, Inc.
*
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
*/

```

```

* You may obtain a copy of the License at
*
* http://www.apache.org/licenses/LICENSE-2.0
*
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
* See the License for the specific language governing permissions and
* limitations under the License.
* ===== */

+function ($) { "use strict";

// TOOLTIP PUBLIC CLASS DEFINITION
// =====

var Tooltip = function (element, options) {
    this.type      =
    this.options   =
    this.enabled   =
    this.timeout   =
    this.hoverState =
    this.$element  = null

    this.init('tooltip', element, options)
}

Tooltip.DEFAULTS = {
    animation: true
    , placement: 'top'
    , selector: false
    , template: '<div class="tooltip"><div class="tooltip-arrow"></div><div class="tooltip-inner"></div></div>'
    , trigger: 'hover focus'
    , title: ""
    , delay: 0
    , html: false
    , container: false
}

Tooltip.prototype.init = function (type, element, options) {
    this.enabled = true
    this.type   = type
    this.$element = $(element)
    this.options = this.getOptions(options)

    var triggers = this.options.trigger.split(' ')
    for (var i = triggers.length; i--;) {
        var trigger = triggers[i]

```

```

if (trigger == 'click') {
  this.$element.on('click.' + this.type, this.options.selector, $.proxy(this.toggle, this))
} else if (trigger != 'manual') {
  var eventIn = trigger == 'hover' ? 'mouseenter' : 'focus'
  var eventOut = trigger == 'hover' ? 'mouseleave' : 'blur'

  this.$element.on(eventIn + '.' + this.type, this.options.selector, $.proxy(this.enter, this))
  this.$element.on(eventOut + '.' + this.type, this.options.selector, $.proxy(this.leave, this))
}
}

this.options.selector ?
  (this._options = $.extend({ }, this.options, { trigger: 'manual', selector: " })) :
  this.fixTitle()
}

Tooltip.prototype.getDefaults = function () {
  return Tooltip.DEFAULTS
}

Tooltip.prototype.getOptions = function (options) {
  options = $.extend({ }, this.getDefaults(), this.$element.data(), options)

  if (options.delay && typeof options.delay == 'number') {
    options.delay = {
      show: options.delay
      , hide: options.delay
    }
  }
}

return options
}

Tooltip.prototype.getDelegateOptions = function () {
  var options = {}
  var defaults = this.getDefaults()

  this._options && $.each(this._options, function (key, value) {
    if (defaults[key] != value) options[key] = value
  })

  return options
}

Tooltip.prototype.enter = function (obj) {
  var self = obj instanceof this.constructor ?
    obj : $(obj.currentTarget)[this.type](this.getDelegateOptions()).data('bs.' + this.type)

  clearTimeout(self.timeout)
  self.hoverState = 'in'
}

```

```

if (!self.options.delay || !self.options.delay.show) return self.show()

self.timeout = setTimeout(function () {
  if (self.hoverState == 'in') self.show()
}, self.options.delay.show)
}

Tooltip.prototype.leave = function (obj) {
  var self = obj instanceof this.constructor ?
    obj : $(obj.currentTarget)[this.type](this.getDelegateOptions()).data('bs.' + this.type)

  clearTimeout(self.timeout)

  self.hoverState = 'out'

  if (!self.options.delay || !self.options.delay.hide) return self.hide()

  self.timeout = setTimeout(function () {
    if (self.hoverState == 'out') self.hide()
  }, self.options.delay.hide)
}

Tooltip.prototype.show = function () {
  var e = $.Event('show.bs.'+ this.type)

  if (this.hasContent() && this.enabled) {
    this.$element.trigger(e)

    if (e.isDefaultPrevented()) return

    var $tip = this.tip()

    this.setContent()

    if (this.options.animation) $tip.addClass('fade')

    var placement = typeof this.options.placement == 'function' ?
      this.options.placement.call(this, $tip[0], this.$element[0]) :
      this.options.placement

    var autoToken = /\s?auto?\s?/
    var autoPlace = autoToken.test(placement)
    if (autoPlace) placement = placement.replace(autoToken, "") || 'top'

    $tip
      .detach()
      .css({ top: 0, left: 0, display: 'block' })
      .addClass(placement)

    this.options.container ? $tip.appendTo(this.options.container) : $tip.insertAfter(this.$element)

    var pos      = this.getPosition()
  }
}

```

```

var actualWidth = $tip[0].offsetWidth
var actualHeight = $tip[0].offsetHeight

if (autoPlace) {
    var $parent = this.$element.parent()

    var orgPlacement = placement
    var docScroll = document.documentElement.scrollTop || document.body.scrollTop
    var parentWidth = this.options.container == 'body' ? window.innerWidth : $parent.outerWidth()
    var parentHeight = this.options.container == 'body' ? window.innerHeight : $parent.outerHeight()
    var parentLeft = this.options.container == 'body' ? 0 : $parent.offset().left

    placement = placement == 'bottom' && pos.top + pos.height + actualHeight - docScroll >
    parentHeight ? 'top' :
        placement == 'top' && pos.top - docScroll - actualHeight < 0 ? 'bottom' :
        placement == 'right' && pos.right + actualWidth > parentWidth ? 'left' :
        placement == 'left' && pos.left - actualWidth < parentLeft ? 'right' :
        placement

    $tip
        .removeClass(orgPlacement)
        .addClass(placement)
}

var calculatedOffset = this.getCalculatedOffset(placement, pos, actualWidth, actualHeight)

this.applyPlacement(calculatedOffset, placement)
this.$element.trigger('shown.bs.' + this.type)
}

Tooltip.prototype.applyPlacement = function(offset, placement) {
    var replace
    var $tip = this.tip()
    var width = $tip[0].offsetWidth
    var height = $tip[0].offsetHeight

    // manually read margins because getBoundingClientRect includes difference
    var marginTop = parseInt($tip.css('margin-top'), 10)
    var marginLeft = parseInt($tip.css('margin-left'), 10)

    // we must check for NaN for ie 8/9
    if (isNaN(marginTop)) marginTop = 0
    if (isNaN(marginLeft)) marginLeft = 0

    offset.top = offset.top + marginTop
    offset.left = offset.left + marginLeft

    $tip
        .offset(offset)
        .addClass('in')
}

```

```

// check to see if placing tip in new offset caused the tip to resize itself
var actualWidth = $tip[0].offsetWidth
var actualHeight = $tip[0].offsetHeight

if (placement == 'top' && actualHeight != height) {
    replace = true
    offset.top = offset.top + height - actualHeight
}

if (/bottom|top/.test(placement)) {
    var delta = 0

    if (offset.left < 0) {
        delta = offset.left * -2
        offset.left = 0

        $tip.offset(offset)

        actualWidth = $tip[0].offsetWidth
        actualHeight = $tip[0].offsetHeight
    }

    this.replaceArrow(delta - width + actualWidth, actualWidth, 'left')
} else {
    this.replaceArrow(actualHeight - height, actualHeight, 'top')
}

if (replace) $tip.offset(offset)
}

Tooltip.prototype.replaceArrow = function(delta, dimension, position) {
    this.arrow().css(position, delta ? (50 * (1 - delta / dimension) + "%") : "")
}

Tooltip.prototype.setContent = function () {
    var $tip = this.tip()
    var title = this.getTitle()

    $tip.find('.tooltip-inner')[this.options.html ? 'html' : 'text'](title)
    $tip.removeClass('fade in top bottom left right')
}

Tooltip.prototype.hide = function () {
    var that = this
    var $tip = this.tip()
    var e = $.Event('hide.bs.' + this.type)

    function complete() {
        if (that.hoverState != 'in') $tip.detach()
    }

    this.$element.trigger(e)
}

```

```

if (e.isDefaultPrevented()) return

$tip.removeClass('in')

$.support.transition && this.$tip.hasClass('fade') ?
$tip
.one($.support.transition.end, complete)
.emulateTransitionEnd(150) :
complete()

this.$element.trigger('hidden.bs.' + this.type)

return this
}

Tooltip.prototype.fixTitle = function () {
var $e = this.$element
if ($e.attr('title') || typeof($e.attr('data-original-title')) != 'string') {
$e.attr('data-original-title', $e.attr('title') || "").attr('title', "")
}
}

Tooltip.prototype.hasContent = function () {
return this.getTitle()
}

Tooltip.prototype.getPosition = function () {
var el = this.$element[0]
return $.extend({}, (typeof el.getBoundingClientRect == 'function') ? el.getBoundingClientRect() : {
width: el.offsetWidth
, height: el.offsetHeight
}, this.$element.offset())
}

Tooltip.prototype.getCalculatedOffset = function (placement, pos, actualWidth, actualHeight) {
return placement == 'bottom' ? { top: pos.top + pos.height, left: pos.left + pos.width / 2 - actualWidth / 2 } :
placement == 'top' ? { top: pos.top - actualHeight, left: pos.left + pos.width / 2 - actualWidth / 2 } :
placement == 'left' ? { top: pos.top + pos.height / 2 - actualHeight / 2, left: pos.left - actualWidth } :
/* placement == 'right' */ { top: pos.top + pos.height / 2 - actualHeight / 2, left: pos.left + pos.width }
}

Tooltip.prototype.getTitle = function () {
var title
var $e = this.$element
var o = this.options

title = $e.attr('data-original-title')
|| (typeof o.title == 'function' ? o.title.call($e[0]) : o.title)
}

```

```

        return title
    }

Tooltip.prototype.tip = function () {
    return this.$tip = this.$tip || $(this.options.template)
}

Tooltip.prototype.arrow = function () {
    return this.$arrow = this.$arrow || this.tip().find('.tooltip-arrow')
}

Tooltip.prototype.validate = function () {
    if (!this.$element[0].parentNode) {
        this.hide()
        this.$element = null
        this.options = null
    }
}

Tooltip.prototype.enable = function () {
    this.enabled = true
}

Tooltip.prototype.disable = function () {
    this.enabled = false
}

Tooltip.prototype.toggleEnabled = function () {
    this.enabled = !this.enabled
}

Tooltip.prototype.toggle = function (e) {
    var self = e ? $(e.currentTarget)[this.type](this.getDelegateOptions()).data('bs.' + this.type) : this
    self.tip().hasClass('in') ? self.leave(self) : self.enter(self)
}

Tooltip.prototype.destroy = function () {
    this.hide().$element.off('.' + this.type).removeData('bs.' + this.type)
}

// TOOLTIP PLUGIN DEFINITION
// =====

var old = $.fn.tooltip

$.fn.tooltip = function (option) {
    return this.each(function () {
        var $this = $(this)
        var data = $this.data('bs.tooltip')
        var options = typeof option === 'object' && option

```

```

        if (!data) $this.data('bs.tooltip', (data = new Tooltip(this, options)))
        if (typeof option == 'string') data[option]()
    })
}

$.fn.tooltip.Constructor = Tooltip

// TOOLTIP NO CONFLICT
// =====

$.fn.tooltip.noConflict = function () {
    $.fn.tooltip = old
    return this
}

}(window.jQuery);

/*
=====
* Bootstrap: popover.js v3.0.0
* http://twbs.github.com/bootstrap/javascript.html#popovers
* =====
* Copyright 2012 Twitter, Inc.
*
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
* You may obtain a copy of the License at
*
* http://www.apache.org/licenses/LICENSE-2.0
*
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
* See the License for the specific language governing permissions and
* limitations under the License.
* ===== */

```

```

+function ($) { "use strict";

// POPOVER PUBLIC CLASS DEFINITION
// =====

var Popover = function (element, options) {
    this.init('popover', element, options)
}

if (!$.fn.tooltip) throw new Error('Popover requires tooltip.js')

Popover.DEFAULTS = $.extend({}, $.fn.tooltip.Constructor.DEFAULTS, {
    placement: 'right'
    , trigger: 'click'
}

```

```

, content: "
, template: '<div class="popover"><div class="arrow"></div><h3 class="popover-title"></h3><div
class="popover-content"></div></div>'
})

// NOTE: POPOVER EXTENDS tooltip.js
// =====

Popover.prototype = $.extend({ }, $fn.tooltip.Constructor.prototype)

Popover.prototype.constructor = Popover

Popover.prototype.getDefaults = function () {
  return Popover.DEFAULTS
}

Popover.prototype.setContent = function () {
  var $tip = this.tip()
  var title = this.getTitle()
  var content = this.getContent()

  $tip.find('.popover-title')[this.options.html ? 'html' : 'text'](title)
  $tip.find('.popover-content')[this.options.html ? 'html' : 'text'](content)

  $tip.removeClass('fade top bottom left right in')

  // IE8 doesn't accept hiding via the `:empty` pseudo selector, we have to do
  // this manually by checking the contents.
  if (!$tip.find('.popover-title').html()) $tip.find('.popover-title').hide()
}

Popover.prototype.hasContent = function () {
  return this.getTitle() || this.getContent()
}

Popover.prototype.getContent = function () {
  var $e = this.$element
  var o = this.options

  return $e.attr('data-content')
    || (typeof o.content == 'function' ?
        o.content.call($e[0]) :
        o.content)
}

Popover.prototype.arrow = function () {
  return this.$arrow = this.$arrow || this.tip().find('.arrow')
}

Popover.prototype.tip = function () {
  if (!this.$tip) this.$tip = $(this.options.template)
}

```

```

        return this.$tip
    }

// POPOVER PLUGIN DEFINITION
// =====

var old = $.fn.popover

$.fn.popover = function (option) {
    return this.each(function () {
        var $this = $(this)
        var data = $this.data('bs.popover')
        var options = typeof option === 'object' && option

        if (!data) $this.data('bs.popover', (data = new Popover(this, options)))
        if (typeof option === 'string') data[option]()
    })
}

$.fn.popover.Constructor = Popover

// POPOVER NO CONFLICT
// =====

$.fn.popover.noConflict = function () {
    $.fn.popover = old
    return this
}

}(window.jQuery);

/*
 * Bootstrap: scrollspy.js v3.0.0
 * http://twbs.github.com/bootstrap/javascript.html#scrollspy
 * =====
 * Copyright 2012 Twitter, Inc.
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 * http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 * ===== */

```

```

+function ($) { "use strict";

// SCROLLSPY CLASS DEFINITION
// =====

function ScrollSpy(element, options) {
  var href
  var process = $.proxy(this.process, this)

  this.$element    = $(element).is('body') ? $(window) : $(element)
  this.$body       = $('body')
  this.$scrollElement = this.$element.on('scroll.bs.scroll-spy.data-api', process)
  this.options     = $.extend({ }, ScrollSpy.DEFAULTS, options)
  this.selector    = (this.options.target
    || ((href = $(element).attr('href')) && href.replace(/.*(?:#[^\s]+|$)/, ""))
    || '') + '.nav li > a'
  this.offsets    = $({})
  this.targets    = $({})
  this.activeTarget = null

  this.refresh()
  this.process()
}

ScrollSpy.DEFAULTS = {
  offset: 10
}

ScrollSpy.prototype.refresh = function () {
  var offsetMethod = this.$element[0] == window ? 'offset' : 'position'

  this.offsets = $({})
  this.targets = $({})

  var self = this
  var $targets = this.$body
    .find(this.selector)
    .map(function () {
      var $el = $(this)
      var href = $el.data('target') || $el.attr('href')
      var $href = /^#/.test(href) && $(href)

      return ($href
        && $href.length
        && [[ $href[offsetMethod]().top + (!$.isWindow(self.$scrollElement.get(0)) &&
          self.$scrollElement.scrollTop()), href ]]) || null
    })
    .sort(function (a, b) { return a[0] - b[0] })
    .each(function () {
      self.offsets.push(this[0])
      self.targets.push(this[1])
    })
}

```

```

        })
    }

ScrollSpy.prototype.process = function () {
    var scrollTop = this.$scrollElement.scrollTop() + this.options.offset
    var scrollHeight = this.$scrollElement[0].scrollHeight || this.$body[0].scrollHeight
    var maxScroll = scrollHeight - this.$scrollElement.height()
    var offsets = this.offsets
    var targets = this.targets
    var activeTarget = this.activeTarget
    var i

    if (scrollTop >= maxScroll) {
        return activeTarget != (i = targets.last()[0]) && this.activate(i)
    }

    for (i = offsets.length; i--;) {
        activeTarget != targets[i]
        && scrollTop >= offsets[i]
        && (!offsets[i + 1] || scrollTop <= offsets[i + 1])
        && this.activate( targets[i] )
    }
}

ScrollSpy.prototype.activate = function (target) {
    this.activeTarget = target

    $(this.selector)
        .parents('.active')
        .removeClass('active')

    var selector = this.selector
        + '[data-target=' + target + "],"
        + this.selector + '[href=' + target + "]"

    var active = $(selector)
        .parents('li')
        .addClass('active')

    if (active.parent('.dropdown-menu').length) {
        active = active
            .closest('li.dropdown')
            .addClass('active')
    }

    active.trigger('activate')
}

// SCROLLSPY PLUGIN DEFINITION
// =====

```

```

var old = $.fn.scrollspy

$.fn.scrollspy = function (option) {
  return this.each(function () {
    var $this = $(this)
    var data = $this.data('bs.scrollspy')
    var options = typeof option === 'object' && option

    if (!data) $this.data('bs.scrollspy', (data = new ScrollSpy(this, options)))
    if (typeof option === 'string') data[option]()
  })
}

$.fn.scrollspy.Constructor = ScrollSpy

// SCROLLSPY NO CONFLICT
// =====

$.fn.scrollspy.noConflict = function () {
  $.fn.scrollspy = old
  return this
}

// SCROLLSPY DATA-API
// =====

$(window).on('load', function () {
  $('[data-spy="scroll"]').each(function () {
    var $spy = $(this)
    $spy.scrollspy($spy.data())
  })
})

}(window.jQuery);

/*
=====
* Bootstrap: tab.js v3.0.0
* http://twbs.github.com/bootstrap/javascript.html#tabs
* =====
* Copyright 2012 Twitter, Inc.
*
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
* You may obtain a copy of the License at
*
* http://www.apache.org/licenses/LICENSE-2.0
*
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
*/

```

```

* See the License for the specific language governing permissions and
* limitations under the License.
* ===== */

+function ($) { "use strict";

// TAB CLASS DEFINITION
// =====

var Tab = function (element) {
  this.element = $(element)
}

Tab.prototype.show = function () {
  var $this = this.element
  var $ul = $this.closest('ul:not(.dropdown-menu)')
  var selector = $this.attr('data-target')

  if (!selector) {
    selector = $this.attr('href')
    selector = selector && selector.replace(/.*(?:#[^\s]*$)/, "") //strip for ie7
  }

  if ($this.parent('li').hasClass('active')) return

  var previous = $ul.find('.active:last a')[0]
  var e = $.Event('show.bs.tab', {
    relatedTarget: previous
  })

  $this.trigger(e)

  if (e.isDefaultPrevented()) return

  var $target = $(selector)

  this.activate($this.parent('li'), $ul)
  this.activate($target, $target.parent(), function () {
    $this.trigger({
      type: 'shown.bs.tab'
      , relatedTarget: previous
    })
  })
}

Tab.prototype.activate = function (element, container, callback) {
  var $active = container.find('> .active')
  var transition = callback
  && $.support.transition
  && $active.hasClass('fade')
}

```

```

function next() {
  $active
    .removeClass('active')
    .find('> .dropdown-menu > .active')
    .removeClass('active')

  element.addClass('active')

  if (transition) {
    element[0].offsetWidth // reflow for transition
    element.addClass('in')
  } else {
    element.removeClass('fade')
  }

  if (element.parent('.dropdown-menu')) {
    element.closest('li.dropdown').addClass('active')
  }

  callback && callback()
}

transition ?
  $active
    .one($.support.transition.end, next)
    .emulateTransitionEnd(150) :
  next()

$active.removeClass('in')
}

// TAB PLUGIN DEFINITION
// =====

var old = $.fn.tab

$.fn.tab = function ( option ) {
  return this.each(function () {
    var $this = $(this)
    var data = $this.data('bs.tab')

    if (!data) $this.data('bs.tab', (data = new Tab(this)))
    if (typeof option === 'string') data[option]()
  })
}

$.fn.tab.Constructor = Tab

// TAB NO CONFLICT
// =====

```

```

$.fn.tab.noConflict = function () {
  $.fn.tab = old
  return this
}

// TAB DATA-API
// =====

$(document).on('click.bs.tab.data-api', '[data-toggle="tab"], [data-toggle="pill"]', function (e) {
  e.preventDefault()
  $(this).tab('show')
})

}(window.jQuery);

/* =====
 * Bootstrap: affix.js v3.0.0
 * http://twbs.github.com/bootstrap/javascript.html#affix
 * =====
 * Copyright 2012 Twitter, Inc.
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 * http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 * ===== */

```

```

+function ($) { "use strict";

// AFFIX CLASS DEFINITION
// =====

var Affix = function (element, options) {
  this.options = $.extend({}, Affix.DEFAULTS, options)
  this.$window = $(window)
  .on('scroll.bs.affix.data-api', $.proxy(this.checkPosition, this))
  .on('click.bs.affix.data-api', $.proxy(this.checkPositionWithEventLoop, this))

  this.$element = $(element)
  this.affixed =
  this.unpin = null
}

```

```

        this.checkPosition()
    }

Affix.RESET = 'affix affix-top affix-bottom'

Affix.DEFAULTS = {
    offset: 0
}

Affix.prototype.checkPositionWithEventLoop = function () {
    setTimeout($.proxy(this.checkPosition, this), 1)
}

Affix.prototype.checkPosition = function () {
    if (!this.$element.is(':visible')) return

    var scrollHeight = $(document).height()
    var scrollTop = this.$window.scrollTop()
    var position = this.$element.offset()
    var offset = this.options.offset
    var offsetTop = offset.top
    var offsetBottom = offset.bottom

    if (typeof offset != 'object') offsetBottom = offsetTop = offset
    if (typeof offsetTop == 'function') offsetTop = offsetTop()
    if (typeof offsetBottom == 'function') offsetBottom = offsetBottom()

    var affix = this.unpin != null && (scrollTop + this.unpin <= position.top) ? false :
        offsetBottom != null && (position.top + this.$element.height() >= scrollHeight - offsetBottom) ?
        'bottom' :
        offsetTop != null && (scrollTop <= offsetTop) ? 'top' : false

    if (this.affixed === affix) return
    if (this.unpin) this.$element.css('top', "")

    this.affixed = affix
    this.unpin = affix == 'bottom' ? position.top - scrollTop : null

    this.$element.removeClass(Affix.RESET).addClass('affix' + (affix ? '-' + affix : ""))

    if (affix == 'bottom') {
        this.$element.offset({ top: document.body.offsetHeight - offsetBottom - this.$element.height() })
    }
}

// AFFIX PLUGIN DEFINITION
// =====
var old = $.fn.affix

$.fn.affix = function (option) {

```

```

return this.each(function () {
  var $this = $(this)
  var data = $this.data('bs.affix')
  var options = typeof option == 'object' && option

  if (!data) $this.data('bs.affix', (data = new Affix(this, options)))
  if (typeof option == 'string') data[option]()
})
}

$.fn.affix.Constructor = Affix

// AFFIX NO CONFLICT
// =====

$.fn.affix.noConflict = function () {
  $.fn.affix = old
  return this
}

// AFFIX DATA-API
// =====

$(window).on('load', function () {
  $('[data-spy="affix"]').each(function () {
    var $spy = $(this)
    var data = $spy.data()

    data.offset = data.offset || {}

    if (data.offsetBottom) data.offset.bottom = data.offsetBottom
    if (data.offsetTop) data.offset.top = data.offsetTop

    $spy.affix(data)
  })
})

})(window.jQuery);

```

```

Dashboard.js
// Check if an alert message is provided and display it
var chartStudent = $.parseJSON('{{ chartStudent | toJson | safe }}'); // Injected from Flask
var chartGrade = $.parseJSON('{{ chartGrade | toJson | safe }}'); // Injected from Flask
console.log(chartStudent);
console.log(chartGrade);

$(document).ready(function () {
  createLineChart(chartStudent, chartGrade, 'lineChart');
});

```

```

let createLineChart = function (chartLabel, chartData, chartElement) {
    // Example chart data for a line chart
    var chartData = {
        type: 'line',
        data: {
            labels: chartLabel,
            datasets: [{{
                label:"",
                data: chartData,
                fill: false,
                borderColor: 'rgba(75, 192, 192, 1)',
                borderWidth: 2,
                pointRadius: 5,
                pointBackgroundColor: 'rgba(75, 192, 192, 1)',
                pointBorderColor: 'rgba(75, 192, 192, 1)',
                pointHoverRadius: 7,
                pointHoverBackgroundColor: 'rgba(75, 192, 192, 1)',
                pointHoverBorderColor: 'rgba(75, 192, 192, 1)'
            }]}
        }
    };
    // Get the canvas element
    var ctx = document.getElementById(chartElement).getContext('2d');
    // Initialize Chart.js line chart
    var lineChart = new Chart(ctx, chartData);
}

```

detectSwitch.js

```

let getCaptureStateSecondsTest = function () {

    var secondsResult = 0;
    $.ajax({
        url: '/api/getCaptureState/' + $("#"userIdLoggedIn").val(),
        type: 'GET',
        async: false,
        success: function (response)
        {
            if(response.switchid == 1)
            {
                var resServerdatetime = response.serverdatetime;
                var resSwitchtime = response.switchtime;

                // Parse the strings into Moment.js objects
                var serverdatetime = moment(resServerdatetime, 'YYYY-MM-DD HH:mm:ss');
                var switchtime = moment(resSwitchtime, 'YYYY-MM-DD HH:mm:ss');

                // Calculate the difference in seconds
                var diffInSeconds = serverdatetime.diff(switchtime, 'seconds');
            }
        }
    });
}

```

```

        // Display the result
        console.log('Difference in seconds:', diffInSeconds);

        secondsResult = diffInSeconds;

    }

    },
error: function (error)
{
    alert(error);
}
});

return secondsResult;
}

document.addEventListener('DOMContentLoaded', function () {
    document.getElementById('btnn').addEventListener('click', goToAnalysis);

    let timerInterval;
    let totalSeconds = getCaptureStateSecondsTest();
    let captureEnded = false;

    // Initially disable the Analysis button
    document.getElementById('btnn').disabled = true;

    function updateButtonState() {
        const btnn = document.getElementById('btnn');
        btnn.classList.toggle('active', !btnn.disabled);
    }

    updateButtonState();

    document.getElementById('btnnn').addEventListener('click', function () {
        stopCapture();
        document.getElementById('btn').style.display = 'inline-block';
        document.getElementById('btnnn').style.display = 'none';
        captureEnded = true;

        // Stop the timer
        clearInterval(timerInterval);
        updateDurationDisplay(); // Update display with the final time

        // Enable Analysis button after End Capture
        document.getElementById('btnn').disabled = false;
        document.getElementById('btnn').classList.remove('active'); // Ensure the active class is removed
        document.getElementById('btnn').style.backgroundColor = '#2382BC'; // Colored
        document.getElementById('btnn').style.cursor = 'pointer'; // Hand cursor

        // Remove the beforeunload event listener when the capture ends
    })
})
});

```

```

window.onbeforeunload = null;
});

function updateDurationDisplay() {
    let minutes = Math.floor(totalSeconds / 60);
    let seconds = totalSeconds % 60;
    document.getElementById('duration').innerText = `${minutes} minutes ${seconds} seconds`;

    const bttn = document.getElementById('bttn');

    // Disable Analysis button during capture
    if (!captureEnded) {
        bttn.disabled = true;
        bttn.classList.remove('active');
        bttn.style.backgroundColor = '#545454'; // Gray color
        bttn.style.cursor = 'default'; // Default cursor
    } else {
        // Enable Analysis button after capture ends
        bttn.disabled = false;
        bttn.classList.add('active');
        bttn.style.backgroundColor = '#2382BC'; // Colored
        bttn.style.cursor = 'pointer'; // Hand cursor
    }
}

document.getElementById('btn').addEventListener('click', function () {
    startCapture();
    doSomethingAfterStartCapture(true);
});

let doSomethingAfterStartCapture = function (resetTotalSeconds) {
    document.getElementById('btn').style.display = 'none';
    document.getElementById('bttnn').style.display = 'inline-block';
    captureEnded = false;

    // Enable Analysis button when starting capture
    document.getElementById('bttn').disabled = false;

    // Start the timer or resume from the last recorded time
    timerInterval = setInterval(function () {
        totalSeconds++;
        updateDurationDisplay();
    }, 1000);

    if(resetTotalSeconds)
    {
        totalSeconds = 0; // Reset the timer
    }

    updateDurationDisplay(); // Update display with the reset time

    // Disable Analysis button when starting a new capture
}

```

```

document.getElementById('btnn').disabled = true;
document.getElementById('btnn').classList.remove('active'); // Ensure the active class is removed
document.getElementById('btnn').style.backgroundColor = '#545454'; // Gray color
document.getElementById('btnn').style.cursor = 'default'; // Default cursor

// Remove the beforeunload event listener when starting a new capture
window.onbeforeunload = null;
}

function goToAnalysis() {
    if (captureEnded) {
        window.location.href = "analysis.html";
    } else {
        // Check if the capture has started
        if (totalSeconds > 0) {
            var confirmation = confirm("The capture is still ongoing. Do you want to proceed to analysis anyway?");
            // Whether the user clicks "OK" or "Cancel", do not redirect and do not stop the timer
            alert("Analysis canceled. The capture is still ongoing.");
            // Add additional logic here if needed
            // The timer will continue running, and the user will stay on the page
        } else {
            // The capture has not started, redirect to analysis without showing the confirmation
            window.location.href = "analysis.html";
        }
    }
}

// Add an event listener to the "Detect" navigation link
document.getElementById('btnDetect').addEventListener('click', function () {
    // Disable Analysis button when "Detect" link is clicked
    document.getElementById('btnn').disabled = true;
    document.getElementById('btnn').classList.remove('active');
    document.getElementById('btnn').style.backgroundColor = '#545454'; // Gray color
    document.getElementById('btnn').style.cursor = 'default'; // Default cursor
});

let startCapture = function () {
    if($("#userIdLoggedIn").val() != "") {
        ajaxCallCapture('/api/startCapture/' + $("#userIdLoggedIn").val());
    }
}

let stopCapture = function () {
    if($("#userIdLoggedIn").val() != "") {
        ajaxCallCapture('/api/endCapture/' + $("#userIdLoggedIn").val());
    }
}

```

```

let ajaxCallCapture = function (url1) {
    $.ajax({
        url: url1,
        type: 'GET',
        success: function (response) {
            console.log(response); // Log the response from the Flask server

            //alert(response.message);
        },
        error: function (error) {
            console.error(error);

            //alert(error);
        }
    });
}

if(totalSeconds > 0)
{
    doSomethingAfterStartCapture(false);
}
});

respond.js
/* NUGET: BEGIN LICENSE TEXT
 *
 * Microsoft grants you the right to use these script files for the sole
 * purpose of either: (i) interacting through your browser with the Microsoft
 * website or online service, subject to the applicable licensing or use
 * terms; or (ii) using the files as included with a Microsoft product subject
 * to that product's license terms. Microsoft reserves all other rights to the
 * files not expressly granted by Microsoft, whether by implication, estoppel
 * or otherwise. Insofar as a script file is dual licensed under GPL,
 * Microsoft neither took the code under GPL nor distributes it thereunder but
 * under the terms set out in this paragraph. All notices and licenses
 * below are for informational purposes only.
 *
 * NUGET: END LICENSE TEXT */
/*! matchMedia() polyfill - Test a CSS media type/query in JS. Authors & copyright (c) 2012: Scott Jehl,
Paul Irish, Nicholas Zakas. Dual MIT/BSD license */
/*! NOTE: If you're already including a window.matchMedia polyfill via Modernizr or otherwise, you don't
need this part */
window.matchMedia = window.matchMedia || (function(doc, undefined){

    var bool,
        docElem = doc.documentElement,
        refNode = docElem.firstChild || docElem.firstChild,
        // fakeBody required for <FF4 when executed in <head>
        fakeBody = doc.createElement('body'),
        div    = doc.createElement('div');

```

```

div.id = 'mq-test-1';
div.style.cssText = "position:absolute;top:-100em";
fakeBody.style.background = "none";
fakeBody.appendChild(div);

return function(q){

    div.innerHTML = '&shy;<style media="'+q+'">#mq-test-1 { width: 42px; }</style>';

    docElem.insertBefore(fakeBody, refNode);
    bool = div.offsetWidth == 42;
    docElem.removeChild(fakeBody);

    return { matches: bool, media: q };
};

})(document);

```

```

/*! Respond.js v1.2.0: min/max-width media query polyfill. (c) Scott Jehl. MIT/GPLv2 Lic. j.mp/respondjs
*/
(function( win ){
    //exposed namespace
    win.respond = {};

    //define update even in native-mq-supporting browsers, to avoid errors
    respond.update = function(){};

    //expose media query support flag for external use
    respond.mediaQueriesSupported = win.matchMedia && win.matchMedia( "only all" ).matches;

    //if media queries are supported, exit here
    if( respond.mediaQueriesSupported ){ return; }

    //define vars
    var doc = win.document,
        docElem = doc.documentElement,
        mediastyles = [],
        rules = [],
        appendedEls = [],
        parsedSheets = {},
        resizeThrottle = 30,
        head = doc.getElementsByTagName( "head" )[0] || docElem,
        base = doc.getElementsByTagName( "base" )[0],
        links = head.getElementsByTagName( "link" ),
        requestQueue = [];

    //loop stylesheets, send text content to translate
    ripCSS = function(){
        var sheets = links,

```

```

        sl          = sheets.length,
        i           = 0,
        //vars for loop:
        sheet, href, media, isCSS;

        for( ; i < sl; i++ ){
            sheet   = sheets[ i ],
            href    = sheet.href,
            media   = sheet.media,
            isCSS   = sheet.rel && sheet.rel.toLowerCase() === "stylesheet";

            //only links plz and prevent re-parsing
            if( !!href && isCSS && !parsedSheets[ href ] ){
                // selectivizr exposes css through the rawCssText expando
                if (sheet.styleSheet && sheet.styleSheet.rawCssText) {
                    translate( sheet.styleSheet.rawCssText, href, media );
                    parsedSheets[ href ] = true;
                } else {
                    if( !/^([a-zA-Z:]*\/\/).test( href ) && !base)
                        || href.replace( RegExp.$1, "" ).split( "/" )[0]
                }
            }
            makeRequests();
        },
        //recurse through request queue, get css text
        makeRequests = function(){
            if( requestQueue.length ){
                var thisRequest = requestQueue.shift();

                ajax( thisRequest.href, function( styles ){
                    translate( styles, thisRequest.href, thisRequest.media );
                    parsedSheets[ thisRequest.href ] = true;
                    makeRequests();
                });
            }
        },
        //find media blocks in css text, convert to style blocks
        translate          = function( styles, href, media ){
            var qs           = styles.match(
                /@media[^{}]+{[^{}]*{[^{}]*}}+/{gi },
                ql             = qs && qs.length || 0,
                //try to get CSS path
                href           = href.substring( 0, href.lastIndexOf( "/" ) ),
            );
        };
    };
}

```

```

repUrls          = function( css ){
    return css.replace( /(url\()|[""]?([^\\""]*[^\:\"\"]+)[\""]?())\)/g, "$1"
+ href + "$2$3" );
},
useMedia         = !ql && media,
//vars used in loop
i                = 0,
j, fullq, thisq, eachq, eql;

//if path exists, tack on trailing slash
if( href.length ){ href += "/"; }

//if no internal queries exist, but media attr does, use that
//note: this currently lacks support for situations where a media attr is specified
on a link AND
//its associated stylesheet has internal CSS media queries.
//In those cases, the media attribute will currently be ignored.
if( useMedia ){
    ql = 1;
}

for( ; i < ql; i++ ){
    j      = 0;

    //media attr
    if( useMedia ){
        fullq = media;
        rules.push( repUrls( styles ) );
    }
    //parse for styles
    else{
        fullq   = qs[ i ].match( /@media *([^\{]+)\{([^\}]+)\}/ )
&& RegExp.$1;
        rules.push( RegExp.$2 && repUrls( RegExp.$2 ) );
    }

    eachq   = fullq.split( "," );
    eql     = eachq.length;

    for( ; j < eql; j++ ){
        thisq   = eachq[ j ];
        mediastyles.push( {
            media : thisq.split( "(" )[ 0 ].match( /(only\s+)?([a-zA-Z]+\s+)?\s*/ ) && RegExp.$2 || "all",
            rules  : rules.length - 1,
            hasquery: thisq.indexOf("(") > -1,
            minw   : thisq.match( /\(min\)-width:[\s]*([\s]*[0-9\.]+)(px|em)[\s]*\)/ ) && parseFloat( RegExp.$1 ) + ( RegExp.$2 || "" ),
            maxw   : thisq.match( /\(max\)-width:[\s]*([\s]*[0-9\.]+)(px|em)[\s]*\)/ ) && parseFloat( RegExp.$1 ) + ( RegExp.$2 || "" )
        } );
    }
}

```

```

        }
    }

    applyMedia();
},

lastCall,
resizeDefer,

// returns the value of 1em in pixels
getEmValue = function() {
    var ret,
        div = doc.createElement('div'),
        body = doc.body,
        fakeUsed = false;

    div.style.cssText = "position:absolute;font-size:1em;width:1em";

    if( !body ){
        body = fakeUsed = doc.createElement( "body" );
        body.style.background = "none";
    }

    body.appendChild( div );

    docElem.insertBefore( body, docElem.firstChild );

    ret = div.offsetWidth;

    if( fakeUsed ){
        docElem.removeChild( body );
    }
    else {
        body.removeChild( div );
    }

    //also update eminpx before returning
    ret = eminpx = parseFloat(ret);

    return ret;
},

//cached container for 1em value, populated the first time it's needed
eminpxx,

//enable/disable styles
applyMedia = function( fromResize ){
    var name = "clientWidth",
        docElemProp = docElem[ name ],
        currWidth = doc.compatMode === "CSS1Compat" &&
docElemProp || doc.body[ name ] || docElemProp,

```

```

        styleBlocks      = {},
        lastLink = links[ links.length-1 ],
        now           = (new Date()).getTime();

    //throttle resize calls
    if( fromResize && lastCall && now - lastCall < resizeThrottle ){
        clearTimeout( resizeDefer );
        resizeDefer = setTimeout( applyMedia, resizeThrottle );
        return;
    }
    else {
        lastCall = now;
    }

    for( var i in mediastyles ){
        var thisstyle = mediastyles[ i ],
            min = thisstyle.minw,
            max = thisstyle.maxw,
            minnull = min === null,
            maxnull = max === null,
            em = "em";

        if( !!min ){
            min = parseFloat( min ) * ( min.indexOf( em ) > -1 ? ( eminpx
|| getEmValue() ) : 1 );
        }
        if( !!max ){
            max = parseFloat( max ) * ( max.indexOf( em ) > -1 ? (
eminpx || getEmValue() ) : 1 );
        }

