A

Mini Project

On

MODELING AND PREDICTING CYBER HACKING BREACHES

(Submitted in partial fulfillment of the requirements for the award of Degree)

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

Madala Hemanth	207R1A0593
Jupalli Venkata Sai	207R1A0582
Nimmala Nithish	207R1A05A7

Under the Guidance of

B.P Deepak Kumar

(Assistant Professor)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CMR TECHNICAL CAMPUS

UGC AUTONOMOUS

(Accredited by NAAC, NBA, Permanently Affiliated to JNTUH, Approved by AICTE, NewDelhi) Recognized Under Section 2(f) & 12(B) of the UGCAct.1956, Kandlakoya (V), Medchal Road, Hyderabad-501401.

2020-2024

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the project entitled **“MODELING AND PREDICTING CYBER HACKING BREACHES”** being submitted by **Madala Hemanth (207R1A0593), Jupalli Venkata Sai (207R1A0582) & Nimmala Nithish (207R1A05A7)** in partial fulfillment of the requirements for the award of the degree of B.Tech in Computer Science and Engineering to the Jawaharlal Nehru Technological University Hyderabad, is a record of bonafide work carried out by them under our guidance and supervision during the year 2022-23.

The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

B.P Deepak Kumar
(Assistant Professor)
INTERNAL GUIDE

Dr. A. Raji Reddy
DIRECTOR

Dr. K SRUJAN RAJU
HOD(CSE)

EXTERNAL EXAMINER

Submitted for viva voice Examination held on ____________________

ACKNOWLEDGEMENT

Apart from the efforts of us, the success of any project depends largely on the encouragement and guidelines of many others. We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project.

We take this opportunity to express my profound gratitude and deep regard to my guide **Mrs. B.P Deepak Kumar** Assistant Professor for her exemplary guidance, monitoring and constant encouragement throughout the project work. The blessing, help and guidance given by her shall carry us a long way in the journey of life on which we are about to embark.

We also take this opportunity to express a deep sense of gratitude to the Project Committee Review (PRC) **Dr. J. NARASIMHA RAO, Ms. SABA SULTANA** for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. K SRUJAN RAJU,** Head, Department of Computer Science and Engineering for providing encouragement and support for completing this project successfully.

We are obliged to **Dr. A. Raji Reddy,** Director for being cooperative throughout the course of this project. We also express our sincere gratitude to Sri. **Ch. Gopal Reddy,** Chairman for providing excellent infrastructure and a nice atmosphere throughout the courseof this project.

The guidance and support received from all the members of **CMR Technical Campus** who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project.

Madala Hemanth **(207R1A0593)**
Jupalli Venkata Sai **(207R1A0582)**
Nimmala Nithish **(207R1A05A7)**

ABSTRACT

Analyzing cyber incident data sets is an important method for deepening our understanding of the evolution of the threat situation. This is a relatively new research topic, and many studies remain to be done. In this paper, we report a statistical analysis of a breach incident data set corresponding to 12 years (2005–2017) of cyber hacking activities that include malware attacks. We show that, in contrast to the findings reported in the literature, both hacking breach incident inter-arrival times and breach sizes should be modeled by stochastic processes, rather than by distributions because they exhibit autocorrelations. Then, we propose particular stochastic process models to, respectively, fit the inter-arrival times and the breach sizes. We also show that these models can predict the inter-arrival times and the breach sizes. In order to get deeper insights into the evolution of hacking breach incidents, we conduct both qualitative and quantitative trend analyses on the data set. We draw a set of cybersecurity insights, including that the threat of cyber hacks is indeed getting worse in terms of their frequency, but not in terms of the magnitude of their damage.

LIST OF FIGURES

LIST OF SCREENSHOTS

TABLE OF CONTENTS

TABLE OF CONTENTS

1. INTRODUCTION

1.INTRODUCTION

1.1 PROJECT SCOPE

The present study is motivated by several questions that have not been investigated until now, such as: Are data breaches caused by cyber attacks increasing, decreasing, or stabilizing? A principled answer to this question will give us a clear insight into the overall situation of cyber threats. This question was not answered by previous studies. Specifically, the dataset analyzed in [7] only covered the time span from 2000 to 2008 and does not necessarily contain the breach incidents that are caused by cyber attacks; the dataset analyzed in [9] is more recent, but contains two kinds of incidents: negligent breaches (i.e., incidents caused by lost, discarded, stolen devices and other reasons) and malicious breaching

1.2 PROJECT PURPOSE

Data breaches are one of the most devastating cyber incidents. The Privacy Rights Clearinghouse [1] reports 7,730 data breaches between 2005 and 2017, accounting for 9,919,228,821 breached records. The Identity Theft Resource Center and Cyber Scout [2] reports 1,093 data breach incidents in 2016, which is 40% higher than the 780 data breach incidents in 2015. The United States Office of Personnel Management (OPM) [3] reports that the personnel information of 4.2 million current and former Federal government employees and the background investigation records of current, former, and prospective federal employees and contractors (including 21.5 million Social Security Numbers) were stolen in 2015

1.3 PROJECT FEATURES

Developing a system for modeling and predicting cyber hacking breaches involves data collection, preprocessing, and feature engineering. It requires implementing anomaly detection and behavioral analysis techniques to identify threats. Threat intelligence integration enhances threat understanding, and real-time monitoring with alerting systems ensures rapid response. Machine learning models, feature selection, and evaluation metrics are used for accurate predictions. The system should prioritize scalability, explainability, and compliance with regulations while considering ethical concerns. Collaboration with security experts, legal coordination, and user training are essential for robust cybersecurity.

2.SYSTEM ANALYSIS

2.SYSTEM ANALYSIS

System analysis is the important phase in the system development process. The System is studied to the minute details and analyzed. The system analyst plays an important role of an interrogator and dwells deep into the working of the present system.

In analysis, a detailed study of these operations performed by the system and their relationships within and outside the system is done. A key question considered here is, “what must be done to solve the problem?”

2.1 PROBLEM DEFINITION

Analyzing cyber incident datasets is an important method for deepening our understanding of the evolution of the threat situation.

2.2 EXISTING SYSTEM

- The study aims to investigate the trend of data breaches caused by cyber attacks.
- Previous studies had limitations: one had a limited time span (2000-2008) and may not include cyber attack-related breaches, while another included both negligent and malicious breaches.
- Negligent breaches caused by human errors are excluded from the study.
- The study focuses specifically on the hacking sub-category of malicious breaches.
- The other sub-categories (insider, payment card fraud, unknown) will be analyzed separately.
- The study seeks to provide a principled answer to the question of whether data breaches caused by cyber attacks are increasing, decreasing, or stabilizing.

2.2.1 DISADVANTAGES OF EXISTING SYSTEM

- The study focuses on a subset of data breaches caused by cyber-attacks, limiting generalizability.
- The data used may not be comprehensive or representative of all cyber-attack-related breaches.
- Methodological challenges exist in studying trends due to evolving and difficult-to-track cyber-attacks.

2.3 PROPOSED SYSTEM

- Stochastic processes are shown to be more suitable for modeling hacking breach incident inter-arrival times and breach sizes than traditional distributions.
- Positive dependence between inter-arrival times and breach sizes is discovered, described by a specific copula model.
- Qualitative and quantitative trend analyses reveal increasing frequency but stabilizing breach sizes in hacking breach incidents.
- The study provides valuable insights for risk mitigation approaches, benefiting insurance companies, government agencies, and regulators.

2.3.1 ADVANTAGES OF THE PROPOSED SYSTEM

- The proposed stochastic process models accurately predict inter-arrival times and breach sizes of hacking breach incidents, aiding in preparation and response.
- The model incorporates positive dependence, improving prediction accuracy and risk assessment.
- Deeper insights into data breach risks empower better decision-making for insurance companies, government agencies, and regulators.

2.4 FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and a business proposalis put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This isto ensure that the proposed system is not a burden to the company. Three key considerations involved in the feasibility analysis:

- Economic Feasibility
- Technical Feasibility
- Social Feasibility

2.2.1 ECONOMIC FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

2.4.2 TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

2.4.3 SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

2.5 HARDWARE & SOFTWARE REQUIREMENTS

2.5.1 HARDWARE REQUIREMENTS :

- Processor: Pentium IV or higher
- RAM: 256 MB
- Space on Hard Disk: minimum 512MB

2.5.2 SOFTWARE REQUIREMENTS :

- Python
- Django
- MySQL
- Wamp server

3.ARCHITECTURE

3. ARCHITECTURE

3.1 PROJECT ARCHITECTURE

This project architecture shows the procedure followed for classification,starting from input to final prediction.

