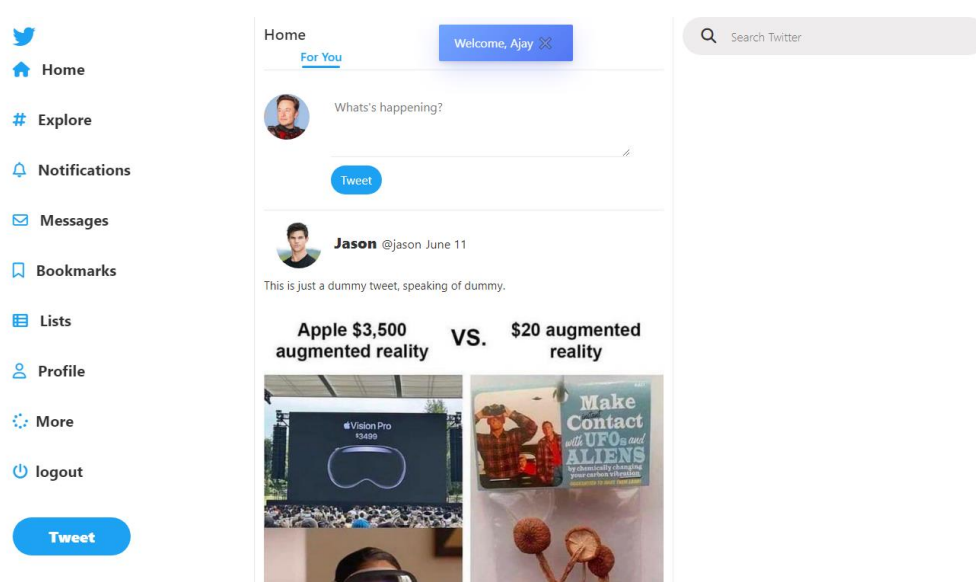
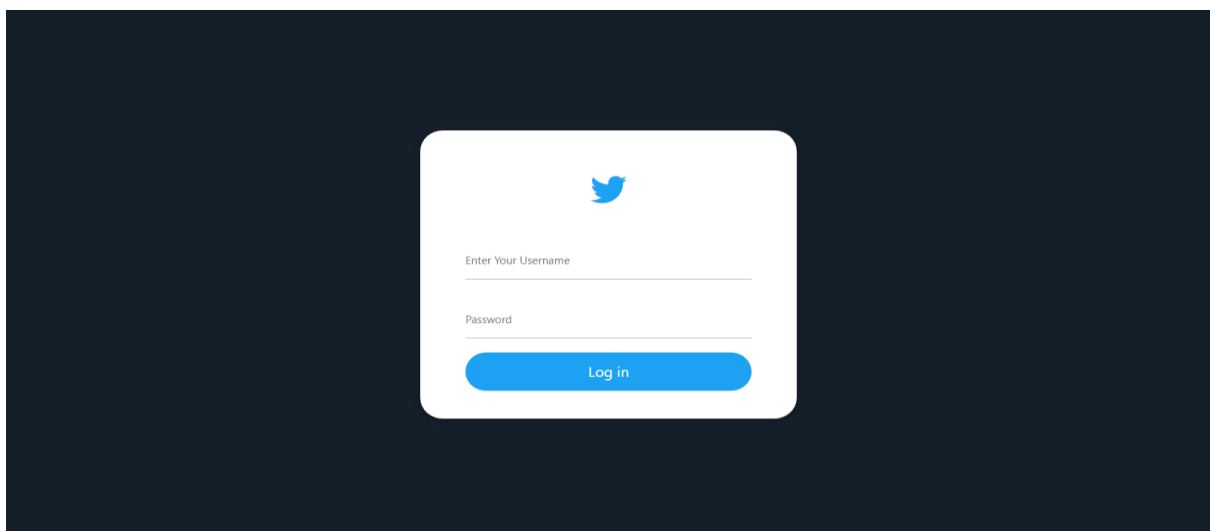
