

ProjectReporton

AI in Cyber Security

**Submittedby:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Roll**  **No.** | **Reg.No** | **Section** | **Group** |
| Aripelly Akshay Kumar | 49 | 12115139 | K21QT | 2 |
| Mohd Ahad | 50 | 12115116 | K21QT | 2 |
| Gannavarapu Rajesh | 51 | 12115363 | K21QT | 2 |

**Submittedto:Akshara Rana**

**DEPARTMENTOF**

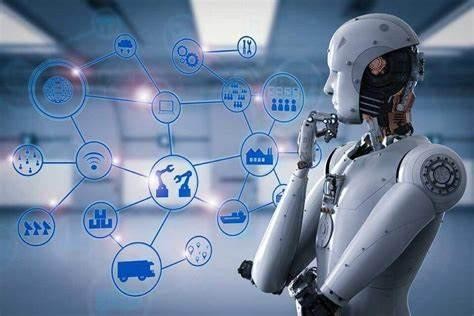
**COMPUTERSCIENCEANDENGINEERING**

# INTRODUCTION:

Role of AI in modernworldthreat to cybersecurityhas become a seriousissue.Artificialintelligence (AI) is a branchof computersciencewherea machineis made capableofpossessinghumandecision-makingability,basedoncertainuniquealgorithmsandrelatedmathematical calculations.On the other side, Cyber Securityconsistsof securitymeasurestoprotectthe virtualworldfromcyberattacksand threats.ArtificialIntelligenceiscapableofsecuringand cleaningupthecyberspacebytakingsecuritymeasuresrelatedtoaccuratealgorithmsandmathematicalcalculations.Withanincreaseinthe

Thecyberattacksurfaceinmodernenterpriseenvironmentsismassive,andit’scontinuingtogrow rapidly.This means that analysingand improvingan organization’scybersecuritypostureneedsmorethanmerehumanintervention.

AI and machinelearningare now becomingessential to informationsecurity,as thesetechnologiesarecapableofswiftlyanalysingmillionsofdatasetsandtrackingdownawidevariety of cyber threats from malware menaces to shady behaviourthat mightresult in aphishingattack.



Thesetechnologiescontinuallylearnandimprove,drawingdatafrompastexperiencesandpresenttopinpointnewvarietiesofattacksthatcanoccurtodayortomorrow.

In thispost, we’reviewthe useof AI in cybersecurity(both good and bad) andwhattheexpertsandexecutiveshavetosayaboutthismatter.

# WhatisCyberSecurity?

When we protect the deviceswhichare connectedto the internet,thisprocess is calledCybersecuritywhichincludesprotectinghardware,software,and data from the threatsofcybercriminals.Individualsand organizationsuse thispracticeto protectagainstunauthorizedaccess to data centresand other computerizedsystems.Thecyber securitypersonnelneed the best cyber securitytrainingto identifyand stop any attacks from takingplace on the system.We need a strategyin cybersecuritythat is strongenoughfor a goodsecurity practiceagainstsome of the maliciousattacks whichare crafted in order to access,tamper,delete,extortor destroy the data of an organizationor individualsystemsand stealsensitivedata. The most instrumentalpart whichpreventscyber-attacksfrom happeningaimingtoweakenordisruptasystem’sordevice’soperationsiscybersecurity.



### ImportanceofCyberSecurity

Nowadays,the numberof users who are usingdevices and programshave increasedconsiderablyinmodernenterprisethatgeneratesalargeamountofdata,manyofwhicharesensitiveorconfidential.Thereforeherecomestheimportanceofcybersecurityasin

thisage,datatheftonthesesystemscontinuestogrow.Theincreaseinvolumeandmoresophisticationinmethodsthatareusedbycyberattackersthroughmanyattacktechniquescreatemanyproblemsevenfurther.