        // if there's no media query at all (the () part), or min or max is not null,
and if either is present, they're true
        if( !thisstyle.hasquery || ( !minnull || !maxnull ) && ( minnull ||
currWidth >= min ) && ( maxnull || currWidth <= max ) ){
            if( !styleBlocks[ thisstyle.media ] ){
                styleBlocks[ thisstyle.media ] = [];
            }
            styleBlocks[ thisstyle.media ].push( rules[
thisstyle.rules ] );
        }
    }

    //remove any existing respond style element(s)
    for( var i in appendedEls ){
        if( appendedEls[ i ] && appendedEls[ i ].parentNode === head ){
            head.removeChild( appendedEls[ i ] );
        }
    }

    //inject active styles, grouped by media type
    for( var i in styleBlocks ){

```

```

        var ss      = doc.createElement( "style" ),
            css      = styleBlocks[ i ].join( "\n" );

        ss.type = "text/css";
        ss.media = i;

        //originally, ss was appended to a documentFragment and sheets were
        appended in bulk.
        //this caused crashes in IE in a number of circumstances, such as when
        the HTML element had a bg image set, so appending beforehand seems best. Thanks to @dvelyk for the
        initial research on this one!
        head.insertBefore( ss, lastLink.nextSibling );

        if ( ss.styleSheet ){
            ss.styleSheet.cssText = css;
        }
        else {
            ss.appendChild( doc.createTextNode( css ) );
        }

        //push to appendedEls to track for later removal
        appendedEls.push( ss );
    }
},
//tweaked Ajax functions from Quirksmode
ajax = function( url, callback ) {
    var req = xmlhttp();
    if (!req){
        return;
    }
    req.open( "GET", url, true );
    req.onreadystatechange = function () {
        if ( req.readyState != 4 || req.status != 200 && req.status != 304 ){
            return;
        }
        callback( req.responseText );
    }
    if ( req.readyState == 4 ){
        return;
    }
    req.send( null );
},
//define ajax obj
xmlhttp = (function() {
    var xmlhttpmethod = false;
    try {
        xmlhttpmethod = new XMLHttpRequest();
    }
    catch( e ){
        xmlhttpmethod = new ActiveXObject( "Microsoft.XMLHTTP" );
    }
    return function(){

```

```

        return xmlhttpmethod;
    };
})();

//translate CSS
ripCSS();

//expose update for re-running respond later on
respond.update = ripCSS;

//adjust on resize
function callMedia(){
    applyMedia( true );
}
if( win.addEventListener ){
    win.addEventListener( "resize", callMedia, false );
}
else if( win.attachEvent ){
    win.attachEvent( "onresize", callMedia );
}
})(this);

```

```

respond.min.js
/* NUGET: BEGIN LICENSE TEXT
*
* Microsoft grants you the right to use these script files for the sole
* purpose of either: (i) interacting through your browser with the Microsoft
* website or online service, subject to the applicable licensing or use
* terms; or (ii) using the files as included with a Microsoft product subject
* to that product's license terms. Microsoft reserves all other rights to the
* files not expressly granted by Microsoft, whether by implication, estoppel
* or otherwise. Insofar as a script file is dual licensed under GPL,
* Microsoft neither took the code under GPL nor distributes it thereunder but
* under the terms set out in this paragraph. All notices and licenses
* below are for informational purposes only.
*
* NUGET: END LICENSE TEXT */
/*! matchMedia() polyfill - Test a CSS media type/query in JS. Authors & copyright (c) 2012: Scott Jehl,
Paul Irish, Nicholas Zakas. Dual MIT/BSD license */
/*! NOTE: If you're already including a window.matchMedia polyfill via Modernizr or otherwise, you don't
need this part */
window.matchMedia=window.matchMedia||(function(e,f){var
c,a=e.documentElement,b=a.firstChild||a.firstChild,d=e.createElement("body"),g=e.createElement(
"div");g.id="mq-test-1";g.style.cssText="position:absolute;top:-100em";d.style.background="none";d.appendChild(g);return function(h){g.innerHTML='<style
media="'+h+'> #mq-test-1 { width: 42px;
}</style>';a.insertBefore(d,b);c=g.offsetWidth==42;a.removeChild(d);return{matches:c,media:h}}})(docu
ment);

/*! Respond.js v1.2.0: min/max-width media query polyfill. (c) Scott Jehl. MIT/GPLv2 Lic. j.mp/respondjs
*/

```

```

(function(e){e.respond={ };respond.update=function(){ };respond.mediaQueriesSupported=e.matchMedia&&e.matchMedia("only all").matches;if(respond.mediaQueriesSupported){return }var w=e.document,s=w.documentElement,i=[],k=[],q=[],o={},h=30,f=w.getElementsByTagName("head")[0]||s,g=w.getElementsByTagName("base")[0],b=f.getElementsByTagName("link"),d=[],a=function(){var D=b,y=D.length,B=0,A,z,C,x;for(B<y;B++){A=D[B],z=A.href,C=A.media,x=A.rel&&A.rel.toLowerCase()==="stylesheet";if(!!(z&&x&&!o[z])&(if(A.styleSheet&&A.styleSheet.rawCssText){m(A.styleSheet.rawCssText,z,C);o[z]=true }else {if((!/^(a-zA-Z:]*)\//.test(z)&&!g)||z.replace(RegExp.$1,"").split("/")[0]===e.location.host){d.push({href:z,media:C})}})}u(),u=function(){if(d.length){var x=d.shift();n(x.href,function(y){m(y,x.href,x.media);o[x.href]=true;u() })},m=function(I,x,z){var G=I.match(/@media[^{}]+{[^{}]*{[^{}]{[^{}]*}}+}/gi),J=G.length||0,x=x.substring(0,x.lastIndexOf("/") ),y=function(K){return K.replace(/(url|()|")?([^\v\\"]|^:|")+"|"?(\))/g,"$1"+x+"<$2$3"},A=!J&&z,D=0,C,E,F,B,H;if(x.length){x+="/" }if(A){J=1}for(D<J;D++) {C=0;if(A){E=z;k.push(y(I))}else{E=G[D].match(/@media[^{}]+{[^{}]+?$/)&&RegExp.$1;k.push(RegExp.$2&&y(RegExp.$2))}B=E.split(",");H=B.length;for(C<H;C++) {F=B[C];i.push({media:F.split("(")[0].match(/(only\s+)?([a-zA-Z]+)\s?/)&&RegExp.$2||"all",rules:k.length-1,hasquery:F.indexOf("(")>-1,minw:F.match(/\(\min\-\width:[\s]*([\s]*[0-9\.\.]+)(px|em)[\s]*\)/)&&parseFloat(RegExp.$1)+(RegExp.$2||""),maxw:F.match(/\(\max\-\width:[\s]*([\s]*[0-9\.\.]+)(px|em)[\s]*\)/)&&parseFloat(RegExp.$1)+(RegExp.$2||""))} }j(),l,r,v=function(){var z,A=w.createElement("div"),x=w.body,y=false;A.style.cssText="position:absolute;font-size:1em;width:1em";if(!x){x=y=w.createElement("body");x.style.background="none"}x.appendChild(A);s.insertBefore(x,s.firstChild);z=A.offsetWidth;if(y){s.removeChild(x)}else{x.removeChild(A)}z=p=parseFloat(z);return z},p,j=function(I){var x="clientWidth",B=s[x],H=w.compatMode==="CSS1Compat"&&B||w.body[x]||B,D={},G=b[b.length-1],z=(new Date()).getTime();if(I&&l&&z-l<h){clearTimeout(r);r=setTimeout(j,h);return }else{l=z}for(var E in i){var K=i[E],C=K.minw,J=K.maxw,A=C==null,L=J==null,y="em";if(!!C){C=parseFloat(C)*(C.indexOf(y)>-1?(p||v()):1)}if(!!J){J=parseFloat(J)*(J.indexOf(y)>-1?(p||v()):1)}if(!K.hasquery||(!A||!L)&&(A||H>=C)&&(L||H<=J)){if(!D[K.media]){D[K.media]=[]}D[K.media].push(k[K.rules])} }for(var E in q){if(q[E]&&q[E].parentNode===f){f.removeChild(q[E])} }for(var E in D){var M=w.createElement("style"),F=D[E].join("\n");M.type="text/css";M.media=E;f.insertBefore(M,G.nextSibling);if(M.styleSheet){M.styleSheet.cssText=F}else{M.appendChild(w.createTextNode(F))}q.push(M)},n=function(x,z){var y=c();if(!y){return }y.open("GET",x,true);y.onreadystatechange=function(){if(y.readyState!=4||y.status!=200&&y.status!=304){return }z(y.responseText)};if(y.readyState==4){return }y.send(null),c=(function(){var x=false;try{x=new XMLHttpRequest()}catch(y){x=new ActiveXObject("Microsoft.XMLHTTP")};return function(){return x}})();a();respond.update=a;function t(){j(true)}if(e.addEventListener){e.addEventListener("resize",t,false)}else{if(e.attachEvent){e.attachEvent("onresize",t)}}}(this);

```

script.js

```

document.addEventListener('DOMContentLoaded', function () {
  document.getElementById('bttn').addEventListener('click', goToAnalysis);

  let timerInterval;
  let totalSeconds = 0;
  let captureEnded = false;

```

```

// Initially disable the Analysis button
document.getElementById('btnn').disabled = true;

function updateButtonState() {
    const btnn = document.getElementById('btnn');
    btnn.classList.toggle('active', !btnn.disabled);
}

updateButtonState();

document.getElementById('btn').addEventListener('click', function () {
    document.getElementById('btn').style.display = 'none';
    document.getElementById('btnnn').style.display = 'inline-block';
    captureEnded = false;
}

// Enable Analysis button when starting capture
document.getElementById('btnn').disabled = false;

// Start the timer or resume from the last recorded time
timerInterval = setInterval(function () {
    totalSeconds++;
    updateDurationDisplay();
}, 1000);
});

document.getElementById('btnnn').addEventListener('click', function () {
    document.getElementById('btn').style.display = 'inline-block';
    document.getElementById('btnnn').style.display = 'none';
    captureEnded = true;
}

// Stop the timer
clearInterval(timerInterval);
updateDurationDisplay(); // Update display with the final time

// Enable Analysis button after End Capture
document.getElementById('btnn').disabled = false;
document.getElementById('btnn').classList.remove('active'); // Ensure the active class is removed
document.getElementById('btnn').style.backgroundColor = '#2382BC'; // Colored
document.getElementById('btnn').style.cursor = 'pointer'; // Hand cursor

// Remove the beforeunload event listener when the capture ends
window.onbeforeunload = null;
});

function updateDurationDisplay() {
    let minutes = Math.floor(totalSeconds / 60);
    let seconds = totalSeconds % 60;
    document.getElementById('duration').innerText = `${minutes} minutes ${seconds} seconds`;

    const btnn = document.getElementById('btnn');

    // Disable Analysis button during capture

```

```

if (!captureEnded) {
    btnn.disabled = true;
    btnn.classList.remove('active');
    btnn.style.backgroundColor = '#545454'; // Gray color
    btnn.style.cursor = 'default'; // Default cursor
} else {
    // Enable Analysis button after capture ends
    btnn.disabled = false;
    btnn.classList.add('active');
    btnn.style.backgroundColor = '#2382BC'; // Colored
    btnn.style.cursor = 'pointer'; // Hand cursor
}
}

document.getElementById('btn').addEventListener('click', function () {
    totalSeconds = 0; // Reset the timer
    updateDurationDisplay(); // Update display with the reset time

    // Disable Analysis button when starting a new capture
    document.getElementById('btnn').disabled = true;
    document.getElementById('btnn').classList.remove('active'); // Ensure the active class is removed
    document.getElementById('btnn').style.backgroundColor = '#545454'; // Gray color
    document.getElementById('btnn').style.cursor = 'default'; // Default cursor

    // Remove the beforeunload event listener when starting a new capture
    window.onbeforeunload = null;
});

function goToAnalysis() {
    if (captureEnded) {
        window.location.href = "analysis.html";
    } else {
        // Check if the capture has started
        if (totalSeconds > 0) {
            var confirmation = confirm("The capture is still ongoing. Do you want to proceed to analysis anyway?");
            // Whether the user clicks "OK" or "Cancel", do not redirect and do not stop the timer
            alert("Analysis canceled. The capture is still ongoing.");
            // Add additional logic here if needed

            // The timer will continue running, and the user will stay on the page
        } else {
            // The capture has not started, redirect to analysis without showing the confirmation
            window.location.href = "analysis.html";
        }
    }
}

// Add an event listener to the "Detect" navigation link
document.getElementById('btnDetect').addEventListener('click', function () {
    // Disable Analysis button when "Detect" link is clicked
}

```

```

document.getElementById('btnn').disabled = true;
document.getElementById('btnn').classList.remove('active');
document.getElementById('btnn').style.backgroundColor = '#545454'; // Gray color
document.getElementById('btnn').style.cursor = 'default'; // Default cursor
});

// script.js
document.getElementById('btn').addEventListener('click', function() {
    // Assuming startCapture function is defined in script.js or loaded before this line
    startCapture();
    // Add your other code here
});

// script1.js

function getRaspberryPiBaseUrl() {
    // Dynamically determine the base URL of the Raspberry Pi API
    const protocol = window.location.protocol;
    const host = window.location.hostname;
    const port = window.location.port || "5001"; // Use port 80 if not specified

    return `${protocol}//${host}:${port}`;
}

function startCapture() {
    const baseUrl = getRaspberryPiBaseUrl();

    fetch(`${baseUrl}/capture`, {
        method: 'POST',
        headers: {
            'Content-Type': 'application/x-www-form-urlencoded',
        },
        body: 'action=start',
    })
    .then(response => response.json())
    .then(data => {
        console.log(data);
        // Handle success, update UI, etc.
    })
    .catch(error => {
        console.error(error);
        // Handle error, show alert, etc.
    });
}

function stopCapture() {
    const baseUrl = getRaspberryPiBaseUrl();

    fetch(`${baseUrl}/capture`, {
        method: 'POST',
        headers: {
            'Content-Type': 'application/x-www-form-urlencoded',
        },
    })
}

```

```

        },
        body: 'action=stop',
    })
    .then(response => response.json())
    .then(data => {
        console.log(data);
        // Handle success, update UI, etc.
    })
    .catch(error => {
        console.error(error);
        // Handle error, show alert, etc.
    });
}
}

const url = 'http://192.168.104.171:5001/capture';
const data = new FormData();
data.append('action', 'start');

fetch(url, {
    method: 'POST',
    body: data,
})
.then(response => response.json())
.then(data => {
    console.log('Success:', data);
    // Handle success, if needed
})
.catch((error) => {
    console.error('Error:', error);
    // Handle error, if needed
});
});

```

```

script2.js
let menu = document.querySelector('#menu-icon');
let navbar = document.querySelector('.navbar');

menu.onclick = () => {
    menu.classList.toggle('bx-x');
    navbar.classList.toggle('open');
}

```

```

scriptreg.js
const wrapper = document.querySelector('.wrapper');
const btnPopup = document.querySelector('.btnlogin-popup');
const iconClose = document.querySelector('.icon-close');
const loginForm = document.getElementById('loginForm');
const registerForm = document.getElementById('registerForm');
const showRegisterFormLink = document.getElementById('showRegisterForm');
const showLoginFormLink = document.getElementById('showLoginForm');

```

```

// Function to open the terms modal
function openModal() {
    const modal = document.getElementById('termsModal');
    modal.style.display = 'flex'; // Use flex to center the content vertically
    document.body.classList.add('modal-open');
}

// Function to close the terms modal
function closeModal() {
    const modal = document.getElementById('termsModal');
    modal.style.display = 'none';
    document.body.classList.remove('modal-open');
}

// Function to handle closing the modal without agreement
function closeModalWithoutAgreement() {
    const termsCheckbox = document.getElementById('termsCheckbox');
    termsCheckbox.checked = false;
    closeModal();
}

// Function to handle agreement and close modal
function agreeTerms() {
    const termsCheckbox = document.getElementById('termsCheckbox');
    termsCheckbox.checked = true;
    closeModal();
}

// Function to handle closing the modal without agreement
function closeModalWithoutAgreement() {
    const termsCheckbox = document.getElementById('termsCheckbox');
    termsCheckbox.checked = false;
    closeModal();
}

// Add an event listener to open the terms modal when the checkbox is clicked
const termsCheckbox = document.getElementById('termsCheckbox');
termsCheckbox.addEventListener('click', openModal);

// Update the event listener for the close button in the terms modal
const closeButton = document.querySelector('.modal .close');
closeButton.addEventListener('click', closeModalWithoutAgreement);

// Update the event listener for the "Agree" button in the terms modal
const agreeButton = document.querySelector('.modal button');
agreeButton.addEventListener('click', agreeTerms);

btnPopup.addEventListener('click', () => {
    wrapper.classList.add('active-popup');
    loginForm.style.display = 'block';
    registerForm.style.display = 'none';
});

iconClose.addEventListener('click', () => {

```

```
wrapper.classList.remove('active-popup');
});

showRegisterFormLink.addEventListener('click', () => {
    loginForm.style.display = 'none';
    registerForm.style.display = 'block';
});

showLoginFormLink.addEventListener('click', () => {
    loginForm.style.display = 'block';
    registerForm.style.display = 'none';
});

// Add the following code to check if the terms checkbox is checked before submitting the form
const registerFormElement = document.querySelector('#registerForm form');
registerFormElement.addEventListener('submit', function (event) {
    const termsCheckbox = document.getElementById('termsCheckbox');
    if (!termsCheckbox.checked) {
        alert('Please agree to the terms and conditions before registering.');
        event.preventDefault(); // Prevent the form from submitting
    }
});
```

d) Web App (Backend)

- Web App 1

```
webapp1 init.py
import os
from flask import Flask, render_template, request, session, redirect, jsonify
from flask_mysqldb import MySQL
from datetime import datetime, timedelta
import pytz # Import the pytz module
import json

try:
    from flask_cors import CORS
except ImportError:
    # If flask_cors is not installed, provide a warning
    print("Warning: flask_cors module not found. Cross-origin resource sharing (CORS) may not work.")
    CORS = lambda app: app # Define a dummy CORS function that does nothing

app = Flask(__name__)
CORS(app)

secret_key = os.urandom(24)
app.secret_key = secret_key

mysql = MySQL(app)

# Set the timezone to Asia/Manila (Philippines timezone)
philippines_timezone = pytz.timezone('Asia/Manila')

@app.route('/')
@app.route('/', methods=['GET','POST'])

def index():

    if request.method == 'POST':

        username = request.form['loginPageUsername']
        password = request.form['loginPagePassword']

        cur = mysql.connection.cursor()

        try:
            # Execute the SELECT query
            cur.execute("SELECT user_id, username, password, email FROM users WHERE username = %s AND password = %s", (username, password))

            # Fetch the result (assuming you are interested in the result)
            user = cur.fetchone()

            if user:
                # User with the given username and password exists
                session["userLoggedIn"] = username
                session["userIdLoggedIn"] = user[0]
```

```

# Get the current UTC time
utc_now = datetime.utcnow()

# Convert UTC time to Philippines timezone
philippines_time = utc_now.replace(tzinfo=pytz.utc).astimezone(philippines_timezone)

# Print or use the Philippines time as needed
print("Philippines Time:", philippines_time)

# Use the stored procedure to log the login attempt with the Philippines time
cur.callproc('LogLoginAttempt', (username, password, 0, 0))

# Commit the changes
mysql.connection.commit()

return redirect('/home')
else:
    session["userLoggedIn"] = ""
    # User does not exist, handle accordingly (e.g., return an error message)
    alert_message = "Login failed. Please check your username and password."
    return render_template('index.html', alert_message=alert_message)

except Exception as e:
    # Handle exceptions and log them for debugging
    print("Error:", str(e))
    mysql.connection.rollback()
    # Handle the error response as needed

finally:
    # Close the cursor after executing the queries
    cur.close()

session["userLoggedIn"] = ""
return render_template(
    'index.html',
    title='Home Page',
)
)

@app.route('/register', methods=['GET','POST'])

def register():

if request.method == 'POST':
    username = request.form['registerPageUsername']
    email = request.form['registerPageEmail']
    password = request.form['registerPagePassword']

    cur = mysql.connection.cursor()

    cur.execute("SELECT * FROM users WHERE username = '" + username + "'")

```

```

user = cur.fetchone()

cur.close()

if user:
    alert_message = "Username already exists!"
    return render_template('register.html', alert_message=alert_message)
else:
    # INSERT NEW USER
    curInsert = mysql.connection.cursor()

    curInsert.execute("INSERT INTO users (username, password, email) VALUES('" + username +
    "','" + password + "','" + email + "')")

    mysql.connection.commit()

    curInsert.close()

    # INSERT ENTRY in tblSwitch once user is created
    curInsertTblSwitch = mysql.connection.cursor()

    curInsertTblSwitch.execute("INSERT INTO tblSwitch VALUES (0, NULL, (SELECT
MAX(user_id) FROM users))")

    mysql.connection.commit()

    curInsertTblSwitch.close()

    alert_message = "Account Successfully Registered!"
    return render_template('register.html', alert_message=alert_message)

return render_template(
    'register.html',
    title='Register',
)

```

```

@app.route('/home')
def home():
    userLoggedIn = session["userLoggedIn"];

    return render_template(
        'home.html',
        title='Home',
        userLoggedIn=userLoggedIn
    )

```

```

@app.route('/about')
def about():
    userLoggedIn = session["userLoggedIn"];

    return render_template(

```

```

'about.html',
title='About',
userLoggedIn=userLoggedIn
)

@app.route('/detect')
def detect():
    userLoggedIn = session["userLoggedIn"];
    userIdLoggedIn = session["userIdLoggedIn"];

    if userLoggedIn == "":
        return redirect('/')
    else:
        return render_template(
            'detect.html',
            title='Detect',
            userLoggedIn=userLoggedIn,
            userIdLoggedIn=userIdLoggedIn
        )

@app.route('/abstract')
def abstract():
    userLoggedIn = session["userLoggedIn"];

    return render_template(
        'abstract.html',
        title='Abstract',
        userLoggedIn=userLoggedIn
    )

@app.route('/members')
def members():
    userLoggedIn = session["userLoggedIn"];

    return render_template(
        'members.html',
        title='Members',
        userLoggedIn=userLoggedIn
    )

@app.route('/test123')
def test123():
    userLoggedIn = session["userLoggedIn"];

    return render_template(
        'test123.html',
        title='Bootstrap Grid',
        userLoggedIn=userLoggedIn
    )

@app.route('/analysis')
def analysis():

```

```

userLoggedIn = session["userLoggedIn"];
userIdLoggedIn = session["userIdLoggedIn"];

cur = mysql.connection.cursor()
# Execute the SELECT query
cur.execute("SELECT dur, protocol, sourceip, destip, destport, starttime, traffic, normal, dos, brutef,
botnet, inf, classify FROM tblanalysis WHERE user_id = " + str(userIdLoggedIn) + " ORDER BY id
DESC LIMIT 1")

analysisRecord = cur.fetchone()

if analysisRecord:
    # User with the given username and password exists
    dur = analysisRecord[0]
    protocol = analysisRecord[1]
    sourceip = analysisRecord[2]
    destip = analysisRecord[3]
    destport = analysisRecord[4]
    starttime = analysisRecord[5]
    traffic = analysisRecord[6]
    normal = analysisRecord[7]
    dos = analysisRecord[8]
    brutef = analysisRecord[9]
    botnet = analysisRecord[10]
    inf = analysisRecord[11]
    classify = analysisRecord[12]

    return render_template(
        'analysis.html',
        title='Analysis',
        userLoggedIn=userLoggedIn,
        userIdLoggedIn=userIdLoggedIn,
        recordExists='1',
        dur=dur,
        protocol=protocol,
        sourceip=sourceip,
        destip=destip,
        destport=destport,
        starttime=starttime,
        traffic=traffic,
        normal=normal,
        dos=dos,
        brutef=brutef,
        botnet=botnet,
        inf=inf,
        classify=classify
    )
else:
    return render_template(
        'analysis.html',
        title='Analysis',
        userLoggedIn=userLoggedIn,

```

```

        userIdLoggedIn=userIdLoggedIn,
        recordExists='0',
    )

@app.route('/statistics')
def statistics():
    userLoggedIn = session["userLoggedIn"];

    return render_template(
        'statistics.html',
        title='Statistics',
        userLoggedIn=userLoggedIn
    )

@app.route('/history')
def history():
    userLoggedIn = session["userLoggedIn"]
    userIdLoggedIn = session["userIdLoggedIn"]

    cur = mysql.connection.cursor()
    # Execute the SELECT query
    cur.execute("SELECT `date`, `time`, `sourceip`, `destip`, `traffic`, `classification` FROM tblhistory
WHERE user_id = " + str(userIdLoggedIn) + " ORDER BY id DESC ")

    historyRecord = cur.fetchall()

    historyJSONdata = []

    for row in historyRecord:
        tblHistoryDate = str(row[0])
        tblHistoryTime = str(row[1])
        tblHistorySourceip = str(row[2])
        tblHistoryDestip = str(row[3])
        tblHistoryTraffic = str(row[4])
        tblHistoryClassification = str(row[5])

        row_data = {
            'date':tblHistoryDate,
            'time':tblHistoryTime,
            'sourceip':tblHistorySourceip,
            'destip':tblHistoryDestip,
            'traffic':tblHistoryTraffic,
            'classification':tblHistoryClassification
        }

        historyJSONdata.append(row_data)

    cur.close()

    return render_template(
        'history.html',
        title='History',

```

```

        userLoggedIn=userLoggedIn,
        userIdLoggedIn=userIdLoggedIn,
        historyJSONdata=json.dumps(historyJSONdata),
    )

@app.route('/dashboard')
def dashboard():
    userLoggedIn = session.get("userLoggedIn")
    userIdLoggedIn = session.get("userIdLoggedIn")

    cur = mysql.connection.cursor()
    # Execute the SELECT query to fetch the latest numalerts
    cur.execute("SELECT numalerts FROM tbldashboardmetrics WHERE user_id = %s ORDER BY id DESC LIMIT 1", (userIdLoggedIn,))
    numalertsRecord = cur.fetchone()

    # Extracting numalerts from fetched record
    numalerts = numalertsRecord[0]

    cur.execute("SELECT total_TCP_count, total_UDP_count FROM tbldashboardmetrics WHERE user_id = %s ORDER BY id DESC LIMIT 1", (userIdLoggedIn,))
    tcp_udp_count_record = cur.fetchone()
    total_tcp_count, total_udp_count = tcp_udp_count_record if tcp_udp_count_record else (0, 0)

    # Execute the SELECT query to fetch the latest 15 records in descending order
    cur.execute("SELECT aveflowpktsrate, aveflowbytsrate, alerts, numalerts FROM tbldashboardmetrics WHERE user_id = %s ORDER BY id DESC LIMIT 15", (userIdLoggedIn,))
    dashboardRecords = cur.fetchall()

    # Get Latest ranking from tblrankings
    cur.execute("SELECT ranking FROM tblrankings WHERE user_id = %s ORDER BY id DESC", (userIdLoggedIn,))
    latestranking = cur.fetchall()

    rankingJSONString = '[';

    for row in latestranking:
        rankingJSONString = rankingJSONString + str(row[0])

    rankingJSONString = rankingJSONString + ']'

    # Extracting data from fetched records
    aveflowpktsrates = [record[0] for record in dashboardRecords]
    aveflowbytsrates = [record[1] for record in dashboardRecords]
    alerts = [record[2] for record in dashboardRecords]

    # Initialize chart data with zeros
    chartDay = ["0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "10", "11", "12", "13", "14", "15"]
    chartPackets = [0] * len(chartDay)

    chartHours = ["0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "10", "11", "12", "13", "14", "15"]
    chartTraffic = [0] * len(chartHours)

    chartWeek = ["0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "10", "11", "12", "13", "14", "15"]
    chartNPackets = [0] * len(chartWeek)

```

```

chartHUT = ["TCP", "UDP"]
chartDt = [0] * len(chartHUT)

# Update chart data with actual values if available
if aveflowbytsrates:
    chartTraffic[:len(aveflowbytsrates)] = aveflowbytsrates
if aveflowpktsrates:
    chartNPackets[:len(aveflowpktsrates)] = aveflowpktsrates
if alerts:
    chartPackets[:len(alerts)] = alerts

return render_template(
    'dashboard.html',
    title='Dashboard',
    userLoggedIn=userLoggedIn,
    userIdLoggedIn=userIdLoggedIn,
    resultExists='1',
    numalerts=numalerts,
    total_tcp_count=total_tcp_count,
    total_udp_count=total_udp_count,
    chartDay=chartDay,
    chartPackets=chartPackets,
    chartHours=chartHours,
    chartTraffic=chartTraffic,
    chartWeek=chartWeek,
    chartNPackets=chartNPackets,
    chartHUT=chartHUT,
    chartDt=chartDt,
    latestranking=rankingJSONString,
)

```

webapp 1 runserver.py

```

from os import environ
from DeTechProgress import app

if __name__ == '__main__':
    HOST = environ.get('SERVER_HOST', '0.0.0.0')
    try:
        PORT = int(environ.get('SERVER_PORT', '5555'))
    except ValueError:
        PORT = 5555
    app.run(HOST, PORT)

```

- Web App 2

```

model1.py
import pandas as pd
import joblib
from joblib import load
from sklearn.preprocessing import StandardScaler, MinMaxScaler, LabelEncoder
import numpy as np
import re
import json
import os
from flask import Flask
from flask_mysqldb import MySQL
from io import BytesIO
from collections import Counter
import tensorflow as tf
import xgboost as xgb
from xgboost import XGBClassifier
import logging
import pytz
from datetime import datetime

# Set up logging configuration
logging.basicConfig(level=logging.INFO)
logger = logging.getLogger(__name__)

app = Flask(__name__)

# Load the machine learning models
def load_models(model_paths):
    models = [load(model_path) for model_path in model_paths]
    logger.info("Models loaded successfully.")
    return models

# Data Preparation
def clean_value(value):
    try:
        if pd.notnull(value):
            cleaned_value = re.sub(r'[a-zA-Z "{}]', ' ', value)
            return cleaned_value.strip()
        return value
    except Exception as e:
        logger.error(f"Error cleaning value: {e}")
        raise

def remove_first_symbol(value):
    try:
        if pd.notnull(value):
            return value[1:] if len(value) > 0 else value
        return value
    except Exception as e:
        logger.error(f"Error removing first symbol: {e}")
        raise

def prepare_data_for_prediction(raw_csv_data):
    try:
        csv_data_io = BytesIO(raw_csv_data)
    
```

```

df = pd.read_csv(csv_data_io)

# Add headers
your_headers = ['src ip', 'dst ip', 'src port', 'dst port', 'protocol',
                'timestamp', 'flow duration', 'flow byts s', 'flow pkts s',
                'fwd pkts s', 'bwd pkts s', 'tot fwd pkts', 'tot bwd pkts',
                'totlen fwd pkts', 'totlen bwd pkts', 'fwd pkt len max',
                'fwd pkt len min', 'fwd pkt len mean', 'fwd pkt len std',
                'bwd pkt len max', 'bwd pkt len min', 'bwd pkt len mean',
                'bwd pkt len std', 'pkt len max', 'pkt len min', 'pkt len mean',
                'pkt len std', 'pkt len var', 'fwd header len', 'bwd header len',
                'fwd seg size min', 'fwd act data pkts', 'flow iat mean',
                'flow iat max', 'flow iat min', 'flow iat std', 'fwd iat tot',
                'fwd iat max', 'fwd iat min', 'fwd iat mean', 'fwd iat std',
                'bwd iat tot', 'bwd iat max', 'bwd iat min', 'bwd iat mean',
                'bwd iat std', 'fwd psh flags', 'bwd psh flags', 'fwd urg flags',
                'bwd urg flags', 'fin flag cnt', 'syn flag cnt', 'rst flag cnt',
                'psh flag cnt', 'ack flag cnt', 'urg flag cnt', 'ece flag cnt',
                'down up ratio', 'pkt size avg', 'init fwd win byts', 'init bwd win byts',
                'active max', 'active min', 'active mean', 'active std', 'idle max',
                'idle min', 'idle mean', 'idle std', 'fwd byts b avg', 'fwd pkts b avg',
                'bwd byts b avg', 'bwd pkts b avg', 'fwd blk rate avg', 'bwd blk rate avg',
                'fwd seg size avg', 'bwd seg size avg', 'cwe flag count', 'subflow fwd pkts',
                'subflow bwd pkts', 'subflow fwd byts', 'subflow bwd byts'
            ]
if len(your_headers) == len(df.columns):
    df.columns = your_headers
else:
    logger.error("Number of headers does not match the number of columns in the CSV.")
    raise ValueError("Number of headers does not match the number of columns in the CSV.")

# Cleans values
df = df.applymap(clean_value)

# Fix the format of values
df = df.applymap(remove_first_symbol)

# Check for NaN values
nan_counts = df.isnull().sum().sum()

if nan_counts > 0:
    logger.warning(f"The CSV data has {nan_counts} NaN values. Filling with 0...")
    df = df.fillna(0)
    logger.info("NaN values filled.")
else:
    logger.info("The CSV data has no NaN values.")

