CHRISLAND UNIVERSITY

AWARD FOR BEST PROJECT IN THE DEPARTMENT OF CYBER SECURITY

PRESENTED TO

OLAWOYIN JOSEPH

CLU200222-594

FOR 2023/2024 SESSION

DONATED BY:
PROFESSOR ISAAC ODUN-AYO

CHRISLAND UNIVERSITY

Intellectual Radiance

PROF. ODUN-AYO'S PRIZE

2023/2024 ACADEMIC SESSION

AWARD

Certificate

This Certificate is presented to

Oluwatoyin Joseph

In Recognition of Being the

BEST GRADUATING STUDENT IN CYBERSECURITY

Dated this 29th Day of October, 2024

OLAWOYIN JOSEPH
Product Management Job Simulation

Certificate of Completion

December 13th, 2024

Over the period of December 2024, OLAWOYIN JOSEPH has completed practical tasks in:

Understand key performance indicators
Plan a data-driven presentation

Tom Brunskill
CEO, Co-Founder of
Forage

OLAWOYIN JOSEPH
Cybersecurity Virtual Experience Program

Certificate of Completion

September 22nd, 2022

Over the period of August 2022 to September 2022, OLAWOYIN JOSEPH has completed practical tasks in:

Design a phishing email simulation
Interpret phishing simulation results

Tom Brunskill
CEO, Co-Founder of Forage
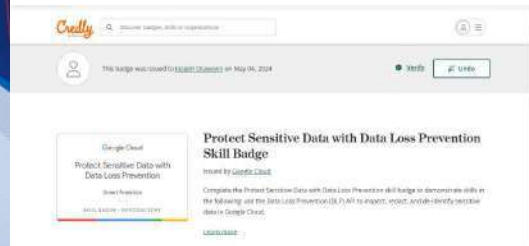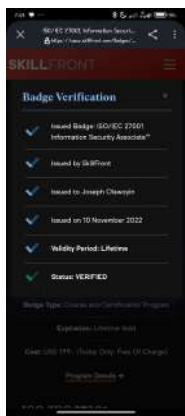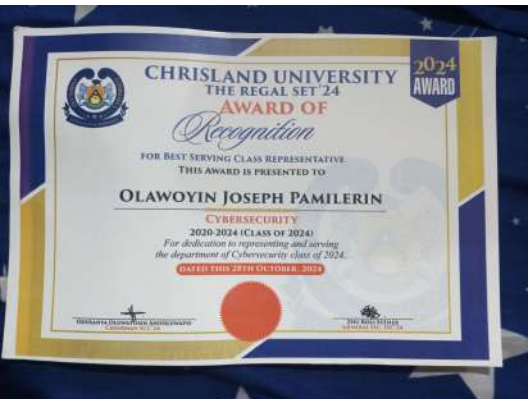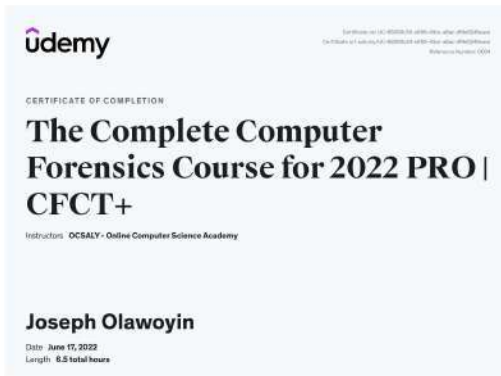
Google Cloud

This acknowledges that

Joseph Olawoyin

has successfully completed all the requirements to be recognized as a

Google Cloud Certified
Professional Cloud Security Engineer

Series ID: 11177
Issued Date: Jun 08, 2024
Expiration Date: Jun 08, 2026
ID: cf85efc16af541a68177325bd417f752
Certified As: Joseph Olawoyin

Thomas Kurian
CEO, Google Cloud

EC-Council

Certification Number
ECC5948162307

CEH Certified Ethical Hacker

This is to acknowledge that

Joseph Olawoyin

has successfully completed all requirements and criteria for

Certified Ethical Hacker

certification through examination administered by EC-Council

Issue Date: 31 August, 2024   Expiry Date: 30 August, 2027

ANAB ACCREDITED
PERSONAL CERTIFICATION BODY

Sanjay Bavisi, President

Qualys.