# ScopeofAIbeyondtraditionalsecuritymeasures:

Traditionally security measuresdepend upon antivirussoftwarelike firewall,quick healandothertoolsondetectingandpreventingwebsecuritythreats.Lookingatthisscenario,timelyupdate of software and the attitudeof a person who is in charge of securitywoulddeterminethe level of security website or virtualplatform.AI depends upon innovativetechnologieslikeMachineLearning,DeepLearning,NaturalLanguageProcessingetctomakedifficultfor hackerstogainaccesstoserversandothervaluableinformationstoredinsidecomputers.

# AIhasreducedhumaninvolvementincybersecurityAffairs:

Cybersecurityprofessionalsareassignedthetasktokeepan eyeonthesecurityofthewebsite.ThislimitsthescopeofAIinvolvementin cybersecurityaffairsashumanbeings control everythingby taking decisions relatedto cybersecurityingeneral.Itisdifficultforcybersecurityprofessionalstoworkforhourswithoutbreak,holidaysorleaves.WhereasAIcanhandlesimilarsituationswithoutanybreakasitisprogrammedtodealwithhighrisk-takingsituationswithoutanyconcern.

# RoleofAIinCyberSecurity:

When we discussartificialintelligencein cybersecurityit is nothingnew. In fact,twoyearsago,inforumspeoplewoulddiscusshowartificialintelligenceandmachinelearningin cyber securitywouldchangethe futureas data is at the centralpart of cyber securitytrends. In cyber security,artificialintelligenceproves to be beneficialas it improvesthewaysecurityexpertsanalyse,study,andunderstandcybercrime.Itimprovesthe

technologiesthat companiesuse to combat cybercriminalsand helpsorganizationskeepcustomerdata safe. But, on the other hand, artificialintelligencecan be a very exhaustiveresourceand may not be practicallyapplicablein every application.Most importantly,itcan alsoserveas a new weapon for cybercriminalswhomay use thistechnologytosharpentheir techniquesandimprovetheir cyberattacks.



### NeedforAIinCybersecurity

It is impossiblefor a normalhumanto identifyand blockall the threatsfacedby acompanybecauseof thefactthateveryyear, hackersfindout a differentway to launchvarioustypesofattacksthathaveadistinctobjectivesFor example,inearliertimeslog4jwas not known thoughit was presentfrom the beginning,finally,it was reintroducedinDecember2021. The networkcan suffermassivedamagewith the introduction of thesenewtypesofunknownthreatsandtheycanhaveadeepimpactontheorganizationifyoufailtodetect,identify,andpreventthem.

# AIinCyberSecurity:Benefits

1. **ArtificialIntelligencebecomesmoreintelligentoverTime**
2. **ArtificialIntelligencehelpsusinidentifyingunknownThreats**
3. **ArtificialIntelligenceCanHandlea LotofData**
4. **ArtificialIntelligencecanmanagevulnerabilitybetter**

# FACERECOGNITIONUSINGAI:

Facial Recognitionis a category of biometricsoftwarethat maps an individual’s facialfeaturesand stores the data as a face print.The softwareuses deep learning algorithmstocompare a livecaptured imageto the stored face printto verifyone’s identity. Imageprocessingandmachinelearningarethebackbonesofthistechnology.Facerecognition hasreceivedsubstantialattention from researchers due to humanactivitiesfoundin variousapplicationsofsecuritylikeairports,criminaldetection,facetracking,forensics,etc.

Comparedtootherbiometrictraitslikepalmprint,iris,fingerprint,etc.,facebiometricscanbenon-intrusive.



Theycan be taken even withoutthe user’s knowledge and furthercan be used for security-based applicationslike criminal detection,face tracking,airport security,and forensicsurveillancesystems.Face recognitioninvolves capturingfaceimagesfrom a videoor asurveillancecamera.Theyarecompared withthestoreddatabase.Facerecognitioninvolvestrainingknown images,classifyingthem withknown classes,and then they are stored in thedatabase. When a test imageis givento the systemit is classifiedand compared with the storeddatabase.