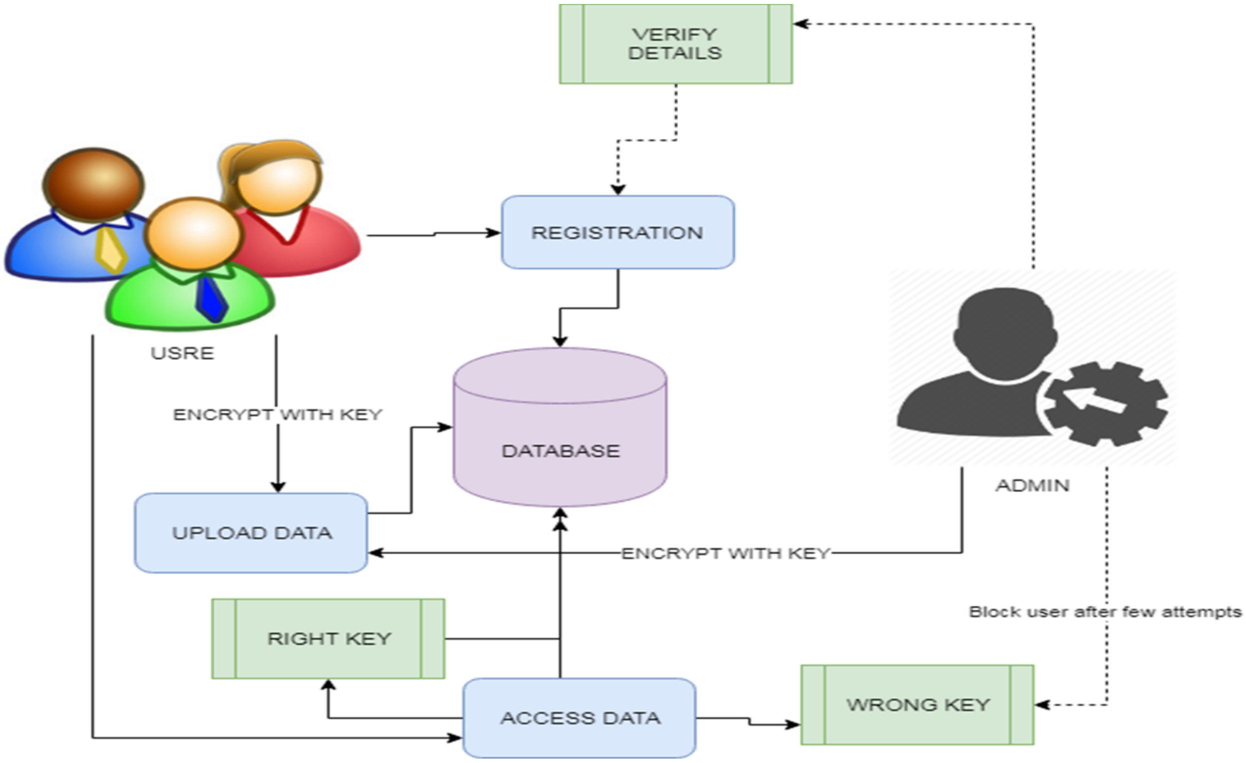


Figure 3.1: Architecture Of Modeling And Predicting Cyber Hacking Breaches

3.2 USE CASE DIAGRAM

In the use case diagram, we have basically one actor who is the user in the trained model. A use case diagram is a graphical depiction of a user's possible interactions with a system. A use case diagram shows various use cases and different types of usersthe system has. The use cases are represented by either circles or ellipses. The actors are often shown as stick figures.

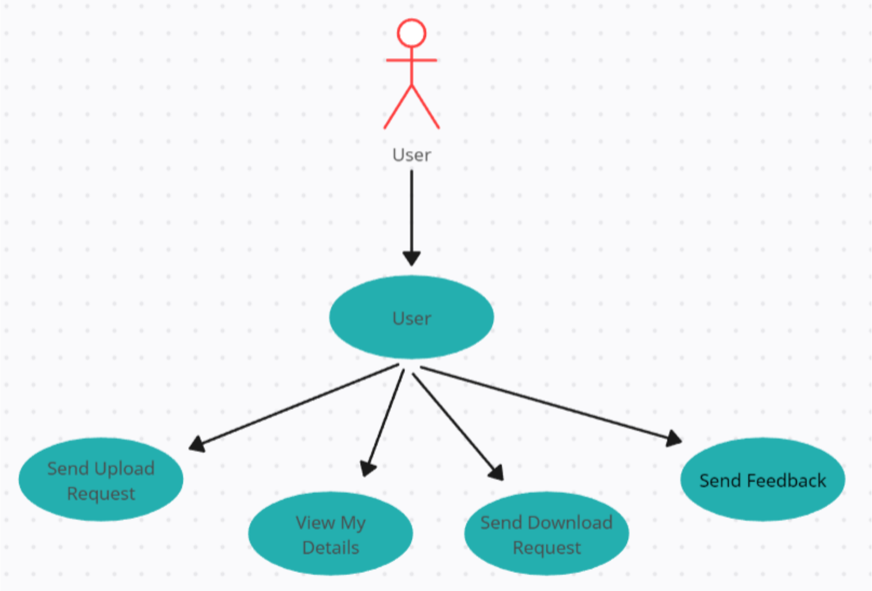


Figure 3.2.1: Use Case Diagram For User

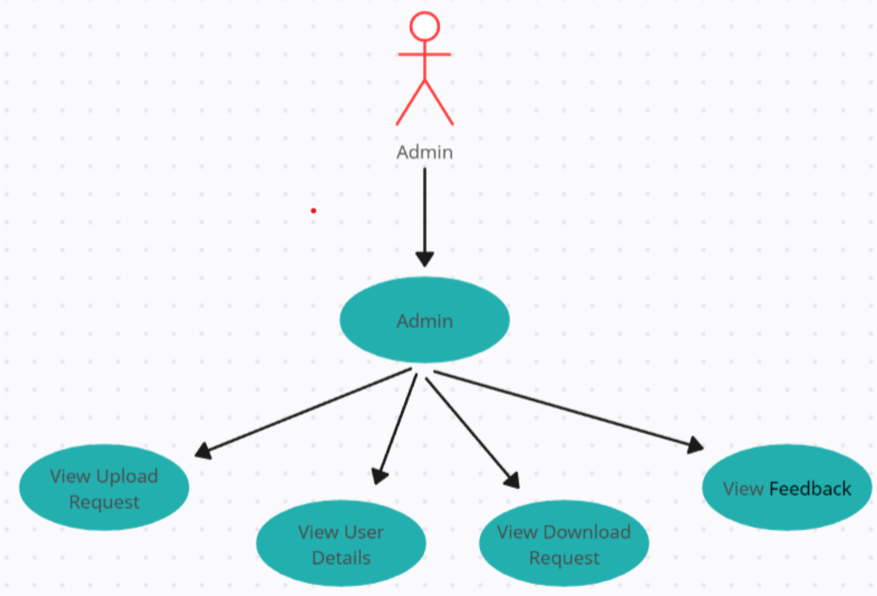


Figure 3.2.2: Use Case Diagram For Admin

3.2 CLASS DIAGRAM

Class diagram is a type of static structure diagram that describes the structure of a system by showing the system’s classes, their attributes, operations (or methods), and the relationships among objects.