Joseph Olawoyin
Chrisland University

has successfully completed the following course and passed the certification exam.

Vulnerability Management Detection Response

Date Completed: FEBRUARY 25, 2021
Course Hours: 5.0

Qualys Certified Specialists can deploy, operate and monitor the Qualys Cloud Platform to implement, manage and protect IT systems, devices and web applications.

Sumedh Thakar
Vice President, Cloud Engineering Support

919 E Hillsdale Blvd, 4th Floor, Foster City, CA 94404 USA   www.qualys.com

QUALYS CERTIFIED SPECIALIST

CERTIFICATE OF COMPLETION

This is to certify that

Olawoyin Joseph

has completed

Counterintelligence Awareness
and Reporting Course for DOD

March 13, 2024

Heather Mardaga
Director, CDSE

EC-Council

Certificate of Attendance

THIS IS TO ACKNOWLEDGE THAT

Joseph olawoyin

HAS SUCCESSFULLY COMPLETED THE FOLLOWING
ACADEMIA SERIES COURSE ON

CEHv12 - Complete Series (Volumes 1 through 4)

THROUGH A REGISTERED EC-COUNCIL ACADEMIA
PARTNERED INSTITUTION

Chrisland University

724104   Aug 30, 2024
CERTIFICATE NUMBER   DATE

Sanjay Bavisi, President

You can verify authenticity of this certificate by visiting
https://aspen.eccouncil.org/VerifyEval

CERTIFICATE OF COMPLETION

This certifies that

OLAWOYIN JOSEPH

has completed Detection Engineering for Beginners
Date: 22/09/2023 | 6 CEU Hours
Certificate ID: cert_s5cq0wfp

Anthony Isherwood
Instructor

TCM SECURITY

CERTIFICATE OF COMPLETION

This certifies that

OLAWOYIN JOSEPH

has completed Practical Malware Analysis & Triage
Date: 09/27/2023 | 9 CEU Hours
Certificate ID: cert_0oztzy15

MATT KIELY
Instructor

TCM SECURITY

CERTIFICATE OF COMPLETION

This certifies that

OLAWOYIN JOSEPH

has completed Practical Malware Analysis & Triage
Date: 09/27/2023 | 9 CEU Hours
Certificate ID: cert_0oztzy15

MATT KIELY
Instructor

TCM SECURITY

CERTIFICATE OF COMPLETION

This certifies that

OLAWOYIN JOSEPH

has completed Practical Windows Forensics
Date: 23/09/2023 | 11 CEU Hours
Certificate ID: cert_b0d9b7w

MARKUS SCHOBER
Instructor

TCM SECURITY

Udemy

CERTIFICATE OF COMPLETION

AWS Services for Solutions
Architect Associate [2021]

Instructors   EdYoda Digital University, Aashish Pandey

Joseph Olawoyin

Date June 10, 2022
Length 11 total hours

Udemy

CERTIFICATE OF COMPLETION

The Complete Computer
Forensics Course for 2022 PRO |
CFCT+

Instructors   OCSALY - Online Computer Science Academy

Joseph Olawoyin

Date June 17, 2022
Length 6.5 total hours

Udemy

CERTIFICATE OF COMPLETION

API Security Testing Guide by
The XSS Rat

Instructors   Wesley Thijs

Joseph Olawoyin

Date July 25, 2022
Length 5 total hours

CHRISLAND UNIVERSITY
THE REGAL SET '24

2024 AWARD

AWARD OF
Recognition

FOR BEST SERVING CLASS REPRESENTATIVE
THIS AWARD IS PRESENTED TO

OLAWOYIN JOSEPH PAMILERIN

CYBERSECURITY
2020-2024 (CLASS OF 2024)
For dedication in representing and serving
the department of Cybersecurity class of 2024.