## ADVANTAGESOFAIINCYBERSECURITY:

Artificialintelligence(AI) may be used to detect cyber risks and potentiallyharmfulactions.Traditionalsoftware systemscan't keep up withthehugevolumeof new virusesproducedeveryweek,thereforethisisanareawhereartificialintelligencecanreallyassist.

AI systemsare beingtrainedto identifymalware,execute pattern recognition,and detecteven thetiniest characteristicsof malwareor ransomwareassaultsbefore theyreach the systemusingcomplexalgorithms.Withnaturallanguageprocessing,AIcanprovidegreaterpredictiveintelligence by skimmingthrougharticles,news, and research on cyber risks andcuratingmaterialonitsown.

Everyday,amid-sizedfirmreceiveswarningsforaround200,000cyberincidents,accordingto text republic. An ordinarycompany's securitystaff wouldbe overwhelmedby this amountof attacks.As a result,someof thesethreatswillgo undiscoveredand inflictsignificantnetwork damage. To operate effectively and protect their organizationsfrom cyber threats,security professionalsrequire significanthelp from intelligentmachinesand moderntechnologysuchasAI.

AI presents manyadvantagesand applicationsin a varietyof areas, cybersecuritybeingoneof them.With fast-evolvingcyberattacksand rapid multiplicationof deviceshappeningtoday,AIandmachinelearningcan helptokeepabreastwithcybercriminals,automatethreat

detection,and respond more effectively than conventional software-driven or manualtechniques.

## Here are a few advantagesandapplicationsof using AI incybersecurity:

* Detectingnewthreats
* BattlingBots
* BreachRiskprediction
* BetterEndPointprediction

# DetectingNewThreats

AI can be used to spot cyber threatsand possiblymaliciousactivities.Traditionalsoftwaresystemssimply cannot keep pace with the sheer numberof new process Created every week,so thisis an area AI can reallyhelpwith by usingsophisticated algorithms,AI systemsarebeing trained to detect malware,run pattern recognition,and detect even the minutestbehavioursof malwareorransomwareattacksbeforeitentersthesystem.



AIallowsforsuperiorpredictiveintelligencewithnaturallanguageprocessingwhichcuratesdataonitsownbyscrapingthrougharticles,news,andstudiesoncyberthreats.

Thiscangiveintelligenceofnewanomalies,cyberattacks,andpreventionstrategies.Afteral,cybercriminalsfollowtrendstoosowhat’spopularwiththemchangesconstantly.

AI-basedcybersecuritysystemscanprovidethelatestknowledgeof globalaswellas

industry-specificdangers tobetterformulatevitalprioritizationdecisionsbasednotmerelyonwhat could be used to attack your systemsbut based on what is most likelyto be used toattackyoursystem

# BattlingBots

Bots make up a huge chunk of internettraffictoday, and they can be dangerous.Fromaccounttakeovers with stolen credentialsto bogus accountcreation and data fraud,bots canbearealmenace.

You can’t tackle automated threats with manual responses alone. AI and machine learninghelp build a thorough understandingof website trafficand distinguishbetween good bots(likesearchenginecrawlers),badbots,andhumans.

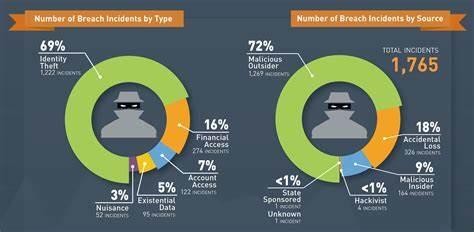
AI enablesustoanalyseavast amountof dataandallowscybersecurityteamstoadapttheirstrategytoacontinuallyalteringlandscape.

By lookingat behaviouralpatterns,businesseswilget answersto thequestions‘whatdoesanaverageuserjourneylooklike’and‘whatdoesariskyunusualjourneylooklike’.Fromhere,we can unpicktheintentof theirwebsitetraffic,gettingand stayingahead of thebad bots“explainsmarkgreenwood”,ChiefTechnicalArchitect&HeadofDataScience.