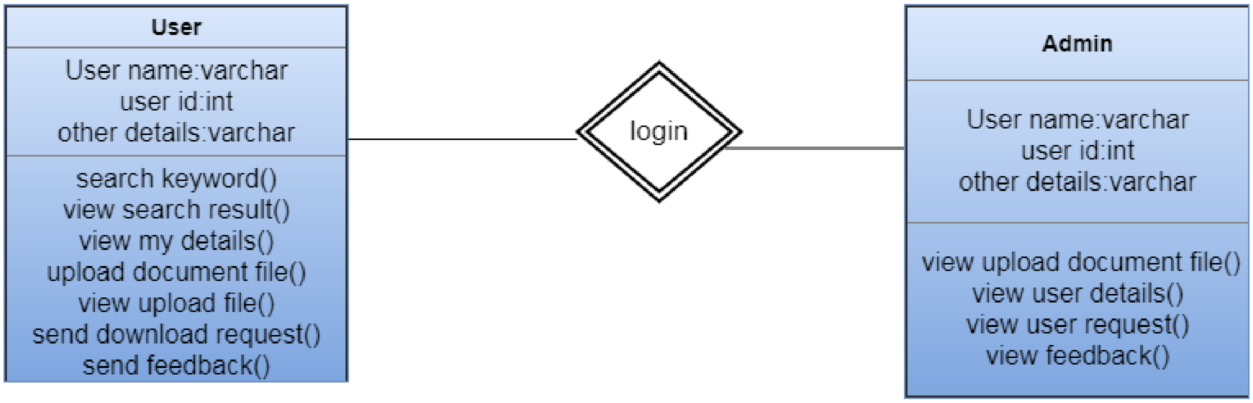


Figure 3.3: Class Diagram for Modeling And Predicting Cyber Hacking Breaches

3.4 SEQUENCE DIAGRAM

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the logical view of the system under development.

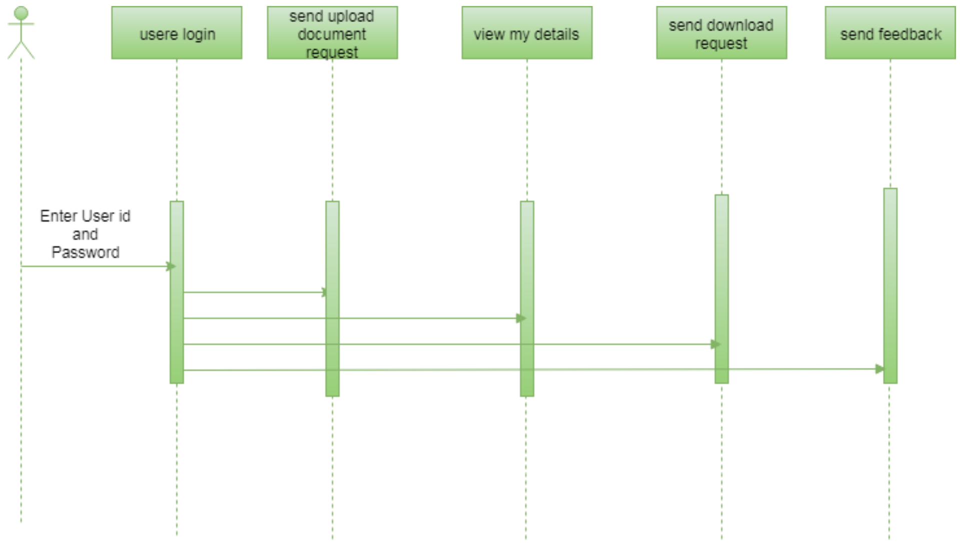


Figure 3.4.1: Sequence Diagram For User

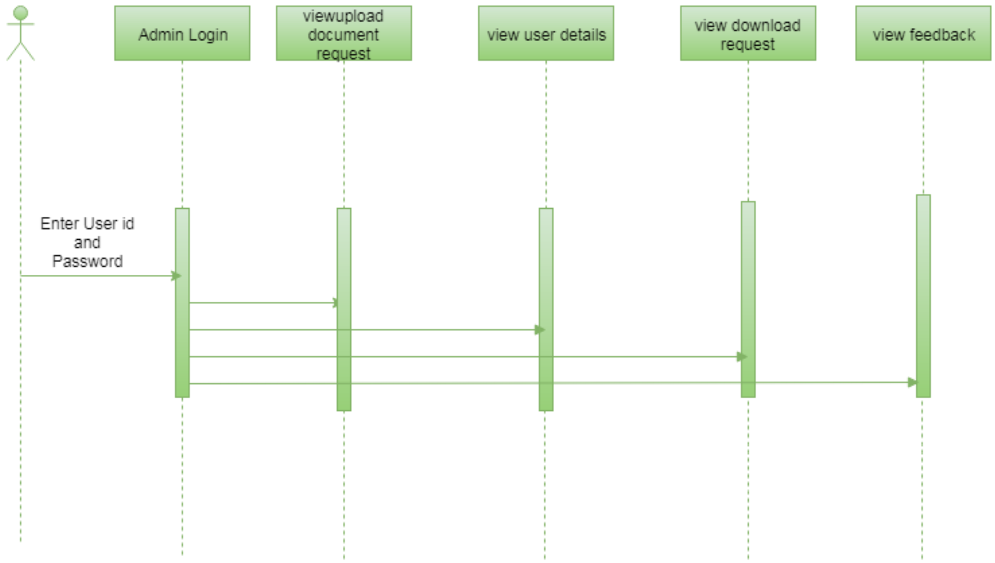


Figure 3.4.2: Sequence Diagram For Admin

3.5 ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. They can alsoinclude elements showing the flow of data between activities through one or more datastores.