DATED THIS 28TH OCTOBER, 2024

SKILLFRONT

Badge Verification

✓ Issued Badge: ISO/IEC 27001
   Information Security Associate™
✓ Issued by SkillFront
✓ Issued to Joseph Olawoyin
✓ Issued on 10 November 2022
✓ Validity Period: Lifetime
✓ Status: VERIFIED

CERTIFICATE of COMPLETION

This Certifies That

Olawoyin Joseph Pamilerin

Has Successfully Completed the Course

Machine Learning

New Horizons
Learn What Earns

MD/CEO   Sep 2024
APPROVED   Date

NO. NHN 0116729

© Copyright 2021, New Horizons Worldwide, LLC. All Rights Reserved.

Credly

Protect Sensitive Data with Data Loss
Prevention
Skill Badge

Issued by Google Cloud

Joseph Pamilerin Olawoyin
joseph.olawoyin@christlanduniversity.edu.ng
ID#: a1e8cb27-babb-43b2-a28f-f731e1-b716b2
www.credly.com/user/joseph-olawoyin.d75b8da

Implement Load Balancing on Compute Engine Skill Badge
Issued by: Google Cloud
Issued to: Joseph Olawoyin
Issued on: 17 April 2024
Description
Complete the Implement Load Balancing on Compute Engine Skill badge to demonstrate skills in the following: write gcloud commands and use Cloud Shell, create and deploy virtual machines in Compute Engine, run containerized applications on Google Kubernetes Engine, and configure network and HTTP load balancers.

Implement Cloud Security Fundamentals on Google Cloud Skill Badge
Issued by: Google Cloud
Issued to: Joseph Olawoyin
Issued on: 19 April 2024
Description
Complete the intermediate Implement Cloud Security Fundamentals on Google Cloud Skill badge to demonstrate skills in the following: creating and assigning roles with Identity and Access Management (IAM); creating and managing service accounts; enabling private connectivity across virtual private cloud (VPC) networks; restricting application access using Identity-Aware Proxy; managing keys and encrypted data using Cloud Key Management Service (KMS); and creating a private Kubernetes cluster.

Build a Secure Google Cloud Network Skill Badge
Issued by: Google Cloud
Issued to: Joseph Olawoyin
Issued on: 21 April 2024
Description
Complete the Build a Secure Google Cloud Network Skill badge to demonstrate skills in the following: build, scale, and secure your applications on Google Cloud.

Protect Sensitive Data with Data Loss Prevention Skill Badge
Issued by: Google Cloud
Issued to: Joseph Olawoyin
Issued on: 4 May 2024
Description
Complete the Protect Sensitive Data with Data Loss Prevention skill badge to demonstrate skills in the following: use the Data Loss Prevention (DLP) API to inspect, redact, and de-identify sensitive data in Google Cloud.

Protect Cloud Traffic with BeyondCorp Enterprise (BCE) Security Skill Badge
Issued by: Google Cloud
Issued to: Joseph Olawoyin
Issued on: 15 May 2024
Description
Complete the intermediate Protect Cloud Traffic with BeyondCorp Enterprise (BCE) security skill badge to demonstrate skills in the following: leverage BeyondCorp Enterprise (BCE) to Provide secure access to critical apps and services, Improve your security posture with a modern Zero Trust platform, Securely provide access to resources using Identity and context-aware access control, and Support hybrid cloud workloads using Client Connector.

Professional Cloud Security Engineer Certification
Issued by: Google Cloud
Issued to: Joseph Olawoyin
Issued on: 8 June 2024
Expires on: 8 June 2026
Description
A Cloud Security Engineer allows organizations to design and implement secure workloads and infrastructure on Google Cloud. Through an understanding of security best practices and industry requirements, this individual designs, develops, and manages a secure solution by using Google security technologies.

