LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

Project Report on

AI in Cyber Security

Submitted by:

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

Submitted to: Akshara Rana

DEPARTMENT OF

COMPUTER SCIENCE AND ENGINEERING

INTRODUCTION:

Role of AI in modern world threat to cybersecurity has become a serious issue. Artificial intelligence (AI) is a branch of computer science where a machine is made capable of possessing human decision-making ability, based on certain unique algorithms and related mathematical calculations. On the other side, Cyber Security consists of security measures to protect the virtual world from cyberattacks and threats. Artificial Intelligence is capable of securing and cleaning up the cyberspace by taking security measures related to accurate algorithms and mathematical calculations. With an increase in the

The cyberattack surface in modern enterprise environments is massive, and it's continuing to grow rapidly. This means that analysing and improving an organization's cybersecurity posture needs more than mere human intervention.
AI and machine learning are now becoming essential to information security, as these technologies are capable of swiftly analysing millions of data sets and tracking down a wide variety of cyber threats from malware menaces to shady behaviour that might result in a phishing attack.

These technologies continually learn and improve, drawing data from past experiences and present to pinpoint new varieties of attacks that can occur today or tomorrow.

In this post, we' review the use of AI in cybersecurity (both good and bad) and whatthe experts and executives have to say about this matter.

What is Cyber Security?

When we protect the devices which are connected to the internet, this process is called Cybersecurity which includes protecting hardware, software, and data from the threats of cybercriminals. Individuals and organizations use this practice to protect against unauthorized access to data centres and other computerized systems. The cyber security personnel need the best cyber security training to identify and stop any attacks from taking place on the system. We need a strategy in cybersecurity that is strong enough for a good security practice against some of the malicious attacks which are crafted in order to access, tamper, delete, extort or destroy the data of an organization or individual systems and steal sensitive data. The most instrumental part which prevents cyber-attacks from happening aiming to weaken or disrupt a system's or device's operations is cybersecurity.

Importance of Cyber Security

Nowadays, the number of users who are using devices and programs have increased considerably in modern enterprise that generates a large amount of data, many of which are sensitive or confidential.Therefore here comes the importance of cybersecurity as in this age, data theft on these systems continues to grow. The increase in volume and more sophistication in methods that are used by cyber attackers through many attack techniques create many problems even further.

Scope of AI beyond traditional security measures:

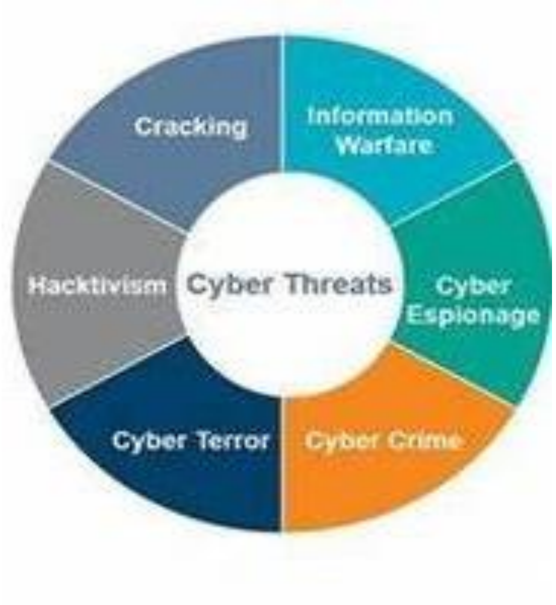
Traditionally security measures depend upon antivirus software like firewall, quick heal and other tools on detecting and preventing web security threats. Looking at this scenario, timely update of software and the attitude of a person who is in charge of security would determine the level of security website or virtual platform. AI depends upon innovative technologies like Machine Learning, Deep Learning, Natural Language Processing etc to make difficult for hackers to gain access to servers and other valuable information stored inside computers.

AI has reduced human involvement in cybersecurityAffairs:

Cybersecurity professionals are assigned the task to keep an eye on the security ofthe website. This limits the scope of AI involvement in cybersecurity affairs as human beings control everything by taking decisions related to cybersecurity in general. It is difficult for cybersecurity professionals to work for hours without break,holidays or leaves. Whereas AI can handle similar situations without any break as itis programmed to deal with high risk-taking situations without any concern.