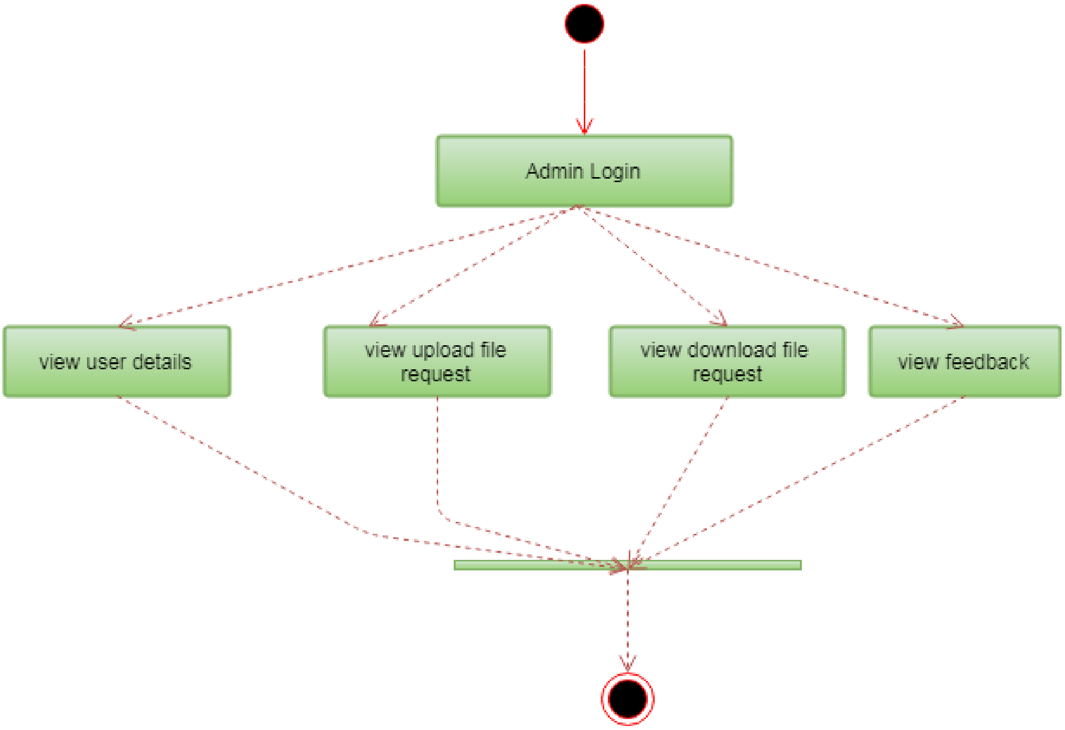


Figure 3.5.1: Activity Diagram For Admin

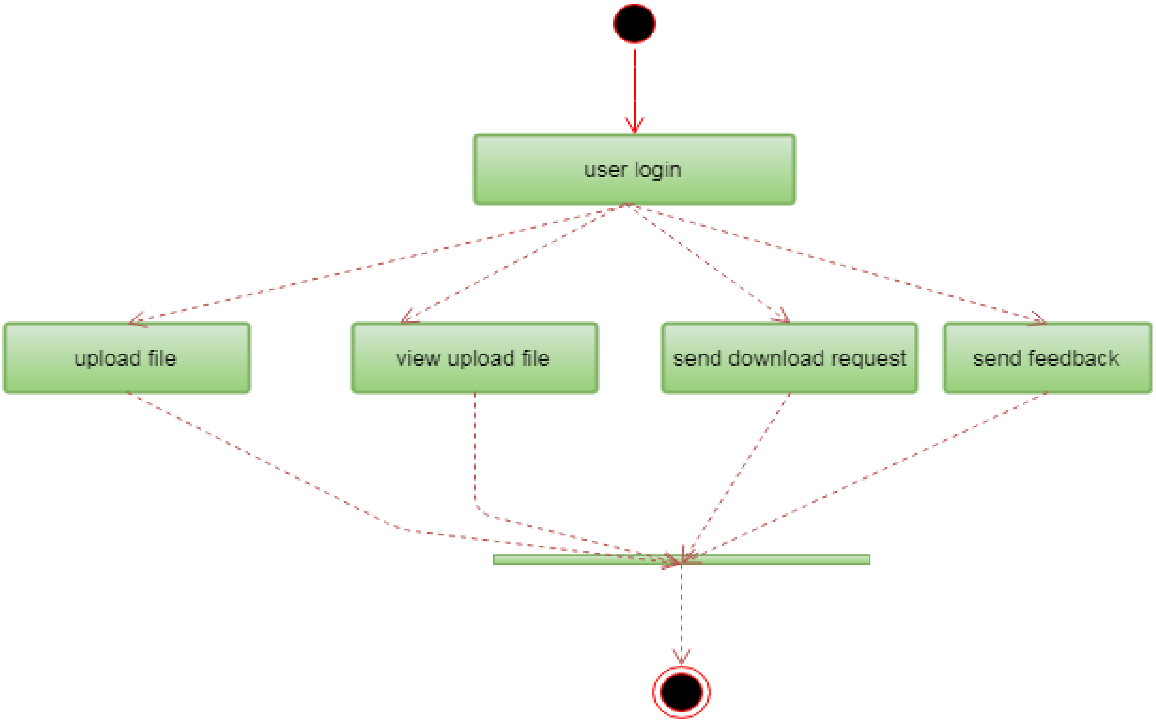


Figure 3.5.2: Activity Diagram For User

4.IMPLEMENTATION

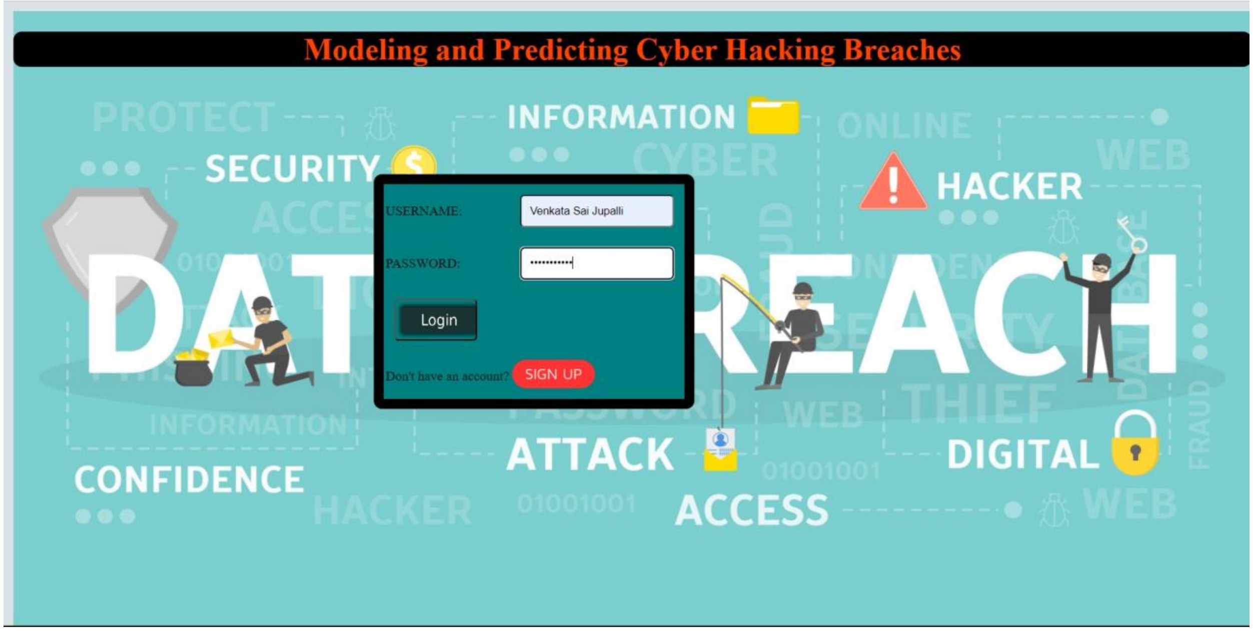
4.1 SAMPLE CODE

```
import re
from django.contrib import messages
from django.contrib.auth import authenticate
from django.db.models import Q, Count
from django.shortcuts import render, redirect

# Create your views here.
from Cyber_Users.forms import UserRegister_Form
from Cyber_Users.models import UserRegister_Model, UserAdd_Model

def user_login(request):
    if request.method == "POST":
        name = request.POST.get('name')
        password = request.POST.get('password')
        try:
            check = UserRegister_Model.objects.get(name=name,password=password)
            request.session['userid'] = check.id
            return redirect('user_adddata')
        except:
            pass
        user = authenticate(name=name,password=password)
        if user is not None:
            if user.is_active:
                return redirect('user_adddata')
        else:
            messages.error(request, 'username or password are not match')
            return redirect('user_login')
    return render(request, 'users/user_login.html')

def user_register(request):
    if request.method == "POST":
        forms = UserRegister_Form(request.POST)
        if forms.is_valid():
            forms.save()
            messages.success(request, 'You have been successfully registered')
            return redirect('user_login')
    else:
        forms = UserRegister_Form()
    return render(request,'users/user_register.html',{'form':forms})

def user_adddata(request):
    userid = request.session["userid"]
    obj = UserRegister_Model.objects.get(id=userid)
    attack1 = []
    attack2, attack3, attack4, attack5, attack6, attack7, attack8, attack9 = [], [], [], [], [], [], [], []
    splt = ''
    Entity = ''
    Year = 0
    Records = ''
    Organizationtype = ''
    Method = ''
    txt =''
    Adddata = ''
    ans = ''
    Time = ''
    if request.method == "POST":
        Entity = request.POST.get("entity")
        Year = request.POST.get("year")
        Records = request.POST.get("records")
        Organizationtype = request.POST.get("organizationtype")
        Method = request.POST.get("method")
        txt = request.POST.get("name")
        Time = request.POST.get("time")
        splt = (re.findall(r"[\w']+", str(txt)))
    for f in splt:
        if f in ('IPid', 'FDDI', 'x25', 'rangingdistance'):
            attack1.append(f)
        elif f in ('tcpchecksum', 'mtcp', 'controlflags', 'tcpoffset', 'tcpport'):
            attack2.append(f)
        elif f in ('ICMPID', 'udptraffic', 'udpunicorn', 'datagramid', 'NTP', 'RIP', 'TFTP'):
            attack3.append(f)
        elif f in ('GETID', 'POSTID', 'openBSD', 'appid', 'sessionid', 'transid', 'physicalid'):
            attack4.append(f)
        elif f in ('SYN', 'ACK', 'synpacket', 'sycookies'):
            attack5.append(f)
        elif f in ('serverattack', 'serverid', 'blockbankwidth'):
            attack6.append(f)
        elif f in ('monlist', 'getmonlist', 'NTPserver'):
            attack7.append(f)
        elif f in ('portid', 'FTPID', 'tryion', 'fragflag'):
            attack8.append(f)
        elif f in ('malwareid', 'gethttpid', 'httpid'):
            attack9.append(f)
    if len(attack1) > len(attack2) and len(attack1) > len(attack3) and len(attack1) > len(attack4) and
len(
            attack1) > len(attack5) and len(attack1) > len(attack6) and len(attack1) > len(attack7) and
len(
        attack1) > len(attack8) and len(attack1) > len(attack9):
        ans = "Man-in-the-middle Attack"
    elif len(attack2) > len(attack1) and len(attack2) > len(attack3) and len(attack2) > len(attack4)
and len(
            attack2) > len(attack5) and len(attack2) > len(attack6) and len(attack2) > len(attack7) and
len(
        attack2) > len(attack8) and len(attack2) > len(attack9):
```

```
        ans = "Phishing and spear phishing attacks"
    elif len(attack3) > len(attack2) and len(attack3) > len(attack1) and len(attack3) > len(attack4)
and len(
            attack1) > len(attack5) and len(attack1) > len(attack6) and len(attack1) > len(attack7) and
len(
        attack1) > len(attack8) and len(attack1) > len(attack9):
        ans = "Drive-by attack"
    elif len(attack4) > len(attack2) and len(attack4) > len(attack3) and len(attack4) > len(attack1)
and len(
            attack4) > len(attack5) and len(attack4) > len(attack6) and len(attack4) > len(attack7) and
len(
        attack4) > len(attack8) and len(attack4) > len(attack9):
        ans = "Password attack"
    elif len(attack5) > len(attack2) and len(attack5) > len(attack3) and len(attack5) > len(attack4)
and len(
            attack5) > len(attack1) and len(attack5) > len(attack6) and len(attack5) > len(attack7) and
len(
        attack5) > len(attack8) and len(attack5) > len(attack9):
        ans = "SQL injection attack"
    elif len(attack6) > len(attack2) and len(attack6) > len(attack3) and len(attack6) > len(attack4)
and len(
            attack6) > len(attack5) and len(attack6) > len(attack1) and len(attack6) > len(attack7) and
len(
        attack6) > len(attack8) and len(attack6) > len(attack9):
        ans = "Cross-site scripting (XSS) attack"
    elif len(attack7) > len(attack2) and len(attack7) > len(attack3) and len(attack7) > len(attack4)
and len(
            attack7) > len(attack5) and len(attack7) > len(attack6) and len(attack7) > len(attack1) and
len(
        attack7) > len(attack8) and len(attack7) > len(attack9):
        ans = "Eavesdropping attack"
    elif len(attack8) > len(attack2) and len(attack8) > len(attack3) and len(attack8) > len(attack4)
```

```
and len(
            attack8) > len(attack5) and len(attack8) > len(attack6) and len(attack8) > len(attack7) and
len(
        attack8) > len(attack1) and len(attack8) > len(attack9):
        ans = "Birthday attack"
    elif len(attack9) > len(attack2) and len(attack9) > len(attack3) and len(attack9) > len(attack4)
and len(
            attack9) > len(attack5) and len(attack9) > len(attack6) and len(attack9) > len(attack7) and
len(
        attack9) > len(attack8) and len(attack9) > len(attack1):
        ans = "Teardrop attack"
    else:
        ans = "Unmalware"

UserAdd_Model.objects.create(uregid=obj,entity=Entity,year=Year,records=Records,organizati
ontype=Organizationtype,method=Method,adddata=txt,attackresult=ans,time=Time)
    return render(request,'users/user_adddata.html')

def user_page(request):
    obj = UserAdd_Model.objects.all()
    return render(request,'users/user_page.html',{'object':obj})

def malware(request):
    obj = UserAdd_Model.objects.filter(Q(attackresult='Man-in-the-middle (MitM) attack') |
Q(attackresult='Phishing and spear phishing attacks') | Q(
        attackresult='Drive-by attack') | Q(attackresult='Password attack') | Q(
        attackresult='SQL injection attack') | Q(attackresult='Cross-site scripting (XSS) attack') |
Q(attackresult='Eavesdropping attack') | Q(
        attackresult='Birthday attack') | Q(attackresult='Teardrop attack'))
    return render(request,'users/malware.html',{'object':obj})

def unmalware(request):
    obj = UserAdd_Model.objects.filter(attackresult='Unmalware')
    return render(request,'users/unmalware.html',{'object':obj})

def breaches_analysis(request):
    chart =
UserAdd_Model.objects.values('attackresult','method').annotate(dcount=Count('attackresult'))
    return render(request,'users/breaches_analysis.html',{'objects':chart})

def chart_page(request,chart_type):
    chart = UserAdd_Model.objects.values('year').annotate(dcount=Count('organizationtype'))
    return render(request,'users/chart_page.html',{'chart_type':chart_type,'objects':chart})
from tkinter import CASCADE
from django.db import models

# Create your models here.
class UserRegister_Model(models.Model):
    name = models.CharField(max_length=50)
    email = models.EmailField(max_length=30)
    password = models.CharField(max_length=10)
    phoneno = models.CharField(max_length=15)
    address = models.CharField(max_length=500)

class UserAdd_Model(models.Model):
    uregid = models.ForeignKey(UserRegister_Model)
    entity = models.CharField(max_length=100)
    year = models.IntegerField()
    records = models.CharField(max_length=1000)
    organizationtype=models.CharField(max_length=1000)
    method = models.CharField(max_length=100)
    adddata = models.CharField(max_length=500)
    attackresult = models.CharField(max_length=500)
    time = models.CharField(max_length=100)
```