Joseph Olawoyin
has successfully completed
Utilize threat intelligence in Microsoft Sentinel
October 17, 2022

Joseph Olawoyin
has successfully completed
Use watchlists in Microsoft Sentinel
October 17, 2022

Joseph Olawoyin
has successfully completed
Query logs in Microsoft Sentinel
October 17, 2022

Joseph Olawoyin
has successfully completed
Create and manage Microsoft Sentinel workspaces
October 17, 2022

Joseph Olawoyin
has successfully completed
Introduction to Microsoft Sentinel
October 17, 2022

Joseph Olawoyin
has successfully completed
Work with data in Microsoft Sentinel using Kusto Query Language
October 17, 2022

Joseph Olawoyin
has successfully completed
Build multi-table statements using KQL
October 17, 2022

Joseph Olawoyin
has successfully completed
Analyze query results using KQL
October 17, 2022

Joseph Olawoyin
has successfully completed
Construct KQL statements for Microsoft Sentinel
October 17, 2022

Joseph Olawoyin
has successfully completed
Build multi-table statements using KQL
October 17, 2022

Joseph Olawoyin
has successfully completed
Analyze query results using KQL
October 17, 2022

Joseph Olawoyin
has successfully completed
Construct KQL statements for Microsoft Sentinel
October 17, 2022

Joseph Olawoyin
has successfully completed
Remediate security alerts using Microsoft Defender for Cloud
October 17, 2022

Joseph Olawoyin
has successfully completed
Explain cloud workload protections in Microsoft Defender for Cloud
October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Manage your cloud security posture management

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Connect non-Azure resources to Microsoft Defender for Cloud

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Connect Azure assets to Microsoft Defender for Cloud

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Plan for cloud workload protections using Microsoft Defender for Cloud

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Utilize Vulnerability Management in Microsoft Defender for Endpoint

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Configure for alerts and detections in Microsoft Defender for Endpoint

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

**Configure and manage automation using Microsoft Defender for Endpoint**

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Perform evidence and entities investigations using Microsoft Defender for Endpoint

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

**Perform actions on a device using Microsoft Defender for Endpoint**

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Perform device investigations in Microsoft Defender for Endpoint

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Implement Windows security enhancements with Microsoft Defender for Endpoint

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Deploy the Microsoft Defender for Endpoint environment

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Protect against threats with Microsoft Defender for Endpoint

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Manage insider risk in Microsoft Purview

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Respond to data loss prevention alerts using Microsoft 365

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Secure your cloud apps and services with Microsoft Defender for Cloud Apps

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Safeguard your environment with Microsoft Defender for Identity

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Remediate risks with Microsoft Defender for Office 365

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Protect your identities with Azure AD Identity Protection

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Mitigate incidents using Microsoft 365 Defender

October 17, 2022

Microsoft

Joseph Olawoyin

has successfully completed

Introduction to Microsoft 365 threat protection
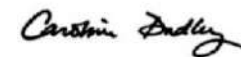
October 17, 2022

accenture

OLAWOYIN JOSEPH
Project Management Job Simulation

Certificate of Completion

December 13th, 2024

Over the period of September 2022 to December 2024, OLAWOYIN JOSEPH has completed practical tasks in:

Understand the approaches to project management
Prepare a proposal for the optimal project management approach
Identify the key attributes of a good project manager or project lead
Importance of communication in project management

Caroline Dudley
Managing Director
North America
Recruiting

Tom Brunskill
CEO, Co-Founder of
Forage

Deloitte.

OLAWOYIN JOSEPH
Technology Virtual Experience Program

Certificate of Completion

September 22nd, 2022

Over the period of September 2022, OLAWOYIN JOSEPH has completed practical tasks in:

Coding
Data Analysis
Development
Cyber Security
Forensic Technology

Tina McCreery
Chief Human
Resources Officer,
Deloitte

Tom Brunskill
CEO, Co-Founder of
Forage

GRADUATION THESIS

Applicant's Name	OLAWOYIN JOSEPH PAMILERIN
Date of Birth	08-FEB-2003
Research Theme	DETECTION ENGINEERING AND IDENTIFICATION OF RANSOMWARE ATTACKS, SQL INJECTION AND CROSS-SITE SCRIPTING ATTACKS FOR ENHANCED CYBER RESILIENCE USING KNN ALGORITHM

Abstract:

This research investigates the application of Artificial Intelligence (AI), specifically the K-Nearest Neighbors (KNN) algorithm, to enhance the detection and identification of sophisticated cyber threats, including ransomware, SQL injection, and cross-site scripting (XSS) attacks. Traditional detection systems, reliant on static, rule-based methods, often struggle to keep pace with the evolving nature of these threats, resulting in reduced effectiveness. This study aims to address these limitations by proposing an AI-driven solution that leverages the adaptability and precision of the KNN algorithm to improve threat detection capabilities.