Role of AI in Cyber Security :

When we discuss artificial intelligence in cyber security it is nothing new. In fact, two years ago, in forums people would discuss how artificial intelligence and machine learning in cyber security would change the future as data is at the central part of cyber security trends. In cyber security, artificial intelligence proves to be beneficial as it improves the way security experts analyse, study, and understand cybercrime. It improves the technologies that companies use to combat cybercriminals and helps organizations keep customer data safe. But, on the other hand, artificial intelligence can be a very exhaustive resource and may not be practically applicable in every application. Most importantly, it can also serve as a new weapon for cybercriminals who may use this technology to sharpen their techniques and improve their cyberattacks.



Need for AI in Cybersecurity

It is impossible for a normal human to identify and block all the threats faced by a company because of the fact that every year, hackers find out a different way to launch various types of attacks that have a distinct objectives For example, in earlier times log4j was not known though it was present from the beginning, finally, it was reintroduced in December 2021. The network can suffer massive damage with the introduction of these new types of unknown threats and they can have a deep impact on the organization if you fail to detect, identify, and prevent them.

AI in Cyber Security: Benefits

1. Artificial Intelligence becomes more intelligent over Time

2. Artificial Intelligence helps us in identifying unknown Threats

3. Artificial Intelligence Can Handle a Lot of Data

4. Artificial Intelligence can manage vulnerability better

FACE RECOGNITION USING AI:

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 airports, criminal detection, face tracking, forensics, 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, classifying 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.

ADVANTAGES OF AI IN CYBER SECURITY:

Artificial intelligence (AI) may be used to detect cyber risks and potentially harmful actions. Traditional software systems can't keep up with the huge volume of new viruses produced every week, therefore this is an area where artificial intelligence can really assist.
AI systems are being trained to identify malware, execute pattern recognition, and detect even the tiniest characteristics of malware or ransomware assaults before they reach the system using complex algorithms. With natural language processing, AI can provide greater predictive intelligence by skimming through articles, news, and research on cyber risks and curating material on its own.

Every day, a mid-sized firm receives warnings for around 200,000 cyber incidents, according to text republic . An ordinary company's security staff would be overwhelmed by this amount of attacks. As a result, some of these threats will go undiscovered and inflict significant network damage. To operate effectively and protect their organizations from cyber threats, security professionals require significant help from intelligent machines and modern technology such as AI.

AI presents many advantages and applications in a variety of areas, cybersecurity being one of them. With fast-evolving cyberattacks and rapid multiplication of devices happening today, AI and machine learning can help to keep abreast with cybercriminals, automate threat detection, and respond more effectively than conventional software-driven or manual techniques.

Here are a few advantages and applications of using AI in cybersecurity:

- Detecting new threats
- Battling Bots
- Breach Risk prediction
- Better End Point prediction

Detecting New Threats

AI can be used to spot cyber threats and possibly malicious activities. Traditional software systems simply cannot keep pace with the sheer number of new process Created every week, so this is an area AI can really help with by using sophisticated algorithms, AI systems are being trained to detect malware, run pattern recognition, and detect even the minutest behaviours of malware or ransomware attacks before it enters the system.

AI allows for superior predictive intelligence with natural language processing which curates data on its own by scraping through articles, news, and studies on cyber threats.

This can give intelligence of new anomalies, cyberattacks, and prevention strategies. After all, cybercriminals follow trends too so what's popular with them changes constantly.

AI-based cybersecurity systems can provide the latest knowledge of global as well as industry-specific dangers to better formulate vital prioritization decisions based not merely on what could be used to attack your systems but based on what is most likely to be used to attack your system

Battling Bots

Bots make up a huge chunk of internet traffic today, and they can be dangerous. From account takeovers with stolen credentials to bogus account creation and data fraud, bots can be a real menace.

You can't tackle automated threats with manual responses alone. AI and machine learning help build a thorough understanding of website traffic and distinguish between good bots (like search engine crawlers), bad bots, and humans.

AI enables us to analyse a vast amount of data and allows cybersecurity teams to adapt their strategy to a continually altering landscape.

