TIC-TAC-TOE GAME

A PROJECT REPORT

Submitted by

M.RAM KUMAR (922018104020)

A.SATHISH KUMAR (922018104024)

in

partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

SRI VIDYA COLLEGE OF ENGINEERING & TECHNOLOGY

VIRUDHUNAGAR 626 005

ANNA UNIVERSITY, CHENNAI 600 025

MAY 2022

ANNA UNIVERSITY: CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this, project report “**TIC TAC TOE GAME** ” is the bonafide work of “**RAMKUMAR M**(922018104020), **SATHISHKUMAR A**(922018104024) ” who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported herein does not from part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE
Mrs.M.Mohana M.E.,
HEAD OF THE DEPARTMENT,
Associate Professor,
Department of CSE,
Sri Vidya College of
Engineering & Technology,
Virudhunagar - 626 005.

SIGNATURE
Mr.S.SATHIS KUMAR M.E.,
SUPERVISOR,
Assistant Professor,
Department of CSE,
Sri Vidya College of
Engineering & Technology,
Virudhunagar - 626 005.

Submitted for the project viva-voce held on ___________ at Sri Vidya College of Engineering & Technology, Virudhunagar.

Internal Examiner

External Examiner

ACKNOWLEDGEMENT

First and foremost we thank the Almighty for this gracious guidance throughout the project.

We express our sincere and respectful regards to chairman **Er.R.THIRUVENKADA RAMANUJA DOSS B.E.,** for providing necessary facilities in carrying of this work.

We endow our thank to Principal, **Dr.T.LOUIE FRANGO M.Tech., Ph.D.,** of Sri Vidya College of Engineering and Technology, who has given us permission and extending facilities for the successful completion of the project.

At the same time, we wish to record our deep sense of gratitude to **Mrs.M.MOHANA M.E.,** Professor and Head of the Department, Computer Science and Engineering for the constant encouragement and valuable suggestion throughout this project.

We wish to thank **Mrs.M.MOHANA M.E.,** Project Guide, generously offered valuable suggestions and guidance throughout the project. She has been very friendly and kind in discussing various ideas with us.

We wish to thank **Mrs.M.MOHANA M.E.,** Project Coordinator, who never hesitated to help us during the course of the project.

Finally, we also thank our parents, friends for their moral support in our project.

ABSTRACT

In Tic-Tac-Toe game when it is played between two players, one player being the user andanother player as the computer, it has been observed by us that applying optimal strategy itusually ends up in a win or draw condition for the first player. In this paper, we havedeveloped a simulation model using min-maxalgorithm over optimal strategy by giving theplayers five more moves to change the previous input to minimize the draw scenario and toincrease the complexity level of the game.

Keywords - game theory, min-max, optimal strategy, Tic-Tac-Toe.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Tic-Tac-Toe is a popular game. It is a game of simple rule, and easy to learn. The originis unknown with indications stated by the ancient Egyptians that they found the Tic-Tac-Toepattern scribbled on the rocks over more than 3500 years. Later they found fun in using thispattern for playing a game. Then the game became popular being played on wooden board ortable or even in a piece of paper. The Tic-Tac-Toe game involves filling up a 3x3 grid with either crosses (‘X’) or noughtsof four turns after which the victory/draw of the game is declared. The player who firstencounters three crosses (‘X’) or three noughts (‘O’) in a particular row, column or diagonalis declared as winner. There are 39 = 19,683 possible states in the game. The purpose offilling the nine spaces can be considered as filling the sequence of nine boxes that ismaximum three in a row, column or diagonal. Therefore, there are 9! = 362,880 ways to fillthe 9th position[2].Interestingly, Tic-Tac-Toe game can be reviewed using game theory, in which rationaldecisions of winning strategy can be considered between the two players. Tic-Tac-Toe usesthe strategy that puts the player in the most preferred position irrespective of the strategy ohis opponents. This strategy is called an optimal strategy.Tic-Tac-Toe uses min-max strategy to choose an optimal move for a player assuming thatthe opponent is also playing optimally. The goal of min-max strategy in the game is tominimize the maximum loss (minimize the worst case condition). In min-max strategy, thegame is said to be fair if maximum value = minimum value = 0, and it is said to be strictlydeterminable if maximum value = minimum value! = 0.In 2012, Al-Khateeb [1] proposed artificial neural networks are used as function evaluators in order to evolve game playing strategies for the game of tic-tac-toe. In 2017,Garg [2] presented a simulation algorithm to predict the win, or draw of a game by knowingthe first move of a player. In 2003, Hochmuth [3] demonstrated how a genetic algorithm canbe used to evolve a perfect Tic-Tac-Toe strategy, which never loses a game who plays thegame. In 2011, Ling [4] proposed an algorithm which is learned by a neural network withdouble transfer function (NNDTF), which is trained by genetic algorithm (GA). In 2013,Mohammadi [5] presented a novel use of Genetic Programming, Co-Evolution andInteractive Fitness to evolve algorithms for the game of Tic-Tac-Toe. In 1995, Pilgrim [6] offered a rule-based expert systems development program called Tic-Tac-Toe as part ofweek-long summer computer science workshop for Middle school students. In 2017, Sharma[7] described two heuristic based algorithms; they are Min-Max and Max-Min for efficienttask scheduling mechanism that should be able to minimize completion time, maximizeresource utilization and minimize makespan.