# BreachRiskPrediction

AIsystemshelpdeterminetheITassetinventorywhichisanaccurateanddetailedrecordofalldevices,users,andapplicationswithdifferentlevelsofaccesstovarioussystems.

Now, consideringthe asset inventoryand threat exposure (as discussed above), AI-basedsystemscan predict how and where you are most likelyto be compromisedso that you canplanandallocateresourcestowardsareasofmostvulnerabilities.

Prescriptiveinsights from AI-based analysisenablesyou to configureand improvecontrolsandprocessestoreinforceyourcyberresilience.

**BetterEndpointProtection**

Thenumberofdevicesusedforworkingremotelyisfastincreasing,andAIhasa crucialroletoplayinsecuringallthoseendpoints.



Sure, antivirussolutionsand VPNs can help against remote malware and ransomwareattacks,but they often work based on signatures. This means that in order to stay protected against thelatestthreats,itbecomesnecessarytokeepupwithsignaturedefinitions.

Thiscanbea concernifvirusdefinitionslagbehind,eitherbecauseofafailuretoupdatetheantivirussolution or a lack of awarenessfrom the softwarevendor.So, if a new type ofmalwareattackoccurs,signatureprotectionmay notbeabletoprotectagainstit.

AI drivenendpointprotectiontakes a differenttack, by establishinga baselineof behaviourfortheendpointthrougharepeatedtrainingprocess.Ifsomethingoutoftheordinaryoccurs,AIcanflagitandtakeactionwhetherthat’ssendinga notificationto a technicianor evenrevertingtoasafestateafteraransomwareattack.Thisprovidesproactiveprotectionagainstthreats, rather than waitingfor signatureupdates ,explainsTim brown, VP of SecurityArchitectureatSolarWinds.

**Importanceof Face Recognition System InArtificialIntelligenceforcybersecurity**

Face recognition systems play an essential role in cybersecurity for AI by providing a reliable and efficient method of identity verification. With the increasing prevalence of digital technologies and the internet, identity theft has become a significant concern, and traditional methods of identification, such as passwords, are no longer considered secure.

Face recognition systems use advanced artificial intelligence algorithms to analyze and identify unique facial features, allowing for secure and accurate identification of individuals. This technology is especially crucial in the context of cybersecurity because it can be used to prevent unauthorized access to sensitive data and systems.

For example, in online banking, face recognition systems can be used to verify the identity of the user before allowing access to the account, thereby reducing the risk of fraud and hacking. Similarly, in government and military applications, face recognition systems can be used to control access to sensitive areas and prevent unauthorized individuals from gaining entry.

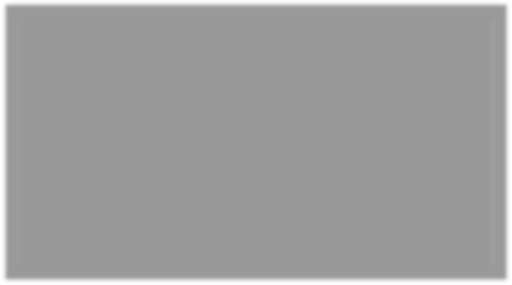
Overall, the importance of face recognition systems in cybersecurity for AI lies in their ability to provide a secure and reliable method of identification, helping to protect sensitive data and systems from cyber threats.

The current technology amazes people with amazing innovations that not only make life simple but also bearable. Face recognition has over time proven to be the least intrusive and fastest form of biometric verification.

Facial Recognition is a category of biometric software that maps an individual’s facial features and stores the data as a face print. The software uses deep learning algorithms to compare a live captured image to the stored face print to verify one’s identity. Image processing and machine learning are the backbones of this technology. Face recognition has received substantial attention from researchers due to human activities found in various applications of security like an airport, criminal detection, face tracking, forensic, etc. Compared to other biometric traits like palm print, iris, fingerprint, etc., face biometrics can be non-intrusive.