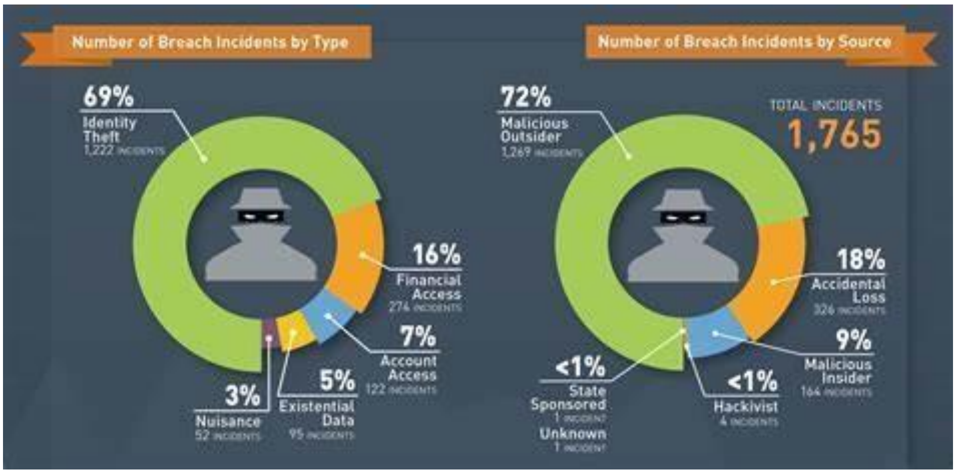
By looking at behavioural patterns, businesses will get answers to the questions 'what does an average user journey look like' and 'what does a risky unusual journey look like'. From here, we can unpick the intent of their website traffic, getting and staying ahead of the bad bots "explains mark greenwood", Chief Technical Architect & Head of Data Science.

Breach Risk Prediction

AI systems help determine the IT asset inventory which is an accurate and detailed record of all devices, users, and applications with different levels of access to various systems.

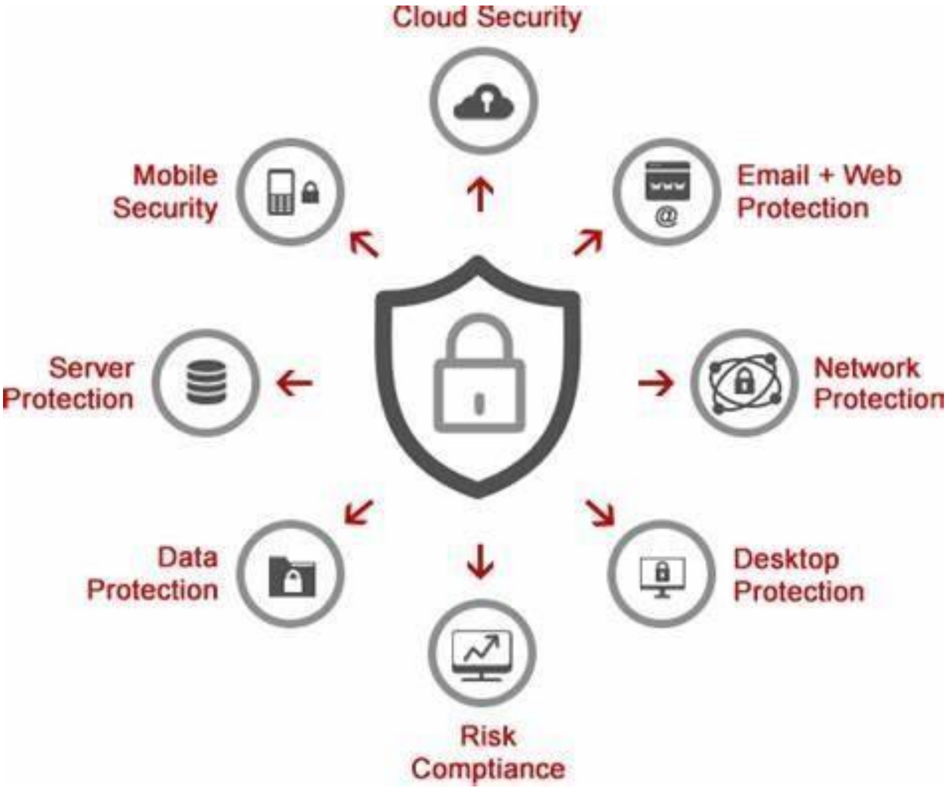
Now, considering the asset inventory and threat exposure (as discussed above), AI-based systems can predict how and where you are most likely to be compromised so that you can plan and allocate resources towards areas of most vulnerabilities.

Prescriptive insights from AI-based analysis enables you to configure and improve controls and processes to reinforce your cyber resilience.



Better Endpoint Protection

The number of devices used for working remotely is fast increasing, and AI has a crucial role to play in securing all those endpoints.



Sure, antivirus solutions and VPNs can help against remote malware and ransomware attacks, but they often work based on signatures. This means that in order to stay protected against the latest threats, it becomes necessary to keep up with signature definitions.

This can be a concern if virus definitions lag behind, either because of a failure to update the antivirus solution or a lack of awareness from the software vendor. So, if a new type of malware attack occurs, signature protection may not be able to protect against it.