We observed that using optimal strategy of the game theory, the first player has themaximum chance to win the game or it will end in draw condition. In this paper, we suggestthe min-max strategy over the optimal strategy to overcome the previous drawback whereboth the players will get the wining condition or else end in a draw.

The paper is organized as: Section 2 discusses the preliminaries and notations. Section 3demonstrates strategies of Tic-Tac-Toe. Section 4 presents tree representation of variousstrategies of game. Section 5 presents the proposed model of Tic-Tac-Toe using min-max the study.

1.2 Objectives :

The goal of the game is **for players to position their marks so that they make a continuous line of three cells vertically, horizontally, or diagonally**. An opponent can prevent a win by blocking the completion of the opponent's line. In our variant of the game, players placed objects on a board

CHAPTER 2

LITERATURE SURVEY

Board position

Tic-Tac-Toe game uses crosses ('X') to specify the first player's move and noughts ('O')to the second player's move. There are only three types of moves initially, namely corner,edge and center. The positions 0,2,6,8 are called 'corners', 1,3,5,7 are called 'edges' andposition 4 is called 'center' position, please refer (cf. Figure 2.1) .Min-max: it is a decision making condition to calculate the optimal move. The conditionevaluates the minimum loss and maximum profit. Using it in tic-tac-toe game, a player trieto ensure two cases:

• Maximize a player's own chances to win.

• Minimize opponent's chances to win.

• Maximize profit: the profit can be maximized by forking or winning. Wining if there are

two X or O in a row then play third chance to get three in a row.

• Minimize loss: The loss can be minimized by a block. Block if two X or O of theopponent are in a row then block it, or else block opponent's

CHAPTER 3

SYSTEM REQUIREMENTS

3.1. HARDWARE REQIREMENTS

Processor	:	Intel(R) Core(TM) i3
Processor Speed	:	3.06 GHz
Ram	:	4 GB
Hard Disk Drive	:	250 GB
CD-ROM Drive	:	Sony
Monitor	:	“17” inches
Keyboard	:	TVS Gold
Mouse	:	Logitech

3.2. SOFTWARE REQUIREMENT

1.visual studio

CHAPTER 4

1.Proposed model of Tic-Tac-Toe using min-max over optimal strategy

In min-max strategy, the first player is offered the first move and the player will havemaximum number of move as compared to the second player.

The first player can choose any position (cf. Figure 5.1 (a)), if the player chooses top right corner and the second player places ‘O’ in the center, (cf. Figure 5.1 (b)). The first player again places in another corner that is in bottom right corner, the min-max strategy evaluates the minimum profit of ‘X’ and second player places in right edge to block the first player’s chance, (cf. Figure 5.1 (c)). Then the first player places ‘X’ in left edge so that the second player does not win in the second move, (cf. Figure 5.1 (d)). The min-max evaluates the maximum profit of the first player and for blocking the second player chance of winning, places ‘X’ at top edge, and the second player minimizes the opponent’s win by placing ‘O’ at top left corner, (cf. Figure. Therefore, this will lead to a draw as

5.1.1 Algorithm for choosing corner

1) Start from the corner (0, 2, 6, and 8).

2) If the opponent plays on an edge (1, 3, 5 and 7), play in the corner that forces the

opponent to play on another side.

3) When the opponent blocks playing on the edge, conquer the center or play in another

corner.