5.SCREENSHOTS



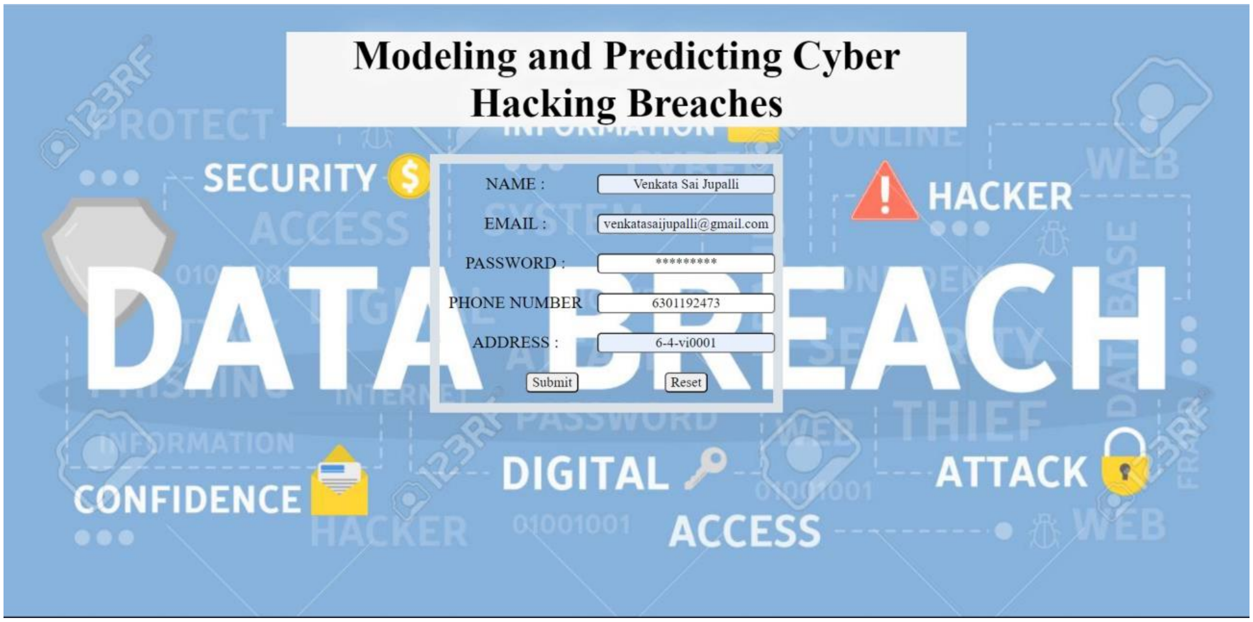
Modeling and Predicting Cyber Hacking Breaches

USERNAME: Venkata Sai Jupalli

PASSWORD: •••••••••••

Don't have an account?