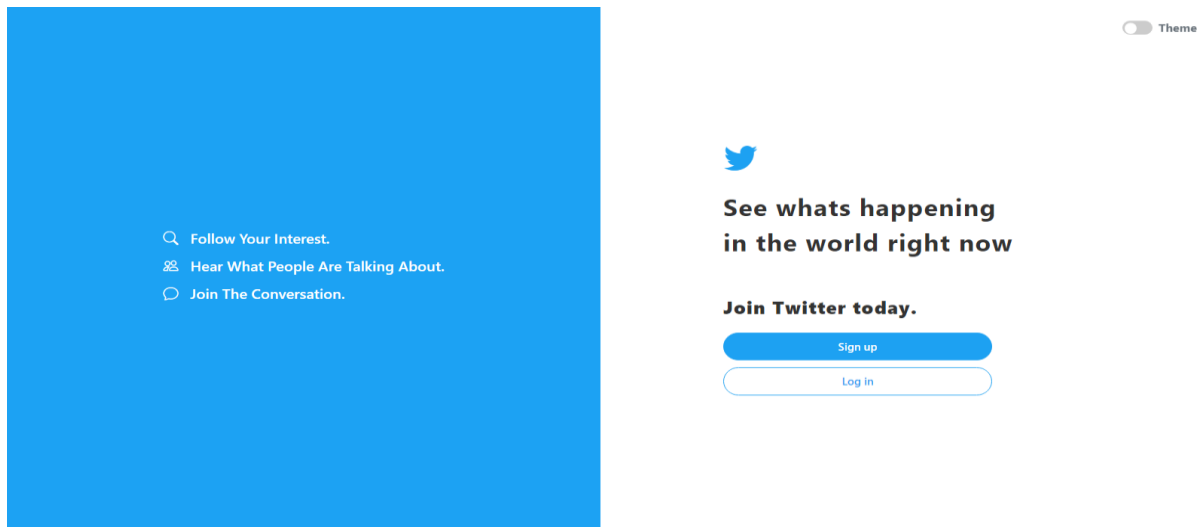
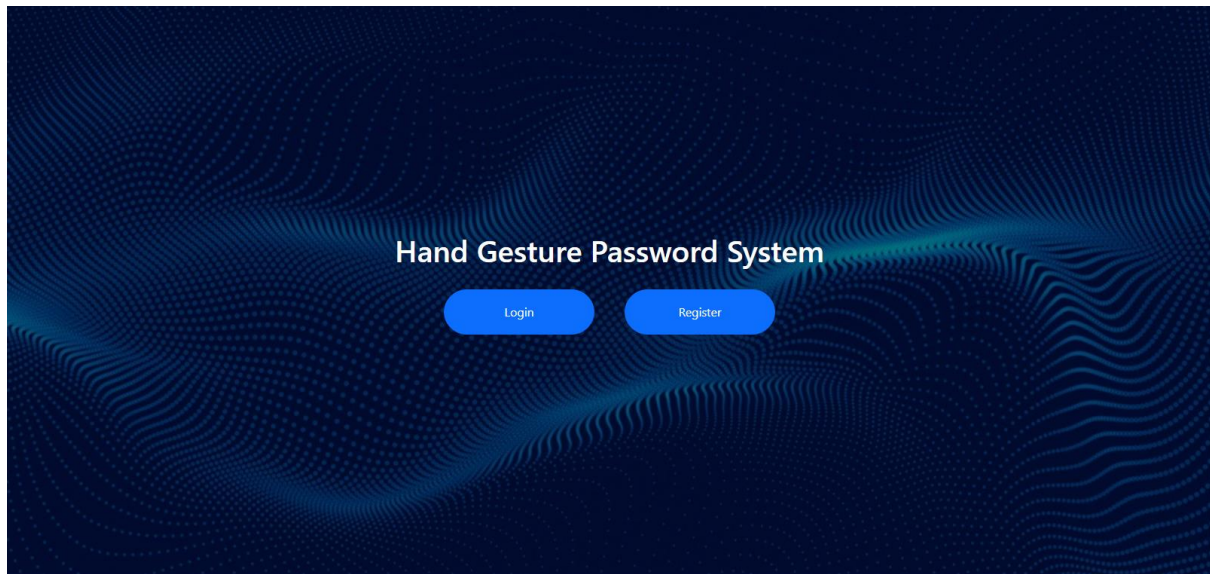