Through extensive experimentation, the KNN-based detection system demonstrated a marked improvement in accuracy, precision, and recall metrics, significantly reducing false positives while increasing the reliability of the system in identifying real threats. The research also highlights the scalability and adaptability of the KNN algorithm in processing large datasets and handling various types of cyber-attacks, positioning AI as a crucial tool for enhancing cybersecurity resilience. These findings provide valuable insights into the potential of AI-based systems in bolstering defenses against increasingly sophisticated cyber-attacks and pave the way for future advancements in intelligent threat detection systems.

Fig.1. New designed (Detection system)

A method of how we reached to a desired result is introduced here, the implementation of the modeled system focused on system design. The complex activity of system development was broken down into smaller sub-activities that communicated with each other to achieve the overall goal of the project
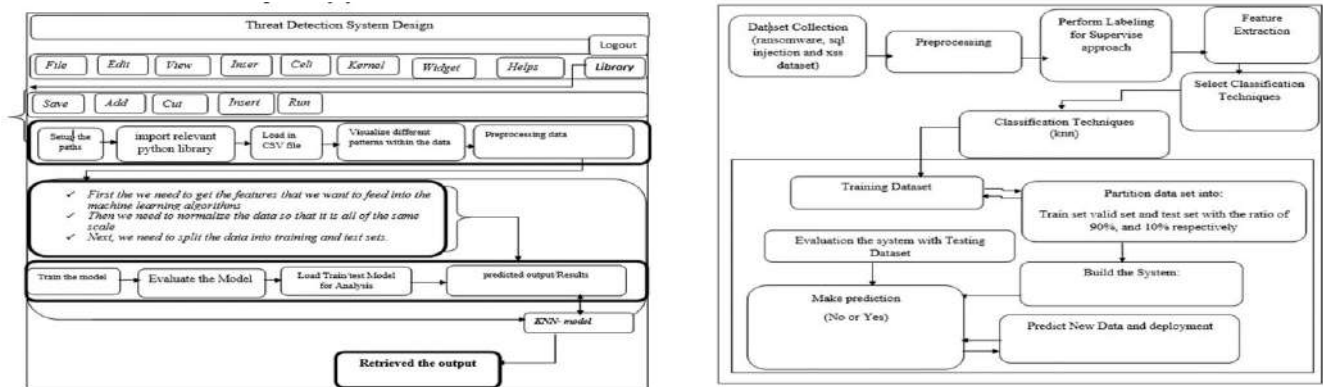

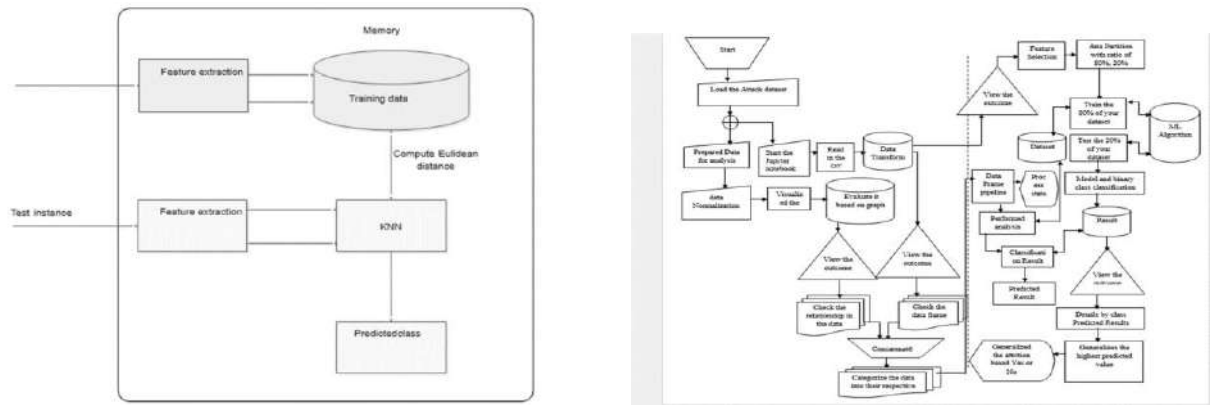Fig.2. System Design and logical design of the system