Figure 5.1: Login Page



Modeling and Predicting Cyber Hacking Breaches

NAME : Venkata Sai Jupalli

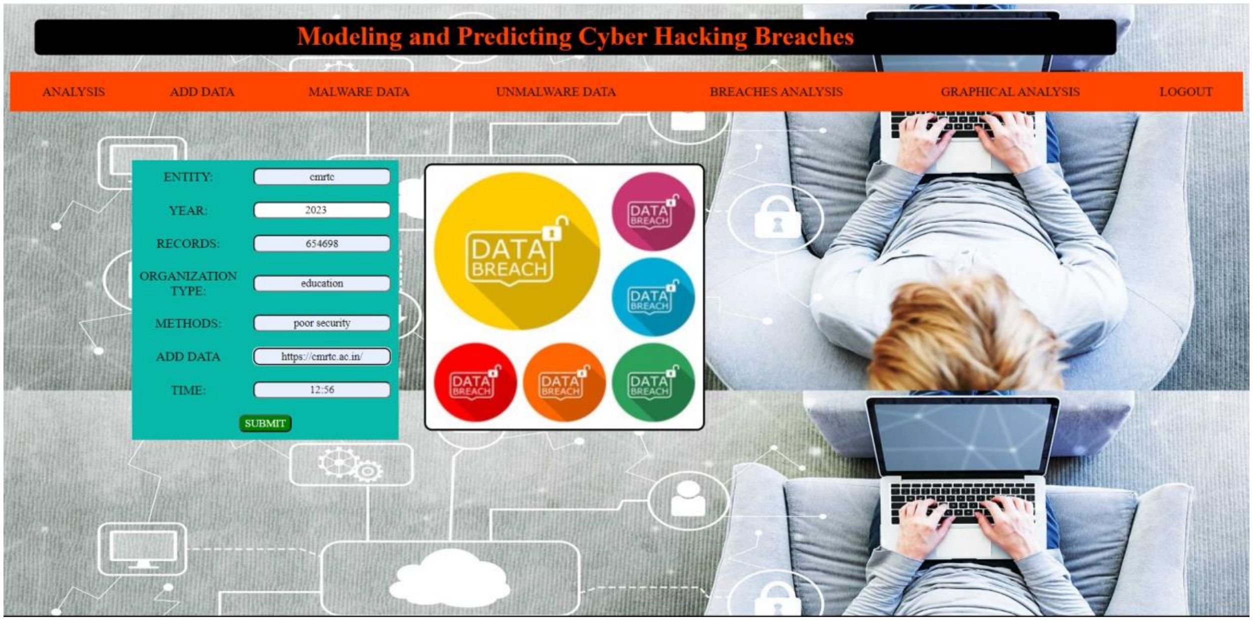
EMAIL : venkatasaijupalli@gmail.com

PASSWORD : *********

PHONE NUMBER 6301192473

ADDRESS : 6-4-vi0001

Figure 5.2: Register Page



ENTITY: cmrtc

YEAR: 2023

RECORDS: 654698

ORGANIZATION TYPE: education

METHODS: poor security

ADD DATA https://cmrtc.ac.in/

TIME: 12:56

Figure 5.3: Add Data page

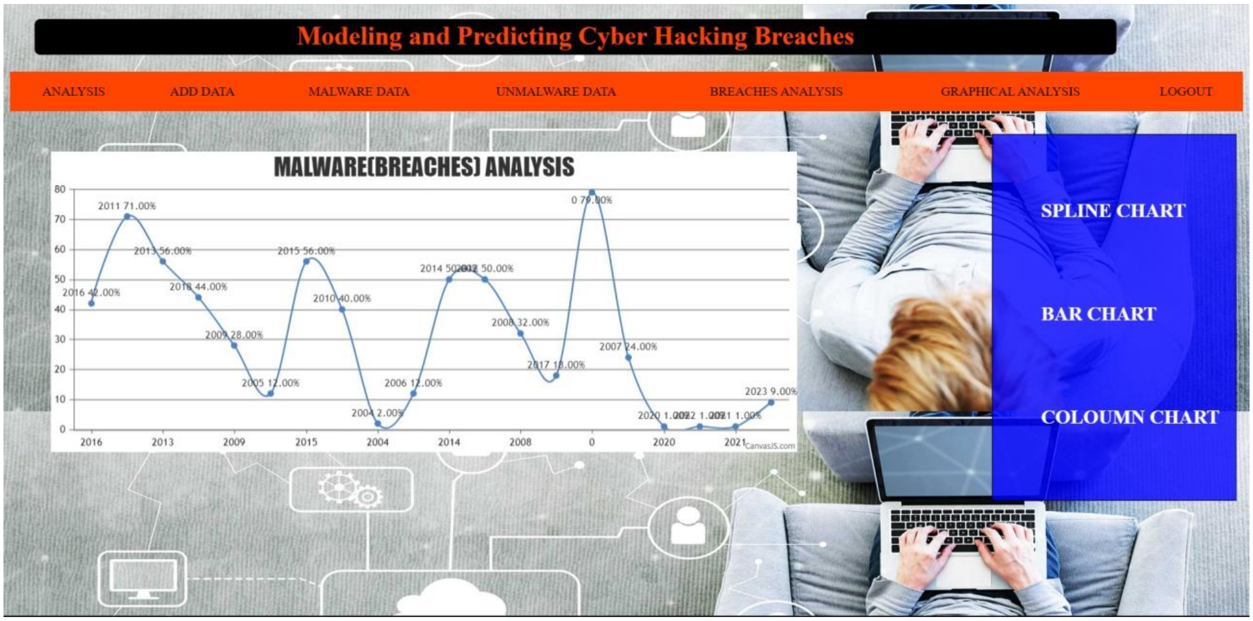
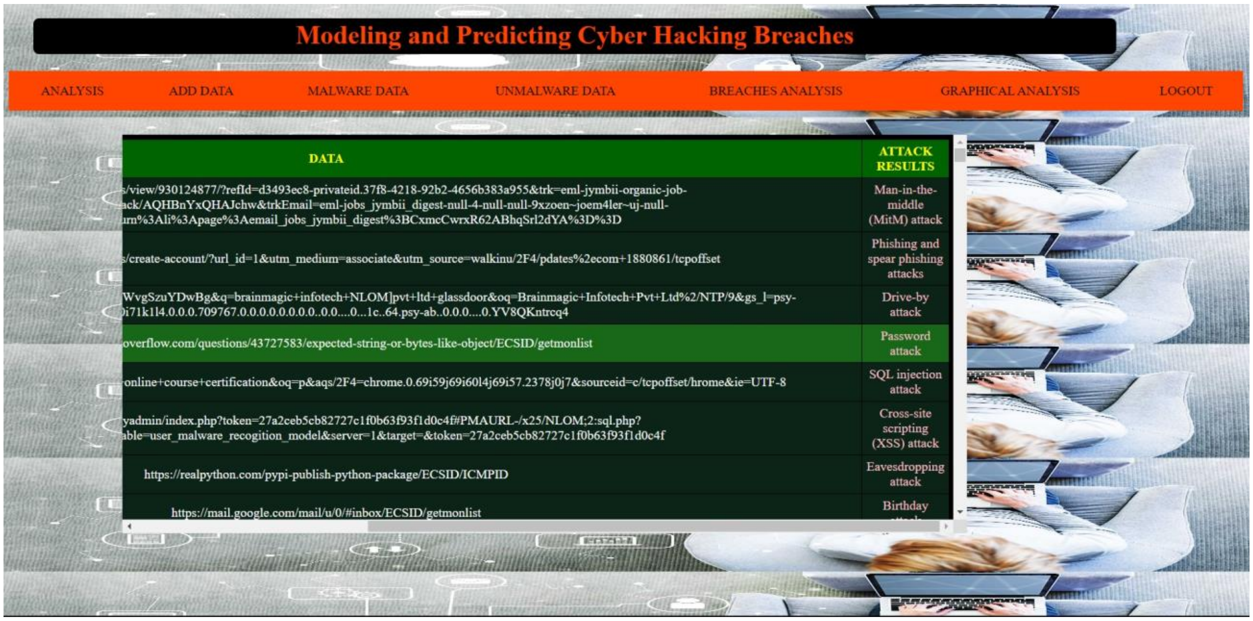
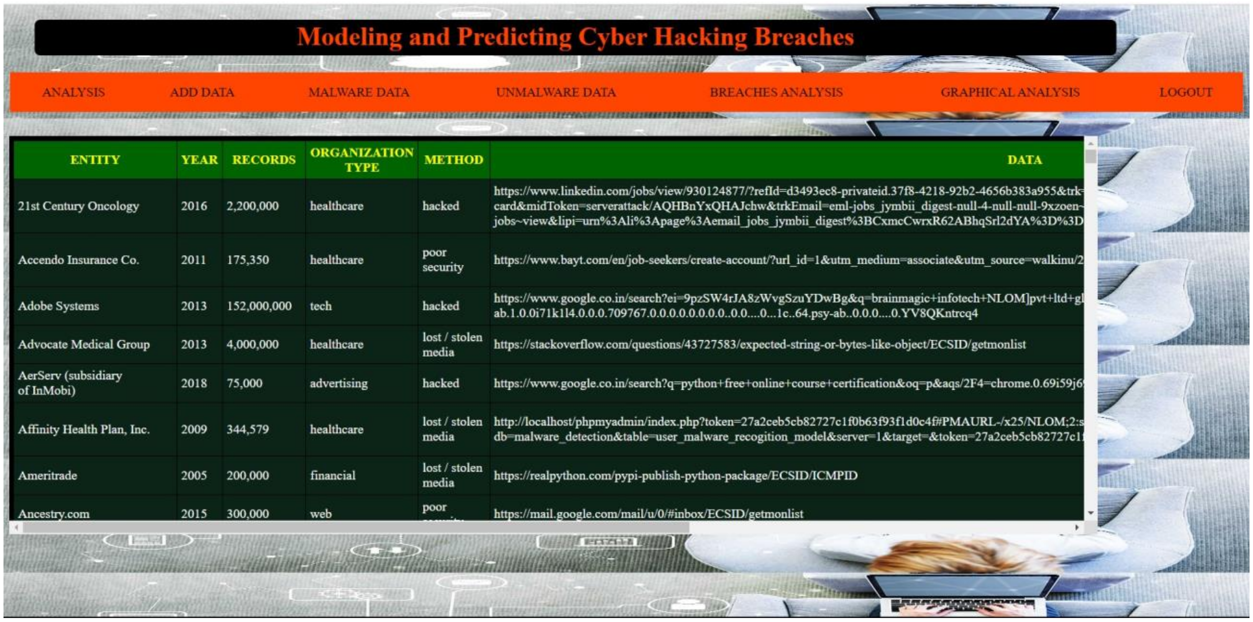