They can be taken even without the user’s knowledge and further can be used for security-based applications like criminal detection, face tracking, airport security, and forensic surveillance systems. Face recognition involves capturing face images from a video or a surveillance camera. They are compared with the stored database. Face recognition involves training known images, classify them with known classes, and then they are stored in the database. When a test image is given to the system it is classified and compared with the stored database.

## IMPLEMENTATIONOFAIINCYBERSECURITY:



ArtificialIntelligence (AI) is transformingthe way we approach cyber security.With itssophisticatedcapabilities,AIcanevaluateenormousvolumes ofdataandidentifypotential

risks fasterand more effectivelythan traditionalsecuritymethods.There are several methodsforimplementingAIincyberdefense:

# Determineyoursecurityneeds:

EstablishyoursecurityrequirementsbeforeincorporatingAIintoyourcyberprotectionplan.Thiswillassist you in decidingwhichAI technologiesare most appropriatefor yourcompany.

# Identifypotentialthreats:

AI can swiftly discover potential threats by analysing enormous volumes of data. You must recognize the most prevalent categories of cyber risks that your company confronts in order toutilizeAIincyberefficiently.

# ChoosetherightAItechnology:

There are variousAI technologiesthat can be employedin cyber protection,includingmachinelearning,naturallanguageprocessing,anddeeplearning.Selecttheonethatbestmeetsyoursecurityneeds.

# Collectandprocessdata:

TotrainyourAIsystem,youneedtocollectandprocessdatafromnumeroussources.Thisincludesinformationfromlogfiles,networktraffic,andothersecuritydatasources.

# TrainyourAIsystem:

After gathering data, you must train your AI system using algorithms that can learn from thedata. The AI system can then utilizethis information to recognizepotential risks and take thenecessaryprecautions.

# ImplementAIinyoursecurityinfrastructure:

Once your AI system is taught,it’s time to incorporate it into your security infrastructure.This involvesconnecting it with your security operations centre, incidentresponse team, andothersecuritysystems.

**CODE FOR FACE RECOGNITION SYSTEM**

# importing libraries

import tkinter as tk

from tkinter import Message, Text

import cv2

import os

import shutil

import csv

import numpy as np

from PIL import Image, ImageTk

import pandas as pd

import datetime

import time

import tkinter.ttk as ttk

import tkinter.font as font

from pathlib import Path

window = tk.Tk()

window.title("Face\_Recogniser")

window.configure(background='white')

window.grid\_rowconfigure(0, weight=1)

window.grid\_columnconfigure(0, weight=1)

message = tk.Label(

window, text="Face-Recognition-System",

bg="green", fg="white", width=50,

height=3, font=('times', 30, 'bold'))

message.place(x=200, y=20)

lbl = tk.Label(window, text="No.",

width=20, height=2, fg="green",

bg="white", font=('times', 15, ' bold '))

lbl.place(x=400, y=200)

txt = tk.Entry(window,

width=20, bg="white",

fg="green", font=('times', 15, ' bold '))

txt.place(x=700, y=215)

lbl2 = tk.Label(window, text="Name",

width=20, fg="green", bg="white",

height=2, font=('times', 15, ' bold '))

lbl2.place(x=400, y=300)

txt2 = tk.Entry(window, width=20,

bg="white", fg="green",

font=('times', 15, ' bold '))

txt2.place(x=700, y=315)

# The function below is used for checking

# whether the text below is number or not ?

def is\_number(s):

try:

float(s)

return True

except ValueError:

pass

try:

import unicodedata

unicodedata.numeric(s)

return True

except (TypeError, ValueError):

pass

return False

# Take Images is a function used for creating

# the sample of the images which is used for

# training the model. It takes 60 Images of

# every new user.

def TakeImages():