AI driven endpoint protection takes a different tack, by establishing a baseline of behaviour for the endpoint through a repeated training process. If something out of the ordinary occurs, AI can flag it and take action whether that's sending a notification to a technic ian or even reverting to a safe state after a ransomware attack. This provides proactive protection against threats, rather than waiting for signature updates ,explains Tim brown, VP of Security Architecture at SolarWinds.

Importance of Face Recognition System In Artificial Intelligence forcybersecurity

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.

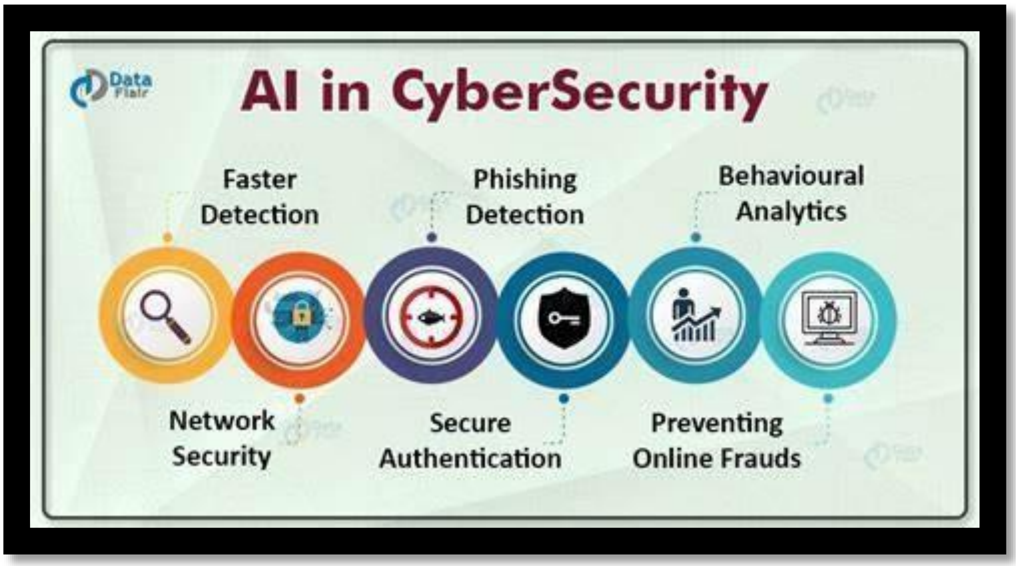
Overall, the importance of face recognition systems in cybersecurity for AI lies in their ability to provide a secure and reliable method of identification, helping to protect sensitive data and systems from cyber threats.

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.

IMPLEMENTATION OF AI IN CYBER SECURITY:



Artificial Intelligence (AI) is transforming the way we approach cyber security. With its sophisticated capabilities, AI can evaluate enormous volumes of data and identify potential risks faster and more effectively than traditional security methods. There are several methodsfor implementing AI in cyber defense:

Determine your security needs:

Establish your security requirements before incorporating AI into your cyber protection plan. This will assist you in deciding which AI technologies are most appropriate for your company.

Identify potential threats:

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 to utilize AI in cyber efficiently.

Choose the right AI technology:

There are various AI technologies that can be employed in cyber protection, including machine learning, natural language processing, and deep learning. Select the one that best meets your security needs.

Collect and process data:

To train your AI system, you need to collect and process data from numerous sources. This includes information from log files, network traffic, and other security data sources.

Train your AI system:

After gathering data, you must train your AI system using algorithms that can learn from the data. The AI system can then utilize this information to recognize potential risks and take the necessary precautions.

Implement AI in your security infrastructure:

Once your AI system is taught, it’s time to incorporate it into your security infrastructure. This involves connecting it with your security operations centre, incident response team, and other security systems.

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
            elif sampleNum > 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:

Artificial intelligence is quickly arising as a high priority innovation for improving the performance of IT security groups. AI gives the genuinely necessary analysis and threat identification proof that can be utilized by security experts to limit breach risk and upgrade security posture. AI can help to discover and focus on risks, direct incident response, and distinguish malware attacks before they come into the scenario. Thus, even with the expected drawbacks, AI will effectively drive cyber security forward and it will assist the organization in practicing a more powerful security posture.

AI has undergone rapid change and progress from mere technical assistance to cybersecurity experts in dealing with challenges related to the detection and preventio n of cyberattacks. Aided and supported by Machine language, AI can find out cybersecurity threats and inform the authorities to take appropriate measures to rectify the same in no time. So with reference to the modern context, the role of AI is increasing various sectors of information technology like Cyber Security, Software Testing.

Github link:
https://github.com/I-Kaizoku/Aiproject.git