Fig 7.5 Flow diagram for User Login

4) After conquering the center or another corner, the three ‘X’ or ‘O’ are formed..

In algorithm for choosing corner, the first player will start in a corner, suppose position 8, if the second player plays on an edge (position 5), first player plays in the corner

(position 6) that forces the opponent to play in another side that is position 7. When the

second player blocks playing on the edge, the first player will conquer the center or play in

another corner. In this case, the player will play in the center position, and the opponent will. block in one of the corner (position 0 or 2). After conquering the center, the three crosses

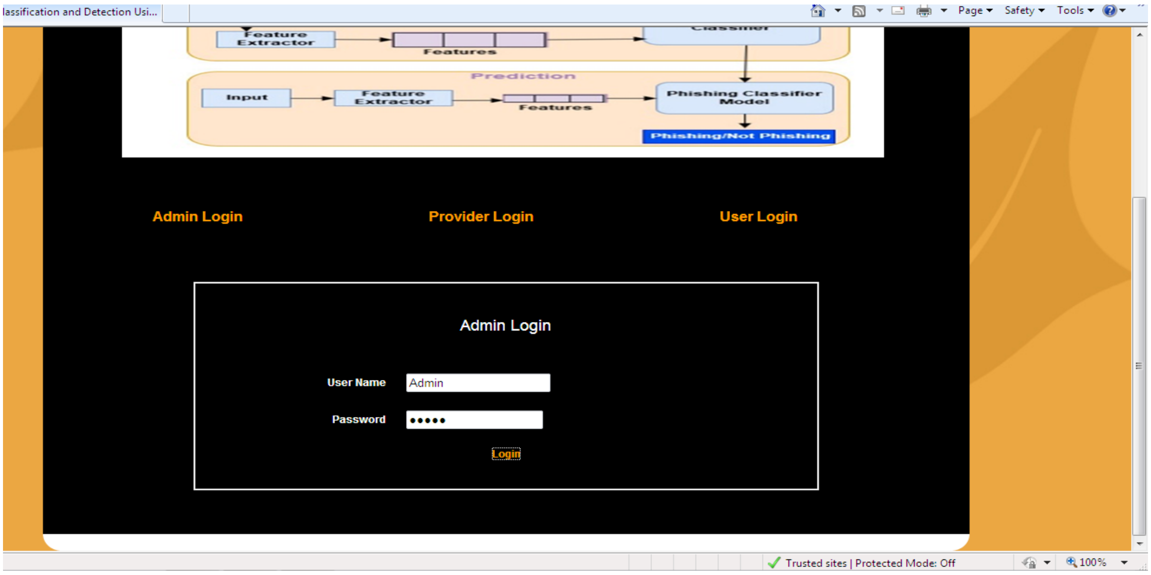
(‘X’) are formed.

5. Algorithm for choosing center

1) Start from the center (4).
2) If the opponent plays on the edge, play in the corner of this edge.
3) The opponent will be forced to block by placing in the far corner.
4) Make three in a row, column or diagonal by placing in the corner or edge aligned to
the conquered corner or edge.

7. Conclusion

In this paper, we present a model to give both player the same chance of winningcondition irrespectively of the strategy. The model is implemented using game theory, min-max and optimal strategy. In an ideal scenario, a player must calculate all the possibilities toensure the success not only by blocking the other player's success but also ensuring thatblocking the opponent will not give more vulnerabilities**.**