# Both ID and Name is used for recognising the Image

Id = (txt.get())

name = (txt2.get())

# Checking if the ID is numeric and name is Alphabetical

if(is\_number(Id) and name.isalpha()):

# Opening the primary camera if you want to access

# the secondary camera you can mention the number

# as 1 inside the parenthesis

cam = cv2.VideoCapture(0)

# Specifying the path to haarcascade file

harcascadePath = "data\haarcascade\_frontalface\_default.xml"

# Creating the classier based on the haarcascade file.

detector = cv2.CascadeClassifier(harcascadePath)

# Initializing the sample number(No. of images) as 0

sampleNum = 0

while(True):

# Reading the video captures by camera frame by frame

ret, img = cam.read()

# Converting the image into grayscale as most of

# the processing is done in gray scale format

gray = cv2.cvtColor(img, cv2.COLOR\_BGR2GRAY)

# It converts the images in different sizes

# (decreases by 1.3 times) and 5 specifies the

# number of times scaling happens

faces = detector.detectMultiScale(gray, 1.3, 5)

# For creating a rectangle around the image

for (x, y, w, h) in faces:

# Specifying the coordinates of the image as well

# as color and thickness of the rectangle.

# incrementing sample number for each image

cv2.rectangle(img, (x, y), (

x + w, y + h), (255, 0, 0), 2)

sampleNum = sampleNum + 1

# saving the captured face in the dataset folder

# TrainingImage as the image needs to be trained

# are saved in this folder

cv2.imwrite(

"TrainingImage\ "+name + "."+Id + '.' + str(

sampleNum) + ".jpg", gray[y:y + h, x:x + w])

# display the frame that has been captured

# and drawn rectangle around it.

cv2.imshow('frame', img)

# wait for 100 milliseconds

if cv2.waitKey(100) & 0xFF == ord('q'):

break

# break if the sample number is more than 60

elifsampleNum> 60:

break

# releasing the resources

cam.release()

# closing all the windows

cv2.destroyAllWindows()

# Displaying message for the user

res = "Images Saved for ID : " + Id + " Name : " + name

# Creating the entry for the user in a csv file

row = [Id, name]

with open('UserDetails\UserDetails.csv', 'a+') as csvFile:

writer = csv.writer(csvFile)

# Entry of the row in csv file

writer.writerow(row)

csvFile.close()

message.configure(text=res)

else:

if(is\_number(Id)):

res = "Enter Alphabetical Name"

message.configure(text=res)

if(name.isalpha()):

res = "Enter Numeric Id"

message.configure(text=res)

# Training the images saved in training image folder

def TrainImages():

# Local Binary Pattern Histogram is an Face Recognizer

# algorithm inside OpenCV module used for training the image dataset

recognizer = cv2.face.LBPHFaceRecognizer\_create()

# Specifying the path for HaarCascade file

harcascadePath = "data\haarcascade\_frontalface\_default.xml"

# creating detector for faces

detector = cv2.CascadeClassifier(harcascadePath)

# Saving the detected faces in variables

faces, Id = getImagesAndLabels("TrainingImage")

# Saving the trained faces and their respective ID's

# in a model named as "trainer.yml".

recognizer.train(faces, np.array(Id))

recognizer.save("TrainingImageLabel\Trainer.yml")

# Displaying the message

res = "Image Trained"

message.configure(text=res)

def getImagesAndLabels(path):

# get the path of all the files in the folder

imagePaths = [os.path.join(path, f) for f in os.listdir(path)]

faces = []

# creating empty ID list

Ids = []

# now looping through all the image paths and loading the

# Ids and the images saved in the folder

for imagePath in imagePaths:

# loading the image and converting it to gray scale

pilImage = Image.open(imagePath).convert('L')

# Now we are converting the PIL image into numpy array

imageNp = np.array(pilImage, 'uint8')