# Remove duplicate rows
prepped_csv = df.drop_duplicates(keep='first')
logger.info("Duplicate rows removed.")

return prepped_csv
except Exception as e:
    logger.error(f"Error preparing data for prediction: {e}")
    raise

```

```

def normalize_for_detection(prepped_csv):
    try:
        df = prepped_csv
        important_features_list = ['dst port','tot fwd pkts','tot bwd pkts','totlen fwd pkts','totlen bwd pkts','fwd pkt len mean','bwd pkt len max','fwd iat mean','flow iat max','flow iat min','fwd iat mean','fwd iat std','bwd iat mean','bwd iat std','bwd iat max','bwd iat min','fwd header len','bwd header len','fwd pkts s','bwd pkts s','pkt len mean','pkt len var','fwd seg size avg','bwd seg size avg','init fwd win byts','init bwd win byts']

        csv_data = df[important_features_list]
        csv_data = csv_data.apply(pd.to_numeric, errors='coerce')

        categorical_cols = ['dst port']
        df_categorical = csv_data[categorical_cols]
        df_numerical = csv_data.drop(columns=categorical_cols)

        std_scaler = StandardScaler()
        df_numerical_scaled = pd.DataFrame(std_scaler.fit_transform(df_numerical),
                                           columns=df_numerical.columns)

        df_normalized = pd.concat([df_numerical_scaled, df_categorical.reset_index(drop=True)], axis=1)
        df_normalized = df_normalized[important_features_list]
        logger.info("Data normalized for detection.")
        return df_normalized
    except Exception as e:
        logger.error(f"Error normalizing data for detection: {e}")
        raise

def svm_predict(csv_data_detect):
    try:
        data = csv_data_detect

        current_directory = os.path.dirname(os.path.abspath(__file__))
        svm_model_path = os.path.join(current_directory, "26-multi_class_svm_model.h5")
        svm_model = tf.keras.models.load_model(svm_model_path)

        svm_predictions_raw = svm_model.predict(data)
        svm_threshold = 0.5 # Set your desired threshold
        svm_predictions = np.where(svm_predictions_raw >= svm_threshold, 1, 0)

        logger.info("SVM prediction completed successfully.")
        return svm_predictions
    except Exception as e:
        logger.error(f"Error making SVM prediction: {e}")
        raise

def nb_predict(csv_data_detect):
    try:
        data = csv_data_detect

        current_directory = os.path.dirname(os.path.abspath(__file__))
        nb_model_path = os.path.join(current_directory, "26-NB_model.pkl")
        nb_model = joblib.load(nb_model_path)

        nb_predictions = nb_model.predict(data)

```

```

label_encoder = LabelEncoder()
nb_predictions_numeric = label_encoder.fit_transform(nb_predictions)

logger.info("Naive Bayes prediction completed successfully.")
return nb_predictions_numeric
except Exception as e:
    logger.error(f"Error making Naive Bayes prediction: {e}")
    raise

def dt_predict(csv_data_detect):
    try:
        data = csv_data_detect

        current_directory = os.path.dirname(os.path.abspath(__file__))
        dt_model_path = os.path.join(current_directory, "26-DT_model.pkl")
        dt_model = joblib.load(dt_model_path)

        dt_predictions = dt_model.predict(data)

        logger.info("Decision Tree prediction completed successfully.")
        return dt_predictions
    except Exception as e:
        logger.error(f"Error making Decision Tree prediction: {e}")
        raise

def ensemble_predict(svm_predict, nb_predict, dt_predict):

    try:
        current_directory = os.path.dirname(os.path.abspath(__file__))
        ensemble_model_path = os.path.join(current_directory, "26-Ensemble_model_multi_class.pkl")
        xgb_model = joblib.load(ensemble_model_path)

        stacked_predictions = np.column_stack((svm_predict, nb_predict, dt_predict))

        classifications = xgb_model.predict(stacked_predictions)

        result_counts = pd.Series(classifications).value_counts(normalize=True) * 100

        # Mapping of labels to terms
        label_to_term = {
            0: 'Normal',
            1: 'Denial of Service',
            3: 'Botnet',
            4: 'Infiltration',
            2: 'Bruteforce'
        }

        # Initialize classification results with all label names set to 0%
        classification_results = {label: "0.00%" for label in label_to_term.values()}

        # Update the classification results with actual percentages
        for label, percentage in result_counts.items():
            term = label_to_term.get(label, 'Unknown') # Get the corresponding term or 'Unknown' if not found
            classification_results[term] = f'{percentage:.2f}%'

        return classification_results
    
```

```

except Exception as e:
    print(f"Error: {e}")

def detect_traffic(csv_data_detect):
    try:
        svm_data = svm_predict(csv_data_detect)
        nb_data = nb_predict(csv_data_detect)
        dt_data = dt_predict(csv_data_detect)
        ensemble_result = ensemble_predict(svm_data, nb_data, dt_data)

        logger.info("Traffic detection completed successfully.")
        return ensemble_result
    except Exception as e:
        logger.error(f"Error detecting traffic: {e}")
        raise

def top_src_ip(raw_csv_data):
    df = raw_csv_data
    df['fwd pkts s'] = pd.to_numeric(df['fwd pkts s'], errors='coerce')
    df['fwd pkts s'] = df['fwd pkts s'].fillna(0)
    sum_fwd_pkts_per_ip = df.groupby('src ip')['fwd pkts s'].sum()
    sum_fwd_pkts_per_ip_df = sum_fwd_pkts_per_ip.reset_index(name='sum of fwd pkts s')
    sum_fwd_pkts_per_ip_df = sum_fwd_pkts_per_ip_df.sort_values(by='sum of fwd pkts s',
                                                               ascending=False)
    json_src_ip = sum_fwd_pkts_per_ip_df.set_index('src ip')['sum of fwd pkts s'].to_dict()

    return json_src_ip

def top_dst_ip(raw_csv_data):
    df = raw_csv_data
    df['bwd pkts s'] = pd.to_numeric(df['bwd pkts s'], errors='coerce')
    df['bwd pkts s'] = df['bwd pkts s'].fillna(0)
    sum_bwd_pkts_per_ip = df.groupby('dst ip')['bwd pkts s'].sum()
    sum_bwd_pkts_per_ip_df = sum_bwd_pkts_per_ip.reset_index(name='sum of bwd pkts s')
    sum_bwd_pkts_per_ip_df = sum_bwd_pkts_per_ip_df.sort_values(by='sum of bwd pkts s',
                                                               ascending=False)
    json_dst_ip = sum_bwd_pkts_per_ip_df.set_index('dst ip')['sum of bwd pkts s'].to_dict()

    return json_dst_ip

def get_service_name(row, service_df):
    port_number = row['dst port']
    if port_number.isdigit() and int(port_number) <= 49151:
        matching_service = service_df.loc[service_df['Port Number'] == port_number, 'Service Name']
        if not matching_service.empty:
            return matching_service.iloc[0]
        else:
            return 'Reserved'
    else:
        return 'Dynamically Assigned Port' if int(port_number) > 49151 else 'Unassigned'

def top_ports(raw_csv_data):
    same_directory = os.path.dirname(os.path.abspath(__file__))
    service_csv_file = os.path.join(same_directory, 'ServiceNamePortNumber.csv')

```

```

service_df = pd.read_csv(service_csv_file)

# Remove leading and trailing whitespaces from 'dst port' column in raw_csv_data
raw_csv_data['dst port'] = raw_csv_data['dst port'].str.strip()

# Convert the 'Port Number' column in service_df to string and remove leading/trailing whitespaces
service_df['Port Number'] = service_df['Port Number'].astype(str).str.strip()

# Merge the raw data DataFrame with the service DataFrame based on port number
merged_df = pd.merge(raw_csv_data, service_df, left_on='dst port', right_on='Port Number', how='left')

# Create a new column 'Service Name' based on the criteria using the get_service_name() function
merged_df['Service Name'] = merged_df.apply(lambda row: get_service_name(row, service_df), axis=1)

# Sum 'flow byts s' for each 'Service Name'
sum_flow_byts = merged_df.groupby('Service Name')['flow byts s'].sum()

# Convert the Series to a DataFrame and reset the index
sum_flow_byts_df = sum_flow_byts.reset_index(name='sum of flow byts s')

# Sort the DataFrame by the summed 'flow byts s' in descending order
sum_flow_byts_df = sum_flow_byts_df.sort_values(by='sum of flow byts s', ascending=False)

# Convert the DataFrame to JSON format
json_ports = sum_flow_byts_df.set_index('Service Name')['sum of flow byts s'].to_dict()

return json_ports

def protocol_distribution(raw_csv_data):
    # Define protocol values
    protocol_values = {
        0: 'HOPOPT',
        1: 'ICMP',
        2: 'IGMP',
        6: 'TCP',
        8: 'EGP',
        17: 'UDP',
        27: 'RDP',
        36: 'XTP',
        88: 'EIGRP',
        89: 'OSPF',
        121: 'SMP'
    }

    df = raw_csv_data.copy()

    # Convert 'protocol' column to integer type
    df['protocol'] = df['protocol'].astype(int)

    # Map protocol numbers to protocol names
    df['protocol'] = df['protocol'].map(protocol_values).fillna('Others')

    # Count occurrences of each protocol
    protocol_counts = df['protocol'].value_counts()

    return protocol_counts

```

```

def analyzeCsvFile(document_id, user_id, csv_prep, csv_data_detect):
    try:
        # Concatenate 'date' and 'time' columns to form a new 'datetime' column
        csv_prep['datetime'] = pd.to_datetime(csv_prep['timestamp'])

        # Extract time component of the first row's timestamp and format as string
        start_time = csv_prep['datetime'].iloc[0].strftime('%H:%M:%S')

        # Extract date component of the first row's timestamp
        file_date = csv_prep['datetime'].dt.date.iloc[0]

        # FLOW DURATION
        # Convert 'flow duration' column to numeric, coercing errors to NaN
        csv_prep['flow duration'] = pd.to_numeric(csv_prep['flow duration'], errors='coerce')

        # Filter out NaN values
        capturing_duration_microseconds = csv_prep['flow duration'].dropna()

        # Calculate total capturing duration in minutes
        total_capturing_duration_minutes = capturing_duration_microseconds.sum() / 60000000

        # Analyze most frequent values
        most_frequent_protocol = csv_prep['protocol'].mode().values[0]
        most_frequent_src_ip = csv_prep['src ip'].mode().values[0]
        most_frequent_dst_ip = csv_prep['dst ip'].mode().values[0]
        most_frequent_dst_port = csv_prep['dst port'].mode().values[0]

        traffic_classification = detect_traffic(csv_data_detect)

        normal = traffic_classification["Normal"]
        dos = traffic_classification["Denial of Service"]
        bruteforce = traffic_classification["Bruteforce"]
        botnet = traffic_classification["Botnet"]
        infiltration = traffic_classification["Infiltration"]

        # Convert percentage strings to floats and find the max
        max_category = max(traffic_classification, key=lambda k: float(traffic_classification[k].rstrip('%')))

        # Classify the result as 'Normal' or 'Malicious'
        traffic_detection = 'Normal' if max_category == 'Normal' else 'Malicious'

        # Check if traffic_detection is 'Malicious'
        alerts = 1 if traffic_detection == 'Malicious' else 0

        logger.info("Analysis completed successfully.")
    except Exception as e:
        logger.error(f"Error analyzing CSV file: {e}")
        raise

    curInsertAnalysis = mysql.connection.cursor()
    curInsertHistory = mysql.connection.cursor()

    last_inserted_id_analysis = 0

    try:

```

```

# Your existing tblanalysis insertion code
curInsertAnalysis.execute(
    "INSERT INTO tblanalysis (dur, protocol, sourceip, destip, destport, user_id, starttime, traffic,
normal, dos, brutef, botnet, inf, classify, alerts) VALUES(" +
        str(total_capturing_duration_minutes) + "," + most_frequent_protocol + "," + most_frequent_src_ip
+
        "," + most_frequent_dst_ip + "," + most_frequent_dst_port + "," + str(user_id) + "," +
        str(start_time) + "," + traffic_detection + "," + str(normal) + "," + str(dos) + "," + str(bruteforce)
+
        "," +
        str(botnet) + "," + str(infiltration) + "," + str(max_category) + "," + str(alerts) + ")")

mysql.connection.commit()

last_inserted_id_analysis = curInsertAnalysis.lastrowid

logger.info("Analysis data inserted successfully.")
except Exception as analysis_error:
    mysql.connection.rollback() # Rollback changes if an error occurs during tblanalysis insertion
    raise analysis_error # Re-raise the exception
finally:
    curInsertAnalysis.close()

try:
    # Your existing tblhistory insertion code
    curInsertHistory.execute(
        "INSERT INTO tblhistory (user_id, date, time, traffic, analysisid, classification, sourceip, destip)
VALUES(" + str(user_id) + "," + str(file_date) + "," + str(start_time) + "," + traffic_detection + "," +
str(last_inserted_id_analysis) + "," + str(max_category) + "," + most_frequent_src_ip + "," +
most_frequent_dst_ip + ")")

    mysql.connection.commit()
    logger.info("History data inserted successfully.")
except Exception as history_error:
    mysql.connection.rollback() # Rollback changes if an error occurs during tblhistory insertion
    raise history_error # Re-raise the exception
finally:
    curInsertHistory.close()

# After your INSERT statements
mysql.connection.commit()

def dashboardResults(document_id, user_id, csv_prep, csv_data_detect):
    df = csv_prep
    try:
        # PACKET CAPTURE
        df['flow pkts s'] = pd.to_numeric(df['flow pkts s'], errors='coerce')
        ave_flowpacket_rate = df['flow pkts s'].mean()

        # TRAFFIC PATTERNS
        df['flow byts s'] = pd.to_numeric(df['flow byts s'], errors='coerce')
        ave_flowbytes_rate = df['flow byts s'].mean()

        # PROTOCOL DISTRIBUTION
        protocol_counts = protocol_distribution(csv_prep)

        HOPOPT_count = protocol_counts.get("HOPOPT", 0)
    
```

```

ICMP_count = protocol_counts.get("ICMP", 0)
IGMP_count = protocol_counts.get("IGMP", 0)
TCP_count = protocol_counts.get("TCP", 0)
EGP_count = protocol_counts.get("EGP", 0)
UDP_count = protocol_counts.get("UDP", 0)
RDP_count = protocol_counts.get("RDP", 0)
XTP_count = protocol_counts.get("XTP", 0)
EIGRP_count = protocol_counts.get("EIGRP", 0)
OSPF_count = protocol_counts.get("OSPF", 0)
SMP_count = protocol_counts.get("SMP", 0)
Others_count = protocol_counts.get("Others", 0)

# Load your raw CSV data into a DataFrame (replace this with your actual data loading code)

# Call each function to get the JSON outputs
json_src_ip = top_src_ip(csv_prep)
json_dst_ip = top_dst_ip(csv_prep)
json_ports = top_ports(csv_prep)

# Combine JSON outputs into a single dictionary
combined_json = {}
for i in range(min(len(json_src_ip), len(json_dst_ip), len(json_ports))):
    combined_json[f"Rank {i+1}"] = {
        "top_src_ip": {k: v for k, v in json_src_ip.items() if v == sorted(json_src_ip.values(), reverse=True)[i]},
        "top_dst_ip": {k: v for k, v in json_dst_ip.items() if v == sorted(json_dst_ip.values(), reverse=True)[i]},
        "top_ports": {k: v for k, v in json_ports.items() if v == sorted(json_ports.values(), reverse=True)[i]}
    }
json_ip_ports = json.dumps(combined_json, indent=4)

# Analyze most frequent values
most_frequent_protocol = csv_prep['protocol'].mode().values[0]
most_frequent_src_ip = csv_prep['src ip'].mode().values[0]
most_frequent_dst_ip = csv_prep['dst ip'].mode().values[0]
most_frequent_dst_port = csv_prep['dst port'].mode().values[0]

traffic_classification = detect_traffic(csv_data_detect)

normal = traffic_classification["Normal"]
dos = traffic_classification["Denial of Service"]
bruteforce = traffic_classification["Bruteforce"]
botnet = traffic_classification["Botnet"]
infiltration = traffic_classification["Infiltration"]

# Convert percentage strings to floats and find the max
max_category = max(traffic_classification, key=lambda k: float(traffic_classification[k].rstrip('%')))

# Classify the result as 'Normal' or 'Malicious'
traffic_detection = 'Normal' if max_category == 'Normal' else 'Malicious'

# Check if traffic_detection is 'Malicious'
alerts = 1 if traffic_detection == 'Malicious' else 0

# Update numalerts based on the current value and the new alerts value

```

```

cur = mysql.connection.cursor()
cur.execute("SELECT numalerts FROM tbldashboardmetrics WHERE user_id = %s", (user_id,))
result = cur.fetchone()
if result is not None:
    numalerts = result[0]
else:
    # If no records found for the user, set numalerts to 0
    numalerts = 0

# Update numalerts in the database
new_numalerts = numalerts + alerts
cur.execute("UPDATE tbldashboardmetrics SET numalerts = %s WHERE user_id = %s",
(new_numalerts, user_id))
mysql.connection.commit()
cur.close()

try:
    # Check if the cursor is None or if it's still connected
    if cur is None or not cur.connection:
        # Reconnect if the cursor is None or not connected
        conn = mysql.connection
        cur = conn.cursor()

    # Fetch the current value of TCP_count with a default value of 0
    cur.execute("SELECT IFNULL(TCP_count, 0) FROM tbldashboardmetrics WHERE user_id = %s",
(user_id,))
    result = cur.fetchone()
    if result is not None:
        current_TCP_count = result[0]
    else:
        current_TCP_count = 0

    # Update TCP_count in the database
    new_TCP_count = current_TCP_count + TCP_count # Add the new TCP count to the current count
    cur.execute("UPDATE tbldashboardmetrics SET TCP_count = %s WHERE user_id = %s",
(new_TCP_count, user_id))

    # Update total_TCP_count with the new total
    cur.execute("UPDATE tbldashboardmetrics SET total_TCP_count = total_TCP_count + %s
WHERE user_id = %s", (TCP_count, user_id))

    # Commit the changes to the database
    mysql.connection.commit()

except Exception as e:
    logger.error(f"Error retrieving Dashboard Results: {e}")
    raise

finally:
    # Close the cursor
    if cur:
        cur.close()

try:
    # Check if the cursor is None or if it's still connected
    if cur is None or not cur.connection:

```

```

# Reconnect if the cursor is None or not connected
conn = mysql.connection
cur = conn.cursor()

# Fetch the current value of UDP_count with a default value of 0
cur.execute("SELECT IFNULL(UDP_count, 0) FROM tbldashboardmetrics WHERE user_id = %s",
(user_id,))
result = cur.fetchone()
if result is not None:
    current_UDP_count = result[0]
else:
    current_UDP_count = 0

# Update UDP_count in the database
new_UDP_count = current_UDP_count + UDP_count # Add the new UDP count to the current count
cur.execute("UPDATE tbldashboardmetrics SET UDP_count = %s WHERE user_id = %s",
(new_UDP_count, user_id))

# Update total_UDP_count with the new total
cur.execute("UPDATE tbldashboardmetrics SET total_UDP_count = total_UDP_count + %s
WHERE user_id = %s", (UDP_count, user_id))

# Commit the changes to the database
mysql.connection.commit()

except Exception as e:
    logger.error(f"Error retrieving Dashboard Results: {e}")
    raise

finally:
    # Close the cursor
    if cur:
        cur.close()

logger.info("Dashboard completed successfully.")
except Exception as e:
    logger.error(f"Error retrieving Dashboard Results: {e}")
    raise

curInsertDashboard = mysql.connection.cursor()

try:
    # Insert calculated metrics along with protocol frequency into MySQL
    curInsertDashboard.execute(
        "INSERT INTO tbldashboardmetrics (user_id, aveflowpktsrate, aveflowbytesrate, alerts, numalerts,
TCP_count, total_TCP_count, UDP_count, total_UDP_count) VALUES('" + str(user_id) + "','" +
str(ave_flowpacket_rate) + "','" + str(ave_flowbytes_rate) + "','" + str(alerts) + "','" + str(new_numalerts) +
','" + str(TCP_count) + "','" + str(new_TCP_count) + "','" + str(UDP_count) + "','" + str(new_UDP_count) +
'"')
    mysql.connection.commit()

    logger.info("Dashboard data inserted successfully.")
except Exception as dashboard_error:
    mysql.connection.rollback()
    raise dashboard_error

```

```

finally:
    curInsertDashboard.close()

curInsertRankings = mysql.connection.cursor()

try:
    # Insert rankings
    curInsertRankings.execute(
        "INSERT INTO tblrankings (ranking, user_id) VALUES(" + str(json_ip_ports) + "", "" + str(user_id)
+ ")")

    mysql.connection.commit()

    logger.info("Dashboard data inserted successfully.")
except Exception as dashboard_error:
    mysql.connection.rollback()
    raise dashboard_error
finally:
    curInsertRankings.close()

# After your INSERT statements
mysql.connection.commit()

__init__.py

from flask import Flask, jsonify, render_template
import os
import requests
import json
import logging
from flask_cors import CORS
import model1
from flask_mysqldb import MySQL
from io import BytesIO
from collections import Counter
import tensorflow as tf
import xgboost as xgb
from xgboost import XGBClassifier
import logging
import time # Import the time module

app = Flask(__name__)
CORS(app)

app.config['MYSQL_HOST'] = 'detech.mysql.pythonanywhere-services.com'
app.config['MYSQL_USER'] = 'detech'
app.config['MYSQL_PASSWORD'] = 'dbdetechpassword'
app.config['MYSQL_DB'] = 'detech$dbdetech'

mysql = MySQL(app)

# Logging setup
logging.basicConfig(level=logging.INFO, format='%(asctime)s %(levelname)s: %(message)s')
logger = logging.getLogger(__name__)

```

```

# MongoDB Data API setup
MONGO_DATA_API_URL      =      "https://ap-southeast-1.aws.data.mongodb-api.com/app/data-tfwys/endpoint/data/v1"
MONGO_DATA_API_KEY = os.environ.get('MONGO_DATA_API_KEY') # MongoDB Data API Key
from environment variable
DATA_SOURCE_NAME = os.environ.get('DATA_SOURCE_NAME') # Data source name from
environment variable

# Define global variables to store processed CSV data
csv_data_detect = None
csv_data_classify = None

# Define a global variable to store the CSV data
raw_csv_data = None

@app.route('/')
def index():
    return render_template('index.html')

def checkUnprocessedMongoDBFilesPerUser():
    try:
        with app.app_context():
            cur = mysql.connection.cursor()
            # Execute the SELECT query
            cur.execute("SELECT id, filename, user_id FROM tblmongodbfies WHERE id IN (SELECT MAX(id) FROM tblmongodbfies WHERE processedstatus = 0 GROUP BY user_id)")

            # Fetch the result (assuming you are interested in the result)
            for record in cur:
                id, filename, user_id = record

                result = retrieveData(str(filename), str(user_id))
                if result == "success":
                    # Wait for analysis to complete
                    time.sleep(1) # Wait for 1 seconds before proceeding to the next file

                    # Mark the file as processed
                    curUpdateProcessedStatus = mysql.connection.cursor()
                    curUpdateProcessedStatus.execute("UPDATE tblmongodbfies SET processedstatus = 1
WHERE id = %s", (id,))
                    mysql.connection.commit()
                    curUpdateProcessedStatus.close()
                else:
                    logger.error("Failed to retrieve and process data for file: %s", filename)

            cur.close()
            return 'success'
    except Exception as err:
        logger.exception("Error occurred while processing MongoDB files: %s", err)
        return 'error'

@app.route('/updateProcessedStatus', methods=['GET'])
def updateProcessedStatus():
    state = checkUnprocessedMongoDBFilesPerUser()
    response = {
        'status': str(state)
    }

```

```

        }

    return jsonify(response)

def retrieveData(document_id, user_id):
    try:
        headers = {
            "Content-Type": "application/json",
            "Access-Control-Request-Headers": "*",
            "api-key": MONGO_DATA_API_KEY
        }

        payload = json.dumps({
            "collection": "Raw CSV",
            "database": "De-TECH",
            "dataSource": DATA_SOURCE_NAME,
            "filter": { "_id": { "$oid": document_id } }
        })

        response = requests.post(f"{MONGO_DATA_API_URL}/action/findOne", headers=headers, data=payload)

        if response.status_code == 200:
            data = response.json()
            if 'document' in data and 'csv_data' in data['document']:
                csv_list = data['document']['csv_data']
                csv_list = [json.dumps(item) for item in csv_list]
                csv_string = '\n'.join(csv_list)
                csv_data = csv_string.encode('utf-8')
                preprocess_result = preprocessData(str(document_id), str(user_id), csv_data)
                return preprocess_result
            else:
                return "Document or csv_data field not found in the database."
        else:
            logger.error("Error retrieving document: %s", response.text)
            return f"Error retrieving document: {response.text}"
    except Exception as e:
        logger.exception("Error in retrieveData route: %s", e)
        return f"Error in retrieving CSV data: {e}"

def preprocessData(document_id, user_id, csv_data):
    try:
        csv_prep = model1.prepare_data_for_prediction(csv_data)
        csv_data_detect = model1.normalize_for_detection(csv_prep)
        model1.analyzeCsvFile(str(document_id), str(user_id), csv_prep, csv_data_detect)
        model1.dashboardResults(str(document_id), str(user_id), csv_prep, csv_data_detect)
        return "success"
    except Exception as e:
        logger.exception("Error in preprocessing data: %s", e)
        return "error"

if __name__ == "__main__":
    app.run(debug=True)

runserver.py
"""

```

This script runs the DeTechProgress application using a development server.
"""

```
from os import environ
from apidetech import app

if __name__ == '__main__':
    HOST = environ.get('SERVER_HOST', '0.0.0.0')
    try:
        PORT = int(environ.get('SERVER_PORT', '5555'))
    except ValueError:
        PORT = 5555
    app.run(HOST, PORT)
```

scheduler.py

```
import time
import schedule
from __init__ import checkUnprocessedMongoDBFilesPerUser

if __name__ == "__main__":
    schedule.every(5).seconds.do(checkUnprocessedMongoDBFilesPerUser)

    while True:
        schedule.run_pending()
        time.sleep(60)
```

requirements.txt

absl-py==1.0.0	atomicwrites==1.4.0
aggdraw==1.3.12	attrs==21.4.0
alabaster==0.7.12	autograd==1.4
alembic==1.7.7	autograd-gamma==0.5.0
aniso8601==9.0.1	Automat==20.2.0
anyio==3.6.1	Babel==2.10.1
appdirs==1.4.4	backcall==0.2.0
arabic-reshaper==2.1.3	banal==1.0.6
argcomplete==2.0.0	bcrypt==3.2.2
argon2-cffi==21.3.0	Beaker==1.11.0
argon2-cffi-bindings==21.2.0	beautifulsoup4==4.11.1
arrow==1.2.2	bidict==0.22.1
arviz==0.11.4	biopython==1.79
asgiref==3.5.2	black==22.3.0
asn1crypto==1.5.1	bleach==5.0.1
astor==0.8.1	blinker==1.4
astropy==5.0.4	bokeh==2.4.3
asttokens==2.0.5	boto==2.49.0
astunparse==1.6.3	boto3==1.23.3
async==0.6.2	botocore==1.26.3
async-generator==1.10	bottle==0.12.19
async-timeout==4.0.2	

bottlenose==1.1.8
Brotli==1.0.9
BTrees==4.10.0
cachelib==0.9.0
cachetools==4.2.4
cairoffi==1.3.0
CairoSVG==2.5.2
cattr==1.10.0
certifi==2022.6.15
cffi==1.15.1
ctime==1.5.1.1
Chameleon==3.10.1
chardet==4.0.0
charset-normalizer==2.1.0
cheroot==8.6.0
CherryPy==18.6.1
click==8.0.3
click-plugins==1.1.1
cligj==0.7.2
cloudpickle==2.0.0
colorama==0.4.4
colorclass==2.2.2
commonmark==0.9.1
compressed-rtf==1.0.6
configobj==5.0.6
constantly==15.1.0
coverage==6.3.3
cryptography==37.0.2
cssselect==1.1.0
cssselect2==0.6.0
cycler==0.11.0
Cython==0.29.30
dash==2.4.1
dash-core-components==2.0.0
dash-html-components==2.0.0
dash-renderer==1.9.1
dash-table==5.0.0
dask==2021.12.0
dataclasses==0.6
dataset==1.5.2
debugpy==1.6.2
decorator==5.1.1
decatee==0.14
defusedxml==0.7.1
Deprecated==1.2.13
dill==0.3.4
distlib==0.3.5
distro==1.7.0
Django==4.0.6
django-blog-zinnia==0.20
django-bootstrap-form==3.4
django-classy-tags==3.0.1
django-contrib-comments==2.2.0
django-formtools==2.3
django-js-asset==2.0.0
django-mptt==0.13.4
django-object-tools==2.0.0
django-sekizai==3.0.1
django-smart-selects==1.5.9
django-tagging==0.5.0
django-tastypie==0.14.4
django-treebeard==4.5.1
django-xmlrpc==0.1.8
djangocms-admin-style==3.1.1
dlib==19.24.0
docker==5.0.3
docopt==0.6.2
docutils==0.17.1
docx2txt==0.8
dominate==2.6.0
easygui==0.98.3
EasyProcess==1.1
ebcdic==1.1.1
EbookLib==0.17.1
english==2020.7.0
entrypoints==0.4
et-xmlfile==1.1.0
exceptiongroup==1.0.0rc6
executing==0.8.3
extract-msg==0.30.12
face-recognition==1.3.0
face-recognition-models==0.3.0
falcon==3.1.0
fastapi==0.78.0
fastjsonschema==2.16.1
fastprogress==1.0.0
fasttext==0.9.2
feedfinder2==0.0.4
feedgenerator==2.0.0
feedparser==6.0.8
filebrowser-safe==1.1.1
filelock==3.4.2
Fiona==1.8.21
Flask==2.1.2
Flask-Admin==1.6.0
Flask-Babel==2.0.0
Flask-Bcrypt==1.0.1
Flask-Bootstrap==3.3.7.1
Flask-Caching==2.1.0
Flask-Compress==1.12
Flask-Cors==4.0.0
Flask-HTTPAuth==4.6.0
Flask-Login==0.6.1
Flask-MySQLdb==2.0.0
Flask-RESTful==0.3.9
Flask-SocketIO==4.3.2
Flask-SQLAlchemy==2.5.1
Flask-SSLify==0.1.5
Flask-WTF==1.0.1
flatbuffers==1.12
fonttools==4.28.5
formulaic==0.3.4

fsspec==2021.11.1
future==0.18.2
gast==0.4.0
Genshi==0.7.7
geographiclib==1.52
geopy==2.2.0
gevent==21.12.0
gitdb==4.0.9
gitdb2==4.0.2
GitPython==3.1.27
glpk==0.4.6
gmpplot==1.4.1
gmpy==1.17
google-api-core==2.8.0
google-api-python-client==2.48.0
google-auth==2.6.6
google-auth-httplib2==0.1.0
google-auth-oauthlib==0.4.6
google-pasta==0.2.0
googleapis-common-protos==1.56.1
graphviz==0.20
grappelli-safe==1.1.1
greenlet==1.1.2
grokcore.component==3.2.0
grpcio==1.46.1
h11==0.13.0
h2==4.1.0
h5py==3.6.0
hpack==4.0.0
html5lib==1.1
httplib2==0.20.4
humanize==4.1.0
hupper==1.10.3
hyperframe==6.0.1
hyperlink==21.0.0
idna==3.3
imageio==2.13.5
imageio-ffmpeg==0.4.7
imagesize==1.3.0
IMAPClient==2.2.0
importlib-metadata==4.11.3
importlib-resources==5.7.1
importscan==0.2
incremental==21.3.0
inflection==0.5.1
iniconfig==1.1.1
interchange==2021.0.4
interface-meta==1.3.0
ipykernel==6.15.1
ipyparallel==8.3.0
ipython==8.3.0
ipython-genutils==0.2.0
ipywidgets==7.7.0
isodate==0.6.1
isort==5.10.1
itemadapter==0.6.0
itemloaders==1.0.4
itsdangerous==2.1.2
jaraco.classes==3.2.1
jaraco.collections==3.5.1
jaraco.context==4.1.1
jaraco.functools==3.5.0
jaraco.text==3.7.0
jdcal==1.4.1
jedi==0.18.1
jellyfish==0.9.0
jieba3k==0.35.1
Jinja2==3.1.2
jmespath==1.0.0
joblib==1.3.2
jsonschema==4.7.2
jupyter==1.0.0
jupyter-client==7.3.4
jupyter-console==6.4.4
jupyter-core==4.11.1
jupyterlab-pygments==0.2.2
jupyterlab-widgets==1.1.1
kaleido==0.2.1
keras==2.9.0
Keras-Aplications==1.0.8
Keras-Preprocessing==1.1.2
kiwisolver==1.3.2
lark-parser==0.12.0
libclang==14.0.1
lifelines==0.27.0
llvmlite==0.38.0
locket==0.2.1
lxml==4.7.1
Mako==1.2.0
Markdown==3.3.7
MarkupSafe==2.1.1
martian==1.5
matplotlib==3.5.2
matplotlib-inline==0.1.3
mechanize==0.4.8
memory-profiler==0.60.0
mglearn==0.1.9
mimerender==0.6.0
mistune==0.8.4
mock==4.0.3
monotonic==1.6
more-itertools==8.13.0
morepath==0.19
mots-vides==2015.5.11
mpmath==1.2.1
mssofcrypto-tool==5.0.0
multipart==0.2.4
munch==2.5.0
mypy-extensions==0.4.3
mysql-connector-python==8.0.29
mysqlclient==2.2.0
nbclient==0.6.6

nbconvert==6.5.0
nbformat==5.4.0
nbstripout==0.5.0
ndg-httpsclient==0.5.1
neo4j==4.4.3
neobolt==1.7.17
neotime==1.7.4
nest-asyncio==1.5.5
netCDF4==1.5.8
netifaces==0.11.0
networkx==2.6.3
nltk==3.6.7
notebook==6.4.11
numba==0.55.1
numexpr==2.8.1
numpy==1.21.6
oauth2client==4.1.3
oauthlib==3.2.0
objgraph==3.5.0
olefile==0.46
oletools==0.60.1
opencv-contrib-python-headless==4.5.5.62
openpyxl==3.0.9
opt-einsum==3.3.0
oscrypto==1.3.0
outcome==1.1.0
packaging==21.3
paho-mqtt==1.6.1
panda==0.3.1
pandas==1.3.5
pandocfilters==1.5.0
pansi==2020.7.3
param==1.12.1
paramiko==2.11.0
parsel==1.6.0
parso==0.8.3
partd==1.2.0
Paste==3.5.0
PasteDeploy==2.1.1
pathlib2==2.3.7.post1
pathspec==0.9.0
patsy==0.5.2
pbr==5.9.0
pcodedmp==1.2.6
peewee==3.14.10
pelican==4.7.2
pep8==1.7.1
persistent==4.9.0
pexpect==4.8.0
pickleshare==0.7.5
Pillow==9.0.0
Pint==0.19.2
pixx==1.0.0
plaster==1.0
plaster-pastedeploy==0.7
platformdirs==2.5.2
plotly==5.8.0
pluggy==1.0.0
pocketsphinx==0.1.15
portend==3.1.0
praw==7.6.0
prawcore==2.3.0
prettytable==3.3.0
priority==2.0.0
proglog==0.1.10
prometheus-client==0.14.1
prompt-toolkit==3.0.30
Protego==0.2.1
protobuf==3.20.1
psutil==5.9.1
psycopg2-binary==2.9.3
ptyprocess==0.7.0
pudb==2022.1.1
pure-eval==0.2.2
py==1.11.0
py2neo==2021.2.3
pyasn1==0.4.8
pyasn1-modules==0.2.8
pybind11==2.10.0
pycairo==1.20.1
pycodestyle==2.8.0
pycparser==2.21
pycryptodome==3.14.1
pydantic==1.9.0
PyDispatcher==2.0.5
pydub==0.25.1
pydyf==0.1.2
pyenchant==3.2.2
pyerfa==2.0.0.1
pyflakes==2.4.0
pyflakes3k==0.4.3
pygal==3.0.0
pygeoip==0.3.2
Pygments==2.12.0
PyGObject==3.42.1
pyHanko==0.13.1
pyhanko-certvalidator==0.19.5
pyhdf==0.10.3
PyJWT==2.4.0
pykka==3.0.2
pymarc==4.2.0
pymc3==3.11.4
pymongo==4.1.1
PyNaCl==1.5.0
pyOpenSSL==22.0.0
pyparsing==2.4.7
PyPDF2==1.27.12
PyPDF3==1.0.6
pyphen==0.12.0
pyquery==1.4.3
pyramid==2.0
pyrsistent==0.18.1

pyserial==3.5
pyshp==2.3.0
PySocks==1.7.1
PyStemmer==2.0.1
pytesseract==0.3.9
pytest==7.1.2
python-amazon-simple-product-api==2.2.11
python-bidi==0.4.2
python-dateutil==2.8.2
python-dotenv==1.0.0
python-editor==1.0.4
python-engineio==3.14.2
python-gettext==4.0
python-Levenshtein==0.12.2
python-magic==0.4.25
python-mimeparse==1.6.0
python-poppler==0.3.0
python-pptx==0.6.21
python-slugify==6.1.2
python-socketio==4.6.1
pytz==2021.3
pytz-deprecation-shim==0.1.0.post0
PyVirtualDisplay==3.0
PyWavelets==1.2.0
PyYAML==6.0
pyzmq==23.2.0
qrcode==7.3.1
qtconsole==5.3.1
QtPy==2.1.0
Quandl==3.7.0
queuelib==1.6.2
rdflib==6.1.1
readability-lxml==0.8.1
redis==4.3.1
reg==0.12
regex==2021.11.10
reportlab==3.6.9
repoze.lru==0.7
requests==2.28.1
requests-cache==0.9.4
requests-file==1.5.1
requests-oauthlib==1.3.1
retrying==1.3.3
rich==11.2.0
rsa==4.8
RTFDE==0.0.2
Rtree==1.0.0
ruffus==2.8.4
s3transfer==0.5.2
schedule==1.2.1
scikit-image==0.19.1
scikit-learn==1.3.2
scipy==1.7.3
seaborn==0.11.2
selenium==4.1.5
semver==2.13.0
Send2Trash==1.8.0
service-identity==21.1.0
setproctitle==1.2.3
sgmllib3k==1.0.0
Shapely==1.8.2
simple-websocket==1.0.0
simplegeneric==0.8.1
simplejson==3.17.6
simpy==4.0.1
singledispatch==3.7.0
six==1.16.0
smart-open==6.0.0
smmap==5.0.0
smmap2==3.0.1
sniffio==1.2.0
snowballstemmer==2.2.0
socketpool==0.5.3
sortedcontainers==2.4.0
soupsieve==2.3.2.post1
SPARQLWrapper==2.0.0
SpeechRecognition==3.8.1
Sphinx==4.5.0
sphinxcontrib-applehelp==1.0.2
sphinxcontrib-devhelp==1.0.2
sphinxcontrib-htmlhelp==2.0.0
sphinxcontrib-jsmath==1.0.1
sphinxcontrib-qthelp==1.0.3
sphinxcontrib-serializinghtml==1.1.5
SQLAlchemy==1.4.36
sqlparse==0.4.2
stack-data==0.3.0
starlette==0.19.1
stevedore==4.0.0
stripe==3.0.0
svglib==1.3.0
sympy==1.9
tables==3.7.0
Tempita==0.5.2
tempora==5.0.1
tenacity==8.0.1
tensorboard==2.9.0
tensorboard-data-server==0.6.1
tensorboard-plugin-wit==1.8.1
tensorflow==2.9.0
tensorflow-estimator==2.9.0
tensorflow-io-gcs-filesystem==0.26.0
termcolor==1.1.0
terminado==0.15.0
texcaller==0
text-unidecode==1.3
textblob==0.17.1
textual==0.1.15
Theano==1.0.5
Theano-PyMC==1.1.2
threadpoolctl==3.0.0
tifffile==2021.11.2

tinycss==0.4
tinycss2==1.1.1
tinysegmenter==0.4
tldextract==3.3.0
toml==0.10.2
tomli==2.0.1
toolz==0.11.2
torch==1.11.0+cpu
torchaudio==0.11.0+rocm4.5.2
torchvision==0.12.0+cpu
tornado==6.2
tqdm==4.62.3
traitlets==5.3.0
transaction==3.0.1
translationstring==1.4
trio==0.20.0
trio-websocket==0.9.2
tweepy==4.9.0
twilio==7.9.1
Twisted==22.4.0
twitter==1.19.3
typed-ast==1.5.3
typing-extensions==3.10.0.2
tzdata==2022.1
tzlocal==4.2
uncertainties==3.1.6
Unidecode==1.3.4
update-checker==0.18.0
uritemplate==4.1.1
uritools==4.0.0
url-normalize==1.4.3
urllib3==1.26.9
urwid==2.1.2
urwid-readline==0.13
userpath==1.8.0
uvicorn==0.17.6
venusian==3.0.0
virtualenv==20.15.1
virtualenv-clone==0.5.7
virtualenvwrapper==4.8.4
visitor==0.1.3
w3lib==1.22.0
waitress==2.1.1
Wand==0.6.7
wcwidth==0.2.5
weasyprint==55.0
webencodings==0.5.1
WebOb==1.8.7
websocket-client==1.3.2
WebTest==3.0.0
Werkzeug==2.1.2
wheezy.caching==3.0.1
wheezy.core==3.0.1
wheezy.html==3.0.1
wheezy.http==3.0.1
wheezy.routing==3.0.1
wheezy.security==3.0.1
wheezy.template==3.1.0
wheezy.validation==3.0.1
wheezy.web==3.0.1
Whoosh==2.7.4
widgetsnbextension==3.6.0
wrapt==1.14.1
WSGIProxy2==0.5.1
wsproto==1.1.0
WTForms==3.0.1
xarray==0.20.2
xgboost==1.6.1
xhtml2pdf==0.2.7
xlrd==2.0.1
XlsxWriter==3.0.3
xlwt==1.3.0
z3c.pt==3.3.1
zc.lockfile==2.0
ZConfig==3.6.0
zdaemon==4.3
ZEO==5.3.0
zipp==3.8.0
ZODB==5.7.0
ZODB3==3.11.0
zodbpickle==2.3
zope.annotation==4.7.0
zope.app.appsetup==4.2.0
zope.app.publication==4.5
zope.app.wsgi==4.3.0
zope.authentication==4.5.0
zope.browser==2.4
zope.browserpage==4.4.0
zope.browserresource==4.4
zope.cachedescriptors==4.3.1
zope.catalog==4.4.0
zope.component==5.0.1
zope.configuration==4.4.1
zope.container==4.5.0
zope.contentprovider==4.2.1
zope.contenttype==4.5.0
zope.datetime==4.3.0
zope.deferredimport==4.4
zope.deprecation==4.4.0
zope.dottedname==4.3
zope.error==4.5.0
zope.event==4.5.0
zope.exceptions==4.5
zope.filerepresentation==5.0.0
zope.formlib==5.0.1
zope.hookable==5.1.0
zope.i18n==4.9.0
zope.i18nmessageid==5.0.1
zope.index==5.2.0
zope.interface==5.4.0
zope.intid==4.4.0
zope.keyreference==5.0.0

zope.lifecycleevent==4.4	zope.security==5.3
zope.location==4.2	zope.securitypolicy==4.3.2
zope.login==2.2	zope.session==4.4.0
zope.minmax==2.2.0	zope.site==4.5.0
zope.pagetemplate==4.6.0	zope.size==4.3
zope.password==4.3.1	zope.tal==4.5
zope.principalregistry==4.2.0	zope.tales==5.1
zope.processlifetime==2.3.0	zope.testbrowser==5.6.1
zope.proxy==4.5.0	zope.testing==4.10
zope.ptresource==4.3.0	zope.traversing==4.4.1
zope.publisher==6.1.0	zope.viewlet==4.3
zope.schema==6.2.0	

C. Manual of Operation

I. Introduction and Overview

1. Purpose of the Manual

- This manual serves as a guide for users of De-TECH, detailing its operation and maintenance.

2. Scope and Applicability

- De-TECH is designed for use in Local Area Networks such as home networks, libraries, or small offices.
- It requires a stable connection to prevent errors from occurring.

II. Security and Safety Protocols

- a. Place De-TECH in a well-ventilated area. Avoid placing the device in tight spaces where heat can accumulate.
- b. Ensure the environment is free from excessive humidity, which can cause condensation and short circuits.
- c. **Emergency Shutdown Procedure:** Push the yellow button on the device. Ensure the blinking has stopped. You can now safely remove the power cord to turn it off.
- d. **Maintenance:** Regularly inspect the Raspberry Pi and its cooling systems for dust accumulation, loose connections, or signs of wear.

III. Standard Operating Procedures (SOPs)

Here are the steps to use De-TECH:

1. Hardware Installation (seek expert assistance for this step):

- a. Attach the power cord to the De-TECH hardware. Place it near a router or switch.
- b. Use a straight-through LAN cable to connect the De-TECH hardware to the router or switch. Ensure the LAN ports are blinking, indicating a proper connection.

c. Access the Raspberry Pi OS of the De-TECH hardware using the RealVNC app or any other remote access viewing app. Enter the address `raspberrypi.local` and the username and password of the device. You can download the app here:

<https://www.realvnc.com/en/connect/download/viewer/>

d. Inside the OS, use the terminal to find connected devices on the network using the `nmap` command. Enter all the IP addresses you want the device to monitor in the program on the Raspberry Pi.

e. Once accomplished, save the program and exit.

2. User Account Registration

- a. Go to `detech.pythonanywhere.com` to access the De-TECH web app.
- b. Create an account by registering on the web app. Enter your username, password, and email.
- c. Then, log in to the web app to access the start/stop button for the capturing device and the dashboard.

3. Starting the Device

- a. Go to the Detect Tab and click 'START CAPTURE' to start the device. Ensure the light on the device is blinking. If not, seek expert assistance.
- b. Go to the Analysis Tab to see the semi-real-time results.
- c. You can also view past results in the History Tab.

4. Stopping the Device

- a. To stop the device, go to the Detect Tab and click 'STOP CAPTURE'. Ensure the light has stopped blinking.
- b. If the stop button on the web app doesn't work, use human intervention by pressing the yellow button on the hardware itself. Ensure the light has stopped blinking.

IV. Equipment and Tools

- De-TECH Hardware (Raspberry Pi 4 Model B)

- Power Cord (USB Type-C)
- LAN Cable (Straight-through)
- Monitoring Device (Laptop, PC, or Smartphone)

V. Contact Support

You can reach us through the following contact details:

1. Caseria, Ranah Mae M. 09184983051
2. Delos Reyes, Khylla Krizel S. 09663723346
3. Felipe, Aliah Fhae A. 09183413998
4. Isaias, Judiel A. 09085182171
5. Pengson, Aila Marie S. 09480129276
6. Ponciano, Mary Grace G. 09602023435

D. Project Duplication Manual

I. Introduction

1. Purpose of the Manual

- This manual provides step-by-step instructions for duplicating the De-TECH project, ensuring consistent replication of the setup and configuration.

2. Scope and Applicability

- This manual is intended for technical personnel who need to duplicate the De-TECH project for deployment in different environments.

II. Pre-requisites

1. Required Hardware and Software

- Raspberry Pi 4 Model B
- MicroSD card (minimum 16GB) with Raspberry Pi OS installed
- Power supply (USB Type-C)
- LAN cable (straight-through)
- Access to a router or switch
- Monitoring device (Laptop, PC, or Smartphone)
- RealVNC or any other remote access viewing app
- nmap software
- Web browser

2. Access Credentials

- Username and password for Raspberry Pi OS
- Username and password for the De-TECH web app

III. Step-by-Step Duplication Process

1. Setup the Packet Capturing Tool

- a. Flash the Raspberry Pi OS onto the MicroSD Card
 - Download the latest Raspberry Pi OS image from the official website.
 - Insert the MicroSD card into the Raspberry Pi.
- b. Initial Setup
 - Connect the Raspberry Pi to the monitor, keyboard, and mouse.

- Power up the Raspberry Pi and follow the on-screen instructions to complete the initial setup.
 - Configure the network settings to connect to the local network.
- c. Install Required Software (type the following in the RPi Terminal)
1. Update and Upgrade the System