Figure 5.4: Graphical Analysis Page



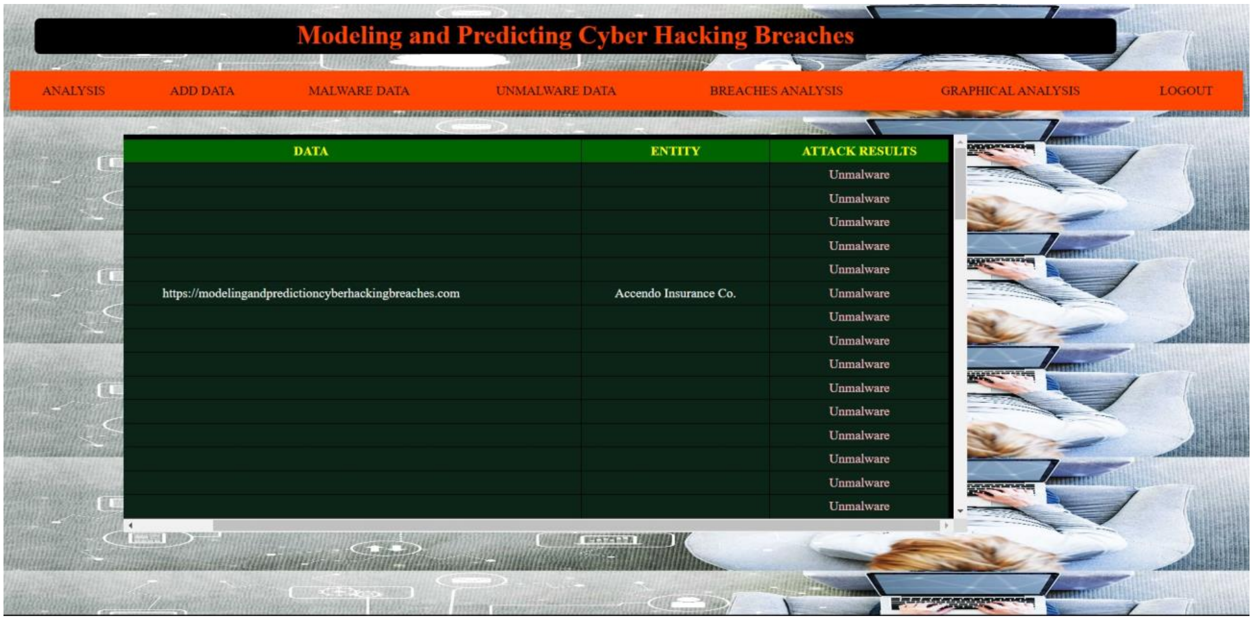
DATA	ATTACK RESULTS
s/view/930124877/?refId=d3493ec8-privateid.37f8-4218-92b2-4656b383a955&trk=eml-jymbii-organic-job- ack/AQHBnYxQHAJchw&trkEmail=eml-jobs_jymbii_digest-null-4-null-null-9xzoen~joem4ler~uj-null- urn%3Ali%3Apage%3Aemail_jobs_jymbii_digest%3BCxmcCwrxR62ABhqSrl2dYA%3D%3D	Man-in-the-middle (MitM) attack
s/create-account/?url_id=1&utm_medium=associate&utm_source=walkinu/2F4/pdates%2ecom+1880861/tcpoffset	Phishing and spear phishing attacks
WvgSzuYDwBg&q=brainmagic+infotech+NLOM]pvt+ltd+glassdoor&oq=Brainmagic+Infotech+Pvt+Ltd%2/NTP/9&gs_l=psy- 0i71k1l4.0.0.0.709767.0.0.0.0.0.0.0.0..0.0....0...1c..64.psy-ab..0.0.0....0.YV8QKntrcq4	Drive-by attack
overflow.com/questions/43727583/expected-string-or-bytes-like-object/ECSID/getmonlist	Password attack
online+course+certification&oq=p&aqs/2F4=chrome.0.69i59j69i60l4j69i57.2378j0j7&sourceid=c/tcpoffset/hrome&ie=UTF-8	SQL injection attack
yadmin/index.php?token=27a2ceb5cb82727c1f0b63f93f1d0c4f#PMAURL-/x25/NLOM;2:sql.php? able=user_malware_recogition_model&server=1&target=&token=27a2ceb5cb82727c1f0b63f93f1d0c4f	Cross-site scripting (XSS) attack
https://realpython.com/pypi-publish-python-package/ECSID/ICMPID	Eavesdropping attack
https://mail.google.com/mail/u/0/#inbox/ECSID/getmonlist	Birthday