# getting the Id from the image

Id = int(os.path.split(imagePath)[-1].split(".")[1])

# extract the face from the training image sample

faces.append(imageNp)

Ids.append(Id)

return faces, Ids

# For testing phase

def TrackImages():

recognizer = cv2.face.LBPHFaceRecognizer\_create()

# Reading the trained model

recognizer.read("TrainingImageLabel\Trainer.yml")

harcascadePath = "data\haarcascade\_frontalface\_default.xml"

faceCascade = cv2.CascadeClassifier(harcascadePath)

# getting the name from "userdetails.csv"

df = pd.read\_csv("UserDetails\UserDetails.csv")

cam = cv2.VideoCapture(0)

font = cv2.FONT\_HERSHEY\_SIMPLEX

while True:

ret, im = cam.read()

gray = cv2.cvtColor(im, cv2.COLOR\_BGR2GRAY)

faces = faceCascade.detectMultiScale(gray, 1.2, 5)

for(x, y, w, h) in faces:

cv2.rectangle(im, (x, y), (x + w, y + h), (225, 0, 0), 2)

Id, conf = recognizer.predict(gray[y:y + h, x:x + w])

if(conf < 50):

aa = df.loc[df['Id'] == Id]['Name'].values

tt = str(Id)+"-"+aa

else:

Id = 'Unknown'

tt = str(Id)

if(conf > 75):

noOfFile = len(os.listdir("ImagesUnknown"))+1

cv2.imwrite("ImagesUnknown\Image" +

str(noOfFile) + ".jpg", im[y:y + h, x:x + w])

cv2.putText(im, str(tt), (x, y + h),

font, 1, (255, 255, 255), 2)

cv2.imshow('im', im)

if (cv2.waitKey(1) == ord('q')):

break

cam.release()

cv2.destroyAllWindows()

takeImg = tk.Button(window, text="Sample",

command=TakeImages, fg="white", bg="green",

width=20, height=3, activebackground="Red",

font=('times', 15, ' bold '))

takeImg.place(x=200, y=500)

trainImg = tk.Button(window, text="Training",

command=TrainImages, fg="white", bg="green",

width=20, height=3, activebackground="Red",

font=('times', 15, ' bold '))

trainImg.place(x=500, y=500)

trackImg = tk.Button(window, text="Testing",

command=TrackImages, fg="white", bg="green",

width=20, height=3, activebackground="Red",

font=('times', 15, ' bold '))

trackImg.place(x=800, y=500)

quitWindow = tk.Button(window, text="Quit",

command=window.destroy, fg="white", bg="green",

width=20, height=3, activebackground="Red",

font=('times', 15, ' bold '))

quitWindow.place(x=1100, y=500)

window.mainloop()

### CONCLUSION:

Artificialintelligenceis quicklyarisingas a highpriorityinnovationfor improvingtheperformanceof IT security groups.AI givesthe genuinelynecessary analysisand threatidentification proof that can be utilizedby securityexperts to limitbreach risk and upgradesecurityposture.AIcanhelptodiscoverandfocusonrisks,directincidentresponse,anddistinguishmalwareattacks beforethey come intothe scenario.Thus,even with theexpecteddrawbacks, AI will effectivelydrive cyber securityforwardand it will assisttheorganizationinpracticingamorepowerful securityposture.

AI has undergonerapidchangeand progressfrom meretechnicalassistancetocybersecurityexpertsindealingwithchallengesrelatedto thedetection andpreventio nofcyberattacks.Aided and supported by Machinelanguage,AI can findout cybersecuritythreatsandinformtheauthoritiestotakeappropriatemeasurestorectifythesameinno

time.So with reference to the modern context,the role of AI is increasingvarioussectors ofinformationtechnologylikeCyberSecurity,SoftwareTesting.

Github link:

<https://github.com/I-Kaizoku/Aiproject.git>

<https://github.com/Ahad275/AI-project/blob/main/AIproject.py>