```
sudo apt update
```

```
sudo apt upgrade
```
 2. Install nmap


```
sudo apt install nmap
```
 3. Install RealVNC Server


```
sudo apt install realvnc-vnc-server
```

```
sudo systemctl enable vncserver-x11-serviced.service
```

```
sudo systemctl start vncserver-x11-serviced.service
```
 4. Start the Device
 - Copy the program for Raspberry Pi inside the Manuscript.
 - Follow the Manual of Operation on how to prepare the raspberry Pi and how to start the device.
2. Set Up the Web App
- a. Deploy the Web App
 - i. Use pythonanywhere for web app hosting.
 - ii. Avail the package that has two web apps: (1) For Visualization
(2) For Prediction
 - iii. Use the codes in the manuscript for frontend and backend of the Web Application
 - iv. Register new user accounts on the De-TECH web app for access.
3. Training the Model
- a. Use the codes or create a program for training a machine learning model.
 - b. Replace the names of the directory of the ML models inside the model1.py script with your newly trained model.

- c. Make sure that the process for training and process in the web app is the same.

4. Verify Functionality

- a. Follow the Manual of Operation to test the functionality of the device.

IV. Contact Support

- Caseria, Ranah Mae M. 09184983051
- Delos Reyes, Khylla Krizel S. 09663723346
- Felipe, Aliah Fhae A. 09183413998
- Isaias, Judiel A. 09085182171
- Pengson, Aila Marie S. 09480129276
- Ponciano, Mary Grace G. 09602023435

E. Survey Form

De-Tech Web Application Questionnaire (Source: ISO / IEC 9126)

Thank you for participating in this survey on web application usage. Your feedback is essential for us to gain a better understanding of your experiences and preferences when using web applications.

Evaluator's Name: _____

Instructions: For each statement or question, please select and put a (✓) in the option that best represents your opinion. The Likert scale ranges from 1 to 5, with 1 indicating strong disagreement and 5 indicating strong agreement.

Characteristics	Sub-Characteristics	Questions	Strongly Agree (5)	Agree (4)	Neutral (3)	Disagree (2)	Strongly Disagree (1)
<i>Functionality</i>	Suitability	Is the software capable of executing the necessary tasks?					
	Accurateness	Does the outcome align with your expectations?					
	Interoperability	Is the system capable of interfacing with another system?					
	Security	Is the software effective in blocking unauthorized access?					
<i>Reliability</i>	Maturity	Is the maturity level satisfactory?					
	Fault Tolerance	Does the software possess the capacity to manage errors?					
	Recoverability	Can the software resume working and restore lost data after failure?					
<i>Usability</i>	Understandability	Is it easy for the user to understand and use the system?					
	Learnability	Can the user learn to use the system easily?					
	Operability	Can the user use the system without much effort?					
	Attractiveness	Does the interface have an appealing appearance?					
<i>Efficiency</i>	Time Behaviour	Is the system's response time fast?					
	Resource Utilisation	Is the system efficient in its utilization of resources?					
<i>Maintainability</i>	Analysability	Can faults be easily diagnosed?					
	Changeability	Can the software be easily modified?					
	Stability	Can the software continue functioning if changes are made?					
	Testability	Can the software be tested easily?					
<i>Portability</i>	Adaptability	Is it possible to transfer the software to different environments?					
	Installability	Can the software be installed easily?					
	Conformance	Is the software in alignment with portability standards?					
	Replaceability	Can the software easily replace other software?					
<i>All Characteristics</i>	Compliance	Does the software comply with laws or regulations?					

Additional Comments / Suggestions:

Your participation is greatly appreciated!

F. Tabulation

Table 5.1 Results of Day 1 Deployment Testing of De-TECH
on ValACE using Model 20

Time	Document ID	Results	Classification	Normal	DoS	Bruteforce	Botnet	Infiltration
10:41:07	1e75f	Malicious	Botnet	17.39	0	0	80.98	1.63
10:44:32	1e768	Malicious	Botnet	5.86	0	0	93.62	0.34
10:47:59	1e777	Malicious	Botnet	8.33	0	0	91.13	0.53
10:51:13	1e77f	Malicious	Botnet	18	0	0	81.28	0.71
10:54:27	1e789	Malicious	Botnet	17.59	0	0.16	81.6	0.65
10:57:41	1e790	Malicious	Botnet	5.85	0	0.18	93.24	0.73
11:01:13	1e7a0	Malicious	Botnet	5.17	0	0.18	94.46	0.18
11:04:33	1e7aa	Malicious	Botnet	15.34	0	0.18	82.89	1.59
11:07:58	1e7b2	Malicious	Botnet	6.29	0	0	85.71	8
11:10:58	1e7bf	Malicious	Botnet	13.68	0	0.16	85.02	1.14
11:14:18	1e7cb	Malicious	Botnet	16.85	0	0	82.52	0.63
11:17:45	1e7d3	Malicious	Botnet	12.86	0	0	85.8	1.34
11:20:58	1e7e0	Malicious	Botnet	9.41	0	0	90.27	0.32
11:24:24	1e7ec	Malicious	Botnet	17.25	0	0.18	80.18	2.39
11:29:35	1e7fd	Malicious	Botnet	14.63	0	0	84.07	1.3
11:32:58	1e809	Malicious	Botnet	17.97	0	0.18	81.67	0.18
11:36:13	1e813	Malicious	Botnet	15.28	0	0.39	83.75	0.58
11:39:20	1e81e	Malicious	Botnet	20.8	0	0	76.43	2.77
11:42:34	1e82a	Malicious	Botnet	13.44	0	0	85.41	1.15
11:45:44	1e831	Malicious	Botnet	13.14	0	0.19	85.52	1.14
11:48:57	1e83d	Normal	Normal	89.56	3.44	0	6.68	0.31
11:52:28	1e848	Malicious	Botnet	24.8	0	0.16	74.72	0.32
11:55:36	1e852	Malicious	Botnet	11.22	0	0	88.46	0.33
11:59:07	1e85e	Malicious	Botnet	21.37	0.13	0	77.82	0.67
12:02:23	1e869	Malicious	Botnet	19.19	0	0	79.97	0.85
12:05:34	1e871	Malicious	Botnet	15.11	0.17	0.17	84.21	0.34
12:08:47	1e87e	Malicious	Botnet	6.75	0	1.21	92.04	0
12:12:10	1e88a	Malicious	Botnet	16.34	0	0.18	82.95	0.53
12:15:15	1e893	Malicious	Botnet	15.82	0	0.88	82.95	0.35
12:18:30	1e89f	Malicious	Botnet	15.83	0	0	83.63	0.54
12:21:42	1e8ab	Malicious	Botnet	21.53	0	0	77.86	0.61
12:25:06	1e8b4	Malicious	Botnet	18.66	0	0.18	80.46	0.7
12:28:54	1e8c0	Malicious	Botnet	13.73	0.88	0.18	84.86	0.35
12:32:45	1e8cf	Malicious	Botnet	15.38	0.17	0.17	84.09	0.17
12:46:56	1e8f9	Malicious	Botnet	16.95	0	0	81.34	1.71
12:50:41	1e906	Malicious	Botnet	23.52	0	1.13	74.65	0.7
12:54:02	1e912	Malicious	Botnet	17.29	0	1.2	80.82	0.68

14:30:21	1ea34	Malicious	Botnet	14.05	0	0.36	84.85	0.73
14:34:51	1ea41	Malicious	Botnet	13.38	0.19	0.37	84.76	1.3
15:48:06	1eb1c	Malicious	Botnet	14.26	0	0.35	83.3	2.09
15:51:28	1eb2c	Malicious	Botnet	18.6	0	0.82	79.28	1.31
16:07:04	1eb5c	Malicious	Botnet	13.59	0	1.13	84.3	0.97
16:11:50	1eb6e	Malicious	Botnet	14.13	0	0.91	84.06	0.91
16:15:06	1eb77	Malicious	Botnet	6.39	0	0.89	92.18	0.53

Table 5.2 Results of Day 2 Deployment Testing of De-TECH
on ValACE using Model 20

Time	Document ID	Results	Classification	Normal	DoS	Bruteforce	Botnet	Infiltration
9:45:47	208a9	Malicious	Botnet	3.72	0	0	95.58	0.71
9:49:02	208b4	Malicious	Botnet	13.45	0	0.17	85.71	0.67
9:53:50	208c3	Normal	Normal	47	3.69	0.92	45.16	3.23
9:56:50	208cb	Normal	Normal	79.32	1.69	0	13.5	5.49
10:00:00	208d9	Malicious	Botnet	35.2	0	0	62.4	2.4
10:03:07	2.08E+05	Malicious	Botnet	38.12	0	0.62	57.5	3.75
10:06:21	208ef	Normal	Normal	53.94	1.21	0	41.21	3.64
10:09:30	208f8	Malicious	Botnet	13.07	10.46	1.96	73.86	0.65
10:12:37	2.09E+04	Malicious	Botnet	39.26	2.22	2.22	54.81	1.48
10:15:50	2090e	Malicious	Botnet	44.38	1.18	1.78	52.07	0.59
10:18:58	2.09E+04	Malicious	Botnet	25.33	0.67	0.67	73.33	0
10:22:02	2.09E+04	Malicious	Botnet	32.2	0	0	65.25	2.54
10:25:10	2092b	Malicious	Botnet	34.92	2.12	0	59.26	3.7
10:28:26	2.09E+04	Malicious	Botnet	35.33	1.33	0.67	59.33	3.33
10:31:33	2.09E+04	Normal	Normal	89.97	0	0.69	7.27	2.08
10:34:43	2094d	Normal	Normal	55.84	1.52	1.02	41.12	0.51
10:37:53	20955	Malicious	Botnet	33.99	0.99	0.49	63.05	1.48
10:41:02	20962	Malicious	Botnet	27.27	10.45	0	58.18	4.09
10:44:12	2096c	Malicious	Botnet	37.85	2.26	2.82	55.37	1.69
10:47:22	20974	Malicious	Botnet	32.7	0.63	0	66.67	0
10:50:36	2097f	Malicious	Botnet	40.11	1.69	0.56	55.93	1.69
10:53:45	2098a	Malicious	Botnet	37.65	1.23	0	59.88	1.23
10:56:54	20997	Malicious	Botnet	20.24	1.19	0.6	77.38	0.6
11:00:03	209a1	Malicious	Botnet	37.63	0	0.54	54.3	7.53
11:03:15	209aa	Malicious	Botnet	13.59	10.33	2.72	72.83	0.54
11:06:26	209b8	Malicious	Botnet	33.11	0	3.31	60.93	2.65
11:09:34	209bf	Malicious	Botnet	23.42	3.8	1.27	69.62	1.9
11:12:50	209c9	Malicious	Botnet	34.21	2.63	1.32	60.53	1.32
11:15:53	209d4	Malicious	Botnet	33.66	3.41	0.49	62.44	0
11:19:14	2.09E+02	Malicious	Botnet	40.89	0	1.48	57.14	0.49

11:22:24	2.09E+11	Malicious	Botnet	15.33	0	0	84.67	0
11:25:44	209f5	Malicious	Botnet	36.84	0.53	1.05	60.53	1.05
11:29:01	20a01	Malicious	Botnet	13.3	11.7	0	73.94	1.06
11:41:59	20a28	Malicious	Botnet	14.8	9.42	1.79	72.2	1.79
11:45:17	20a33	Malicious	Botnet	38.27	2.04	2.04	55.61	2.04
11:48:37	20a3e	Malicious	Botnet	31.56	11.03	3.8	52.47	1.14
11:52:16	20a4b	Malicious	Botnet	33.33	9.6	2.53	50.51	4.04
11:55:23	20a57	Malicious	Botnet	38.01	2.34	0	56.14	3.51
12:14:00	20a8e	Malicious	Botnet	26.26	3.03	2.02	68.18	0.51
12:17:14	20a9a	Malicious	Botnet	41.54	1.54	0	53.85	3.08
12:20:24	20aa4	Malicious	Botnet	39.13	1.86	1.86	55.28	1.86
12:23:35	20aac	Malicious	Botnet	39.78	12.71	1.1	44.75	1.66
12:26:53	20abb	Malicious	Botnet	22.01	1.89	0	74.84	1.26
12:30:18	20ac5	Malicious	Botnet	39.23	1.44	0.48	56.94	1.91
12:33:44	20ace	Malicious	Botnet	35.42	1.04	1.04	61.98	0.52
12:37:10	20adc	Malicious	Botnet	40.09	1.38	0.92	54.84	2.76
12:40:28	20ae6	Malicious	Botnet	26.19	1.43	1.9	69.05	1.43
12:43:37	20af1	Malicious	Botnet	33.85	1.54	0	63.08	1.54
12:57:50	20b1b	Malicious	Botnet	33.33	10.53	1.75	52.05	2.34
13:01:31	20b29	Malicious	Botnet	37.87	0.59	1.78	59.76	0
13:04:45	20b34	Malicious	Botnet	36.87	3.03	1.52	56.06	2.53
13:07:59	20b3f	Malicious	Botnet	40.39	9.02	1.57	48.24	0.78
13:11:24	20b4a	Malicious	Botnet	34.25	2.74	1.37	60.96	0.68
13:30:00	20b85	Malicious	Botnet	35.75	4.15	3.63	55.44	1.04
13:33:09	20b8e	Malicious	Botnet	36.42	1.32	0.66	60.26	1.32
13:36:18	20b98	Malicious	Botnet	40.11	1.69	3.39	53.11	1.69

Table 5.3 Results of Day 2Deployment Testing of De-TECH
on ValACE using Model 39

Time	Document ID	Results	Classification	Normal	DoS	Bruteforce	Botnet	Infiltration
14:18:47	20c1b	Normal	Normal	63.35	0	0	0	36.65
14:57:26	20c91	Normal	Normal	67.66	0	0	0	32.34
15:00:49	20c9d	Normal	Normal	67.11	0	0	0	32.89
15:18:39	20cd8	Malicious	Infiltration	12.94	0	0	0	87.06
15:22:09	20ce0	Normal	Normal	65.73	0	0	0	34.27
15:25:24	20ceb	Malicious	Infiltration	25.85	0	0	12.71	61.44
15:28:39	20cf5	Malicious	Infiltration	20.66	0	0	13.62	65.73
15:43:01	20d25	Malicious	Infiltration	11.41	0	0	7.38	81.21
15:47:36	20d30	Malicious	Infiltration	18.3	0	0	18.3	77.12
15:50:58	20d3f	Normal	Normal	70.04	0	0	0	29.96
15:54:15	20d49	Malicious	Infiltration	28.52	0	0	22.27	49.22

15:57:34	20d55	Malicious	Infiltration	14.72	0	0	27.17	58.11
16:00:45	20d5d	Malicious	Infiltration	13.41	0	0	42.15	44.44
16:03:58	20d6a	Malicious	Infiltration	49.35	0	0	0	50.65
16:07:11	20d74	Malicious	Infiltration	22.01	0	0	4.4	73.58
16:10:19	20d7e	Malicious	Infiltration	29.29	0	0	5.56	65.15
16:13:38	20d88	Malicious	Infiltration	19.85	0	0	6.11	74.05
16:22:01	20da5	Malicious	Infiltration	27.1	0	0	14.95	57.94
16:25:28	20db0	Normal	Normal	65.49	0	0	0	34.51
16:29:07	20dbd	Malicious	Infiltration	26.82	0	0	2.79	70.39
16:32:19	20dc5	Normal	Normal	60.17	0	0	0	39.83
16:40:29	20de0	Malicious	Infiltration	31.25	0	0	7.21	61.54
16:43:50	20Dec	Malicious	Infiltration	12.5	0	0	2.68	84.82
16:47:04	20df4	Normal	Normal	55.13	0	0	0	44.87
16:50:12	20dff	Normal	Normal	64	0	0	0	36
16:53:20	20e0a	Malicious	Infiltration	17.22	0	0	3.31	79.47
16:56:28	20 e13	Normal	Normal	59.3	0	0	0	40.7
16:59:39	20 e20	Malicious	Infiltration	16.41	0	0	6.25	77.34
17:02:51	20e2b	Malicious	Infiltration	26.71	0	0	9.32	63.98
17:05:56	20 e35	Malicious	Infiltration	20	0	0	9.63	70.37
17:09:03	20e3e	Malicious	Infiltration	31.76	0	0	2.94	65.29
17:12:10	20 e49	Malicious	Infiltration	24.81	0	0	3.76	71.43
17:15:20	20 e52	Malicious	Infiltration	19.09	0	0	1.82	79.09
17:18:28	20e5e	Malicious	Infiltration	19.44	0	0	3.7	76.85
17:21:33	20 e67	Malicious	Infiltration	16.09	0	0	2.3	81.61
17:24:52	20 e71	Malicious	Infiltration	8.54	0	0	4.88	86.59
17:27:50	20e7d	Malicious	Infiltration	36	0	0	2.4	61.6
17:30:51	20 e88	Malicious	Infiltration	11.7	0	0	2.13	86.17
17:34:05	20 e91	Malicious	Infiltration	15.79	0	0	4.21	80
17:37:05	20e9c	Malicious	Infiltration	25.25	0	0	4.04	70.71
17:40:11	20ea6	Malicious	Infiltration	20.93	0	0	2.33	76.74
17:43:18	20eb0	Malicious	Infiltration	14.29	0	0	4.76	80.95
17:46:34	20eba	Malicious	Infiltration	33.87	0	0	25	41.13
17:49:39	20ec6	Malicious	Infiltration	19.48	0	0	3.9	76.62
17:52:39	20ed1	Malicious	Infiltration	15.94	0	0	1.45	82.61
17:55:56	20ed8	Malicious	Infiltration	24.66	0	0	1.37	73.97
17:58:58	20ee6	Malicious	Infiltration	33.04	0	0	3.57	63.39
18:02:21	20eea	Malicious	Infiltration	22.81	0	0	0	77.19
18:05:20	20ef9	Malicious	Infiltration	16.07	0	0	1.79	82.14
18:08:10	20f06	Malicious	Infiltration	4.17	0	0	0	95.83
18:11:15	20f0d	Malicious	Infiltration	10	0	0	0	90
18:14:17	20f17	Malicious	Infiltration	25.76	0	0	6.06	68.18
18:17:41	20f1f	Malicious	Infiltration	36.84	0	0	3.95	59.21
18:20:29	20f2e	Malicious	Infiltration	17.19	0	0	7.81	75

18:23:37	20f38	Malicious	Infiltration	4.76	0	0	2.38	92.86
18:26:57	20f3f	Malicious	Infiltration	22.22	0	0	0	77.78
18:29:51	20f4a	Malicious	Infiltration	37.36	0	0	5.49	57.14
18:32:57	20f56	Malicious	Infiltration	20	0	0	4.29	75.71
18:36:17	20f60	Malicious	Infiltration	33.87	0	0	11.29	54.84
18:39:13	20f6d	Malicious	Infiltration	5.97	0	0	1.49	92.54
18:42:17	20f74	Malicious	Infiltration	32.89	0	0	2.63	64.47
18:45:18	20f7e	Malicious	Infiltration	5.17	0	0	3.45	91.38
18:48:30	20f89	Malicious	Infiltration	12.9	0	0	3.23	83.87
18:51:35	20f95	Malicious	Infiltration	25	0	0	3.26	71.74
18:54:45	20f9c	Malicious	Infiltration	8.96	0	0	2.99	88.06
18:57:46	20fa4	Malicious	Infiltration	17.39	0	0	0	82.61
19:00:55	20fb3	Malicious	Infiltration	7.94	0	0	1.59	90.48
19:03:58	20fbe	Malicious	Infiltration	9.26	0	0	1.85	88.89
19:07:15	20fc4	Malicious	Infiltration	5.36	0	0	0	94.64
19:10:37	20fd1	Malicious	Infiltration	6.45	0	0	3.23	90.32
19:13:29	20fda	Malicious	Infiltration	15.38	0	0	6.41	78.21
19:16:28	20fe4	Malicious	Infiltration	37.89	0	0	6.32	55.79
19:19:31	20fef	Malicious	Infiltration	26.39	0	0	6.94	66.67
19:22:44	20ff8	Malicious	Infiltration	14.29	0	0	0	85.71
19:26:00	21005	Malicious	Infiltration	16.18	0	0	2.94	80.88
19:29:01	21010	Malicious	Infiltration	4.44	0	0	4.44	91.11
19:32:46	21019	Malicious	Infiltration	7.27	0	0	0	92.73
19:36:03	21022	Malicious	Infiltration	30.65	0	0	1.61	67.74
19:38:46	2102e	Malicious	Infiltration	4.65	0	0	0	95.35
19:41:31	21037	Malicious	Infiltration	2.38	0	0	0	97.62
19:44:40	21043	Malicious	Infiltration	34.85	0	0	1.52	63.64
19:47:26	2104f	Malicious	Infiltration	7.89	0	0	0	92.11
19:50:42	21056	Malicious	Infiltration	2.08	0	0	0	97.92
19:54:04	2105f	Malicious	Infiltration	2.78	0	0	0	97.22
19:56:37	2106b	Malicious	Infiltration	25	0	0	0	75
19:59:43	21077	Malicious	Infiltration	8.33	0	0	0	91.67
20:02:59	21081	Malicious	Infiltration	5.71	0	0	0	94.29
20:06:15	2108c	Malicious	Infiltration	37.5	0	0	0	62.5
20:09:12	21096	Malicious	Infiltration	36.36	0	0	1.52	62.12
20:12:20	2109e	Malicious	Infiltration	19.12	0	0	4.41	76.47
20:15:22	210a9	Malicious	Infiltration	41.46	0	0	6.1	52.44
20:18:21	210b4	Malicious	Infiltration	25	0	0	2.94	72.06
20:21:31	210bf	Malicious	Infiltration	11.11	0	0	0	88.89
20:25:06	210c7	Malicious	Infiltration	7.32	0	0	0	92.68
20:28:21	210cf	Malicious	Infiltration	26.79	0	0	1.79	71.43
20:30:41	210dc	Malicious	Infiltration	26.32	0	0	3.51	70.18
20:33:56	210 e8	Malicious	Infiltration	24.24	0	0	1.52	74.24

20:37:03	210f0	Malicious	Infiltration	2.86	0	0	0	97.14
20:40:08	210f9	Malicious	Infiltration	28.3	0	0	1.89	69.81
20:43:07	21106	Malicious	Infiltration	13.33	0	0	2.22	84.44
20:46:16	21110	Malicious	Infiltration	5.41	0	0	0	94.59
20:49:21	2111d	Malicious	Infiltration	2.78	0	0	0	97.22
20:52:30	21124	Malicious	Infiltration	7.14	0	0	0	92.86
20:55:46	21139	Malicious	Infiltration	23.68	0	0	2.63	73.68
20:58:34	21145	Normal	Normal	49.3	0	0	2.82	47.89
21:01:49	2114f	Malicious	Infiltration	25	0	0	8.93	66.07
21:04:51	2115a	Malicious	Infiltration	0	0	0	0	100
21:08:11	21161	Malicious	Infiltration	3.85	0	0	0	96.15
21:11:06	2116d	Malicious	Infiltration	3.57	0	0	0	96.43
21:14:24	21175	Malicious	Infiltration	25	0	0	0	75
21:17:11	21181	Malicious	Infiltration	6.67	0	0	0	93.33
21:20:42	2118b	Malicious	Infiltration	35.71	0	0	0	64.29
21:23:24	21197	Malicious	Infiltration	3.03	0	0	6.06	90.91
21:27:13	211a0	Malicious	Infiltration	12.2	0	0	0	87.8
21:30:11	211ac	Malicious	Infiltration	0	0	0	0	100
21:32:39	211b6	Malicious	Infiltration	0	0	0	0	100
21:36:01	211bf	Malicious	Infiltration	7.14	0	0	0	92.86
21:39:01	211c8	Malicious	Infiltration	0	0	0	0	100
21:42:07	211d1	Malicious	Infiltration	38	0	0	0	62
21:45:31	211db	Malicious	Infiltration	3.45	0	0	0	96.55
21:48:41	211 e7	Malicious	Infiltration	6.45	0	0	0	93.55
21:51:41	211ef	Malicious	Infiltration	3.33	0	0	0	96.67
21:54:55	211f7	Malicious	Infiltration	0	0	0	0	100
21:58:01	21206	Malicious	Infiltration	3.45	0	0	0	96.55
22:01:01	21210	Malicious	Infiltration	3.57	0	0	0	96.43
22:04:07	21217	Normal	Normal	52.78	0	0	0	47.22
22:07:06	21224	Malicious	Infiltration	0	0	0	0	100
22:10:11	2122e	Malicious	Infiltration	0	0	0	0	100
22:13:31	21237	Malicious	Infiltration	6.06	0	0	0	93.94
22:16:31	22d23	Malicious	Infiltration	0	0	0	0	100

Table 5.4 Results of Day 3 Deployment Testing of De-TECH
on ValACE using Model 39

Time	Document ID	Results	Classification	Normal	DoS	Bruteforce	Botnet	Infiltration
12:55:20	22df4	Normal	Normal	65.6	0	0	0	34.4
14:01:58	22 e53	Malicious	Infiltration	25	0	0	10.71	64.29
14:32:49	22e5b	Malicious	Infiltration	22.73	0	0	4.55	72.73
14:36:16	22 e93	Malicious	Infiltration	16.34	0	0	5.88	77.78

14:53:32	22ea1	Malicious	Infiltration	15.28	0	0	4.86	79.86
14:57:18	22eab	Malicious	Infiltration	21.97	0	0	18.39	59.64
15:00:42	22f49	Malicious	Infiltration	26.19	0	0	4.76	69.05
15:51:39	22f7b	Normal	Normal	74.11	0	0	0	25.89
16:06:15	22f82	Malicious	Infiltration	26.5	0	0	2.14	71.37
16:09:32	22f83	Normal	Normal	80	0	0	0	20
16:09:32	22f8c	Normal	Normal	80	0	0	0	20
16:12:40	22f99	Normal	Normal	76.74	0	0	0	23.26
16:15:51	22fa4	Malicious	Infiltration	24.09	0	0	6.2	69.71
16:19:06	22fad	Malicious	Infiltration	23.11	0	0	4.2	72.69
16:22:15	22fb8	Normal	Normal	80.25	0	0	0	19.75
16:25:22	22fc1	Normal	Normal	68.5	0	0	0	31.5
16:28:27	22fcb	Malicious	Infiltration	23.18	0	0	4.64	72.19
16:31:46	22fd6	Malicious	Infiltration	28.57	0	0	1.79	69.64
16:34:59	22fe2	Normal	Normal	75.49	0	0	0	24.51
16:38:00	22fed	Malicious	Infiltration	19.9	0	0	6.12	73.98
16:41:14	22ff6	Normal	Normal	72.15	0	0	0	27.85
16:44:24	23002	Normal	Normal	76.34	0	0	0	23.66
16:47:31	2300b	Malicious	Infiltration	19.15	0	0	3.72	77.13
16:50:42	23014	Normal	Normal	75.86	0	0	0	24.14
16:53:51	23022	Malicious	Infiltration	10.6	0	0	3.31	86.09
16:56:57	2302d	Malicious	Infiltration	11.93	0	0	2.27	85.8
17:00:11	23036	Malicious	Infiltration	18.8	0	0	4.27	76.92
17:03:30	23043	Malicious	Infiltration	11.93	0	0	3.67	84.4
17:06:53	2304d	Malicious	Infiltration	11.58	0	0	0	88.42
17:09:56	23053	Malicious	Infiltration	16.04	0	0	4.72	79.25
17:12:57	23060	Malicious	Infiltration	10.68	0	0	2.91	86.41
17:16:05	2306b	Malicious	Infiltration	7.14	0	0	1.19	91.67
17:19:11	23074	Malicious	Infiltration	7.76	0	0	2.59	89.66
17:22:17	23081	Malicious	Infiltration	11.81	0	0	1.57	86.61
17:25:27	23089	Malicious	Infiltration	17.19	0	0	1.56	81.25
17:28:30	23093	Malicious	Infiltration	18.25	0	0	2.38	79.37
17:31:38	2309e	Malicious	Infiltration	11.11	0	0	2.56	86.32
17:34:45	230aa	Normal	Normal	70.45	0	0	0	29.55
17:37:55	230b2	Malicious	Infiltration	20.34	0	0	5.93	73.73
17:41:02	230bb	Malicious	Infiltration	17.53	0	0	1.03	81.44
17:44:10	230c8	Malicious	Infiltration	19.72	0	0	5.63	74.65
17:47:18	230d2	Malicious	Infiltration	7.58	0	0	25.76	66.67
17:50:24	230db	Malicious	Infiltration	7.23	0	0	4.82	87.95
17:53:39	230 e5	Malicious	Infiltration	18.27	0	0	17.31	64.42
17:56:39	230f0	Malicious	Infiltration	40	0	0	4.14	55.86
17:59:59	230fd	Malicious	Infiltration	5.63	0	0	0	94.37
18:02:52	23103	Malicious	Infiltration	8.57	0	0	1.43	90

18:06:01	2310f	Malicious	Infiltration	8.86	0	0	8.86	82.28
18:09:10	2311b	Malicious	Infiltration	7.14	0	0	0	92.86
18:12:19	23125	Malicious	Infiltration	11.39	0	0	0	88.61
18:15:26	23131	Malicious	Infiltration	12.07	0	0	0	87.93
18:18:24	23139	Malicious	Infiltration	10.67	0	0	0	89.33
18:21:44	23143	Malicious	Infiltration	10.77	0	0	0	89.23
18:24:38	2314b	Malicious	Infiltration	6.85	0	0	0	93.15
18:27:46	2315a	Malicious	Infiltration	10.45	0	0	0	89.55
18:30:48	231 61	Malicious	Infiltration	7.94	0	0	0	92.06
18:34:08	2316b	Malicious	Infiltration	11.11	0	0	0	88.89
18:37:04	23177	Malicious	Infiltration	17.74	0	0	0	82.26
18:40:26	2317f	Malicious	Infiltration	7.58	0	0	0	92.42
18:43:28	2318c	Malicious	Infiltration	20.73	0	0	2.44	76.83
18:46:20	23194	Malicious	Infiltration	25.81	0	0	3.23	70.97
18:49:37	231a0	Malicious	Infiltration	15.94	0	0	4.35	79.71
18:52:43	231a9	Malicious	Infiltration	18.99	0	0	1.27	79.75
18:55:50	231b4	Malicious	Infiltration	16.13	0	0	0	83.87
18:59:05	231be	Malicious	Infiltration	9.38	0	0	1.56	89.06
19:02:06	231c9	Malicious	Infiltration	6.38	0	0	0	93.62
19:05:02	231d5	Malicious	Infiltration	7.14	0	0	1.79	91.07
19:08:13	231df	Malicious	Infiltration	11.76	0	0	0	88.24
19:11:15	231 e7	Malicious	Infiltration	10.17	0	0	0	89.83
19:14:20	231f3	Malicious	Infiltration	5.97	0	0	1.49	92.54
19:17:50	231ff	Malicious	Infiltration	10	0	0	2	88
19:20:39	23207	Malicious	Infiltration	25	0	0	5	70
19:23:54	23210	Malicious	Infiltration	10.34	0	0	1.72	87.93
19:26:57	2321d	Malicious	Infiltration	3.92	0	0	0	96.08
19:30:06	23228	Malicious	Infiltration	14.55	0	0	0	85.45
19:33:04	23233	Malicious	Infiltration	16.67	0	0	1.39	81.94
19:36:09	2323a	Malicious	Infiltration	35.59	0	0	3.39	61.02
19:39:11	23246	Malicious	Infiltration	8.62	0	0	3.45	87.93
19:42:28	2324f	Malicious	Infiltration	12	0	0	1.33	86.67
19:45:28	2325b	Malicious	Infiltration	5.88	0	0	0	94.12
19:48:39	23267	Malicious	Infiltration	10.53	0	0	0	89.47
19:51:48	2326e	Malicious	Infiltration	7.69	0	0	3.85	88.46
19:54:48	23276	Malicious	Infiltration	11.54	0	0	1.92	86.54
19:58:12	23285	Normal	Normal	50	0	0	4.69	45.31
20:01:07	2328f	Malicious	Infiltration	11.54	0	0	1.92	86.54
20:04:03	23297	Malicious	Infiltration	32.35	0	0	0	67.65
20:07:09	232a3	Malicious	Infiltration	5.66	0	0	1.89	92.45
20:10:57	232ad	Malicious	Infiltration	23.44	0	0	3.12	73.44
20:13:35	232b7	Malicious	Infiltration	22.22	0	0	0	77.78
20:17:11	232c2	Malicious	Infiltration	21.74	0	0	0	78.26

20:19:55	232ce	Malicious	Infiltration	24.59	0	0	0	75.41
20:23:38	232d9	Malicious	Infiltration	16.98	0	0	0	83.02
20:26:07	232 e3	Malicious	Infiltration	14.29	0	0	2.04	83.67
20:29:13	232eb	Malicious	Infiltration	27.87	0	0	0	72.13
20:32:21	232f6	Malicious	Infiltration	28.77	0	0	0	71.23
20:35:26	23301	Malicious	Infiltration	29.23	0	0	0	70.77
20:38:29	2330c	Malicious	Infiltration	18.33	0	0	0	81.67
20:42:09	23314	Malicious	Infiltration	2.44	0	0	0	97.56
20:44:49	2331c	Malicious	Infiltration	10.2	0	0	2.04	87.76
20:47:48	23329	Malicious	Infiltration	35.44	0	0	1.27	63.29
20:51:05	23335	Malicious	Infiltration	13.73	0	0	0	86.27
20:54:08	2333e	Malicious	Infiltration	18.52	0	0	1.85	79.63
20:57:07	23345	Malicious	Infiltration	3.85	0	0	1.92	94.23
21:00:15	23353	Malicious	Infiltration	38.57	0	0	0	61.43
21:03:36	2335e	Malicious	Infiltration	12.24	0	0	6.12	81.63
21:06:38	23368	Malicious	Infiltration	37.25	0	0	1.96	60.78
21:09:38	23374	Malicious	Infiltration	39.73	0	0	2.74	57.53
21:12:44	2337b	Malicious	Infiltration	10.34	0	0	0	89.66
21:15:48	23386	Malicious	Infiltration	28.33	0	0	1.67	70
21:18:56	23391	Malicious	Infiltration	43.94	0	0	3.03	53.03
21:22:57	2339c	Malicious	Infiltration	9.62	0	0	0	90.38
21:25:08	233a7	Malicious	Infiltration	21.88	0	0	0	78.12
21:28:39	233b2	Malicious	Infiltration	37.78	0	0	5.56	56.67
21:31:34	233ba	Malicious	Infiltration	44.63	0	0	4.96	50.41
21:34:46	233c3	Malicious	Infiltration	30.12	0	0	6.02	63.86
21:38:57	233cf	Malicious	Infiltration	21.88	0	0	1.56	76.56
21:40:58	233db	Malicious	Infiltration	4.17	0	0	0	95.83
21:44:58	233 e4	Malicious	Infiltration	16.67	0	0	0	83.33
21:47:10	233ee	Malicious	Infiltration	6.25	0	0	0	93.75
21:50:18	233f9	Malicious	Infiltration	12.96	0	0	0	87.04
21:53:24	23404	Malicious	Infiltration	14.63	0	0	0	85.37
21:56:38	2340d	Malicious	Infiltration	26.53	0	0	2.04	71.43
21:59:38	23417	Malicious	Infiltration	9.76	0	0	0	90.24
22:02:48	23423	Malicious	Infiltration	12.5	0	0	0	87.5
22:05:49	2342e	Malicious	Infiltration	36.49	0	0	9.46	54.05
22:08:56	23435	Malicious	Infiltration	24.68	0	0	2.6	72.73
22:12:44	23441	Malicious	Infiltration	36.36	0	0	4.55	59.09
22:16:06	2344c	Malicious	Infiltration	21.67	0	0	0	78.33
22:18:16	23456	Malicious	Infiltration	16.36	0	0	0	83.64
22:21:28	23462	Malicious	Infiltration	5	0	0	0	95
22:24:35	2346a	Malicious	Infiltration	2.13	0	0	0	97.87
22:27:38	23474	Malicious	Infiltration	6.82	0	0	0	93.18
22:30:38	2347b	Malicious	Infiltration	10	0	0	2	88

22:33:47	2348b	Malicious	Infiltration	20.37	0	0	0	79.63
22:36:57	23495	Malicious	Infiltration	19.61	0	0	0	80.39
22:40:03	2349e	Malicious	Infiltration	22	0	0	0	78
22:43:01	234a7	Malicious	Infiltration	28.4	0	0	4.94	66.67
22:46:15	234b4	Malicious	Infiltration	26.32	0	0	0	73.68
22:49:17	234bc	Malicious	Infiltration	28.33	0	0	0	71.67
22:52:33	234c9	Malicious	Infiltration	26.67	0	0	1.11	72.22
22:55:33	234d1	Malicious	Infiltration	36.23	0	0	1.45	62.32
22:58:45	234db	Malicious	Infiltration	34.97	0	0	29.37	35.66
23:01:47	234 e7	Malicious	Infiltration	19.51	0	0	3.66	76.83
23:04:54	234f2	Malicious	Infiltration	12.5	0	0	0	87.5
23:07:56	234fc	Malicious	Infiltration	12.73	0	0	0	87.27
23:11:07	23502	Malicious	Infiltration	13.16	0	0	0	86.84
23:14:11	23510	Malicious	Infiltration	10.87	0	0	0	89.13
23:17:18	2351a	Malicious	Infiltration	14.29	0	0	0	85.71
23:20:18	23525	Malicious	Infiltration	2.63	0	0	0	97.37
23:23:25	23531	Malicious	Infiltration	2.38	0	0	0	97.62
23:26:38	23538	Malicious	Infiltration	26.56	0	0	6.25	67.19
23:29:38	23542	Malicious	Infiltration	9.3	0	0	0	90.7