Figure 5.5: Analysis Page



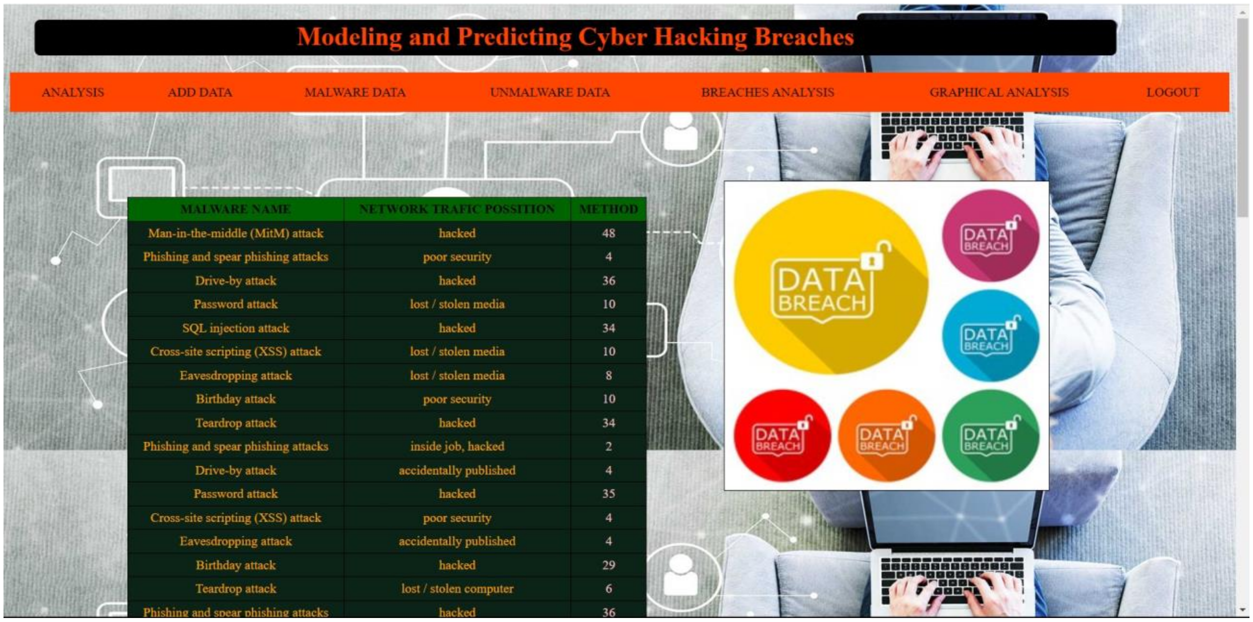
ENTITY	YEAR	RECORDS	ORGANIZATION TYPE	METHOD	DATA
21st Century Oncology	2016	2,200,000	healthcare	hacked	https://www.linkedin.com/jobs/view/930124877/?refId=d3493ec8-privateid.37f8-4218-92b2-4656b383a955&trk= card&midToken=serverattack/AQHBnYxQHAJchw&trkEmail=eml-jobs_jymbii_digest-null-4-null-null-9xzoen- jobs~view&lipi=urn%3Ali%3Apage%3Aemail_jobs_jymbii_digest%3BCxmcCwrxR62ABhqSrl2dYA%3D%3D
Accendo Insurance Co.	2011	175,350	healthcare	poor security	https://www.bayt.com/en/job-seekers/create-account/?url_id=1&utm_medium=associate&utm_source=walkinu/2
Adobe Systems	2013	152,000,000	tech	hacked	https://www.google.co.in/search?ei=9pzSW4rJA8zWvgSzuYDwBg&q=brainmagic+infotech+NLOM]pvt+ltd+gl ab.1.0.0i71k1l4.0.0.0.709767.0.0.0.0.0.0.0.0..0.0....0...1c..64.psy-ab..0.0.0....0.YV8QKntrcq4
Advocate Medical Group	2013	4,000,000	healthcare	lost / stolen media	https://stackoverflow.com/questions/43727583/expected-string-or-bytes-like-object/ECSID/getmonlist
AerServ (subsidiary of InMobi)	2018	75,000	advertising	hacked	https://www.google.co.in/search?q=python+free+online+course+certification&oq=p&aqs/2F4=chrome.0.69i59j6
Affinity Health Plan, Inc.	2009	344,579	healthcare	lost / stolen media	http://localhost/phpmyadmin/index.php?token=27a2ceb5cb82727c1f0b63f93f1d0c4f#PMAURL-/x25/NLOM;2:s db=malware_detection&table=user_malware_recogition_model&server=1&target=&token=27a2ceb5cb82727c1
Ameritrade	2005	200,000	financial	lost / stolen media	https://realpython.com/pypi-publish-python-package/ECSID/ICMPID
Ancestry.com	2015	300,000	web	poor	https://mail.google.com/mail/u/0/#inbox/ECSID/getmonlist

Figure 5.6: Malware Data Page



DATA	ENTITY	ATTACK RESULTS
		Unmalware
		Unmalware
		Unmalware
		Unmalware
		Unmalware
https://modelingandpredictioncyberhackingbreaches.com	Accendo Insurance Co.	Unmalware
		Unmalware
		Unmalware
		Unmalware
		Unmalware
		Unmalware
		Unmalware
		Unmalware
		Unmalware
		Unmalware

Figure 5.7: Unmalware Data Page



MALWARE NAME	NETWORK TRAFIC POSSITION	METHOD
Man-in-the-middle (MitM) attack	hacked	48
Phishing and spear phishing attacks	poor security	4
Drive-by attack	hacked	36
Password attack	lost / stolen media	10
SQL injection attack	hacked	34
Cross-site scripting (XSS) attack	lost / stolen media	10
Eavesdropping attack	lost / stolen media	8
Birthday attack	poor security	10
Teardrop attack	hacked	34
Phishing and spear phishing attacks	inside job, hacked	2
Drive-by attack	accidentally published	4
Password attack	hacked	35
Cross-site scripting (XSS) attack	poor security	4
Eavesdropping attack	accidentally published	4
Birthday attack	hacked	29
Teardrop attack	lost / stolen computer	6
Phishing and spear phishing attacks	hacked	36

Figure 5.8: Breaches Analysis Page

6.TESTING

6.TESTING

6.1 INTRODUCTION TO TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

6.2 TYPES OF TESTING

6.2.1 UNIT TESTING

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application. It is done after the completion of an individual unit before integration. This is a structural testing that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application and/or system configuration.

6.2.2 INTEGRATION TESTING

Integration tests are designed to test integrated software components to determine if they actually run as one program. Integration tests demonstrate that although the components were individually satisfactory, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

6.2.3 FUNCTIONAL TESTING

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input: identified classes of valid input must be accepted.

Invalid Input: identified classes of invalid input mustbe rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputsmust be exercised.

Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases.

6.2 TEST CASES

S.no	Test Case	Excepted Result	Result	Remarks(IF Fails)
1.	User Register	If User registration successfully.	Pass	If already user email exist then it fails.
2.	User Login	If User name and password is correct then it will getting valid page.	Pass	Un Register Users will not logged in.
3.	Start Data Pre process	Image has to upload	Pass	Corona Discharge Image must be select
4	Models Executed	For out four algorithms has executed and calculated 3 features	Pass	Models executed and predicted the results
5	Admin login	Admin can login with his login credential. If success he get his home page	Pass	Invalid login details will not allowed here
6.	Admin can activate the register users	Admin can activate the register user id	Pass	If user id not found then it won’t login.

7.CONCLUSION

&

FUTURE SCOPE

7.CONCLUSION & FUTURE SCOPE

7.1 PROJECT CONCLUSION

We analyzed a hacking breach dataset from the points of view of the incidents inter-arrival time and the breach size, and showed that they both should be modeled by stochastic processes rather than distributions. The statistical models developed in this paper show satisfactory fitting and prediction accuracies.

7.2 FUTURE SCOPE

The future of modeling and predicting cyber hacking breaches holds great potential with advancements in machine learning, behavioral analytics, IoT, cloud security, and quantum computing threats. As the cybersecurity landscape evolves, predictive models will play a crucial role in enhancing threat detection and prevention. Collaboration, compliance, and ethical considerations will also be significant factors in shaping this field

8.REFERENCES

8. REFERENCES

8.1 REFERENCES

[1] P. R. Clearinghouse, “Privacy rights clearinghouse’s chronology of data breaches.” https://www.privacyrights.org/data-breaches, Last accessed on November 9, 2017.

[2] I. T. R. Center, “http://www.idtheftcenter.org/2016databreaches.html.”

[3] C. R. Center, “Cybersecurity incidents.” https://www.opm.gov/ cybersecurity/cybersecurity-incidents/, Last accessed on November 9, 2017.

[4] I. Security, “https://www.ibm.com/security/data-breach/index.html.”

[5] N. . C. C. Study, “https://netdiligence.com/wp-content/uploads/2016/10/ P02 NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf.”

[6] M. Eling and W. Schnell, “What do we know about cyber risk and cyber risk insurance?,” The Journal of Risk Finance, vol. 17, no. 5, pp. 474– 491, 2016.

[7] T. Maillart and D. Sornette, “Heavy-tailed distribution of cyber-risks,” The European Physical Journal B-Condensed Matter and Complex Systems, vol. 75, no. 3, pp. 357–364, 2010.

8.2 GITHUB LINK

https://github.com/venkatasairao/MODELING-AND-PREDICTING-CYBER-HACKING-BREACHES