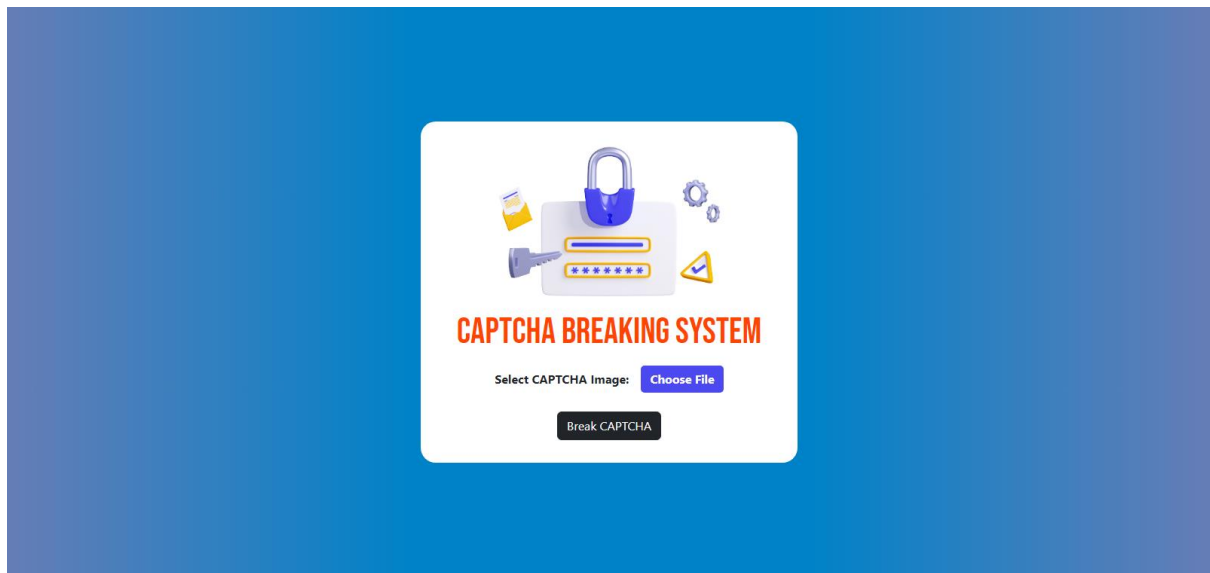
# 1. Twitter App