23:32:48	2354e	Malicious	Infiltration	10.26	0	0	0	89.74
23:35:48	23556	Malicious	Infiltration	14.71	0	0	0	85.29
23:38:58	23560	Malicious	Infiltration	2.63	0	0	0	97.37
23:42:18	2356b	Malicious	Infiltration	0	0	0	0	100
23:45:14	23577	Malicious	Infiltration	14.63	0	0	0	85.37
23:48:18	23581	Malicious	Infiltration	5	0	0	0	95
23:51:27	2358b	Malicious	Infiltration	6.9	0	0	0	93.1
23:54:38	23595	Malicious	Infiltration	0	0	0	0	100
23:57:48	235a0	Malicious	Infiltration	7.89	0	0	0	92.11

Table 5.5 Results of Day 4 Deployment Testing of De-TECH on ValACE using Model 39

Time	Document ID	Results	Classification	Normal	DoS	Bruteforce	Botnet	Infiltration
0:00:36	235a9	Malicious	Infiltration	9.09	0	0	0	90.91
0:03:48	235b2	Malicious	Infiltration	13.51	0	0	0	86.49
0:06:48	235bf	Malicious	Infiltration	13.64	0	0	0	86.36
0:09:54	235c9	Malicious	Infiltration	9.3	0	0	0	90.7
0:12:58	235d3	Malicious	Infiltration	8.89	0	0	0	91.11
0:16:08	235db	Malicious	Infiltration	5.88	0	0	0	94.12
0:19:30	2.35E+09	Malicious	Infiltration	10	0	0	0	90
0:22:18	235f0	Malicious	Infiltration	9.3	0	0	0	90.7
0:25:31	235fc	Malicious	Infiltration	0	0	0	0	100

0:28:28	2.36E+04	Malicious	Infiltration	2.27	0	0	0	97.73
0:31:35	2360f	Malicious	Infiltration	0	0	0	0	100
0:34:38	2.36E+04	Malicious	Infiltration	0	0	0	0	100
0:37:48	2.36E+04	Malicious	Infiltration	0	0	0	0	100
0:40:52	2362d	Malicious	Infiltration	5.56	0	0	0	94.44
0:43:55	2.36E+04	Malicious	Infiltration	0	0	0	0	100
0:47:08	2.36E+04	Malicious	Infiltration	2.78	0	0	0	97.22
0:50:08	2364e	Malicious	Infiltration	0	0	0	0	100
0:53:12	23657	Malicious	Infiltration	0	0	0	0	100
0:56:18	23662	Malicious	Infiltration	9.09	0	0	0	90.91
0:59:24	2366c	Malicious	Infiltration	0	0	0	0	100
1:02:36	23675	Malicious	Infiltration	0	0	0	0	100
1:05:36	23681	Malicious	Infiltration	0	0	0	0	100
1:08:48	2368a	Malicious	Infiltration	0	0	0	0	100
1:11:48	23695	Malicious	Infiltration	10	0	0	0	90
1:14:58	236a1	Malicious	Infiltration	7.5	0	0	0	92.5
1:17:58	236aa	Malicious	Infiltration	11.43	0	0	0	88.57
1:21:23	236b1	Malicious	Infiltration	0	0	0	0	100
1:24:11	236bf	Malicious	Infiltration	0	0	0	0	100
1:27:18	236cb	Malicious	Infiltration	6.25	0	0	0	93.75
1:30:28	236d4	Malicious	Infiltration	0	0	0	0	100
1:33:34	236dd	Malicious	Infiltration	0	0	0	0	100
1:36:48	2.36E+10	Malicious	Infiltration	0	0	0	0	100
1:39:40	236f4	Malicious	Infiltration	0	0	0	0	100
1:42:58	236fb	Malicious	Infiltration	0	0	0	0	100
1:46:08	23707	Malicious	Infiltration	12.9	0	0	0	87.1
1:49:08	23712	Malicious	Infiltration	8.11	0	0	0	91.89
1:52:08	2371b	Malicious	Infiltration	3.57	0	0	0	96.43
1:55:06	23721	Malicious	Infiltration	8.57	0	0	0	91.43
1:58:19	23730	Malicious	Infiltration	5.26	0	0	0	94.74
2:01:28	2373a	Malicious	Infiltration	0	0	0	0	100
2:04:36	23747	Malicious	Infiltration	5.56	0	0	0	94.44
2:07:36	2374e	Malicious	Infiltration	51.71	0	0	0	94.21
2:10:44	23759	Malicious	Infiltration	0	0	0	0	100
2:13:48	23765	Malicious	Infiltration	7.5	0	0	0	92.5
2:16:58	2376c	Malicious	Infiltration	0	0	0	0	100
2:19:55	23777	Malicious	Infiltration	0	0	0	0	100
2:23:08	23783	Malicious	Infiltration	0	0	0	0	100
2:26:18	2378e	Malicious	Infiltration	6.9	0	0	0	93.1
2:29:08	23796	Malicious	Infiltration	0	0	0	0	100
2:32:18	237a1	Malicious	Infiltration	2.86	0	0	0	97.14
2:35:38	237ab	Malicious	Infiltration	0	0	0	0	100
2:38:35	237b8	Malicious	Infiltration	9.52	0	0	0	90.48

2:41:48	237bf	Malicious	Infiltration	6.25	0	0	0	93.75
2:44:41	237c7	Malicious	Infiltration	0	0	0	0	100
2:47:54	237d6	Malicious	Infiltration	2.5	0	0	0	97.5
2:50:54	2.37E+02	Malicious	Infiltration	9.76	0	0	0	90.24
2:54:05	2.37E+09	Malicious	Infiltration	0	0	0	0	100
2:57:08	237f1	Malicious	Infiltration	2.94	0	0	0	97.06
3:00:06	237fd	Malicious	Infiltration	0	0	0	0	100
3:03:18	23809	Malicious	Infiltration	0	0	0	0	100
3:06:28	23815	Malicious	Infiltration	6.06	0	0	0	93.94
3:09:38	2381f	Malicious	Infiltration	8.33	0	0	0	91.67
3:12:48	23826	Malicious	Infiltration	2.17	0	0	0	97.83
3:15:48	23831	Malicious	Infiltration	8.11	0	0	0	91.89
3:18:48	2383d	Malicious	Infiltration	9.76	0	0	0	90.24
3:21:55	23844	Malicious	Infiltration	0	0	0	0	100
3:24:55	2384c	Malicious	Infiltration	0	0	0	0	100
3:28:18	2385b	Malicious	Infiltration	0	0	0	0	100
3:31:08	23867	Malicious	Infiltration	0	0	0	0	100
3:34:19	2386d	Malicious	Infiltration	0	0	0	0	100
3:37:18	23879	Malicious	Infiltration	8.33	0	0	0	91.67
3:40:22	23883	Malicious	Infiltration	0	0	0	0	100
3:43:33	23890	Malicious	Infiltration	2.63	0	0	0	97.37
3:46:48	23897	Malicious	Infiltration	7.14	0	0	0	92.86
3:49:48	238a0	Malicious	Infiltration	3.23	0	0	0	96.77
3:52:48	238ab	Malicious	Infiltration	0	0	0	0	100
3:57:05	238b8	Malicious	Infiltration	0	0	0	0	100
3:59:21	238c1	Malicious	Infiltration	9.84	0	0	0	90.16
4:02:11	238cd	Malicious	Infiltration	35	0	0	0	65
4:05:16	238d5	Malicious	Infiltration	29.41	0	0	0	70.59
4:08:19	238df	Normal	Normal	66.67	0	0	0	33.33
4:13:07	238eb	Normal	Normal	66.67	0	0	0	33.33
4:14:30	238f4	Normal	Normal	50	0	0	20	30
4:19:07	23900	Normal	Normal	60	0	0	0	40
4:21:07	23908	Malicious	Infiltration	40	0	0	0	60
4:24:20	23915	Malicious	Botnet	23.53	0	0	39.22	37.25
4:26:58	2391c	Malicious	Infiltration	3.33	0	0	0	96.67
4:30:05	23925	Malicious	Infiltration	0	0	0	0	100
4:32:58	23932	Malicious	Infiltration	0	0	0	0	100
4:36:08	2393d	Malicious	Infiltration	0	0	0	0	100
4:39:34	23948	Malicious	Infiltration	2.17	0	0	0	97.83
4:42:18	23950	Malicious	Infiltration	0	0	0	0	100
4:45:28	2395d	Malicious	Infiltration	4	0	0	0	96
4:48:28	23968	Malicious	Infiltration	2.22	0	0	0	97.78
4:52:04	2396f	Malicious	Infiltration	0	0	0	0	100

4:54:38	23979	Malicious	Infiltration	9.38	0	0	0	90.62
4:57:48	23986	Malicious	Infiltration	0	0	0	0	100
5:00:58	2398d	Malicious	Infiltration	3.7	0	0	0	96.3
5:03:58	2399a	Malicious	Infiltration	2.5	0	0	0	97.5
5:07:17	239a5	Malicious	Infiltration	2.7	0	0	0	97.3
5:10:07	239aa	Malicious	Infiltration	0	0	0	0	100
5:13:13	239b8	Malicious	Infiltration	11.63	0	0	0	88.37
5:16:18	239c3	Malicious	Infiltration	0	0	0	0	100
5:19:28	239cb	Malicious	Infiltration	2.44	0	0	0	97.56
5:22:29	239d5	Malicious	Infiltration	2.63	0	0	0	97.37
5:25:38	2.39E+03	Malicious	Infiltration	0	0	0	0	100
5:28:48	239ed	Malicious	Infiltration	10.81	0	0	0	81.19
5:31:48	239f4	Malicious	Infiltration	0	0	0	0	100
5:35:25	239fc	Malicious	Infiltration	11.43	0	0	0	88.57
5:37:58	23a0b	Malicious	Infiltration	2.56	0	0	0	97.44
5:41:08	23a15	Malicious	Infiltration	3.57	0	0	0	96.43
5:44:16	23a1c	Malicious	Infiltration	2.5	0	0	0	97.5
5:47:34	23a2c	Malicious	Infiltration	11.11	0	0	0	88.89
5:50:28	23a3d	Malicious	Infiltration	4.17	0	0	0	95.83
5:53:38	23a49	Malicious	Infiltration	8.33	0	0	0	91.67
5:56:48	23a51	Malicious	Infiltration	9.68	0	0	0	90.32
5:59:38	23a5b	Malicious	Infiltration	5.71	0	0	0	94.29
6:02:57	23a66	Malicious	Infiltration	5.71	0	0	0	94.29
6:06:08	23a72	Malicious	Infiltration	4.55	0	0	0	95.45
6:08:58	23a7c	Malicious	Infiltration	10.26	0	0	0	89.74
6:12:18	23a86	Malicious	Infiltration	8.82	0	0	0	91.18
6:15:07	23a90	Malicious	Infiltration	0	0	0	0	100
6:18:20	23a99	Malicious	Infiltration	3.85	0	0	0	96.15
6:21:18	23aa7	Malicious	Infiltration	0	0	0	0	100
6:24:28	23aae	Malicious	Infiltration	2.27	0	0	0	97.73
6:27:48	23ab7	Malicious	Infiltration	0	0	0	0	100
6:30:41	23ac5	Malicious	Infiltration	3.85	0	0	0	96.15
6:33:50	23acc	Malicious	Infiltration	2.27	0	0	0	97.73
6:36:58	23ad5	Malicious	Infiltration	3.33	0	0	0	96.67
6:39:58	23ae3	Malicious	Infiltration	2.7	0	0	0	97.3
6:43:08	23aed	Malicious	Infiltration	0	0	0	0	100
6:46:18	23af7	Malicious	Infiltration	16	0	0	0	84
6:49:10	23b02	Malicious	Infiltration	8.33	0	0	0	91.67
6:52:20	23b0d	Malicious	Infiltration	0	0	0	0	100
6:55:23	23b15	Malicious	Infiltration	0	0	0	0	100
6:58:38	23b1f	Malicious	Infiltration	2.7	0	0	0	97.3
7:01:48	23b27	Malicious	Infiltration	6.9	0	0	0	93.1
7:04:38	23b36	Malicious	Infiltration	0	0	0	0	100

7:07:48	23b3d	Malicious	Infiltration	0	0	0	0	100
7:10:58	23b47	Malicious	Infiltration	4	0	0	0	96
7:14:04	23b54	Malicious	Infiltration	2.27	0	0	0	97.73
7:17:08	23b5c	Malicious	Infiltration	3.33	0	0	0	96.67
7:20:05	23b65	Malicious	Infiltration	2.63	0	0	0	97.37
7:23:13	23b72	Malicious	Infiltration	10.81	0	0	0	89.19
7:26:47	23b7b	Malicious	Infiltration	5.26	0	0	0	94.74
7:29:26	23b88	Malicious	Infiltration	0	0	0	0	100
7:32:38	23b90	Malicious	Infiltration	2.63	0	0	0	97.37
7:35:38	23b98	Malicious	Infiltration	2.44	0	0	0	97.56
7:38:48	23ba6	Malicious	Infiltration	9.3	0	0	0	90.7
7:41:56	23bb1	Malicious	Infiltration	9.38	0	0	0	90.62
7:45:05	23bb9	Malicious	Infiltration	9.38	0	0	0	90.62
7:48:06	23bc2	Malicious	Infiltration	13.33	0	0	0	86.67
7:51:08	23bcf	Malicious	Infiltration	16.67	0	0	0	83.33
7:54:18	23bd9	Malicious	Infiltration	3.92	0	0	0	96.08
7:57:18	23be2	Malicious	Infiltration	5.56	0	0	0	94.44
8:00:21	23bee	Malicious	Infiltration	8.33	0	0	0	91.67
8:03:28	23bf7	Malicious	Infiltration	20	0	0	3.33	76.67
8:06:35	23c00	Malicious	Infiltration	19.57	0	0	0	80.43
8:09:39	23c0d	Malicious	Infiltration	16.22	0	0	0	83.78
8:12:44	23c18	Malicious	Infiltration	17.86	0	0	0	82.14
8:15:52	23c21	Malicious	Infiltration	16.67	0	0	0	83.33
8:19:26	23c29	Malicious	Infiltration	26.56	0	0	0	73.44
8:22:43	23c36	Malicious	Infiltration	12.5	0	0	7.5	80
8:25:08	23c3e	Malicious	Infiltration	12	0	0	0	88
8:28:20	23c49	Malicious	Infiltration	3.45	0	0	0	96.55
8:31:28	23c58	Malicious	Infiltration	5.13	0	0	0	94.87
8:34:51	23c61	Malicious	Infiltration	12.73	0	0	0	87.27
8:38:43	23c6d	Malicious	Infiltration	11.32	0	0	0	88.68
8:41:48	23c75	Malicious	Infiltration	13.79	0	0	0	86.21
8:45:01	23c82	Malicious	Infiltration	27.64	0	0	34.96	37.4
8:48:08	23c8c	Malicious	Infiltration	12.5	0	0	2.5	85
8:51:14	23c93	Malicious	Infiltration	8.33	0	0	0	91.67
8:54:22	23ca3	Malicious	Infiltration	7.5	0	0	0	92.5
8:57:28	23caa	Malicious	Infiltration	7.32	0	0	0	92.68
9:00:38	23cb2	Malicious	Infiltration	12.77	0	0	0	87.23
9:03:37	23cc1	Malicious	Infiltration	13.04	0	0	0	86.96
9:07:07	23ccb	Malicious	Infiltration	7.5	0	0	0	92.5
9:10:01	23cd3	Normal	Normal	49.03	0	0	1.94	49.03
9:13:08	23cdc	Malicious	Infiltration	36.84	0	0	5.26	57.89
9:16:06	23ce9	Malicious	Infiltration	22.86	0	0	2.86	74.49
9:19:12	23cf3	Malicious	Infiltration	34.65	0	0	7.09	58.27

9:22:23	23cff	Malicious	Infiltration	22.86	0	0	3.68	49.08
9:25:29	23d0a	Malicious	Infiltration	34.65	0	0	4.49	58.97
9:28:37	23d11	Malicious	Infiltration	38.17	0	0	11.62	50.21
9:31:54	23d19	Malicious	Infiltration	22.13	0	0	4.1	73.77
9:34:55	23d7a	Malicious	Infiltration	19.83	0	0	7.44	72.73
9:38:15	23d67	Malicious	Infiltration	16.5	0	0	7.77	75.73
13:15:55	23d5e	Normal	Normal	63.12	0	0	0	36.88
13:20:15	23d5d	Malicious	Infiltration	8.41	0	0	5.61	85.98
13:23:16	23d65	Malicious	Infiltration	16.79	0	0	8.76	74.45
13:39:01	23d6f	Malicious	Infiltration	12.93	0	0	4.31	82.76
13:42:19	23daf	Malicious	Infiltration	27.34	0	0	6.47	66.19
13:45:22	23db8	Malicious	Infiltration	44.5	0	0	0	55.5
14:05:10	23dc2	Malicious	Infiltration	7.58	0	0	4.55	87.88
14:08:54	23dcd	Malicious	Infiltration	33.15	0	0	2.76	64.09
14:12:08	23dd8	Malicious	Infiltration	32.02	0	0	3.45	64.53
14:15:21	23de4	Malicious	Infiltration	21.36	0	0	17.96	60.68
14:18:32	23ea0	Malicious	Infiltration	16.42	0	0	5.22	78.36
14:22:18	23eab	Malicious	Infiltration	10.16	0	0	3.91	85.94
15:41:02	23eb7	Malicious	Infiltration	15.15	0	0	3.03	81.82
15:44:28	23ebe	Malicious	Infiltration	12.33	0	0	2.74	84.93
15:47:41	23ecb	Malicious	Infiltration	22.16	0	0	4.79	73.05
15:50:54	23ed4	Malicious	Infiltration	11.86	0	0	1.69	86.44
15:54:06	23edf	Normal	Normal	68.6	0	0	0	31.4
15:57:14	23eec	Malicious	Infiltration	14.5	0	0	2.29	83.21
16:00:43	23ef6	Normal	Normal	69.82	0	0	0	30.18
16:03:59	23efe	Malicious	Infiltration	19.31	0	0	5.52	75.17
16:07:11	23f0a	Malicious	Infiltration	17.8	0	0	0.85	81.36
16:10:15	23f14	Malicious	Infiltration	8.6	0	0	2.15	89.25
16:13:16	23f15	Malicious	Infiltration	9.78	0	0	2.17	88.04
16:16:34	23f23	Normal	Normal	66.26	0	0	0	33.74
16:16:43	23f2a	Normal	Normal	60	0	0	10	30
16:19:44	23f33	Normal	Normal	60.68	0	0	0	39.32
16:22:47	23f41	Malicious	Infiltration	23.36	0	0	4.38	72.26
16:25:56	23f42	Malicious	Infiltration	14.13	0	0	2.17	83.7
16:28:45	23f4c	Normal	Normal	60.61	0	0	12.12	27.27
16:29:00	23f54	Malicious	Infiltration	15.7	0	0	11.57	72.73
16:32:10	23f69	Malicious	Infiltration	27.65	0	0	2.35	70
16:34:53	23f73	Normal	Normal	58.54	0	0	19.51	21.95
16:40:50	23f80	Malicious	Infiltration	17.09	0	0	2.56	80.34
16:43:50	23f84	Malicious	Infiltration	23.49	0	0	9.64	66.87
16:46:52	23f8c	Normal	Normal	69.93	0	0	0	30.07
16:48:22	23f98	Normal	Normal	63.89	0	0	16.67	19.44
16:50:06	23f99	Malicious	Infiltration	18.49	0	0	10.96	70.55

16:53:21	23fa1	Malicious	Infiltration	32.92	0	0	8.07	59.01
16:53:24	23f68	Normal	Normal	53.33	0	0	0	46.67
16:56:23	23f7b	Malicious	Infiltration	22.14	0	0	5	72.86
16:56:26	23f81	Normal	Normal	62.5	0	0	15	22.5
17:16:42	23f86	Malicious	Infiltration	11.11	0	0	1.01	87.88
17:19:57	23f8d	Malicious	Infiltration	10.11	0	0	2.25	87.64
17:22:57	23f8b	Malicious	Infiltration	11.22	0	0	3.06	85.71
17:25:58	23f8a	Malicious	Infiltration	11.36	0	0	0	88.64
17:29:02	23f8c	Malicious	Infiltration	19	0	0	3	78
17:32:15	23f8f	Malicious	Infiltration	20.54	0	0	2.68	76.79
17:16:31	23f8e	Normal	Normal	63.89	0	0	11.11	25
17:39:27	23f9a	Malicious	Infiltration	25.83	0	0	2.5	71.67
17:42:31	23fa8	Malicious	Infiltration	20.66	0	0	3.31	76.03
17:45:42	23faf	Malicious	Infiltration	22.12	0	0	1.92	75.96
17:48:41	23fad	Malicious	Infiltration	19.35	0	0	4.84	75.81
17:51:54	23faa	Malicious	Infiltration	23.58	0	0	3.77	72.64
17:54:57	23fac	Malicious	Infiltration	25.66	0	0	12.39	61.95
17:58:05	1310b	Malicious	Infiltration	47.22	0	0	11.11	41.67
18:01:12	13173	Normal	Normal	41.28	0	0	8.26	50.46

Table 5.6 Results of Day 5 Deployment Testing of De-TECH
on ValACE using Model 39

Time	Document ID	Results	Classification	Normal	DoS	Bruteforce	Botnet	Infiltration
10:22:36	131ba	Malicious	Infiltration	9.8	0	0	2.94	87.25
10:58:09	131d9	Normal	Normal	70.75	0	0	0	29.25
11:19:35	131f0	Malicious	Infiltration	12	0	0	4	84
11:27:43	131fd	Malicious	Infiltration	13.27	0	0	5.1	81.63
11:35:45	13208	Malicious	Infiltration	11.24	0	0	1.12	87.64
11:39:45	13213	Malicious	Infiltration	8.21	0	0	3.73	88.06
11:43:09	1328b	Malicious	Infiltration	8.33	0	0	4.17	87.5
11:47:34	1.33E+04	Malicious	Infiltration	9.35	0	0	1.87	88.79
12:24:53	1329f	Malicious	Infiltration	9.35	0	0	1.87	88.79
12:28:28	1.33E+04	Malicious	Infiltration	7.84	0	0	4.9	87.25
12:31:45	1331f	Malicious	Infiltration	9.68	0	0	1.08	89.25
13:03:41	1332c	Malicious	Infiltration	13.27	0	0	2.65	84.07
13:12:14	1.33E+04	Malicious	Infiltration	10.74	0	0	0	89.26
13:15:59	1.34E+04	Normal	Normal	64.18	0	0	0	35.82
13:19:18	1.34E+04	Malicious	Infiltration	18.18	0	0	1.52	80.3
13:35:00	1337c	Malicious	Infiltration	11.11	0	0	2.38	86.51
13:38:23	1.34E+04	Malicious	Infiltration	15.79	0	0	1.5	82.71
13:41:44	133be	Normal	Normal	55.14	0	0	0	44.68

13:45:59	133d7	Normal	Normal	57.94	0	0	0	42.06
14:01:08	134a4	Malicious	Infiltration	6.31	0	0	2.7	90.99
14:08:55	134b1	Malicious	Infiltration	13.45	0	0	3.36	83.19
15:17:26	134d7	Malicious	Infiltration	15.81	0	0	3.42	80.77
15:21:15	1.34E+03	Malicious	Infiltration	16.09	0	0	2.87	81.03
15:32:54	13528	Malicious	Infiltration	33.53	0	0	5.39	61.08
15:36:28	13535	Normal	Normal	60.53	0	0	0	39.47
15:59:40	13540	Malicious	Infiltration	28.26	0	0	7.07	64.67
16:03:17	13588	Malicious	Infiltration	16.08	0	0	3.5	80.42
16:06:40	135a9	Malicious	Infiltration	23.33	0	0	2.67	74
16:29:23	135b6	Normal	Normal	58.86	0	0	0	41.14
16:40:20	135bf	Malicious	Infiltration	23.46	0	0	5.56	70.99
16:44:06	135ca	Malicious	Infiltration	18.38	0	0	6.62	75
16:47:14	135d4	Malicious	Infiltration	14.71	0	0	1.47	83.82
16:50:27	135df	Normal	Normal	71.43	0	0	0	28.57
16:53:35	135ea	Malicious	Infiltration	22.75	0	0	7.78	69.46
16:56:43	135f5	Malicious	Infiltration	20.92	0	0	5.23	73.86
17:00:01	13600	Malicious	Infiltration	17.56	0	0	3.05	79.39
17:03:19	1360c	Malicious	Infiltration	12.98	0	0	4.58	82.44
17:06:34	13616	Malicious	Infiltration	10.43	0	0	0	89.57
17:09:55	13620	Malicious	Infiltration	35.67	0	0	1.75	62.57
17:12:59	1362a	Malicious	Infiltration	16.03	0	0	1.53	82.44
17:16:11	13637	Malicious	Infiltration	11.96	0	0	0	88.04
17:19:22	1363e	Malicious	Infiltration	16.67	0	0	2.22	81.11
17:22:29	13649	Malicious	Infiltration	9.9	0	0	1.98	88.12
17:25:40	13654	Malicious	Infiltration	22.73	0	0	0.91	76.36
17:28:43	1365c	Malicious	Infiltration	11.21	0	0	2.8	85.98
17:31:52	13663	Malicious	Infiltration	16.51	0	0	0	83.49
17:34:57	13673	Malicious	Infiltration	35.59	0	0	22.42	41.99
17:38:06	1367d	Malicious	Infiltration	10	0	0	3	87
17:41:12	13685	Malicious	Infiltration	34.22	0	0	9.63	56.15
17:44:22	13694	Malicious	Infiltration	15.79	0	0	0	84.21
17:47:26	1369b	Malicious	Infiltration	15.38	0	0	2.2	82.42
17:50:34	136a5	Malicious	Infiltration	10.39	0	0	0	89.61
17:53:38	136b0	Malicious	Infiltration	13.04	0	0	0	86.96
17:56:44	136bc	Malicious	Infiltration	12.31	0	0	0	87.69
17:59:50	136c7	Malicious	Infiltration	30.59	0	0	0	69.41
18:03:06	136d1	Malicious	Infiltration	8.54	0	0	0	91.46
18:06:03	136d9	Malicious	Infiltration	5.48	0	0	0	94.52
18:08:24	1.36E+06	Malicious	Infiltration	9.72	0	0	0	90.28
18:12:18	136f0	Malicious	Infiltration	15.58	0	0	0	84.42
18:15:30	136f8	Malicious	Infiltration	6.1	0	0	0	93.9
18:18:29	13702	Malicious	Infiltration	9.33	0	0	1.33	89.33

18:21:38	13709	Malicious	Infiltration	36.17	0	0	14.89	48.94
18:24:53	13719	Normal	Normal	54.3	0	0	0	45.7
18:28:01	13723	Malicious	Infiltration	42.31	0	0	11.54	46.15
18:31:01	1372b	Malicious	Infiltration	20.29	0	0	2.9	76.81
18:34:12	1373a	Malicious	Infiltration	33.96	0	0	5.66	60.38
18:37:34	13741	Malicious	Infiltration	38.39	0	0	7.14	54.46
18:41:15	1374a	Normal	Normal	60.87	0	0	0	39.13
18:43:35	13757	Malicious	Infiltration	31.63	0	0	10.2	58.16
18:46:45	1375f	Normal	Normal	68.52	0	0	0	31.48
18:49:53	1376c	Malicious	Infiltration	18.06	0	0	1.39	80.56
18:53:06	13775	Malicious	Infiltration	20.97	0	0	0	79.03
18:56:21	13780	Malicious	Infiltration	23.53	0	0	0	76.47
18:59:16	1378a	Malicious	Infiltration	15	0	0	0	85
19:02:19	13795	Malicious	Infiltration	13.11	0	0	0	86.89
19:05:23	1379e	Malicious	Infiltration	17.91	0	0	1.49	80.6
19:08:55	137a8	Malicious	Infiltration	13.33	0	0	0	86.67
19:11:40	137b1	Malicious	Infiltration	13.79	0	0	8.62	77.59
19:14:46	137bf	Malicious	Infiltration	36.67	0	0	5.56	57.78
19:17:52	137c9	Malicious	Infiltration	29.79	0	0	8.51	61.7
19:21:08	137d2	Malicious	Infiltration	29.63	0	0	8.64	61.73
19:24:17	137dc	Malicious	Infiltration	22.95	0	0	6.56	70.49
19:27:14	1.37E+09	Malicious	Infiltration	14.29	0	0	3.17	82.54
19:30:20	137ef	Malicious	Infiltration	24.29	0	0	5.71	70
19:33:37	137fd	Malicious	Infiltration	19.61	0	0	0	80.39
19:36:38	13805	Malicious	Infiltration	19.75	0	0	3.7	76.54
19:39:48	13811	Malicious	Infiltration	15	0	0	3.75	81.25
19:42:49	1381c	Malicious	Infiltration	23.08	0	0	5.49	71.43
19:45:58	13825	Normal	Normal	59.62	0	0	0	40.38
19:49:20	13830	Malicious	Infiltration	12.77	0	0	2.13	85.11
19:52:09	1383b	Malicious	Infiltration	17.14	0	0	1.43	81.43
19:55:19	13844	Malicious	Infiltration	31.18	0	0	4.3	64.52
19:58:25	1384e	Malicious	Infiltration	31.58	0	0	5.26	63.16
20:01:37	13856	Malicious	Infiltration	17.76	0	0	1.87	80.37
20:04:42	13865	Malicious	Infiltration	18.39	0	0	4.6	77.01
20:07:47	1386c	Malicious	Infiltration	10.59	0	0	5.88	83.53
20:10:54	13877	Malicious	Infiltration	16.67	0	0	2.78	80.56
20:14:07	13882	Malicious	Infiltration	14.86	0	0	4.05	81.08
20:17:23	1388d	Malicious	Infiltration	20	0	0	3.75	76.25
20:20:11	13898	Malicious	Infiltration	20	0	0	1.33	78.67
20:23:29	138a1	Malicious	Infiltration	13.04	0	0	0	86.96
20:26:33	138ae	Malicious	Infiltration	13.33	0	0	1.33	85.33
20:29:31	138b8	Malicious	Infiltration	14.29	0	0	3.3	82.42
20:32:43	138c2	Normal	Normal	65	0	0	0	35

20:35:47	138cc	Malicious	Infiltration	14.94	0	0	3.45	81.61
20:39:10	138d5	Malicious	Infiltration	12.99	0	0	2.6	84.42
20:42:07	1.38E+03	Malicious	Infiltration	21.51	0	0	4.3	74.19
20:45:12	138ea	Normal	Normal	50	0	0	0	50
20:48:22	138f4	Malicious	Infiltration	15.66	0	0	1.2	83.13
20:51:30	138fc	Malicious	Infiltration	12.2	0	0	2.44	85.37
20:54:36	1390b	Malicious	Infiltration	10.78	0	0	6.86	82.35
20:57:44	13915	Malicious	Infiltration	30.28	0	0	5.5	64.22
21:00:52	1391e	Malicious	Infiltration	15.79	0	0	4.21	80
21:04:03	13929	Malicious	Infiltration	10.53	0	0	2.63	86.84
21:07:14	13933	Malicious	Infiltration	11.59	0	0	1.45	86.96
21:10:18	1393c	Malicious	Infiltration	17.14	0	0	2.86	80
21:13:25	13949	Malicious	Infiltration	9.35	0	0	2.8	87.85
21:16:35	13954	Malicious	Infiltration	13.82	0	0	0	86.18
21:19:40	1395a	Malicious	Infiltration	11.02	0	0	4.24	84.75
21:22:51	13966	Malicious	Infiltration	11.72	0	0	4.69	83.59
21:26:04	13972	Normal	Normal	87.6	0	0	0	12.4
21:29:27	1397b	Malicious	Infiltration	32.35	0	0	0	67.65
21:32:09	13987	Malicious	Infiltration	17.07	0	0	0	82.93
21:35:18	13990	Normal	Normal	68.14	0	0	0	31.86
21:38:29	1399a	Malicious	Infiltration	9.09	0	0	2.48	88.43
21:41:42	139a2	Malicious	Infiltration	18.6	0	0	0	81.4
21:45:02	139b1	Malicious	Infiltration	37.5	0	0	0	62.5
21:47:46	139b8	Malicious	Infiltration	11.32	0	0	2.83	85.85
21:51:38	139c3	Malicious	Infiltration	10.09	0	0	0.92	88.99
21:54:09	139ce	Malicious	Infiltration	9.52	0	0	0	90.48
21:57:16	139d8	Malicious	Infiltration	25	0	0	0.86	74.14
22:00:37	1.39E+04	Normal	Normal	92.92	0	0	0	7.08
22:03:19	139ed	Normal	Normal	84	0	0	0	16
22:06:29	139f6	Malicious	Infiltration	7.32	0	0	0.81	91.87
22:09:35	13a03	Malicious	Infiltration	8	0	0	3.2	88.8
22:12:38	13a0b	Malicious	Infiltration	7.14	0	0	1.59	91.27
22:15:49	13a13	Normal	Normal	85.71	0	0	0	14.29
22:19:01	13a1f	Malicious	Infiltration	14.62	0	0	1.54	83.85
22:22:05	13a2c	Normal	Normal	86.99	0	0	0	13.01
22:25:09	13a35	Normal	Normal	86.18	0	0	0	13.82
22:28:32	13a41	Malicious	Infiltration	11.81	0	0	2.36	85.83
22:31:44	13a4d	Malicious	Infiltration	11.9	0	0	1.59	86.51
22:34:41	13a54	Normal	Normal	84.13	0	0	0	15.87
22:38:13	13a5e	Normal	Normal	88.8	0	0	0	11.2
22:40:39	13a6b	Malicious	Infiltration	9.38	0	0	0	90.62
22:43:42	13a75	Malicious	Infiltration	12	0	0	3.2	84.8
22:46:55	13a7b	Malicious	Infiltration	16.67	0	0	0	83.33

22:50:15	13a86	Normal	Normal	92.79	0	0	0	7.21
22:53:16	13a93	Malicious	Infiltration	11.81	0	0	2.36	85.83
22:56:16	13a9c	Malicious	Infiltration	11.11	0	0	0.79	88.1
22:59:13	13aaa	Malicious	Infiltration	19.17	0	0	2.5	78.33
23:03:12	13ab3	Normal	Normal	89.74	0	0	0	10.26
23:06:05	13abd	Normal	Normal	88.98	0	0	0	11.02
23:08:52	13ac8	Normal	Normal	92.04	0	0	0	7.96
23:12:00	13ad2	Malicious	Infiltration	9.68	0	0	1.61	88.71
23:15:19	13ad9	Malicious	Infiltration	4.39	0	0	1.75	93.86
23:18:24	13ae6	Malicious	Infiltration	21.19	0	0	1.69	77.12
23:21:24	13aed	Malicious	Infiltration	8.74	0	0	0	91.26
23:24:26	13afa	Malicious	Infiltration	15.15	0	0	2.02	82.83
23:27:33	13b07	Malicious	Infiltration	12	0	0	2	86
23:30:45	13b0e	Malicious	Infiltration	17.35	0	0	1.02	81.63
23:33:57	13b18	Malicious	Infiltration	6.59	0	0	0	93.41
23:36:53	13b25	Malicious	Infiltration	5.56	0	0	0	94.44
23:40:00	13b2f	Malicious	Infiltration	5.26	0	0	2.11	92.63
23:43:58	13b39	Malicious	Infiltration	0	0	0	0	100
23:46:13	13b43	Malicious	Infiltration	16.67	0	0	0	83.33
23:49:13	13b4c	Malicious	Infiltration	2.78	0	0	0	97.22
23:52:32	13b58	Malicious	Infiltration	0	0	0	0	100
23:55:23	13b61	Malicious	Infiltration	9.68	0	0	0	90.32
23:58:35	13b6b	Malicious	Infiltration	0	0	0	0	100

Table 5.7 Results of Day 6 Deployment Testing of De-TECH
on ValACE using Model 39

Time	Document ID	Results	Classification	Normal	DoS	Bruteforce	Botnet	Infiltration
0:01:53	13b73	Malicious	Infiltration	3.57	0	0	3.57	92.86
0:04:41	13b82	Malicious	Infiltration	5.26	0	0	0	94.74
0:07:53	13b89	Malicious	Infiltration	10	0	0	2.5	87.5
0:10:55	13b93	Malicious	Infiltration	8.33	0	0	0	91.67
0:14:06	13b9f	Malicious	Infiltration	24.59	0	0	8.2	67.21
0:17:13	13baa	Malicious	Infiltration	21.95	0	0	0	78.05
0:20:09	13bb2	Malicious	Infiltration	18.6	0	0	0	81.4
0:23:19	13bbe	Malicious	Infiltration	2.94	0	0	0	97.06
0:26:33	13bc7	Malicious	Infiltration	9.09	0	0	0	90.91
0:30:10	13bd4	Malicious	Infiltration	14.63	0	0	0	85.37
0:32:34	13bdd	Malicious	Infiltration	8.11	0	0	0	91.89
0:35:53	13be9	Malicious	Infiltration	7.14	0	0	0	92.86
0:38:43	13bf0	Malicious	Infiltration	7.5	0	0	2.5	90
0:42:02	13bf8	Malicious	Infiltration	0	0	0	0	100

0:45:12	13c07	Malicious	Infiltration	7.5	0	0	0	92.5
0:48:01	13c11	Malicious	Infiltration	11.11	0	0	0	88.89
0:51:13	13c19	Malicious	Infiltration	8.57	0	0	0	91.43
0:54:23	13c24	Malicious	Infiltration	15.15	0	0	0	84.85
0:57:18	13c2f	Malicious	Infiltration	33.96	0	0	0	66.04
1:00:25	13c3a	Malicious	Infiltration	2.78	0	0	0	97.22
1:03:33	13c43	Malicious	Infiltration	3.23	0	0	0	96.77
1:06:43	13c4c	Malicious	Infiltration	11.43	0	0	0	88.57
1:09:53	13c58	Malicious	Infiltration	12.12	0	0	0	87.88
1:13:03	13c64	Malicious	Infiltration	2.7	0	0	0	97.3
1:16:01	13c6e	Malicious	Infiltration	7.41	0	0	0	92.59
1:19:04	13c78	Malicious	Infiltration	3.12	0	0	0	96.88
1:22:13	13c7e	Malicious	Infiltration	0	0	0	0	100
1:25:14	13c8c	Malicious	Infiltration	9.09	0	0	0	90.91
1:28:33	13c96	Malicious	Infiltration	2.27	0	0	0	97.73
1:31:20	13c9f	Malicious	Infiltration	3.57	0	0	0	96.43
1:34:38	13cad	Malicious	Infiltration	0	0	0	0	100
1:37:43	13cb4	Malicious	Infiltration	0	0	0	0	100
1:40:41	13cbe	Malicious	Infiltration	6.06	0	0	0	93.94
1:43:53	13cca	Malicious	Infiltration	0	0	0	0	100
1:46:53	13cd5	Malicious	Infiltration	14.63	0	0	4.88	80.49
1:50:03	13cdf	Malicious	Infiltration	2.94	0	0	0	97.06
1:53:13	13ce7	Malicious	Infiltration	0	0	0	0	100
1:56:13	13cf2	Malicious	Infiltration	9.38	0	0	3.12	87.5
1:59:32	13cfc	Malicious	Infiltration	21.15	0	0	1.92	76.92
2:02:23	13d08	Malicious	Infiltration	14.29	0	0	2.86	82.86
2:05:27	13d11	Malicious	Infiltration	9.52	0	0	2.38	88.1
2:08:38	13d1b	Malicious	Infiltration	11.11	0	0	0	88.89
2:11:53	13d24	Malicious	Infiltration	9.68	0	0	0	90.32
2:14:53	13d32	Malicious	Infiltration	0	0	0	2.78	97.22
2:17:53	13d3c	Malicious	Infiltration	20.51	0	0	0	79.49
2:20:57	13d44	Malicious	Infiltration	3.45	0	0	3.45	93.1
2:24:03	13d4f	Malicious	Infiltration	7.89	0	0	2.63	89.47
2:27:13	13d5a	Malicious	Infiltration	7.5	0	0	2.5	90