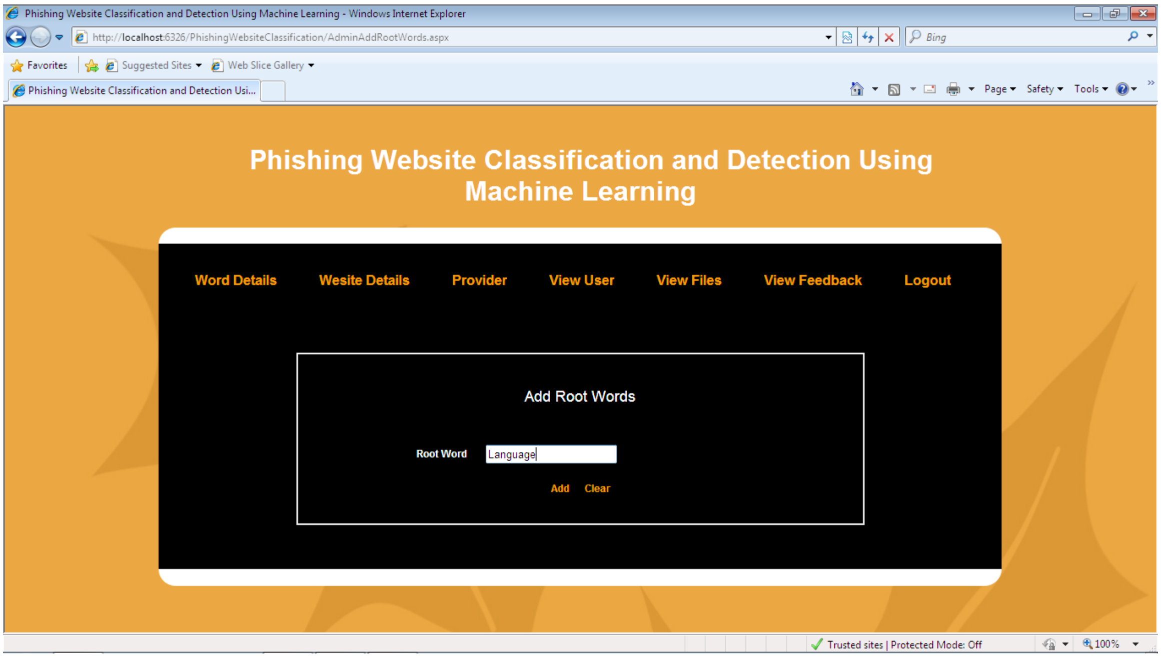
Admin Login

User Name Admin

Password •••••

Fig 9.2 Admin Login

Add Root Words

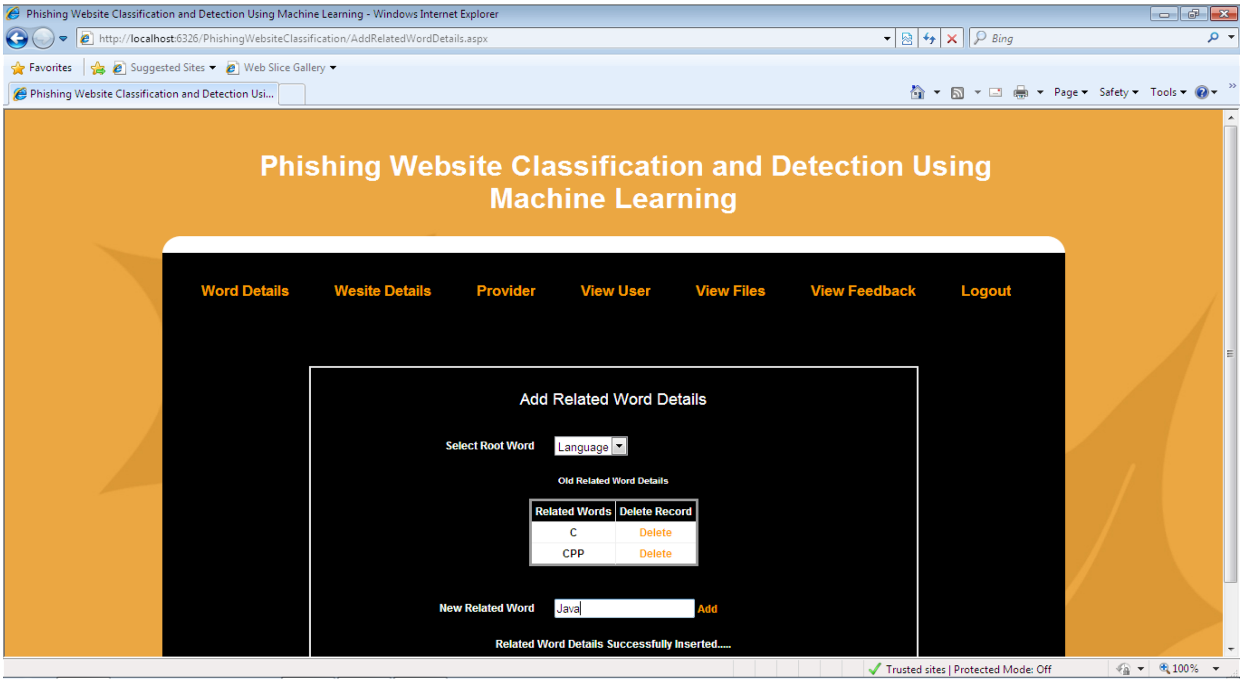

Phishing Website Classification and Detection Using Machine Learning - Windows Internet Explorer
http://localhost:6326/PhishingWebsiteClassification/AdminAddRootWords.aspx
Bing
Favorites
Suggested Sites
Web Slice Gallery
Phishing Website Classification and Detection Usi...
Page
Safety
Tools
Phishing Website Classification and Detection Using Machine Learning
Word Details
Wesite Details
Provider
View User
View Files
View Feedback
Logout
Add
Clear
Trusted sites | Protected Mode: Off
100%