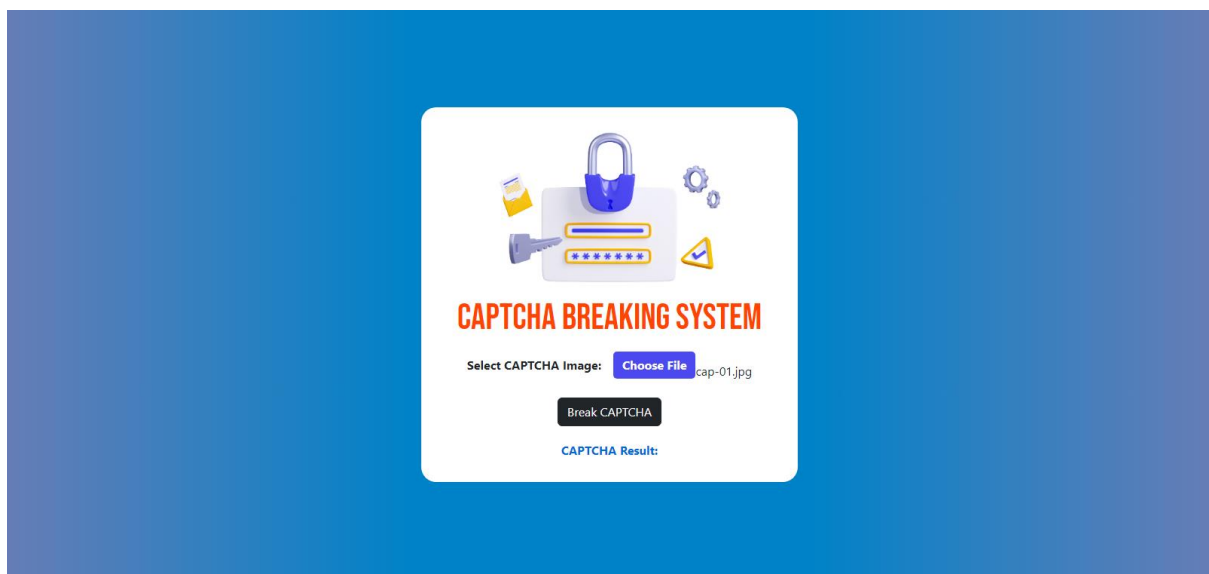
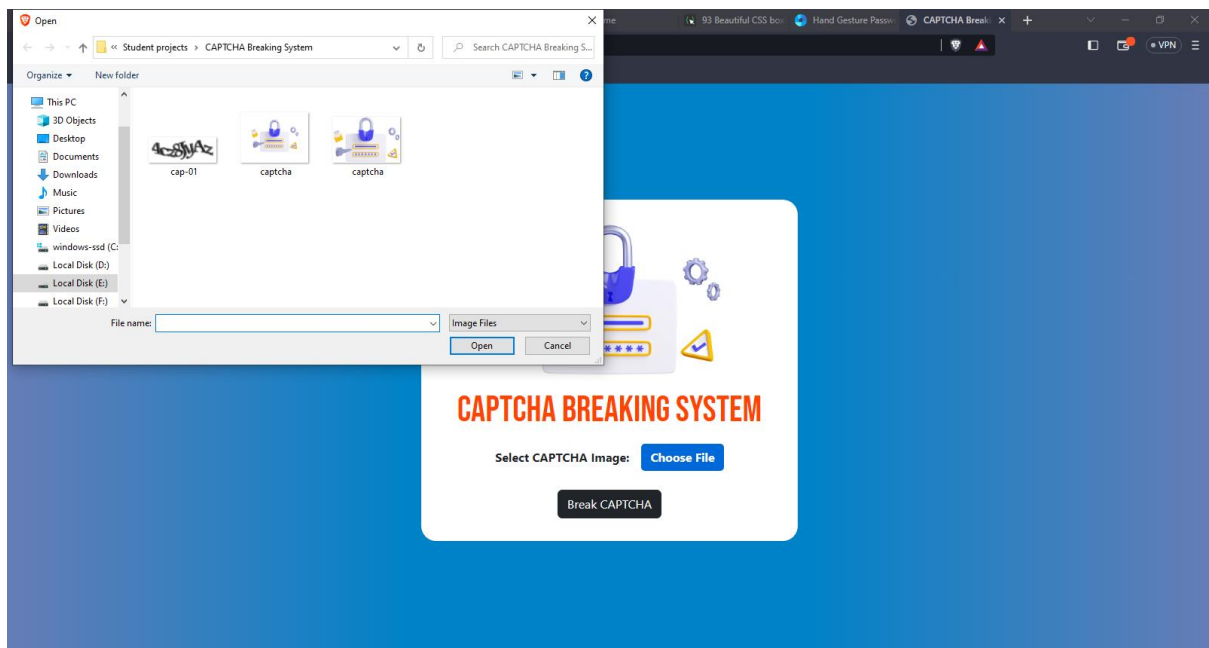