2:30:23	13d64	Malicious	Infiltration	14.29	0	0	0	85.71
2:33:23	13d71	Malicious	Infiltration	12.2	0	0	2.44	85.37
2:36:33	13d78	Malicious	Infiltration	9.68	0	0	3.23	87.1
2:39:36	13d82	Malicious	Infiltration	11.76	0	0	2.94	85.29
2:42:43	13d8c	Malicious	Infiltration	11.11	0	0	0	88.89
2:46:01	13d98	Malicious	Infiltration	12.5	0	0	0	87.5
2:49:29	13da3	Malicious	Infiltration	2.5	0	0	2.5	95
2:52:03	13dae	Malicious	Infiltration	20.51	0	0	0	79.49
2:55:08	13db3	Malicious	Infiltration	7.5	0	0	0	92.5

2:58:13	13dbf	Malicious	Infiltration	11.63	0	0	0	88.37
3:01:20	13dc7	Malicious	Infiltration	0	0	0	0	100
3:04:33	13dd6	Malicious	Infiltration	3.03	0	0	0	96.97
3:07:41	13ddd	Malicious	Infiltration	9.09	0	0	0	90.91
3:10:38	13de9	Malicious	Infiltration	9.38	0	0	0	90.62
3:13:46	13df4	Malicious	Infiltration	2.44	0	0	0	9.56
3:17:03	13dfa	Malicious	Infiltration	0	0	0	0	100
3:19:53	1.30E+08	Malicious	Infiltration	9.09	0	0	0	90.91
3:23:13	1.30E+13	Malicious	Infiltration	8.57	0	0	0	91.43
3:26:06	13e1c	Malicious	Infiltration	2.86	0	0	0	97.14
3:29:38	1.30E+27	Malicious	Infiltration	9.3	0	0	0	90.7
3:32:38	1.30E+34	Malicious	Infiltration	6.06	0	0	0	93.94
3:35:20	13e3a	Malicious	Infiltration	8.57	0	0	0	91.43
3:38:23	1.30E+46	Malicious	Infiltration	5.13	0	0	0	94.87
3:41:29	13e4c	Malicious	Infiltration	6.25	0	0	0	93.75
3:44:41	13e5b	Malicious	Infiltration	0	0	0	0	100
3:47:53	1.30E+66	Malicious	Infiltration	5.71	0	0	0	94.29
3:50:58	13e6d	Malicious	Infiltration	0	0	0	0	100
3:54:03	1.30E+76	Malicious	Infiltration	0	0	0	0	100
3:57:23	1.30E+84	Malicious	Infiltration	21.43	0	0	2.38	76.19
4:00:14	13e8c	Malicious	Infiltration	38.18	0	0	1.82	60
4:03:10	1.30E+96	Malicious	Infiltration	27.78	0	0	0	72.22
4:06:18	13ea1	Normal	Normal	64.71	0	0	0	35.29
4:09:21	13eaa	Normal	Normal	50	0	0	0	50
4:13:18	13eb6	Normal	Normal	41.67	0	0	16.67	41.67
4:17:18	13ec2	Malicious	Infiltration	0	0	0	0	100
4:19:18	13ec9	Normal	Normal	71.43	0	0	0	28.57
4:23:18	13ed1	Normal	Normal	66.67	0	0	0	33.33
4:25:20	13ee0	Normal	Normal	66.67	0	0	0	33.33
4:29:17	13eea	Normal	Normal	42.86	0	0	28.57	28
4:31:20	13ef2	Normal	Normal	75	0	0	0	25
4:35:18	13efd	Normal	Normal	60	0	0	0	40
4:37:20	13f08	Normal	Normal	75	0	0	0	25
4:40:24	13f11	Normal	Normal	66.67	0	0	0	33.33
4:43:20	13f1e	Malicious	Infiltration	14.29	0	0	28.57	57.14
4:47:18	13f26	Normal	Normal	80	0	0	0	20
4:50:24	13f30	Normal	Normal	75	0	0	0	25
4:53:18	13f3d	Normal	Normal	62.5	0	0	0	37.5
4:57:18	13f44	Normal	Normal	66.67	0	0	0	33.33
4:59:18	13f4d	Normal	Normal	62.5	0	0	25	12.5
5:03:18	13f57	Normal	Normal	66.67	0	0	0	33.33
5:05:20	13f65	Normal	Normal	57.14	0	0	0	42.86
5:09:18	13f6e	Normal	Normal	60	0	0	0	40

5:11:20	13f79	Normal	Normal	75	0	0	0	25
5:14:30	13f83	Normal	Normal	40	0	0	20	40
5:17:20	13f8c	Malicious	Infiltration	25	0	0	33.93	41.07
5:20:27	13f98	Malicious	Infiltration	0	0	0	0	100
5:23:43	13fa4	Malicious	Infiltration	0	0	0	0	100
5:26:43	13faa	Malicious	Infiltration	0	0	0	0	100
5:29:53	13fb4	Malicious	Infiltration	0	0	0	0	100
5:32:47	13fc2	Malicious	Infiltration	0	0	0	0	100
5:36:03	13fcb	Malicious	Infiltration	0	0	0	0	100
5:39:13	13fd4	Malicious	Infiltration	0	0	0	0	100
5:42:11	13fe0	Malicious	Infiltration	3.23	0	0	0	96.77
5:45:13	13fea	Malicious	Infiltration	0	0	0	0	100
5:48:33	13ff4	Malicious	Infiltration	0	0	0	0	100
5:51:21	14000	Malicious	Infiltration	11.11	0	0	0	88.89
5:54:39	14008	Malicious	Infiltration	3.85	0	0	0	96.15
5:57:38	14014	Malicious	Infiltration	10	0	0	0	90
6:00:43	1401c	Malicious	Infiltration	8.11	0	0	0	91.89
6:03:53	14029	Malicious	Infiltration	0	0	0	0	100
6:06:53	14033	Malicious	Infiltration	18.18	0	0	0	81.82
6:10:01	1403c	Malicious	Infiltration	5.41	0	0	0	94.59
6:13:03	14045	Malicious	Infiltration	0	0	0	0	100
6:16:13	14051	Malicious	Infiltration	16.22	0	0	2.7	81.08
6:19:13	1405a	Malicious	Infiltration	11.54	0	0	0	88.46
6:22:36	14065	Malicious	Infiltration	17.5	0	0	2.5	80
6:25:27	1406f	Malicious	Infiltration	4	0	0	2	94
6:29:13	14079	Malicious	Infiltration	10.34	0	0	0	89.66
6:31:53	14081	Malicious	Infiltration	14.71	0	0	2.94	82.35
6:34:53	14090	Malicious	Infiltration	10.71	0	0	0	89.29
6:37:53	1409a	Malicious	Infiltration	5.26	0	0	0	94.74
6:41:13	140a4	Malicious	Infiltration	4.55	0	0	0	95.45
6:44:03	140ae	Malicious	Infiltration	15.38	0	0	5.13	79.49
6:47:25	140b8	Malicious	Infiltration	24.53	0	0	1.89	73.58
6:50:23	140c2	Malicious	Infiltration	24.53	0	0	3.77	71.7
6:53:20	140ca	Malicious	Infiltration	15.15	0	0	3.03	81.82
6:56:39	140d4	Malicious	Infiltration	39.13	0	0	4.35	56.52
7:00:33	140de	Malicious	Infiltration	8.57	0	0	2.86	88.57
7:02:43	140ea	Malicious	Infiltration	18.64	0	0	0	81.36
7:06:20	140f3	Malicious	Infiltration	0	0	0	0	100
7:09:41	140fe	Malicious	Infiltration	20.51	0	0	2.56	76.92
7:12:03	1410a	Malicious	Infiltration	3.7	0	0	0	96.3
7:15:13	14114	Malicious	Infiltration	20	0	0	0	80
7:18:10	1411a	Malicious	Infiltration	13.95	0	0	2.33	83.72
7:22:05	14128	Malicious	Infiltration	6.25	0	0	0	93.75

7:24:20	14132	Malicious	Infiltration	6.45	0	0	0	93.55
7:27:43	1413a	Malicious	Infiltration	4.35	0	0	0	95.65
7:30:31	14147	Malicious	Infiltration	11.11	0	0	0	88.89
7:33:43	14153	Malicious	Infiltration	8.82	0	0	0	91.18
7:36:58	14159	Malicious	Infiltration	3.77	0	0	0	96.23
7:39:55	14166	Malicious	Infiltration	10	0	0	0	90
7:43:14	14171	Malicious	Infiltration	9.43	0	0	0	90.57
7:46:00	1417b	Malicious	Infiltration	13.21	0	0	1.89	84.91
7:49:17	14183	Malicious	Infiltration	16.67	0	0	1.85	81.48
7:52:25	1418f	Malicious	Infiltration	13.33	0	0	0	86.48
7:55:33	14199	Malicious	Infiltration	16.98	0	0	7.55	75.67
7:58:29	141a2	Malicious	Infiltration	9.68	0	0	1.61	88.71
8:01:49	141af	Malicious	Infiltration	26.23	0	0	3.28	70.49
8:04:51	141b7	Malicious	Infiltration	11.76	0	0	0	88.24
8:07:57	141c1	Malicious	Infiltration	30.12	0	0	7.23	62.65
8:10:53	141ce	Malicious	Infiltration	28.81	0	0	1.69	69.49
8:14:04	141d8	Malicious	Infiltration	2.5	0	0	0	97.5
8:16:59	1.41E+03	Malicious	Infiltration	14.29	0	0	1.59	84.13
8:20:13	1.41E+11	Malicious	Infiltration	14.04	0	0	0	85.96
8:23:49	141f6	Malicious	Infiltration	34.21	0	0	0	65.79
8:26:22	14200	Malicious	Infiltration	36.46	0	0	5.21	58.33
8:29:45	1420b	Malicious	Infiltration	41.77	0	0	2.53	55.7
8:32:38	14217	Malicious	Infiltration	3.33	0	0	30	66.67
8:35:54	1421e	Malicious	Infiltration	7.84	0	0	1.96	90.2
8:38:42	14229	Malicious	Infiltration	15.52	0	0	0	84.48
8:41:54	14235	Malicious	Infiltration	1.64	0	0	1.64	96.72
8:44:57	1423f	Malicious	Infiltration	30.56	0	0	2.78	66.67
8:48:05	14244	Malicious	Infiltration	30.11	0	0	1.08	68.82
8:51:14	14253	Malicious	Infiltration	32.65	0	0	1.02	66.33
8:54:18	1425c	Malicious	Infiltration	39.13	0	0	4.35	56.52
8:57:34	14268	Malicious	Infiltration	36.94	0	0	1.8	61.26
9:00:35	14274	Malicious	Infiltration	21.52	0	0	3.8	74.68
9:03:44	1427b	Malicious	Infiltration	13.92	0	0	1.27	84.81
9:06:54	14289	Malicious	Infiltration	30.77	0	0	3.3	65.93
9:09:54	14291	Malicious	Infiltration	39.86	0	0	2.1	58.04
9:13:03	1429c	Malicious	Infiltration	47.53	0	0	1.23	51.23
9:16:09	142a6	Malicious	Infiltration	16.67	0	0	2.08	81.25
9:19:16	142af	Malicious	Infiltration	13.83	0	0	4.26	81.91
9:22:30	142bd	Malicious	Infiltration	21.54	0	0	2.31	76.15
9:25:45	142c7	Malicious	Infiltration	27.59	0	0	4.83	67.59
9:28:46	142d0	Normal	Normal	60.26	0	0	0	39.74
9:32:04	142dd	Malicious	Infiltration	32	0	0	2.67	65.33
9:35:13	13bd6	Malicious	Infiltration	30.88	0	0	8.09	61.03

9:38:21	13a87	Malicious	Infiltration	19.51	0	0	3.25	77.24
9:41:34	139c5	Malicious	Infiltration	21.58	0	0	2.16	76.26
9:44:45	1337a	Malicious	Infiltration	70.7	0	0	0	29.3
9:47:52	126fe	Malicious	Infiltration	20.55	0	0	4.79	74.66
9:51:03	11a8a	Malicious	Infiltration	23.61	0	0	6.94	69.44
9:54:09	10f44	Normal	Normal	53.91	0	0	0	46.09
9:57:23	1.02E+05	Normal	Normal	60.44	0	0	0	39.56
10:00:34	f6de	Normal	Normal	67.22	0	0	0	32.78
10:03:40	ecf5	Malicious	Infiltration	19.73	0	0	8.16	72.11
10:06:53	ecff	Normal	Normal	59.38	0	0	0	40.62
10:10:18	ed0a	Normal	Normal	68.93	0	0	0	31.07
10:13:48	e631	Malicious	Infiltration	24.48	0	0	5.21	70.31
10:17:03	d998	Malicious	Infiltration	28.08	0	0	3.94	67.98
10:20:18	d9a3	Malicious	Infiltration	33.9	0	0	5.51	60.59
10:23:46	d9ae	Normal	Normal	61.4	0	0	0	38.6
10:27:05	ac09	Normal	Normal	62.57	0	0	0	37.43
10:30:20	89bf	Malicious	Infiltration	20	0	0	4.38	75.62

Table 5.8 Results of Day 6 Deployment Testing of De-TECH
on ValACE using Model 20

Time	Document ID	Results	Classification	Normal	DoS	Bruteforce	Botnet	Infiltration
10:47:53	89c5	Normal	Normal	88.33	3.33	5.56	1.67	1.11
11:01:03	4ac6	Normal	Normal	80.66	11.6	2.21	1.66	3.87
11:04:13	3d5d	Normal	Normal	81.73	12.02	2.88	0.96	2.4
11:44:00	32f1	Normal	Normal	92.36	0.69	2.08	0.69	4.17
11:47:12	2.81E+03	Normal	Normal	85.11	1.42	2.84	2.84	7.8
11:50:27	1a2e	Normal	Normal	88.73	0	6.34	2.11	2.82
11:57:10	1.54E+03	Normal	Normal	77.33	14	2.67	0.67	5.33
11:53:42	154b	Normal	Normal	85.08	2.21	4.97	2.21	5.52
12:00:34	1.58E+03	Normal	Normal	77.04	15.56	2.96	1.48	2.96
12:03:50	158b	Normal	Normal	84.33	3.73	4.48	1.49	5.97
12:19:38	1.59E+03	Normal	Normal	86.67	3.03	4.24	3.64	2.42
12:23:05	159e	Normal	Normal	69.57	3.91	4.35	0.43	21.74
12:26:26	15a7	Normal	Normal	86.01	4.9	4.2	2.8	2.1
12:29:39	15b4	Normal	Normal	88.14	5.65	3.39	2.26	0.56
12:32:46	15bf	Normal	Normal	86.45	4.52	3.23	1.29	4.52
12:36:00	15c8	Normal	Normal	91.39	0.48	0.96	1.44	5.74
12:39:30	15f8	Normal	Normal	84.21	8.77	0.58	2.34	4.09
12:42:52	15ff	Normal	Normal	80.84	9.58	1.15	3.83	4.6
12:56:43	16f6	Normal	Normal	86.84	5.26	1.32	2.63	3.95
12:59:57	1772	Normal	Normal	78.26	13.66	1.86	4.35	1.86

14:20:04	177c	Normal	Normal	81.29	10.53	1.75	2.92	3.51
15:00:44	1788	Normal	Normal	86.41	0	3.8	3.8	5.98
15:03:52	178f	Normal	Normal	90.77	1.85	2.21	1.48	3.69
15:06:57	179f	Normal	Normal	87.74	5.35	4.09	1.89	0.94
15:10:19	17a9	Normal	Normal	77.98	11.9	2.38	2.38	5.36
15:13:54	180b	Normal	Normal	90.91	2.42	2.42	0.61	3.64
15:17:03	1812	Normal	Normal	83.1	13.38	0.7	0.7	2.11
15:48:50	181b	Normal	Normal	90.99	0	0.9	1.8	6.31
15:51:48	1825	Normal	Normal	82.08	8.09	0.58	3.47	5.78
15:54:58	1833	Normal	Normal	89.92	0	7.75	0	2.33
15:58:02	183a	Normal	Normal	89.63	0.61	2.44	6.71	0.61
16:01:19	1847	Normal	Normal	94.68	0	1.06	0	4.26
16:04:25	1853	Normal	Normal	80	2.07	0	0	17.93
16:07:26	185c	Normal	Normal	93.1	0	1.15	1.15	4.6
16:10:34	1868	Normal	Normal	83.44	12.27	1.84	1.84	0.61
16:13:48	1872	Normal	Normal	92.68	1.63	0.81	0.81	4.07
16:16:52	187b	Normal	Normal	98.35	0	0	0	1.65
16:20:18	1889	Normal	Normal	97.83	0	0	0	2.17
16:23:33	1893	Normal	Normal	90.68	0	1.69	2.54	5.08
16:26:42	189b	Normal	Normal	95.05	0	0.99	0	3.96
16:29:47	18a7	Normal	Normal	96.91	1.03	0	0	2.06
16:33:08	18b1	Normal	Normal	83.57	9.29	0	1.43	5.71
16:36:08	18b9	Normal	Normal	96.26	0	0.93	0.93	1.87
16:39:26	18c7	Normal	Normal	91.23	1.75	0	2.63	4.39
16:42:27	2840	Normal	Normal	81.84	0	2.56	5.34	10.26
16:45:50	31a5	Normal	Normal	88.19	3.15	1.57	2.36	4.72

Table 5.9 Results of Day 7 Deployment Testing of De-TECH on ValACE using Model 26

Time	Document ID	Results	Classification	Normal	DoS	Bruteforce	Botnet	Infiltration
15:44:16	31b7	Malicious	Infiltration	40	2	0	0	58
15:48:00	31c0	Malicious	Infiltration	41.67	0	0	0	58.33
15:52:24	31cc	Malicious	Infiltration	13.48	1.12	0	0	85.39
15:55:39	31ea	Malicious	Infiltration	12.24	0	0	0	87.76
15:58:46	3.20E+03	Malicious	Infiltration	43.43	0	0	0	56.57
16:08:17	320c	Malicious	Infiltration	33.33	0.85	0	0	65.81
16:15:51	3.22E+03	Malicious	Infiltration	32.35	0	0	0	67.65
16:18:57	3.22E+03	Normal	Normal	72.64	0	0	0	27.36
16:22:06	322f	Malicious	Infiltration	4.1	0.82	0	0	95.08
16:25:27	3.24E+03	Malicious	Infiltration	44.32	0	0	0	55.68
16:28:33	3.24E+03	Malicious	Infiltration	8.86	0	0	0	91.14

16:31:31	3.25E+03	Malicious	Infiltration	3.79	1.52	0	0	94.7
16:34:37	3.26E+03	Malicious	Infiltration	5.43	0	0	0	94.57
16:37:53	3.26E+03	Malicious	Infiltration	9.52	1.9	0	0	88.57
16:40:56	326a	Malicious	Infiltration	3.33	0	0	0	96.67
16:43:57	3.28E+03	Malicious	Infiltration	10.48	0	0	0	89.52
16:47:10	3.28E+03	Malicious	Infiltration	15.04	0.88	0	0	84.07
16:50:12	3.29E+03	Malicious	Infiltration	47.67	1.74	0	0	50.58
16:53:25	3296	Malicious	Infiltration	39.86	0	0	4.47	55.67
16:56:37	32a1	Normal	Normal	54.67	0.27	0	0	45.07
16:59:52	32a9	Malicious	Infiltration	35	0	0	0	65
17:03:00	32b2	Malicious	Infiltration	26.25	0	0	0	73.75
17:06:02	32bf	Malicious	Infiltration	4.65	0	0	0	95.35
17:09:12	32c8	Malicious	Infiltration	37.5	0	0	0	62.5
17:12:19	32d4	Malicious	Infiltration	33.66	0.99	0	0	65.35
17:15:31	32dd	Malicious	Infiltration	7.79	0	0	0	92.21
17:18:31	3.20E+08	Malicious	Infiltration	10.39	1.3	0	0	88.31
17:21:37	32ef	Malicious	Infiltration	41.89	1.35	0	0	56.76
17:24:44	32fe	Malicious	Infiltration	33.2	0	0	1.95	64.84
17:27:52	3308	Malicious	Infiltration	44.25	2.65	0	0	53.1
17:30:59	3310	Malicious	Infiltration	38.27	0	0	0	61.73
17:34:06	331b	Malicious	Infiltration	11.76	0	0	0	88.24
17:37:12	3327	Malicious	Infiltration	13.24	2.94	0	0	83.82
17:40:18	332f	Malicious	Infiltration	12.28	0	0	0	87.72
17:43:38	333a	Malicious	Infiltration	33.9	3.39	0	0	62.71
17:46:49	3342	Malicious	Infiltration	29.03	0	0	0	70.97
17:49:50	3350	Malicious	Infiltration	12	0	0	0	88
17:52:50	3358	Malicious	Infiltration	6.82	0	0	0	93.18
17:55:51	3361	Malicious	Infiltration	30.95	0	0	0	69.05
17:59:10	336e	Malicious	Infiltration	28.99	0	0	0	71.01
18:02:10	3379	Malicious	Infiltration	5.56	0	0	0	94.44
18:05:00	3381	Malicious	Infiltration	43.75	0	0	0	56.25
18:08:19	338e	Normal	Normal	61.05	3.16	0	0	35.79
18:11:20	3397	Malicious	Infiltration	25.93	2.47	0	0	71.6
18:14:26	33a2	Normal	Normal	49.02	1.96	0	0	49.02
18:17:54	33ac	Malicious	Infiltration	14.52	3.23	0	0	82.26
18:20:36	33b5	Malicious	Infiltration	22.73	0	0	0	77.27
18:23:43	33c2	Normal	Normal	88	0	0	0	12
18:27:03	33cc	Malicious	Infiltration	7.69	0	0	0	92.31
18:30:06	33d6	Normal	Normal	50	2.38	0	0	47.92
18:33:05	33df	Malicious	Infiltration	6.67	0	0	0	93.33
18:36:24	33ea	Malicious	Infiltration	20.83	1.04	0	0	78.12
18:39:20	33f3	Malicious	Infiltration	11.58	1.05	0	0	87.37

18:42:21	3400	Malicious	Denial of Service	28.83	55.86	0	0	15.32
18:45:37	3408	Malicious	Infiltration	29.57	0.87	0	0	69.57
18:48:38	3.41E+03	Malicious	Infiltration	16.5	1.94	0	0	81.55
18:51:40	341a	Malicious	Infiltration	19.82	0	0	0	80.18
18:54:46	3429	Malicious	Denial of Service	15.53	51.46	0	0	33.01
18:58:01	3433	Malicious	Infiltration	17.31	0	0	0	82.69
19:01:00	343b	Malicious	Infiltration	13.08	2.8	0	0	84.11
19:04:21	3451	Malicious	Infiltration	20.59	0	0	0	79.41
19:07:21	345b	Malicious	Infiltration	15.46	0	0	0	84.54
19:10:21	3467	Malicious	Denial of Service	17.89	76.84	0	0	5.26
19:13:26	3472	Malicious	Infiltration	34.78	2.17	0	0	63.04
19:16:41	3478	Malicious	Denial of Service	12.24	52.04	0	0	35.71
19:19:41	3484	Malicious	Denial of Service	35.37	59.76	0	0	4.88
19:23:01	3490	Malicious	Denial of Service	31.76	57.65	0	0	10.59
19:26:13	3498	Malicious	Infiltration	15.91	2.27	0	0	81.82
19:29:03	349f	Malicious	Denial of Service	3.41	84.09	0	0	12.5
19:32:21	34ae	Malicious	Denial of Service	10.75	58.06	0	0	31.18
19:35:21	34b8	Malicious	Denial of Service	10.28	52.34	0	0	37.38
19:38:21	34c0	Malicious	Infiltration	34.07	0	0	0	65.93
19:41:41	34cf	Malicious	Infiltration	33.33	0	0	0	66.67
19:44:41	34d6	Malicious	Denial of Service	40.54	56.76	0	0	2.7
19:47:39	3.40E+01	Malicious	Infiltration	25	0	0	0	75
19:50:49	34ec	Malicious	Infiltration	11.54	0	0	0	88.46
19:53:52	34f7	Normal	Normal	50.29	0	0	0	49.71
19:57:01	3501	Malicious	Infiltration	12.96	0	0	0	87.04
20:00:21	350d	Malicious	Denial of Service	29.07	62.79	0	0	8.14
20:03:21	3515	Malicious	Infiltration	31.46	1.12	0	0	67.42
20:06:21	351e	Malicious	Infiltration	28.05	0	0	0	71.95
20:09:41	352a	Malicious	Denial of Service	28.57	61.54	0	0	9.89
20:12:41	3536	Malicious	Denial of Service	31.25	60	0	0	8.75
20:15:39	353d	Malicious	Infiltration	44.64	1.79	0	0	53.57
20:19:02	3545	Malicious	Infiltration	25.81	0	0	0	74.19
20:22:02	3554	Malicious	Infiltration	8.82	0	0	0	91.18

20:25:04	355e	Malicious	Infiltration	6.45	0	0	0	93.55
20:28:14	3567	Normal	Normal	62.86	0	0	0	37.14
20:31:38	3575	Malicious	Denial of Service	19.35	54.84	0	0	25.81
20:34:21	357c	Malicious	Infiltration	20	0	0	0	80
20:37:35	3586	Malicious	Infiltration	11.43	0	0	0	88.57
20:40:42	3593	Malicious	Infiltration	17.14	0	0	0	82.86
20:43:50	359d	Malicious	Denial of Service	22.22	50	0	0	27.78
20:46:49	35a7	Malicious	Infiltration	9.68	0	0	0	90.32
20:49:49	35af	Malicious	Infiltration	10	0	0	0	90
20:52:59	35bb	Malicious	Infiltration	0	0	0	0	100
20:56:05	35c4	Normal	Normal	76.47	0	0	0	23.53
20:59:09	35cf	Malicious	Infiltration	27.03	5.41	0	0	67.57
21:02:15	35db	Malicious	Infiltration	3.7	0	0	0	96.3
21:06:15	3.50E+04	Malicious	Infiltration	3.03	0	0	0	96.97
21:08:58	35ea	Malicious	Infiltration	6.9	0	0	0	93.1
21:11:49	35f8	Normal	Normal	57.78	0	0	0	42.22
21:14:45	3604	Malicious	Infiltration	7.41	0	0	0	92.59
21:17:49	360e	Malicious	Denial of Service	3.57	64.29	0	0	32.14
21:20:59	3618	Malicious	Infiltration	16.67	3.33	0	0	80
21:24:05	3622	Malicious	Denial of Service	3.57	64.29	0	0	32.14
21:27:07	362b	Malicious	Infiltration	3.03	0	0	0	96.97
21:30:19	3638	Malicious	Denial of Service	11.11	66.67	0	0	22.22
21:33:24	3643	Malicious	Infiltration	6.67	0	0	0	93.33
21:36:29	364a	Malicious	Infiltration	12.5	3.12	0	0	84.38
21:39:39	3655	Malicious	Infiltration	0	3.45	0	0	96.55
21:43:10	3660	Normal	Normal	66.67	0	0	0	33.33
21:45:49	366b	Malicious	Infiltration	10	3.33	0	0	86.67
21:48:56	3674	Malicious	Infiltration	11.11	0	0	0	88.89
21:52:05	3681	Malicious	Infiltration	3.23	0	0	0	96.77
21:55:27	3689	Normal	Normal	50.57	0	0	0	49.43
21:58:27	3691	Malicious	Infiltration	46.77	0	0	0	53.23
22:01:25	369d	Normal	Normal	64.18	2.99	0	0	32.84
22:04:29	36a7	Malicious	Infiltration	3.45	0	0	0	96.55
22:07:49	36b0	Malicious	Infiltration	3.45	0	0	0	96.55
22:10:49	36bd	Malicious	Denial of Service	14.29	60.71	0	0	25
22:13:49	36c8	Malicious	Infiltration	3.33	0	0	0	96.67
22:16:59	36d2	Malicious	Infiltration	3.33	0	0	0	96.67

22:20:03	36da	Malicious	Denial of Service	0	62.96	0	0	37.04
22:23:07	3.60E+07	Malicious	Infiltration	6.67	3.33	0	0	90
22:26:09	36ef	Normal	Normal	66.67	0	0	0	33.33
22:29:19	36fa	Malicious	Denial of Service	13.33	60	0	0	26.67
22:32:39	3704	Malicious	Infiltration	4	0	0	0	96
22:35:27	370f	Malicious	Denial of Service	14.81	59.26	0	0	25.93
22:38:39	371b	Malicious	Infiltration	3.7	0	0	0	96.3
22:41:47	3722	Malicious	Infiltration	28.12	0	0	0	71.88
22:44:49	3730	Malicious	Infiltration	0	0	0	0	100
22:48:06	3738	Malicious	Infiltration	0	0	0	0	100
22:51:09	3743	Malicious	Infiltration	3.33	0	0	0	96.67
22:54:06	374d	Malicious	Denial of Service	0	75	0	0	25
22:57:09	3756	Normal	Normal	51.28	0	0	0	48.72
23:00:29	3761	Malicious	Denial of Service	8.33	70.83	0	0	20.83
23:03:18	376a	Malicious	Infiltration	0	0	0	0	100
23:06:39	3776	Malicious	Infiltration	15.62	0	0	0	84.38
23:09:39	377f	Malicious	Infiltration	2.94	0	0	0	97.06
23:12:49	3787	Normal	Normal	80.65	0	0	0	19.35
23:15:49	3794	Malicious	Infiltration	0	0	0	0	100
23:18:49	37a1	Malicious	Infiltration	0	0	0	0	100
23:21:59	37a7	Normal	Normal	76.36	0	0	0	23.64
23:25:09	37b4	Malicious	Infiltration	12.5	0	0	0	87.5
23:28:29	37bc	Normal	Normal	72	0	0	0	28
23:31:24	37c8	Malicious	Infiltration	0	0	0	0	100
23:34:39	37d2	Malicious	DoS	4.55	77.27	0	0	18.18
23:37:29	37dc	Normal	Normal	69.81	0	0	0	30.19
23:40:34	3.70E+09	Malicious	Infiltration	35	0	0	0	65
23:43:49	37f0	Malicious	Infiltration	3.57	0	0	0	96.43
23:46:59	37fc	Malicious	Infiltration	0	0	0	0	100
23:50:06	3807	Malicious	Infiltration	8.33	0	0	0	91.67
23:53:09	3812	Malicious	Infiltration	4.17	0	0	0	95.83
23:56:06	3818	Malicious	Infiltration	0	0	0	0	100
23:59:09	3825	Normal	Normal	57.58	0	0	0	42.42

Table 5.10 Results of Day 8 Deployment Testing of De-TECH on ValACE using Model 26

Time	Document ID	Results	Classification	Normal	DoS	Bruteforce	Botnet	Infiltration
0:02:29	268f	Normal	Normal	74.36	0	0	0	25.64
0:05:19	382f	Normal	Normal	87.23	0	0	0	12.77
0:08:39	3.84E+03	Malicious	Infiltration	4.35	0	0	0	95.65
0:11:49	3.84E+03	Malicious	Infiltration	0	0	0	0	100
0:14:49	3.85E+03	Malicious	Infiltration	8.7	0	0	0	91.3
0:17:59	385a	Malicious	DoS	8	68	0	0	24
0:20:51	3.86E+03	Malicious	Infiltration	0	0	0	0	100
0:23:53	386b	Malicious	Infiltration	4	0	0	0	96
0:27:09	3.88E+03	Normal	Normal	69.23	0	0	0	30.77
0:30:06	3.88E+03	Malicious	Infiltration	4.35	0	0	0	95.65
0:33:19	388c	Malicious	Infiltration	3.85	0	0	0	96.15
0:36:29	3.90E+03	Malicious	Infiltration	0	0	0	0	100
0:39:24	389f	Malicious	Infiltration	4.17	0	0	0	95.83
0:42:39	38ab	Normal	Normal	70.83	0	0	0	29.17
0:45:39	38b7	Malicious	Infiltration	0	0	0	0	100
0:48:49	38be	Malicious	Infiltration	8	0	0	0	92
0:51:59	38c6	Normal	Normal	88.46	0	0	0	11.54
0:54:59	38d3	Malicious	Infiltration	8.7	0	0	0	91.3
0:58:06	38df	Malicious	Infiltration	24.24	0	0	0	75.76
1:01:09	3.80E+08	Malicious	Infiltration	4	0	0	0	96
1:04:06	38f3	Normal	Normal	93.75	0	0	0	6.25
1:07:27	38fd	Normal	Normal	73.08	0	0	0	26.92
1:10:29	3907	Malicious	Infiltration	9.09	0	0	0	90.91
1:13:29	3913	Normal	Normal	72.5	0	0	0	27.5
1:16:29	391b	Malicious	Infiltration	0	3.7	0	0	96.3
1:19:46	3926	Malicious	DoS	4.55	77.27	0	0	18.18
1:22:49	3932	Malicious	Infiltration	4.17	0	0	0	95.83
1:25:59	3939	Malicious	Infiltration	4.76	0	0	0	95.24
1:28:51	3943	Malicious	DoS	14.29	60.71	0	0	25
1:31:59	3950	Malicious	Infiltration	0	0	0	0	100
1:34:59	395a	Malicious	DoS	4.35	73.91	0	0	21.74
1:38:19	3960	Malicious	Infiltration	7.69	0	0	0	92.31
1:41:24	396e	Malicious	Infiltration	0	0	0	0	100
1:44:22	3978	Malicious	Infiltration	4	0	0	0	96
1:47:29	3981	Malicious	Infiltration	0	0	0	0	100
1:50:39	398f	Malicious	Infiltration	8	0	0	0	92
1:53:49	3996	Malicious	Infiltration	4.35	0	0	0	95.65
1:56:49	39a0	Normal	Normal	53.12	0	0	0	46.88
1:59:59	39ad	Malicious	Infiltration	4.76	0	0	0	95.24

2:02:58	39b7	Malicious	Infiltration	3.85	0	0	0	96.15
2:06:09	39c1	Normal	Normal	69.57	0	0	0	30.43
2:09:02	39ca	Normal	Normal	97.67	0	0	0	2.33
2:12:19	39d0	Normal	Normal	63.33	0	0	0	36.67
2:15:24	39df	Malicious	Infiltration	4.55	0	0	0	95.45
2:18:29	3.90E+10	Malicious	DoS	8	68	0	0	24
2:21:25	39f0	Malicious	Infiltration	41.46	0	0	0	58.54
2:24:39	39fc	Malicious	Infiltration	7.69	0	0	0	92.31
2:27:49	3a09	Normal	Normal	65.38	0	0	0	34.62
2:30:49	3a14	Malicious	Infiltration	4	0	0	0	96
2:33:51	3a1b	Malicious	Infiltration	4.17	0	0	0	95.83
2:37:02	3a22	Malicious	Infiltration	8	0	0	0	92
2:40:09	3a32	Malicious	Infiltration	19.23	0	0	0	80.77
2:43:02	3a3c	Malicious	Infiltration	0	0	0	0	100
2:46:19	3a45	Malicious	Infiltration	4	0	0	0	96
2:49:24	3a50	Malicious	Infiltration	8.7	0	0	0	91.3
2:52:21	3a59	Malicious	Infiltration	0	0	0	0	100
2:55:29	3a65	Malicious	Infiltration	4.55	0	0	0	95.45
2:58:39	3a6e	Malicious	Infiltration	30.3	0	0	0	69.7
3:01:49	3a76	Malicious	Infiltration	4	0	0	0	96
3:04:49	3a82	Malicious	Dos	0	73.91	0	0	26.09
3:07:59	3a8f	Malicious	Dos	8.33	70.83	0	0	20.83
3:10:59	3a97	Normal	Normal	81.25	0	0	0	18.75
3:13:58	3aa2	Normal	Normal	92.31	1.92	0	0	5.77
3:17:09	3aad	Malicious	Infiltration	4	0	0	0	96
3:20:19	3ab7	Malicious	Infiltration	4.35	0	0	0	95.65
3:23:24	3ac4	Malicious	Infiltration	4.17	0	0	0	95.83
3:26:21	3acb	Malicious	Infiltration	4	0	0	0	96
3:29:26	3ad5	Normal	Normal	79.17	0	0	0	20.83
3:32:39	3ae0	Malicious	Infiltration	0	0	0	0	100
3:35:49	3aeb	Malicious	Infiltration	4.55	0	0	0	95.45
3:38:49	3af3	Malicious	Infiltration	7.69	0	0	0	92.31
3:41:59	3afb	Malicious	Infiltration	0	0	0	0	100
3:45:02	3b07	Malicious	Infiltration	4.35	0	0	0	95.65
3:48:09	3b14	Malicious	Infiltration	0	0	0	0	100
3:51:02	3b1c	Malicious	Infiltration	3.7	0	0	0	96.3
3:54:19	3b26	Malicious	Infiltration	4.35	0	0	0	95.65
3:57:19	3b31	Malicious	Infiltration	42.31	0	0	0	57.69
4:00:22	3b3c	Malicious	Infiltration	8	0	0	0	92
4:03:29	3b47	Malicious	Infiltration	4	0	0	0	96
4:06:37	3b53	Normal	Normal	69.39	0	0	0	30.61
4:09:49	3b5a	Malicious	Infiltration	8.7	0	0	0	91.3
4:12:59	3b66	Normal	Normal	65.38	0	0	0	34.62

4:15:59	3b71	Normal	Normal	64.29	21.43	0	0	14.29
4:18:52	3b7a	Normal	Normal	83.33	0	0	0	16.67
4:22:09	3b80	Malicious	Infiltration	4.17	0	0	0	95.83
4:25:09	3b8f	Normal	Normal	78.85	0	0	0	21.15
4:28:19	3b99	Malicious	Infiltration	0	0	0	0	100
4:31:19	3ba1	Malicious	Infiltration	0	0	0	0	100
4:34:22	3bb0	Normal	Normal	83.33	0	0	0	16.67
4:37:24	3bb7	Normal	Normal	78.95	0	0	0	21.05
4:40:39	3bc0	Normal	Normal	100	0	0	0	0
4:43:49	3bcd	Normal	Normal	83.78	0	0	0	16.22
4:46:53	3bd5	Malicious	Infiltration	36.67	0	0	0	63.33
4:49:54	3bdf	Normal	Normal	72.22	0	0	0	27.78
4:53:07	3bec	Malicious	Infiltration	0	0	0	0	100
4:57:03	3bf3	Malicious	Infiltration	20	0	0	0	80
4:59:22	3c00	Malicious	Infiltration	0	0	0	0	100
5:03:03	3c07	Normal	Normal	71.41	0	0	0	28.57
5:06:22	3c14	Malicious	Infiltration	16.67	0	0	0	83.33
5:08:19	3c1e	Malicious	Infiltration	0	0	0	0	100
5:11:29	3c25	Malicious	DoS	15.38	69.23	0	0	15.38
5:14:39	3c35	Malicious	Infiltration	4.17	0	0	0	95.83
5:17:49	3c3f	Malicious	Infiltration	0	0	0	0	100
5:20:59	3c47	Malicious	Infiltration	4.55	0	0	0	95.45
5:23:52	3c51	Malicious	Infiltration	0	0	0	0	100
5:27:03	3c5d	Normal	Normal	68.49	0	0	0	31.51
5:30:09	3c66	Malicious	Infiltration	0	4.17	0	0	95.83
5:33:09	3c6f	Malicious	Infiltration	15.38	0	0	0	84.62
5:36:09	3c7b	Malicious	Infiltration	0	0	0	0	100
5:39:19	3c84	Malicious	Infiltration	0	0	0	0	100
5:42:29	3c90	Malicious	Infiltration	3.7	0	0	0	96.3
5:45:29	3c99	Malicious	Infiltration	4.35	0	0	0	95.65
5:48:46	3ca3	Malicious	Infiltration	4	0	0	0	96
5:51:49	3cab	Malicious	DoS	8.7	73.91	0	0	17.39
5:54:46	3cb9	Malicious	Infiltration	0	0	0	0	100
5:57:59	3cc0	Malicious	Infiltration	26.67	0	0	0	73.33
6:01:09	3ccb	Malicious	Infiltration	8.7	0	0	0	91.3
6:03:58	3cd6	Malicious	Infiltration	0	0	0	0	100
6:07:26	3ce1	Malicious	Infiltration	47.27	0	0	0	52.73
6:10:30	3cea	Normal	Normal	51.92	0	0	0	48.08
6:13:19	3cf7	Normal	Normal	82.61	0	0	0	17.39
6:16:29	3cff	Malicious	Infiltration	7.69	0	0	0	92.31
6:19:29	3d08	Normal	Normal	100	0	0	0	0
6:22:46	3d14	Malicious	Infiltration	7.14	0	0	0	92.86
6:25:49	3d20	Normal	Normal	86.21	0	0	0	13.79

6:28:41	3d27	Normal	Normal	84.91	0	0	0	15.09
6:31:49	3d2f	Malicious	Infiltration	7.69	0	0	0	92.31