Fig.3. Architectural framework and System flowchart of the proposed system

The ROC-AUC (Receiver Operating Characteristic - Area Under Curve) score of 0.70 for this kNN model indicates moderate performance, showing that the model is better than random guessing at distinguishing between classes, but there is still room for improvement. The ROC curve, which plots sensitivity against the false positive rate, confirms this by showing an area under the curve (AUC) of 0.70.
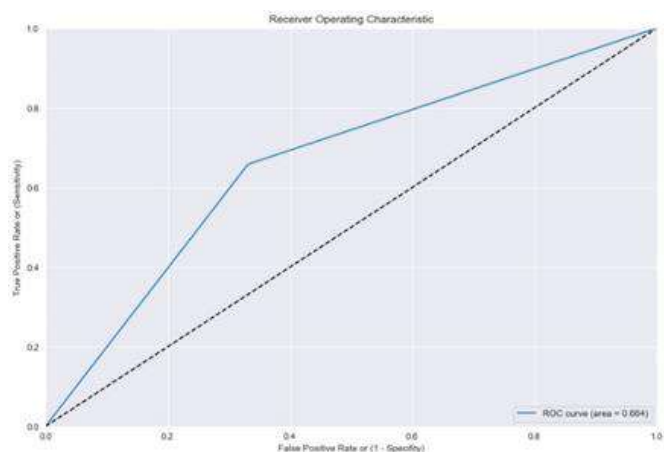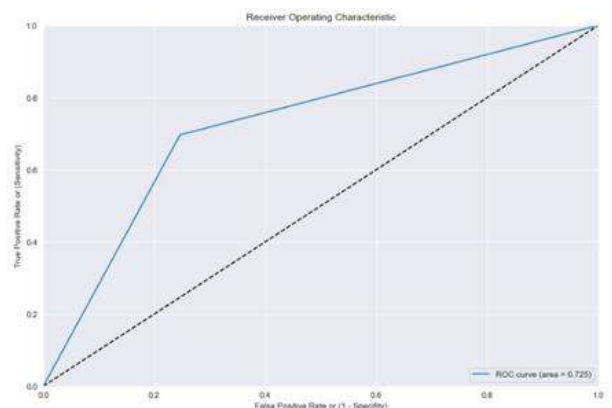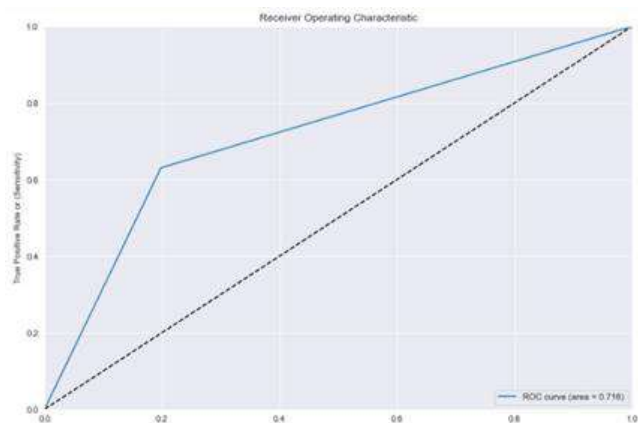
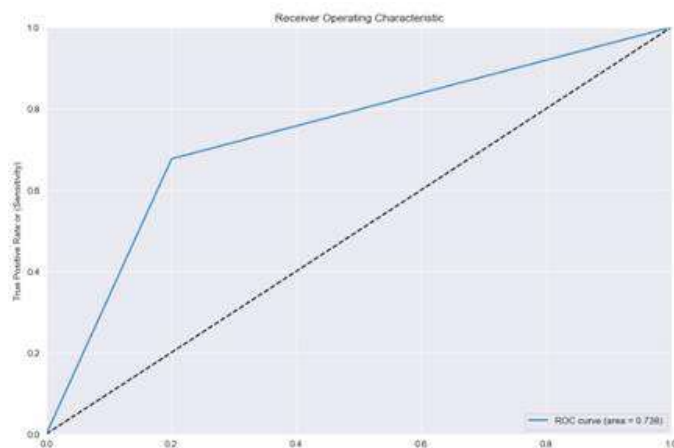Results:
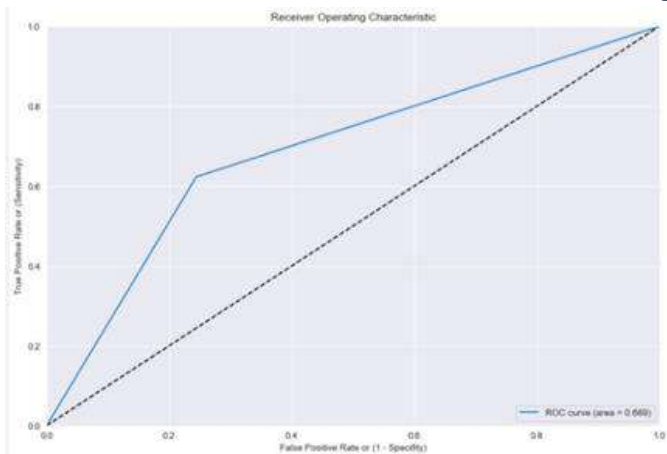
Graph.1. logistic Regression
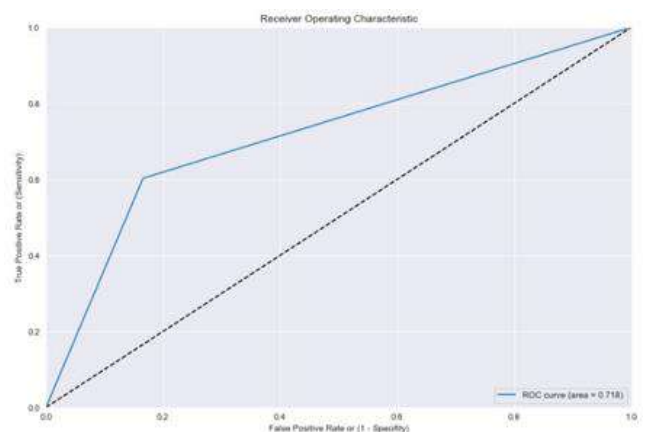
Graph.2. KNN Model

Graph.3. Decision Tree

Graph.4. Random Forest

Graph.5. Adaboost   Graph.6. Artificial Neural Network

Conclusions:

➤ Moderate Model Performance: The k-Nearest Neighbors (kNN) model developed for ransomware detection has shown moderate effectiveness, with an overall accuracy of 70%. While the model correctly identifies a majority of ransomware instances, the presence of false positives and false negatives suggests that there is room for improvement.

➤ Balanced Precision and Recall: The model's precision (0.72) and recall (0.69) are reasonably balanced, indicating that the model can identify actual ransomware while maintaining a moderate level of false alarms. However, the recall is slightly lower, meaning that the model misses a notable percentage of ransomware cases.

➤ Room for Improvement in Recall: The relatively lower recall rate indicates that the model is prone to missing some ransomware attacks, which could lead to undetected threats. This is a critical concern in cybersecurity, where the cost of false negatives can be significant.

➤ Fair Discriminative Ability: The ROC-AUC score of 0.70 suggests that the model has a fair ability to distinguish between ransomware and non-ransomware instances. However, a higher score would be preferable to ensure greater confidence in the model's