## 2. Hand Gesture Based Password System

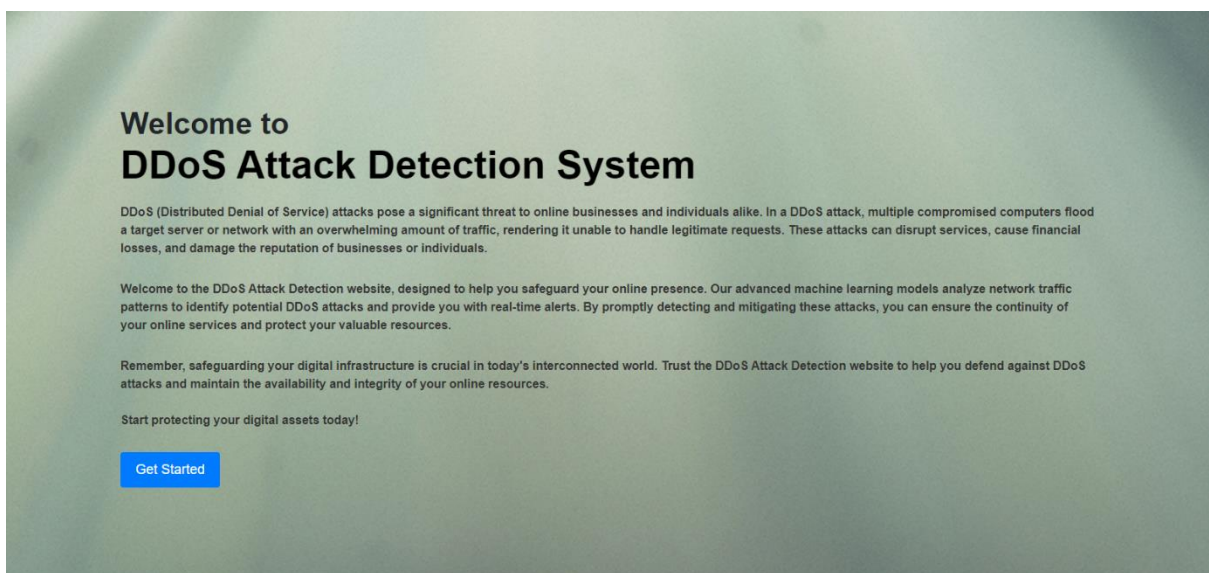


## 3. CAPTCHA Breaking System





## 4.DDoS Attack Detection System



[Go Back](#)



### DDoS Attack Detection Form

Upload CSV File:

[Choose File](#)

No file chosen

[Detect](#)

## 4. WIFI Intrusion/Attack Detection System

### Welcome to Wifi Attack Detection System

A WiFi intrusion/attack detection system is a vital component in securing wireless networks from unauthorized access, malicious activities, and potential security threats. By leveraging machine learning techniques, such as anomaly detection and pattern recognition, it becomes possible to detect and mitigate WiFi intrusions more effectively.

WiFi intrusion detection systems (IDS) monitor network traffic, analyze it in real-time, and identify any suspicious or malicious behavior. Machine learning algorithms are trained on a large dataset of normal network traffic to learn the patterns and characteristics of regular network behavior. Once the model is trained, it can identify deviations from the normal behavior and raise alerts when potential intrusions or attacks are detected.

[Get Started](#)

Go Back



### Wifi Attack Detection Form

Upload CSV File:

Choose File

No file chosen

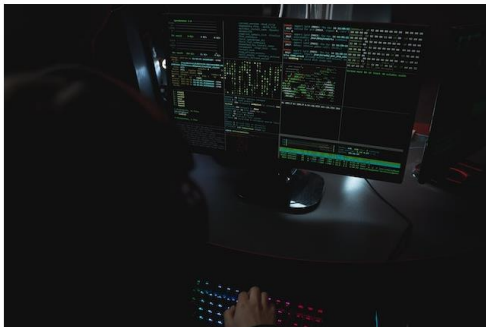
Detect

## 6. DGA Attack Detection System

Welcome to  
**DGA** ATTACK  
DETECTION  
SYSTEM

Get Started





## DGA Attack Detection Form

Upload CSV File:

Choose File

No file chosen

Detect

# 7. Firewall Attack Detection System

## Welcome to Firewall Attack Detection System

In today's digital landscape, network security is of paramount importance. Firewalls play a critical role in protecting computer networks from unauthorized access and malicious activities. To enhance the effectiveness of firewalls, we have developed an advanced Firewall System that leverages the power of machine learning.

Our website offers a user-friendly interface that allows you to upload CSV files containing network traffic data. This data is then sent to the backend, where our machine learning model performs analysis and prediction to determine whether the network traffic represents a Firewall attack or is deemed normal.

Get Started





Go Back



## Firewall Attack Detection Form

Upload CSV File:

Choose File

No file chosen

Detect