6:35:09	3d3e	Malicious	Infiltration	0	0	0	0	100
6:38:09	3d48	Malicious	Infiltration	7.69	0	0	0	92.31
6:41:19	3d50	Malicious	Infiltration	4.17	0	0	0	95.83
6:44:19	3d5b	Malicious	Infiltration	0	0	0	0	100
6:47:24	3d66	Malicious	Infiltration	4.17	0	0	0	95.83
6:50:29	3d6f	Malicious	Infiltration	4.55	0	0	0	95.45
6:53:25	3d7a	Malicious	Infiltration	0	0	0	0	100
6:56:46	3d85	Malicious	Infiltration	21.88	0	0	0	78.12
6:59:39	3d8e	Malicious	DoS	0	78.26	0	0	21.74
7:02:49	3d98	Malicious	DoS	31.85	69.23	0	0	26.92
7:05:59	3da4	Malicious	Infiltration	4.35	0	0	0	95.65
7:08:53	3daf	Malicious	Infiltration	45	0	0	0	55
7:12:09	3db4	Normal	Normal	59.46	18.92	0	0	21.62
7:15:05	3dc3	Normal	Normal	85.11	2.13	0	0	12.77
7:18:09	3dcd	Malicious	Infiltration	3.85	0	0	0	96.15
7:21:19	3dd5	Malicious	Infiltration	4	0	0	0	96
7:24:29	3de4	Malicious	Infiltration	38.89	0	0	0	61.11
7:27:29	3deb	Normal	Normal	56.86	0	0	0	43.14
7:30:47	3df6	Malicious	Infiltration	4.35	0	0	0	95.65
7:33:49	3.00E+02	Malicious	Infiltration	0	0	0	0	100
7:36:49	3.00E+08	Malicious	Infiltration	3.85	0	0	0	96.15
7:39:59	3.00E+14	Malicious	DoS	0	77.27	0	0	22.73
7:43:09	3.00E+02	Malicious	DoS	7.69	65.38	0	0	26.92
7:45:59	3.00E+29	Malicious	Infiltration	0	0	0	0	100
7:49:19	3.00E+32	Malicious	Infiltration	4.35	0	0	0	95.65
7:52:19	3e3e	Malicious	Infiltration	4.17	0	0	0	95.83
7:55:24	3.00E+46	Malicious	DoS	8.33	70.83	0	0	20.83
7:58:29	3.00E+53	Malicious	Infiltration	26.32	0	0	0	73.68
8:01:26	3e5c	Normal	Normal	80.56	0	0	0	19.44
8:04:39	3.00E+66	Malicious	Infiltration	0	0	0	0	100
8:07:49	3.00E+70	Malicious	Infiltration	0	0	0	0	100
8:10:48	3e7a	Malicious	Infiltration	0	0	0	0	100
8:13:53	3.00E+84	Normal	Normal	67.86	0	0	0	32.14
8:17:27	3.00E+91	Normal	Normal	57.75	0	0	0	42.25
8:20:13	3e9a	Malicious	Infiltration	46.88	0	0	0	53.12
8:23:11	3ea7	Malicious	Infiltration	43.81	0	0	0	56.19
8:26:24	3eaf	Normal	Normal	62.22	0	0	0	37.78
8:30:15	3eb8	Normal	Normal	77.27	0	0	0	22.73
8:32:37	3ec4	Malicious	Infiltration	16.67	3.33	0	0	80
8:35:39	3ed0	Normal	Normal	64.29	0	0	0	35.71
8:38:47	3ed7	Normal	Normal	73.81	0	0	0	26.19

8:41:49	3edf	Normal	Normal	71.43	0	0	0	28.57
8:45:31	3eee	Malicious	Infiltration	37.5	2.5	0	0	60
8:48:07	3ef5	Malicious	Infiltration	42.59	0	0	0	57.41
8:51:14	3f02	Malicious	Infiltration	19.05	0	0	0	80.95
8:54:13	3f0d	Malicious	Infiltration	8.11	0	0	0	91.89
8:57:34	3f17	Malicious	Infiltration	0	0	0	0	100
9:00:34	3f1f	Malicious	Infiltration	5.56	0	0	0	94.44
9:03:34	3f2a	Normal	Normal	68.63	0	0	0	31.37
9:06:36	3f32	Normal	Normal	56.76	24.42	0	0	18.92
9:09:49	3f41	Malicious	Infiltration	26.09	0	0	0	73.91
9:12:47	3f4b	Malicious	Infiltration	33.33	3.17	0	0	63.49
9:16:07	3f54	Malicious	Infiltration	45.95	0	0	0	54.05
9:19:05	3f5d	Normal	Normal	59.38	0	0	0	40.62
9:22:07	3f72	Normal	Normal	63.87	0	0	0	36.13
9:25:14	3f7c	Malicious	Infiltration	19.23	0	0	0	80.77
9:28:21	3f86	Malicious	Infiltration	27.94	0	0	0	72.06
9:31:28	3f91	Malicious	Infiltration	13.04	0	0	0	86.96
9:34:35	3f9e	Malicious	Infiltration	14.47	0	0	0	85.53
9:37:41	3fa6	Malicious	Infiltration	21.74	0	0	0	78.26
9:40:47	3fb0	Malicious	Infiltration	37.39	0.87	0	0	61.74
9:44:01	3fbc	Malicious	Infiltration	6.35	0	0	0	93.65
9:47:08	3fc7	Malicious	Infiltration	23.42	0	0	0	76.58
9:50:13	3fcf	Malicious	Infiltration	41.38	1.15	0	0	57.47
9:53:13	3fd8	Malicious	Infiltration	42.76	0	0	0	57.24
9:56:22	3fe3	Malicious	Infiltration	33.05	1.69	0	0	65.25
9:59:29	3fef	Malicious	Infiltration	40.4	0	0	0	59.6
10:02:35	3ff8	Malicious	Infiltration	27.97	0.85	0	0	71.19
10:05:42	4003	Malicious	Infiltration	9.2	0	0	0	90.8
10:08:49	400f	Normal	Normal	53.68	0	0	0	46.32
10:12:02	401a	Malicious	Infiltration	38.95	0	0	0	61.05
10:15:03	4023	Malicious	Infiltration	17.58	0	0	0	82.42
10:18:08	402f	Malicious	Infiltration	13.19	1.1	0	0	85.71
10:21:15	4038	Malicious	Infiltration	29.37	0.79	0	0	69.84
10:24:26	4040	Malicious	Infiltration	27.03	0	0	0	72.97
10:27:30	404c	Malicious	Infiltration	30.43	0	0	0	69.57
10:30:37	4058	Malicious	Infiltration	12.15	0.93	0	0	86.92
10:33:43	4062	Malicious	Infiltration	11	2	0	0	87
10:36:50	406b	Malicious	Infiltration	41.01	0.56	0	0	58.43
10:40:06	4076	Malicious	Infiltration	5.21	1.04	0	0	93.75
10:43:09	407f	Malicious	Infiltration	11.01	0	0	0	88.99
10:46:14	408b	Malicious	Infiltration	12.12	2.02	0	0	85.86
10:49:18	4094	Normal	Normal	50.09	0	0	1.73	48.18
10:52:36	409e	Malicious	Infiltration	33.75	3.72	0	4.33	58.2

10:55:49	40a8	Malicious	Infiltration	38.98	0	0	0.34	60.68
10:58:50	40b5	Malicious	Infiltration	40.87	0	0	1.44	57.69
11:02:04	40bf	Malicious	Infiltration	43.37	0	0	1.28	55.36
11:05:25	76f5	Normal	Normal	50.88	0.88	0	0	48.25
11:08:55	7.10E+05	Malicious	Infiltration	48.39	0.14	0	1.4	50.07
11:11:55	7701	Normal	Normal	56.72	0	0	1.71	41.58

Table 5.11 Results of Day 9 Deployment Testing of De-TECH on UITC using Model 26

Time	Document ID	Results	Classification	Normal	DoS	Bruteforce	Botnet	Infiltration
16:21:08	76f6	Malicious	Infiltration	34.92	1.59	2.38	0	61.11
16:24:20	7.70E+03	Malicious	Infiltration	25.83	0.66	0	0	73.51
16:24:15	770a	Malicious	Infiltration	47.2	0	0	1.24	51.55
16:27:33	7.72E+03	Malicious	Infiltration	46.85	0.9	0	0	52.25
16:30:40	7.72E+03	Malicious	Infiltration	20.37	0	1.85	0	77.78
16:33:51	7.73E+03	Malicious	Infiltration	42.86	0	0	0	57.14
16:37:01	773c	Malicious	Infiltration	46.62	0	0	0	53.38
16:40:08	7.75E+03	Malicious	Infiltration	32.04	0	1.94	0	66.02
16:43:17	7.76E+03	Malicious	Infiltration	9.68	0	0	0	90.32
16:46:28	775e	Malicious	Infiltration	42.86	0	0	0	57.14
16:49:35	7.77E+03	Malicious	Infiltration	36.56	0	2.15	0	61.29
16:52:45	7.77E+03	Malicious	Infiltration	46.39	0	2.06	0	51.55
16:55:56	777f	Malicious	Infiltration	23.08	0	0	0	76.92
16:59:06	778d	Malicious	Infiltration	31.58	0	0	0	68.42
17:02:09	7.80E+03	Malicious	Infiltration	21.43	0	2.38	0	76.19
17:05:28	77a5	Normal	Normal	61.63	0	1.16	0	37.21
17:08:29	77ae	Malicious	Infiltration	47.37	0	2.63	0	50
17:11:38	77b9	Malicious	Infiltration	27.83	0	0.87	0	71.3
17:14:50	77c2	Malicious	Infiltration	15.66	1.2	1.2	0	81.93
17:18:00	77d2	Normal	Normal	52.22	0	2.22	0	45.56
17:21:03	77dd	Malicious	Infiltration	22.35	0	2.35	0	75.29
17:24:14	7.70E+07	Normal	Normal	62.28	0	0	0	37.72
17:27:21	77f4	Normal	Normal	62.07	1.15	1.15	0	35.63
17:30:31	77fd	Normal	Normal	59.46	0	2.7	0	37.84
17:33:38	780c	Normal	Normal	58.02	0	0	0	41.98
17:36:47	7814	Malicious	Infiltration	45.3	0	0	0	54.7
17:39:56	7822	Normal	Normal	65.17	2.25	4.49	0	28.09
17:43:08	782a	Malicious	Infiltration	42.86	0	1.3	0	55.84
17:46:12	7838	Malicious	Infiltration	28.89	1.11	0	0	70
17:49:22	7843	Malicious	Infiltration	43.97	0	0	0	56.03
17:52:31	784c	Malicious	Infiltration	25	0	0	0	75

17:55:31	785a	Normal	Normal	65.48	0	1.19	0	33.33
17:58:52	7867	Malicious	Infiltration	24.18	0	0	0	75.82
18:01:57	786f	Malicious	Infiltration	35.61	1.52	0	0.76	62.12
18:05:07	787d	Malicious	Infiltration	16.25	0	0	0	83.75
18:08:13	7888	Normal	Normal	70	0	2.5	0	27.5
18:11:22	7895	Malicious	Infiltration	41.41	0	0.78	0	57.81
18:14:33	789e	Normal	Normal	68.6	0	0	0	31.4
18:17:40	78a9	Malicious	Infiltration	38.3	0	0	0	61.7
18:20:49	78b1	Normal	Normal	49.21	0	1.59	0	49.21
18:23:59	78c2	Normal	Normal	51.11	0	0	0	48.89
18:27:04	78cd	Malicious	Infiltration	36.84	1.32	0	0	61.84
18:30:13	78d7	Malicious	Infiltration	36.84	2.63	2.63	0	57.89
18:33:23	7.80E+03	Normal	Normal	51.52	3.03	1.52	0	43.94
18:36:33	78ee	Malicious	Infiltration	43.75	2.08	0	0	54.17
18:39:38	78f7	Malicious	Infiltration	21.05	0	1.32	0	77.63
18:42:45	7906	Malicious	Infiltration	44.74	0	2.63	0	52.63
18:45:54	7912	Malicious	Infiltration	44.9	2.04	0	0	53.06
18:49:01	791e	Malicious	Infiltration	40.91	0	0	0	59.09
18:52:12	7926	Malicious	Infiltration	41.27	0	1.59	0	57.14
18:55:16	7933	Malicious	Infiltration	45.95	0	2.7	0	51.35
18:58:26	793e	Malicious	Infiltration	45.31	0	0	1.56	53.12
19:01:36	7948	Malicious	Infiltration	45.95	0	2.7	0	51.35
19:04:43	7952	Malicious	Infiltration	47.22	0	2.78	0	50
19:07:49	7960	Malicious	Infiltration	45.71	0	0	0	54.29
19:10:57	796c	Malicious	Infiltration	40.82	0	0	0	59.18
19:14:07	7.98E+03	Malicious	Infiltration	30.95	0	2.38	0	66.67
19:17:18	7982	Malicious	Infiltration	44.74	0	0	0	55.26
19:20:22	798d	Normal	Normal	50	0	2.17	0	47.83
19:23:33	7998	Malicious	Infiltration	34.29	0	0	0	65.71
19:26:39	79a5	Malicious	Infiltration	39.62	3.77	1.89	0	54.72
19:29:48	79ae	Malicious	Infiltration	42.86	0	2.86	0	54.29
19:32:55	79bb	Malicious	Infiltration	41.18	0	0	0	58.82
19:36:05	79c5	Malicious	Infiltration	44	0	2	0	54
19:39:16	79d2	Malicious	Infiltration	46.51	0	2.33	0	51.16
19:42:20	79de	Normal	Normal	50	0	0	0	50
19:45:27	7.90E+09	Normal	Normal	49.15	0	1.69	1.69	47.46
19:48:38	79f3	Malicious	Infiltration	37.84	0	0	1.35	60.81
19:51:48	79ff	Normal	Normal	51.52	0	1.52	0	46.97
19:54:59	7a0c	Malicious	Infiltration	44.74	0	0	0	55.26
19:58:00	7a13	Malicious	Infiltration	42.86	0	1.79	1.79	53.57
20:01:10	7a21	Normal	Normal	48.28	0	1.72	1.72	48.28
20:04:20	7a2c	Malicious	Infiltration	48.84	0	0	0	51.16
20:07:29	7a39	Malicious	Infiltration	39.39	0	3.03	0	57.58

20:10:33	7a46	Malicious	Infiltration	45.1	0	1.96	0	52.94
20:13:44	7a4e	Malicious	Infiltration	41.86	0	0	0	58.14
20:16:51	7a5a	Malicious	Infiltration	47.83	0	2.17	0	50
20:20:01	7a67	Normal	Normal	53.49	0	2.33	0	44.19
20:23:10	7a71	Malicious	Infiltration	37.14	0	0	0	62.86
20:26:16	7a7f	Normal	Normal	57.14	0	0	0	42.86
20:29:27	7a88	Malicious	Infiltration	29.73	0	5.41	0	64.86
20:32:38	7a93	Malicious	Infiltration	32.14	0	0	0	67.86
20:35:49	7a9f	Malicious	Infiltration	44.44	0	0	0	55.56
20:38:52	7aac	Malicious	Infiltration	37.5	0	0	0	62.5
20:42:00	7ab5	Malicious	Infiltration	30.77	0	0	0	69.23
20:45:11	7ac2	Malicious	Infiltration	26.67	0	0	0	73.33
20:48:21	7acd	Malicious	Infiltration	39.29	0	0	0	60.71
20:51:31	7ad9	Malicious	Infiltration	37.5	0	0	0	62.5
20:54:35	7ae3	Malicious	Infiltration	40.62	0	0	0	59.38
20:57:43	7af1	Malicious	Infiltration	38.46	0	0	0	61.54
21:00:54	7afc	Malicious	Infiltration	34.62	0	0	0	65.38
21:04:02	7b05	Malicious	Infiltration	29.03	0	0	0	70.97
21:07:06	7b10	Malicious	Infiltration	37.5	0	0	0	62.5
21:10:15	7b1d	Malicious	Infiltration	38.24	0	0	0	61.76
21:13:24	7b28	Normal	Normal	57.69	0	0	0	42.31
21:16:31	7b33	Malicious	Infiltration	34.62	0	0	0	65.38
21:19:39	7b41	Malicious	Infiltration	29.73	0	0	0	70.27
21:22:49	7b4c	Malicious	Infiltration	43.59	0	0	0	56.41
21:25:55	7b58	Malicious	Infiltration	38.89	0	0	0	61.11
21:29:04	7b61	Malicious	Infiltration	48.15	0	0	0	51.85
21:32:15	7b6d	Normal	Normal	54.17	0	0	0	45.83
21:35:22	7b7a	Malicious	Infiltration	38.17	0	0	0	61.29
21:38:33	7b86	Malicious	Infiltration	20.69	0	0	0	79.31
21:41:44	7b8e	Malicious	Infiltration	33.33	0	0	0	66.67
21:44:49	7b97	Malicious	Infiltration	30.43	0	0	0	69.57
21:47:58	7ba7	Malicious	Infiltration	40.74	0	0	0	59.26
21:51:07	7baf	Malicious	Infiltration	32.14	3.57	0	0	64.29
21:54:17	7bbd	Malicious	Infiltration	44.44	0	0	0	55.56
21:57:27	7bc8	Malicious	Infiltration	46.15	0	0	0	53.85
22:00:35	7bd3	Malicious	Infiltration	37.14	0	0	0	62.86
22:03:46	7be1	Malicious	Infiltration	32	4	0	0	64
22:06:56	7beb	Malicious	Infiltration	18.18	4.55	0	0	77.27
22:09:59	7bf6	Malicious	Infiltration	34.62	0	0	0	65.38
22:13:09	7bfe	Malicious	Infiltration	28.57	0	0	0	71.43
22:16:19	7c0d	Malicious	Infiltration	39.62	0	0	0	60.38
22:19:29	7c16	Malicious	Infiltration	25.49	0	0	0	74.51
22:22:35	7c25	Malicious	Infiltration	33.33	0	0	0	66.67

22:25:52	7c2e	Malicious	Infiltration	19.39	0	0	0	80.61
22:28:56	7c3a	Malicious	Infiltration	22.95	3.28	0	0	73.77
22:32:07	7c45	Malicious	Infiltration	30	0	3.33	0	66.67
22:35:11	7c52	Malicious	Infiltration	21.21	3.03	0	0	75.76
22:38:22	7c5d	Malicious	Infiltration	22.81	0	0	0	77.19
22:41:33	7c66	Malicious	Infiltration	18.33	0	0	0	81.67
22:44:37	7c73	Normal	Normal	60.71	0	0	0	39.29
22:47:46	7c7f	Malicious	Infiltration	46.43	0	0	0	53.57
22:50:56	7c8c	Malicious	Infiltration	38.46	0	0	0	61.54
22:54:07	7c94	Malicious	Infiltration	34.62	3.85	0	0	61.54
22:57:18	7ca1	Malicious	Infiltration	22.86	0	0	0	77.14
23:00:18	7cad	Malicious	Infiltration	27.27	0	0	0	72.73
23:03:28	7cb8	Malicious	Infiltration	44.44	0	0	0	55.56
23:06:38	7cc5	Malicious	Infiltration	14.81	0	0	0	85.19
23:09:48	7cd1	Malicious	Infiltration	31.25	0	0	0	68.75
23:12:54	7cdc	Malicious	Infiltration	34.62	0	0	0	65.38
23:16:04	7ce6	Malicious	Infiltration	43.48	0	0	0	56.52
23:19:09	7cf2	Malicious	Infiltration	24.14	0	0	0	75.86
23:22:19	7cff	Malicious	Infiltration	44	0	0	0	56
23:25:26	7d08	Malicious	Infiltration	36.67	0	0	0	63.33
23:28:35	7d12	Malicious	Infiltration	20.69	0	0	0	79.31
23:31:45	7d1e	Malicious	Infiltration	46.43	0	0	0	53.57
23:34:51	7d2c	Malicious	Infiltration	41.86	0	0	0	58.14
23:38:00	7d34	Malicious	Infiltration	42.86	0	0	0	57.14
23:41:10	7d3e	Malicious	Infiltration	20	0	0	0	80
23:44:19	7d4d	Malicious	Infiltration	25.81	0	0	0	74.19
23:47:26	7d57	Malicious	Infiltration	44.44	0	0	0	55.56
23:50:34	7d61	Malicious	Infiltration	21.74	0	0	0	73.91
23:53:41	7d6e	Normal	Normal	52	0	0	0	48
23:56:52	7d7c	Normal	Normal	52.17	0	0	0	47.83
23:59:57	7d85	Malicious	Infiltration	30.3	0	0	0	69.7
0:03:07	7d91	Malicious	Infiltration	16.67	0	0	0	83.33
0:06:16	7d9d	Malicious	Infiltration	31.25	0	0	0	68.75
0:09:22	7da6	Malicious	Infiltration	30	0	0	0	66.67
0:12:32	7db5	Malicious	Infiltration	29.63	0	0	0	70.37
0:15:38	7dc1	Malicious	Infiltration	37.5	0	0	0	62.5
0:18:49	7dca	Malicious	Infiltration	23.08	0	0	0	76.92
0:21:58	7dd5	Malicious	Infiltration	35.71	0	0	0	64.29
0:25:03	7de2	Malicious	Infiltration	45.83	3.33	0	0	54.17
0:28:13	7ded	Malicious	Infiltration	44.44	0	0	0	55.56
0:31:23	7df9	Malicious	Infiltration	32.26	0	0	0	67.74
0:34:28	7.00E+03	Malicious	Infiltration	19.23	0	0	0	80.77
0:37:39	7e0f	Malicious	Infiltration	22.58	0	0	0	77.42

0:40:44	7.00E+19	Malicious	Infiltration	28	0	0	0	72
0:43:54	7.00E+26	Normal	Normal	52	0	0	0	48
0:47:02	7.00E+32	Malicious	Infiltration	16.67	0	0	0	83.33
0:50:12	7e3c	Malicious	Infiltration	48.15	0	0	0	51.85
0:53:20	7.00E+46	Malicious	Infiltration	28	0	0	0	72
0:56:31	7.00E+53	Malicious	Infiltration	33.33	0	0	0	66.67
0:59:35	7e5d	Malicious	Infiltration	46.15	0	0	0	53.85
1:02:44	7e6b	Malicious	Infiltration	23.08	0	0	0	76.92
1:05:53	7.00E+77	Malicious	Infiltration	38.46	0	0	0	61.54
1:09:08	E+80	Malicious	Infiltration	25	7.14	0	0	67.86
1:12:15	7e8f	Normal	Normal	50	0	0	0	50
1:15:26	E+98	Malicious	Infiltration	40.74	0	0	0	59.26
1:18:31	7ea3	Malicious	Infiltration	18.18	4.55	0	0	77.27
1:21:42	7ead	Malicious	Infiltration	48.15	0	0	0	51.85
1:24:52	7ebb	Malicious	Infiltration	28	0	0	0	72
1:27:56	7ec7	Normal	Normal	48	4	0	0	48
1:31:05	7ece	Malicious	Infiltration	20	0	0	0	80
1:34:12	7edd	Malicious	Infiltration	36.36	4.55	0	0	59.09
1:37:23	7ee8	Malicious	Infiltration	20.83	0	4.17	0	75
1:40:28	7ef3	Malicious	Infiltration	28	0	0	0	72
1:43:37	7f00	Normal	Normal	50	0	0	0	50
1:46:46	7f0c	Malicious	Infiltration	26.67	0	0	0	73.33
1:49:57	7f15	Normal	Normal	53.85	0	0	0	46.15
1:53:08	7f1e	Malicious	Infiltration	38.46	0	0	0	61.54
1:56:17	7f2d	Malicious	Infiltration	26.67	0	0	0	73.33
1:59:23	7f3a	Malicious	Infiltration	18.18	0	0	0	81.82
2:02:28	7f43	Malicious	Infiltration	21.74	0	0	0	78.26
2:05:38	7f51	Malicious	Infiltration	35.71	0	0	0	64.29
2:08:46	7f5c	Malicious	Infiltration	33.33	0	0	0	66.67
2:11:55	7f66	Malicious	Infiltration	32.14	0	0	0	67.86
2:15:05	7f6c	Malicious	Infiltration	11.54	0	0	0	88.46
2:18:15	7f7d	Normal	Normal	50	0	0	0	50
2:21:19	7f88	Malicious	Infiltration	30.56	0	0	0	69.44
2:24:30	7f93	Malicious	Infiltration	20.83	0	0	0	79.17
2:27:40	7f9f	Malicious	Infiltration	34.48	0	0	0	65.52
2:30:48	7fac	Malicious	Infiltration	20.83	0	0	0	79.17
2:33:58	7fb4	Malicious	Infiltration	39.29	0	0	0	60.71
2:37:05	7fc0	Malicious	Infiltration	20	4	0	0	76
2:40:16	7fcd	Malicious	Infiltration	35.48	0	0	0	60.71
2:43:23	7fd7	Malicious	Infiltration	26.92	0	0	0	76
2:46:34	7fe5	Malicious	Infiltration	36.36	0	0	0	72.08
2:49:38	7ff1	Malicious	Infiltration	34.62	0	0	0	63.64
2:55:56	7ff9	Malicious	Infiltration	32.14	3.57	0	0	64.29

3:11:42	8006	Malicious	Infiltration	48.15	0	0	0	51.85
3:11:42	800e	Malicious	Infiltration	48.15	0	0	0	51.85
2:59:08	8025	Malicious	Infiltration	17.24	0	0	0	82.76
2:59:08	8030	Malicious	Infiltration	17.24	0	0	0	82.76
3:17:30	803c	Normal	Normal	57.69	3.85	0	0	38.46
3:20:38	8049	Malicious	Infiltration	20	0	0	0	80
3:23:48	8054	Malicious	Infiltration	44	0	0	0	56
3:26:59	805f	Malicious	Infiltration	24	0	0	0	76
3:30:03	8069	Malicious	Infiltration	40	0	0	0	60
3:33:11	8075	Malicious	Infiltration	24.14	0	0	0	75.86
3:36:20	807e	Malicious	Infiltration	32.14	0	0	0	67.86
3:39:33	808c	Malicious	Infiltration	23.33	0	0	0	76.67
3:42:44	8099	Malicious	Infiltration	24	0	0	0	76
3:45:51	80a4	Malicious	Infiltration	46.63	0	0	0	53.57
3:49:01	80af	Malicious	Infiltration	19.35	0	0	0	80.65
3:52:11	80bc	Malicious	Infiltration	30.3	0	0	0	69.7
3:55:18	80c5	Malicious	Infiltration	36	0	0	0	64
3:58:25	80cf	Malicious	Infiltration	26.92	3.85	0	0	69.23
4:01:39	80dd	Malicious	Infiltration	33.33	0	0	0	66.67
4:04:47	8.00E+09	Malicious	Infiltration	20.69	0	0	0	79.31
4:07:58	80f1	Normal	Normal	57.69	0	0	0	42.31
4:11:02	80ff	Malicious	Infiltration	31.03	0	0	0	68.97
4:14:12	810b	Malicious	Infiltration	34.62	0	0	0	65.38
4:17:22	8114	Malicious	Infiltration	16.67	4.17	0	0	79.17
4:20:32	8122	Malicious	Infiltration	26.09	0	4.35	0	69.57
4:23:42	812b	Malicious	Infiltration	21.88	0	0	0	78.12
4:26:52	8139	Malicious	Infiltration	33.33	0	0	0	66.67
4:29:58	8141	Malicious	Infiltration	40	0	0	0	60
4:33:06	814f	Malicious	Infiltration	20.69	0	0	0	79.31
4:36:17	8158	Malicious	Infiltration	44	0	0	0	56
4:39:24	8167	Malicious	Infiltration	25	0	0	0	75
4:42:33	8173	Malicious	Infiltration	14.29	0	0	0	85.71
4:45:43	817d	Malicious	Infiltration	38.46	0	0	0	61.54
4:48:51	8187	Normal	Normal	52.46	0	0	0	47.54
4:52:04	8194	Malicious	Infiltration	49.06	0	0	0	50.94
4:55:13	819f	Malicious	Infiltration	36.11	0	0	0	63.89
4:58:24	81ad	Malicious	Infiltration	35.29	0	0	0	64.71
5:01:35	81b5	Malicious	Infiltration	44.44	0	0	0	55.56
5:04:43	81c2	Malicious	Infiltration	34.78	0	0	0	65.22
5:07:53	81ce	Malicious	Infiltration	38.71	0	0	0	61.29
5:10:58	81d7	Malicious	Infiltration	21.88	0	0	0	78.12
5:14:09	8.10E+05	Malicious	Infiltration	32.43	0	0	0	67.57
5:17:19	81ef	Malicious	Infiltration	36.67	0	0	0	63.33

5:20:24	81f8	Malicious	Infiltration	40	2.22	0	0	57.78
5:23:34	8207	Malicious	Infiltration	45	0	0	0	55
5:26:44	8213	Malicious	Infiltration	38.46	0	0	0	61.54
5:29:54	821e	Normal	Normal	50	0	0	0	50
5:33:05	822a	Malicious	Infiltration	33.33	0	0	0	66.67
5:36:16	8236	Malicious	Infiltration	27.27	0	0	0	72.73
5:39:20	823f	Malicious	Infiltration	26.67	6.67	0	0	66.67
5:42:29	824a	Malicious	Infiltration	44.12	0	0	0	55.88
5:45:39	8254	Malicious	Infiltration	28.12	0	0	0	71.88
5:48:48	8261	Normal	Normal	50	0	0	0	50
5:51:54	826e	Malicious	Infiltration	43.33	0	0	0	56.67
5:55:02	8276	Malicious	Infiltration	39.47	0	0	0	60.53
5:58:13	8285	Malicious	Infiltration	27.27	0	0	0	72.73
6:01:24	828f	Malicious	Infiltration	44.83	0	0	0	55.17
6:04:29	8299	Malicious	Infiltration	42.11	0	0	0	57.89
6:07:39	82a5	Malicious	Infiltration	38.1	0	0	0	61.9
6:10:49	82b3	Malicious	Infiltration	29.58	0	0	0	70.42
6:13:59	82bf	Malicious	Infiltration	47.46	3.39	0	0	49.15
6:17:12	82c9	Malicious	Infiltration	19.23	0	0	0	80.77
6:20:20	82d4	Malicious	Infiltration	38.3	2.13	0	0	59.57
6:23:31	82df	Malicious	Infiltration	46.15	0	0	0	53.85
6:26:42	82eb	Malicious	Infiltration	19.23	0	0	0	80.77
6:29:52	82f8	Normal	Normal	53.85	3.85	0	0	42.31
6:32:57	8304	Malicious	Infiltration	44.44	0	0	0	55.56
6:36:04	830d	Malicious	Infiltration	35.71	0	0	0	64.29
6:39:17	831b	Malicious	Infiltration	15.38	0	0	0	84.62
6:42:26	8327	Malicious	Infiltration	27.59	0	0	0	72.41
6:45:33	832f	Normal	Normal	50	0	0	0	50
6:48:41	833c	Malicious	Infiltration	43.48	0	0	0	56.52
6:51:51	ba33	Malicious	Infiltration	36.36	0	0	0	63.64
6:55:02	ba46	Malicious	Infiltration	39.47	2.63	0	0	57.89

Table 5.12 Results of Testing Model 20 (Ibraheem, Hypertuned) using Generated Traffic

	Actual Testing	Results	Classification	Normal	DoS	Brute-force	Bot-net	Infiltration
DoS	DOS	Normal	Normal	100	0	0	0	0
	dos2	Normal	Normal	100	0	0	0	0
	dos3	Normal	Normal	100	0	0	0	0
	dos4	Normal	Normal	100	0	0	0	0
	dos5	Normal	Normal	100	0	0	0	0
	dos6	Normal	Normal	100	0	0	0	0
	dos7	Normal	Normal	100	0	0	0	0
	dos8	Normal	Normal	100	0	0	0	0

	dos9	Malicious	Botnet	1.64	0	0	98.36	0
	dos10	Normal	Normal	100	0	0	0	0
New DoS	newdos1	Normal	Normal	98.7	0	0	0	1.3
	newdos2	Malicious	Botnet	0.66	0	0	99.01	0.33
	newdos3	Normal	Normal	99.67	0	0	0	0.33
	newdos4	Normal	Normal	99.67	0	0	0	0.33
	newdos5	Normal	Normal	98.7	0	0.65	0	0.65
	newdos6	Normal	Normal	100	0	0	0	0
	newdos7	Normal	Normal	100	0	0	0	0
	newdos8	Normal	Normal	99.67	0	0	0	0.33
	newdos9	Normal	Normal	99.67	0	0	0	0.33
	newdos10	Normal	Normal	100	0	0	0	0
Infiltration	INFIL	Malicious	Botnet	40	0	16.67	43.33	0
	infil2	Normal	Normal	46.67	0	20	33.33	0
	infil3	Malicious	Botnet	20	0	0	45.71	34.29
	infil4	Normal	Normal	76.92	0	15.38	7.69	0
	infil5	Malicious	Botnet	20	0	17.14	45.71	17.14
	infil6	Malicious	Botnet	41.38	0	17.24	41.38	0
	infil7	Malicious	Botnet	41.67	0	16.67	41.67	0
	infil8	Malicious	Botnet	41.67	0	16.67	41.67	0
	infil9	Malicious	Botnet	20.59	0	20.59	41.18	17.65
	infil10	Normal	Normal	55.17	0	17.24	27.59	0
Bruteforce	BRUTEFORCE	Malicious	Botnet	4.49	0	0.22	94.16	1.12
	brute2	Malicious	Botnet	18.73	0	2.12	79.15	0
	brute3	Malicious	Botnet	4.88	0	1.95	93.17	0
	brute4	Malicious	Botnet	5.63	0	0	91.06	3.31
	brute5	Malicious	Botnet	4.07	0	0.54	95.39	0
	brute6	Malicious	Botnet	2.35	0	0	91.18	6.47
	brute7	Malicious	Botnet	3.66	0	0.3	96.04	0
	brute8	Malicious	Botnet	3.14	0	0	96.86	0
	brute9	Malicious	Botnet	4.18	0	0.35	95.47	0
	brute10	Malicious	Botnet	3.39	0	0.23	93.91	2.48
Botnet	botnet1	Normal	Normal	45.71	3.57	0	25.71	25
	botnet2	Malicious	Botnet	48.93	0	0.68	49.58	0.81
	botnet3	Malicious	Botnet	20	0	0	40	40
	botnet4	Malicious	Botnet	14.44	0.7	0	81.34	3.52
	botnet5	Malicious	Botnet	36.36	0	0	59.09	4.55
Normal	normal1	Normal	Normal	100	0	0	0	0
	normal2	Normal	Normal	100	0	0	0	0
	normal3	Normal	Normal	100	0	0	0	0
	normal4	Normal	Normal	100	0	0	0	0
	normal5	Normal	Normal	100	0	0	0	0
	normal6	Normal	Normal	100	0	0	0	0
	normal7	Normal	Normal	75	0	0	0	25
	normal8	Normal	Normal	100	0	0	0	0
	normal9	Normal	Normal	100	0	0	0	0
	normal10	Normal	Normal	100	0	0	0	0
New Normal	NOR1	Normal	Normal	75	0	0	0	25
	NOR2	Normal	Normal	100	0	0	0	0
	NOR3	Normal	Normal	75	0	0	0	25
	NOR4	Normal	Normal	100	0	0	0	0
	NOR5	Normal	Normal	100	0	0	0	0
	NOR6	Normal	Normal	66.67	0	0	33.33	0

	NOR7	Normal	Normal	100	0	0	0	0
	NOR8	Normal	Normal	100	0	0	0	0
	NOR9	Normal	Normal	100	0	0	0	0
	NOR10	Normal	Normal	100	0	0	0	0

Table 5.13 Confusion Matrix and Performance Results of Model 20
(Ibraheem, Hypertuned) using Generated Traffic

DE-TECH TESTING						
Model Name:	"20-IBRAHEEM-hypertuned-newEnsemble_model.pkl"					
[Testing]	[Results]		Total			
	Normal	Malicious		Accuracy	66%	
Normal	20	0	20	Precision	48%	
Malicious	22	23	45	Recall	100%	
Total	42	23	65	F1-score	65%	

Table 5.14 Results of Testing Model 26 using Generated Traffic

	Actual Testing	Results	Classification	Normal	DoS	Brute-force	Bot-net	Infiltration
Infiltration	INFIL	Normal	Normal	56.67	0	0	0	43.33
	infil2	Normal	Normal	66.67	0	0	0	33.33
	infil3	Normal	Normal	60	2.86	0	0	37.14
	infil4	Normal	Normal	69.23	3.85	0	0	26.92
	infil5	Normal	Normal	57.14	0	0	0	42.86
	infil6	Normal	Normal	82.76	0	0	0	17.24
	infil7	Normal	Normal	58.33	0	0	0	41.67
	infil8	Normal	Normal	62.5	0	0	0	37.5
	infil9	Normal	Normal	64.71	0	0	0	35.29
	infil10	Normal	Normal	75.86	0	0	0	24.14
Bruteforce	BRUTEFORCE	Malicious	Infiltration	2.02	0.9	0	0	97.08
	brute2	Malicious	Infiltration	4.95	2.83	0	0	92.23
	brute3	Malicious	Infiltration	0	0	0	0	100
	brute4	Malicious	Infiltration	4.64	0.66	0	0	94.7
	brute5	Malicious	Infiltration	0.54	0.27	0	0	99.19
	brute6	Malicious	Infiltration	2.94	0.29	0	0	96.76
	brute7	Malicious	Infiltration	8.23	0	0	0	91.77
	brute8	Malicious	Infiltration	9.02	0	0	0	90.98
	brute9	Malicious	Infiltration	6.97	0.35	0	0	92.68
	brute10	Malicious	Infiltration	2.03	0.68	0	0	97.29
Botnet	botnet1	Normal	Normal	79.29	0	0	1.43	19.29
	botnet2	Malicious	Infiltration	1.62	0	0	0	98.38
	botnet3	Normal	Normal	80	0	0	0	20
	botnet4	Malicious	Infiltration	23.24	0	0	0	76.76
	botnet5	Malicious	Infiltration	45.45	0	0	0	54.55
Normal	normal1	Normal	Normal	50	0	0	0	50
	normal2	Normal	Normal	71.43	0	0	0	28.57
	normal3	Normal	Normal	71.43	0	0	0	28.57
	normal4	Normal	Normal	71.43	0	0	0	28.57
	normal5	Normal	Normal	71.43	0	0	0	28.57
	normal6	Normal	Normal	100	0	0	0	0
	normal7	Normal	Normal	50	25	0	0	25
	normal8	Normal	Normal	100	0	0	0	0
	normal9	Normal	Normal	100	0	0	0	0

	normal10	Normal	Normal	100	0	0	0	0
New Normal	NOR1	Normal	Normal	75	0	0	0	25
	NOR2	Normal	Normal	71.43	0	0	0	28.57
	NOR3	Normal	Normal	75	0	0	0	25
	NOR4	Normal	Normal	71.43	0	0	0	28.57
	NOR5	Normal	Normal	66.67	0	0	0	33.33
	NOR6	Normal	Normal	77.78	0	0	0	22.22
	NOR7	Normal	Normal	75	0	0	0	25
	NOR8	Normal	Normal	100	0	0	0	0
	NOR9	Normal	Normal	100	0	0	0	0
	NOR10	Normal	Normal	100	0	0	0	0
NEW DOS 2	dos1	Normal	Normal	100	0	0	0	0
	dos2	Malicious	Infiltration	30.6	0	0	0	69.4
	dos3	Normal	Normal	61.66	1.61	23.86	2.14	10.72
	dos4	Normal	Normal	56.1	2.44	0	0	41.46
	dos5	Malicious	DOS	26.79	34.45	32.06	0	6.7
	dos6	Normal	Normal	82.32	0	0	0	17.68
	dos7	Normal	Normal	88.35	0	0	0	11.65
	dos8	Normal	Normal	50	0	0	0	50
	dos9	Normal	Normal	70.21	0.5	0	0	29.29
	dos10	Malicious	Infiltration	39.69	0	0	0	60.31
	dos11	Normal	Normal	50	0	0	0	50
	dos12	Normal	Normal	50	0	0	0	50
	dos13	Malicious	Infiltration	42.86	0.39	0.04	0	56.71
	dos14	Normal	Normal	59.79	0	0	0	40.21
	dos15	Normal	Normal	38.42	27.05	0	0	34.54
	dos16	Malicious	Infiltration	15.52	1.72	4.02	0	78.74
	dos17	Normal	Normal	78.85	0.51	0.05	0	20.59
	dos18	Normal	Normal	100	0	0	0	0
	dos19	Malicious	Infiltration	0.07	0	0	0	99.93

Table 5.15 Confusion Matrix and Performance Results of Model 26 using Generated Traffic

DE-TECH TESTING						
Model Name:	'26-Ensemble_model_multi_class.pkl'					
[Testing]	[Results]		Total	Performance Results		
	Normal	Malicious		Accuracy	60.94%	
Normal	20	0	20	Precision	44.44%	
Malicious	25	19	44	Recall	100.00%	
Total	45	19	64	F1-score	61.54%	

Table 5.16 Results of Testing Model 39 (reduced 50-50, Linear Regression-Hypertuned) using Generated Traffic

	Actual Testing	Results	Classification	Normal	DoS	Brute-force	Bot-net	Infiltration
DoS	DOS	Normal	Normal	100	0	0	0	0
	dos2	Normal	Normal	100	0	0	0	0
	dos3	Normal	Normal	100	0	0	0	0
	dos4	Normal	Normal	100	0	0	0	0
	dos5	Normal	Normal	100	0	0	0	0
	dos6	Normal	Normal	100	0	0	0	0
	dos7	Normal	Normal	100	0	0	0	0

	dos8	Normal	Normal	100	0	0	0	0
	dos9	Normal	Normal	100	0	0	0	0
	dos10	Normal	Normal	100	0	0	0	0
New DoS	newdos1	Malicious	Botnet	0	0	0	100	0
	newdos2	Malicious	Botnet	0	0	0	99.34	0.66
	newdos3	Normal	Normal	99.67	0	0	0	0.33
	newdos4	Malicious	Botnet	0	0	0	99.67	0.33
	newdos5	Malicious	Botnet	0.65	0	0	98.38	0.97
	newdos6	Malicious	Botnet	0	0	0	100	0
	newdos7	Normal	Normal	100	0	0	0	0
	newdos8	Normal	Normal	99.67	0	0	0	0.33
	newdos9	Normal	Normal	99.67	0	0	0	0.33
	newdos10	Normal	Normal	100	0	0	0	0
Infiltration	INFIL	Malicious	Bruteforce	20	0	50	26.67	3.33
	infil2	Malicious	Bruteforce	36.67	0	40	20	3.33
	infil3	Malicious	Bruteforce	22.86	0	51.43	25.71	0
	infil4	Malicious	Bruteforce	3.85	0	46.15	50	0
	infil5	Malicious	Bruteforce	22.86	0	51..43	25.71	0
	infil6	Malicious	Bruteforce	24.14	0	51.72	24.14	0
	infil7	Malicious	Bruteforce	20.83	0	50	25	4.17
	infil8	Malicious	Bruteforce	25	0	50	25	0
	infil9	Malicious	Bruteforce	17.65	0	41.18	38.24	2.94
	infil10	Malicious	Bruteforce	17.24	0	51.72	24.14	6.9
Bruteforce	BRUTEFORCE	Malicious	Botnet	0	0	4.72	95.28	0
	brute2	Malicious	Botnet	0	0	13.43	86.57	0
	brute3	Malicious	Botnet	0	0	3.41	96.59	0
	brute4	Malicious	Botnet	0.66	0	6.95	92.38	0
	brute5	Malicious	Botnet	0	0	3.25	96.75	0
	brute6	Malicious	Botnet	0.59	0	7.06	92.35	0
	brute7	Malicious	Botnet	0	0	2.74	97.26	0
	brute8	Malicious	Botnet	1.18	0	2.35	96.08	0.39
	brute9	Malicious	Botnet	0	0	3.83	96.17	0
	brute10	Malicious	Botnet	0	0	4.51	95.49	0
Botnet	botnet1	Malicious	Infiltration	11.43	0	10.71	38.57	39.29
	botnet2	Malicious	Botnet	39.15	0	0.92	50.43	9.5
	botnet3	Malicious	Botnet	40	0	20	40	0
	botnet4	Normal	Normal	46.48	0	11.27	11.27	30.99
	botnet5	Malicious	Botnet	27.27	0	9.09	59.09	4.55
Normal	normal1	Normal	Normal	100	0	0	0	0
	normal2	Malicious	Botnet	42.86	0	0	57.14	0
	normal3	Malicious	Botnet	42.86	0	0	57.14	0
	normal4	Malicious	Botnet	42.86	0	0	57.14	0
	normal5	Malicious	Botnet	42.86	0	0	57.14	0
	normal6	Normal	Normal	100	0	0	0	0
	normal7	Normal	Normal	50	0	0	25	25
	normal8	Normal	Normal	100	0	0	0	0
	normal9	Normal	Normal	100	0	0	0	0
	normal10	Normal	Normal	100	0	0	0	0
New Normal	NOR1	Malicious	Botnet	25	0	0	75	0
	NOR2	Malicious	Botnet	28.57	0	0	71.43	0
	NOR3	Malicious	Botnet	25	0	0	75	0
	NOR4	Malicious	Botnet	42.86	0	0	57.14	0
	NOR5	Malicious	Botnet	33.33	0	0	66.67	0

	NOR6	Malicious	Botnet	22.22	0	0	66.67	11.11
	NOR7	Normal	Normal	50	0	0	50	0
	NOR8	Normal	Normal	100	0	0	0	0
	NOR9	Normal	Normal	100	0	0	0	0
	NOR10	Normal	Normal	100	0	0	0	0
NEW DOS 2	dos1	Normal	Normal	99.54	0	0	0	0.46
	dos2	Normal	Normal	44.07	0	0	36.62	19.31
	dos3	Malicious	Infiltration	42.63	0	0	13.4	43.97
	dos4	Malicious	Botnet	21.95	0	0	65.85	12.2
	dos5	Malicious	Infiltration	13.88	0	41.15	18.18	26.79
	dos6	Normal	Normal	42.69	0	0	40.77	16.55
	dos7	Normal	Normal	55.56	0	0	0	44.44
	dos8	Malicious	Botnet	30	0	0	60	10
	dos9	Malicious	Botnet	0.03	0	0	99.97	0
	dos10	Normal	Normal	62.66	0	0	24.66	12.68
	dos11	Malicious	Botnet	16.67	0	0	66.67	16.67
	dos12	Malicious	Infiltration	37.5	0	0	12.5	50
	dos13	Normal	Normal	61.51	0	0	14.35	24.14
	dos14	Normal	Normal	60.95	0	0	23.56	15.49
	dos15	Malicious	Infiltration	29.12	0	0	16.46	54.41
	dos16	Malicious	Botnet	8.05	0	0	75	16.95
	dos17	Malicious	Botnet	0.04	0	0	99.96	0
	dos18	Normal	Normal	98.22	0	0	0	1.78
	dos19	Malicious	Botnet	41.3	0	0	53.94	4.76

Table 5.17 Confusion Matrix and Performance Results of Model 39
(reduced 50-50, Linear Regression-Hypertuned) using Generated Traffic

DE-TECH TESTING					
Model Name:	'reduced-39-LR-5050-hypertuned-newEnsemble_model.pkl'				
[Testing]	[Results]		Total	Accuracy	70.31%
	Normal	Malicious			
Normal	10	10	20	Precision	52.63%
Malicious	9	35	44	Recall	50.00%
Total	19	45	64	F1-score	51.28%

Table 5.18 Functionality Evaluation of each Respondents

Evaluator	Functionality			
	Suitability	Accurateness	Interoperability	Security
Project Evaluator No. 1	4	4	4	3
Project Evaluator No. 2	4	4	4	4
Project Evaluator No. 3	4	5	4	3
Project Evaluator No. 4	5	4	4	4
Project Evaluator No. 5	4	4	4	4
Project Evaluator No. 6	4	4	5	5
Project Evaluator No. 7	4	4	5	3

Table 5.19 Reliability Evaluation of each Respondents

Evaluator	Reliability		
	Maturity	Fault Tolerance	Recoverability
Project Evaluator No. 1	4	4	4
Project Evaluator No. 2	4	4	4
Project Evaluator No. 3	4	4	3
Project Evaluator No. 4	5	4	4
Project Evaluator No. 5	4	3	3
Project Evaluator No. 6	5	4	4
Project Evaluator No. 7	4	3	5

Table 5.20 Usability Evaluation of each Respondents

Evaluator	Usability			
	Understandability	Learnability	Operability	Attractiveness
Project Evaluator No. 1	2	2	4	3
Project Evaluator No. 2	4	4	4	4
Project Evaluator No. 3	4	3	4	3
Project Evaluator No. 4	4	3	4	5
Project Evaluator No. 5	4	4	4	5
Project Evaluator No. 6	4	5	5	4
Project Evaluator No. 7	3	5	5	3

Table 5.21 Efficiency Evaluation of each Respondents

Evaluator	Efficiency	
	Time Behaviour	Resource Utilisation
Project Evaluator No. 1	5	4
Project Evaluator No. 2	4	4
Project Evaluator No. 3	4	4
Project Evaluator No. 4	4	5
Project Evaluator No. 5	4	4
Project Evaluator No. 6	4	5
Project Evaluator No. 7	4	4

Table 5.22 Maintability Evaluation of each Respondents

Evaluator	Maintability			
	Analsability	Changeability	Stability	Testability
Project Evaluator No. 1	4	3	3	3
Project Evaluator No. 2	4	4	4	4
Project Evaluator No. 3	3	3	4	4
Project Evaluator No. 4	4	4	4	5
Project Evaluator No. 5	4	3	3	3
Project Evaluator No. 6	3	5	5	4
Project Evaluator No. 7	4	3	4	3

Table 5.23 Portability Evaluation of each Respondents

Evaluator	Portability			
	Adaptability	Installability	Conformance	Replaceability
Project Evaluator No. 1	3	3	3	3
Project Evaluator No. 2	4	4	4	4
Project Evaluator No. 3	3	4	3	3
Project Evaluator No. 4	3	5	4	3
Project Evaluator No. 5	3	3	4	3
Project Evaluator No. 6	5	5	4	4
Project Evaluator No. 7	3	5	4	5

Table 5.24 All Characteristics Evaluation of each Respondents

Evaluator	All Characteristics
	Compliance
Project Evaluator No. 1	3
Project Evaluator No. 2	4
Project Evaluator No. 3	4
Project Evaluator No. 4	5
Project Evaluator No. 5	3
Project Evaluator No. 6	4
Project Evaluator No. 7	3



Ranah Mae M. Caseria

CONTACT

Phone: 09184983051

Email: caseria.ranah@gmail.com

Address: Putatan, Muntinlupa City

Birthday: September 6, 2001

TECHNICAL SKILLS

- Basic Python Programming
- Basic JavaScript Programming
- Circuit Design and Analysis
- Web Development

PERSONAL SKILLS

- Problem-Solving
- Coding
- Flexible and Adaptable
- Copywriting
- Time Management

CONTACT REFERENCE

Engr. Jay Fel C. Quijano

Research Coordinator

TUP – Manila

jayfel_quijano@tup.edu.ph

CAREER OBJECTIVE

A competent person who has a good work ethic. I consistently put my best effort to accomplishing a task. I am trained in programming languages like MATLAB, allowing me to use this tool for data analysis and problem-solving. Additionally, I am familiar at utilizing PowerPoint to create powerful presentations and have experience with using Excel for data analysis and manipulation.

EDUCATION

2020 - Present **Bachelor of Science in Electronics and Communications Engineering**

Technological University of the Philippines - Manila
Ayala Blvd, Ermita, Manila, 1000 Metro Manila

2018 - 2020 **Science, Technology, Engineering and Mathematics (STEM)**

SouthernSide Montessori School
Katihan Rd, Poblacion, Muntinlupa, 63017 Metro Manila

2014 - 2018 **Junior High School**

Muntinlupa Cosmopolitan School
1 National Road, Putatan, Muntinlupa, 1772 Metro Manila

2008 - 2014 **Elementary School**

Living Light Academy
Mercury Street, Nuwhrain Village, Bruger Subdivision, Putatan, Muntinlupa, 1772 Metro Manila

ACHIEVEMENTS

2020 **MSD SCHOLAR**

A scholarship student of the Muntinlupa Scholarship Division (MSD)

2020 **With Honors**

SouthernSide Montessori School

2014 – 2018 **Honorable Mention**

Muntinlupa Cosmopolitan School

2008 – 2014 **Honorable Mention**

Living Light Academy

AFFILIATIONS AND RESPONSIBILITIES

Member

Technological University of the Philippines Manila - Organization of Electronics Engineering Students (TUP-OECES)
Ermita, Manila
2020-2024

WORK EXPERIENCE

Intern

ITISI

Jovan Condominium Building, Samat, Mandaluyong, Metro Manila
2023

Work Immersion

Creotec Philippines Inc.

117 Technology Ave, Laguna Technopark, Biñan, 4020 Laguna
2019

SEMINARS AND TRAININGS ATTENDED

2024	5G in the Philippines: Tech Deployment and Dev Drivers Technological University of the Philippines
2024	AI and Cybersecurity: Foundations and Promise Technological University of the Philippines
2024	EPIC Series: Practical Opamps Circuit Analysis Technological University of the Philippines
2024	Building Regulations Compliances and Data Privacy for ECE Technological University of the Philippines
2024	Securing Intellectual Property: A Comprehensive Guide Technological University of the Philippines
2024	Fostering Creativity and Collaboration: Robotics Education Technological University of the Philippines
2024	Crafting your pitch deck to attract investors Technological University of the Philippines
2024	Cybersecurity: Beyond Hacking Technological University of the Philippines
2024	Gusto ko sa Telco, Sa'n ako patungo? Technological University of the Philippines
2024	Introduction to Large Language Models Technological University of the Philippines
2024	Empowering Modern Infrastructure: The Crucial Role of ECEs in Building Auxilliary Systems Technological University of the Philippines
2024	Data Science Unwired: The Spark of ECE in Data Science Technological University of the Philippines



Khylla Krizel S. Delos Reyes

CONTACT

Phone: 0993723346

Email: khyllakrizeldelosreyes@gmail.com

Address: Tambo, Parañaque City

Birthday: September 25, 2002

TECHNICAL SKILLS

- Basic Python Programming
- Basic Arduino Programming
- Circuit Design and Analysis
- PCB Design

PERSONAL SKILLS

- Problem-Solving
- Clerical Support
- Flexible and Adaptable
- Interpersonal Skills
- Time Management

CONTACT REFERENCE

Engr. Jay Fel C. Quijano

Research Coordinator

TUP – Manila

jayfel_quijano@tup.edu.ph

CAREER OBJECTIVE

Current student with a hunger for real-world experience. Thrives in meeting deadlines, both solo and on a team. Reliable and eager to learn, ready to contribute to your company's growth. My strong work ethic and quick learning abilities ensure I'll be an asset from day one.

EDUCATION

2020 - Present **Bachelor of Science in Electronics and Communications Engineering**

Technological University of the Philippines - Manila
Ermita, Manila

2018 - 2020 **Science, Technology, Engineering and Mathematics (STEM)**

University of Perpetual Help DALTA
Alabang– Zapote Rd, Las Piñas

2014 - 2018 **Junior High School**

Parañaque National High School Baclaran
Baclaran, Paranaque City

2012 - 2014 **Elementary School**

Tambo Elementary School – MAIN
NAIA Rd. Tambo, Parañaque

ACHIEVEMENTS

2020 **First Year – First Semester Dean's Lister**
Technological University of the Philippines - Manila

2020 **With Honors**

University of Perpetual Help DALTA

2018 **With Honors**

Parañaque National High School Baclaran

2014 **6th Honorable Mention**

Tambo Elementary School - Main

AFFILIATIONS AND RESPONSIBILITIES

Member

Technological University of the Philippines Manila - Organization of Electronics Engineering Students (TUP-OECES)
Ermita, Manila
2020-2024

WORK EXPERIENCE

Intern

NOW Telecom
España Blvd, Sampaloc,
Manila
2023

SEMINARS AND TRAININGS ATTENDED

2024	5G in the Philippines: Tech Deployment and Dev Drivers Technological University of the Philippines
2024	AI and Cybersecurity: Foundations and Promise Technological University of the Philippines
2024	EPIC Series: Practical Opamps Circuit Analysis Technological University of the Philippines
2024	Building Regulations Compliances and Data Privacy for ECE Technological University of the Philippines
2024	Securing Intellectual Property: A Comprehensive Guide Technological University of the Philippines
2024	Fostering Creativity and Collaboration: Robotics Education Technological University of the Philippines
2024	Crafting your pitch deck to attract investors Technological University of the Philippines
2024	Cybersecurity: Beyond Hacking Technological University of the Philippines/
2024	Gusto ko sa Telco, Sa'n ako patungo? Technological University of the Philippines
2024	Introduction to Large Language Models Technological University of the Philippines
2024	Empowering Modern Infrastructure: The Crucial Role of ECEs in Building Auxilliary Systems Technological University of the Philippines
2024	Data Science Unwired: The Spark of ECE in Data Science Technological University of the Philippines



Aliah Fhae A. Felipe

CONTACT

Phone: 09183413998

Email: aliahfelipe@gmail.com

Address: Meycauayan, Bulacan

Birthday: June 15, 2001

TECHNICAL SKILLS

- Basic Python Programming
- Basic Arduino Programming
- Web Development
- Database Design and Modeling
- Querying and Optimization
- Development and Integration

PERSONAL SKILLS

- Problem Solving
- Clerical Support
- Flexible and Adaptable
- Interpersonal Skills
- Time Management

CONTACT REFERENCES

Engr. Jay Fel C. Quijano

Research Coordinator

TUP – Manila

jayfel_quijano@tup.edu.ph

Napoleon Pastor

Philippine Orthopedic Center

09183415809

Khryzzanne Kyle Constatino

Reed Elsevier Shared Services

09174547444

CAREER OBJECTIVE

An independent and responsible employee who received numerous honors and awards for both academic and extra-curricular activities, and who is excellent in communication skills and proved the ability to juggle multiple high priority tasks. Who also proved that there is always new learnings in anything you do and loves to make progress and difference.

EDUCATION

2020 – Present	Technological University of the Philippines - Manila Bachelor of Science in Electronics Engineering (BSECE)
2018 - 2020	University of the East - Manila With Honors
2014 - 2018	Quezon City Academy Junior High School With Honors
2012 - 2014	San Francisco Elementary School Elementary 5 th Honorable Mention

ACHIEVEMENTS

2020 - Present	Dean's Lister Technological University of the Philippines – Manila
2021	Outstanding Freshman Award Technological University of the Philippines – Manila

AFFILIATIONS AND RESPONSIBILITIES

Graduation Ball Coordinator	GradHawks: Graduation Committee Technological University of the Philippines – Manila 2024
Member	OECES (Organization of Electronics Engineering Students) Technological University of the Philippines – Manila Ermita, Manila 2020-2024

WORK EXPERIENCE

Intern	NOW Telecom España Blvd, Sampaloc, Manila 2023
--------	---

SEMINARS AND TRAININGS ATTENDED

- 2024 **Data Science Unwired: The Spark of ECE in Data Science**
Technological University of the Philippines
- 2024 **Empowering Modern Infrastructure: The Crucial Role of ECEs in Building Auxiliary Systems**
Technological University of the Philippines
- 2024 **Introduction to Large Language Models**
Technological University of the Philippines
- 2024 **Gusto ko sa Telco, Sa'n ako patungo?**
Technological University of the Philippines
- 2024 **Cybersecurity: Beyond Hacking**
Technological University of the Philippines
- 2024 **Crafting your Pitch Deck to Attract Investors**
Technological University of the Philippines
- 2024 **Fostering Creativity and Collaboration: Robotics Education**
Technological University of the Philippines
- 2024 **Securing Intellectual Property: A Comprehensive Guide**
Technological University of the Philippines
- 2024 **Building Regulations Compliances and Data Privacy for ECE**
Technological University of the Philippines
- 2024 **EPIC Series: Practical Opamps Circuit Analysis**
Technological University of the Philippines
- 2024 **AI and Cybersecurity: Foundations and Promise**
Technological University of the Philippines
- 2024 **5G in the Philippines: Tech Deployment and Dev Drivers**



Judiel A. Isaias

CONTACT

Phone: 09085182171
Email: judielisaias@gmail.com
Address: Phase 3, Package 1, Block 26, Lot excess, Bagong Silang, Caloocan City
Birthday: December 30, 2002

TECHNICAL SKILLS

- Basic Python Programming
- MS Office Applications
- Basic Arduino Programming
- Basic Skill in PCB and Circuit Designing
- Basic Raspberry pi Programming

PERSONAL SKILLS

- Multi-Tasking
- Flexible and Adaptable
- Problem Solving
- Time Management
- Critical Thinking

CONTACT REFERENCE

Engr. Jay Fel C. Quijano
Research Coordinator
TUP – Manila
jayfel_quijano@tup.edu.ph

CAREER OBJECTIVE

As a highly motivated Electronics Engineering student, I aim to leverage my technical skills and practical experience in innovative projects, continuously enhancing my knowledge while making a meaningful impact on the organization. Passionate about combining traditional and advanced technologies, I am committed to delivering exceptional support and advancing technology to improve user experiences.

EDUCATION

2020 - Present	Bachelor of Science in Electronics and Communications Engineering Technological University of the Philippines - Manila Ermita, Manila
2018 - 2020	Science, Technology, Engineering and Mathematics (STEM) Mystical Rose School of Caloocan Inc. BLK 1 LT 15 Ilang Ilang St. Almar Subd. 177, Caloocan City
2014 - 2018	Junior High School Bagong Silang High School Phase 3, Bagong Silang, Caloocan City
2012 - 2014	Elementary School Silanganan Elementary School Phase3, Bagong Silang, Caloocan City

ACHIEVEMENTS

2018	With Honors Bagong Silang High School
-------------	---

AFFILIATIONS AND RESPONSIBILITIES

Member	Technological University of the Philippines Manila - Organization of Electronics Engineering Students (TUP-OECES) Ermita, Manila 2020-2024
Member	Institute of Electronics Engineers of the Philippines (IECEP) Manila 2020-2021

WORK EXPERIENCE

Intern

Firestop Philippines Construction Corp.
fort palm spring condominium unit 8d, 8th floor, 1st ave, cor 30th St, Taguig, Metro Manila

SEMINARS AND TRAININGS ATTENDED

2024	5G in the Philippines: Tech Deployment and Dev Drivers Technological University of the Philippines
2024	AI and Cybersecurity: Foundations and Promise Technological University of the Philippines
2024	EPIC Series: Practical Opamps Circuit Analysis Technological University of the Philippines
2024	Building Regulations Compliances and Data Privacy for ECE Technological University of the Philippines
2024	Securing Intellectual Property: A Comprehensive Guide Technological University of the Philippines
2024	Fostering Creativity and Collaboration: Robotics Education Technological University of the Philippines
2024	Crafting your pitch deck to attract investors Technological University of the Philippines
2024	Cybersecurity: Beyond Hacking Technological University of the Philippines/
2024	Gusto ko sa Telco, Sa'n ako patungo? Technological University of the Philippines
2024	Introduction to Large Language Models Technological University of the Philippines
2024	Empowering Modern Infrastructure: The Crucial Role of ECEs in Building Auxilliary Systems Technological University of the Philippines
2024	Data Science Unwired: The Spark of ECE in Data Science Technological University of the Philippines



Aila Marie S. Pengson

CONTACT

Phone: 09480129276
Email: pengsonaila@gmail.com
Address: San Mateo, Rizal
Birthday: January 28, 2002

TECHNICAL SKILLS

- Basic Python Programming
- Basic Java Script Programming
- PCB Design
- Web Development

PERSONAL SKILLS

- Digital Illustration and Drawing
- Problem Solving Skill
- Conceptualization and Copywriting
- Photography and Editing
- Flexible and Adaptable

CONTACT REFERENCE

Engr. Jay Fel C. Quijano
Research Coordinator
TUP – Manila
jayfel_quijano@tup.edu.ph

CAREER OBJECTIVE

A competent engineering student who displays a strong work ethic and put all-out effort in accomplishing the work tasks. Creative in her own way. Proficient with PowerPoint, Word on a computer, and some familiarity with Excel, etc.

EDUCATION

2020 - Present	Bachelor of Science in Electronics and Communications Engineering Technological University of the Philippines Ermita, Manila
2018 - 2020	Science, Technology, Engineering and Mathematics (STEM) Pamantasan ng Lungsod ng Marikina (PLMar) Rainbow St. cor. Russet St., SSS Village, Concepcion Dos, Marikina City, Metro Manila
2014 - 2018	Junior High School San Mateo National High School (SMNHS) 491 GSIS Road, 1, San Mateo, Rizal
2012 - 2014	Elementary School Dulong Bayan Elementary School 210 G. Alberto Street, Dulongbayan I, San Mateo, Rizal

ACHIEVEMENTS

2020	With Honor Pamantasan ng Lungsod ng Marikina (PLMar)
2018	Completer With Honor San Mateo National High School
2014	Honorable Mention Dulong Bayan Elementary School

AFFILIATIONS AND RESPONSIBILITIES

Member	Technological University of the Philippines Manila - Organization of Electronics Engineering Students (TUP-OECES) Ermita, Manila 2020-2024
--------	---

WORK EXPERIENCE

Student Assistant	Barangay Hall Malanday, San Mateo, Rizal May-June 2019
--------------------------	---

Intern	Infinity Technosys Innovation Solution Inc. Unit 610, Jovan Condominium Building, Samat, Mandaluyong, Metro Manila 2023
---------------	--

SEMINARS AND TRAININGS ATTENDED

- 2024 5G in the Philippines: Tech Deployment and Dev Drivers**
Technological University of the Philippines
- 2024 AI and Cybersecurity: Foundations and Promise**
Technological University of the Philippines
- 2024 EPIC Series: Practical Opamps Circuit Analysis**
Technological University of the Philippines
- 2024 Building Regulations Compliances and Data Privacy for ECE**
Technological University of the Philippines
- 2024 Securing Intellectual Property: A Comprehensive Guide**
Technological University of the Philippines
- 2024 Fostering Creativity and Collaboration: Robotics Education**
Technological University of the Philippines
- 2024 Crafting your pitch deck to attract investors**
Technological University of the Philippines
- 2024 Cybersecurity: Beyond Hacking**
Technological University of the Philippines/
- 2024 Gusto ko sa Telco, Sa'n ako patungo?**
Technological University of the Philippines
- 2024 Introduction to Large Language Models**
Technological University of the Philippines
- 2024 Empowering Modern Infrastructure: The Crucial Role of ECEs
in Building Auxiliary Systems**
Technological University of the Philippines
- 2024 Data Science Unwired: The Spark of ECE in Data Science**
Technological University of the Philippines



Mary Grace C. Ponciano

CONTACT

Phone: 09602023435

Email: poncianomarygrace@gmail.com

Address: B21 L29 Hamilton Homes,
Bucandala I, Imus City, Cavite

Birthday: May 24, 2002

TECHNICAL SKILLS

- Python Programming
- Spreadsheets
- Arduino

PERSONAL SKILLS

- Problem Solving Skills
- Analytical Skills
- Team Player

CONTACT REFERENCE

Marvin J. Ponciano

IT Director | Project Management –
Corporate Applications
TaskUs
09171305584

CAREER OBJECTIVE

Seeking for an opportunity that will allow me to use my technical expertise and innovative perspectives in the field of electronics engineering, and one that will allow me to develop my career and make a significant contribution to the company.

EDUCATION

2020 - Present Bachelor of Science in Electronics and Communications Engineering

Technological University of the Philippines
Ermita, Manila

2018 - 2020 Program

Benedictine Institute of Learning
Address
Abad Homes, 177 General Yengco St, Medicion, Imus, 4103 Cavite

ACHIEVEMENTS

2023 Academic Achiever

Technological University of the Philippines - Manila

2022 Academic Achiever

Technological University of the Philippines - Manila

2021 Academic Achiever

Technological University of the Philippines - Manila

2020 DOST Merit Scholar

AFFILIATIONS AND RESPONSIBILITIES

Secretary OECES – Graduating Class Division

Technological University of the Philippines - Manila
2023-2024

Secretary General OECES

Technological University of the Philippines - Manila
2022-2023

Member Developments Lead GDSC TUP Manila

TUP Manila
2022-2023

Member IECEP-MSC

Manila
2022-2024

WORK EXPERIENCE

Intern DFI Retail Group

Ortigas Center, Pasig City, Philippines
2023

Learner Creotec Philippines

17 Technology Ave, Laguna Technopark, Biñan, 4024
Laguna
2019

SEMINARS AND TRAININGS ATTENDED

- 2024 5G in the Philippines: Tech Deployment and Dev Drivers**
Technological University of the Philippines
- 2024 AI and Cybersecurity: Foundations and Promise**
Technological University of the Philippines
- 2024 EPIC Series: Practical Opamps Circuit Analysis**
Technological University of the Philippines
- 2024 Building Regulations Compliances and Data Privacy for ECE**
Technological University of the Philippines
- 2024 Securing Intellectual Property: A Comprehensive Guide**
Technological University of the Philippines
- 2024 Fostering Creativity and Collaboration: Robotics Education**
Technological University of the Philippines
- 2024 Crafting your pitch deck to attract investors.**
Technological University of the Philippines
- 2024 Cybersecurity: Beyond Hacking**
Technological University of the Philippines/
- 2024 Gusto ko sa Telco, Sa'n ako patungo?**
Technological University of the Philippines
- 2024 Introduction to Large Language Models**
Technological University of the Philippines
- 2024 Empowering Modern Infrastructure: The Crucial Role of ECEs
in Building Auxiliary Systems**
Technological University of the Philippines
- 2024 Data Science Unwired: The Spark of ECE in Data Science**
Technological University of the Philippines