Add Root Words

Root Word: Language

Fig 9.3 Adding Root words

Add Related Word Details


Phishing Website Classification and Detection Using Machine Learning - Windows Internet Explorer
http://localhost:6326/PhishingWebsiteClassification/AddRelatedWordDetails.aspx
Bing
Favorites
Suggested Sites
Web Slice Gallery
Phishing Website Classification and Detection Usi...
Page
Safety
Tools
Phishing Website Classification and Detection Using Machine Learning
Word Details
Wesite Details
Provider
View User
View Files
View Feedback
Logout
Add
Trusted sites | Protected Mode: Off
100%

Add Related Word Details

Select Root Word: Language

Old Related Word Details

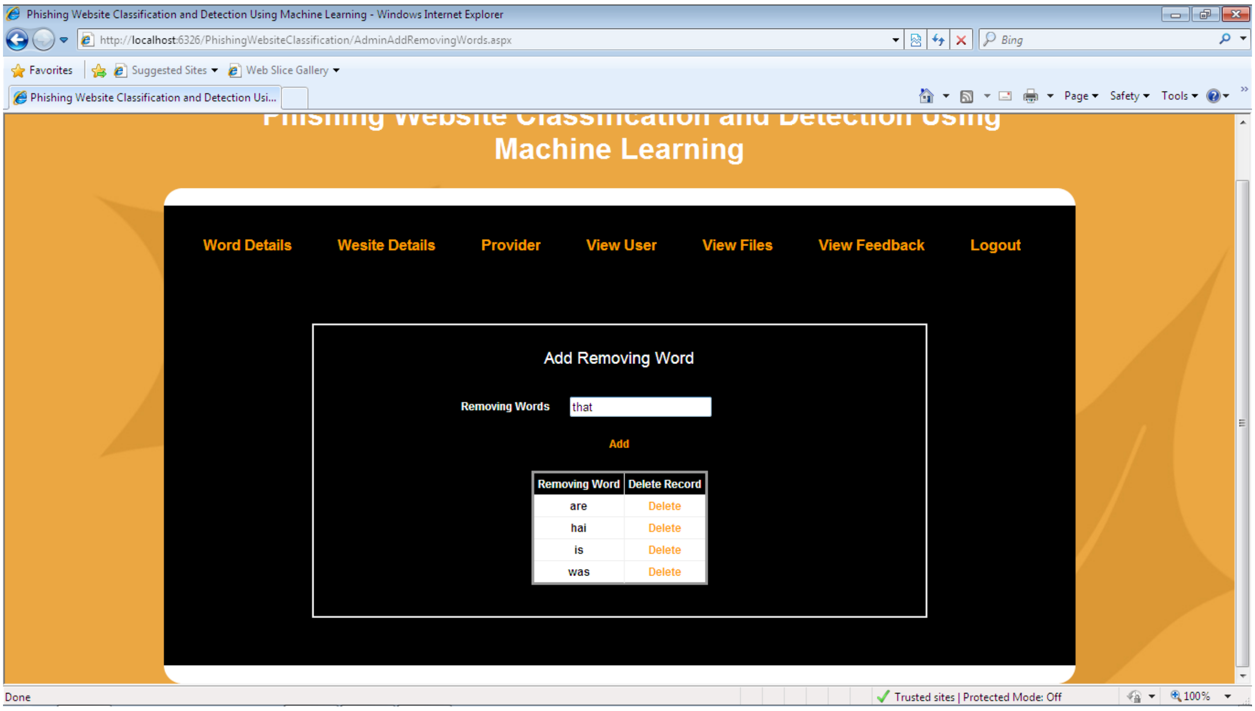
Related Words	Delete Record
C	Delete
CPP	Delete

New Related Word: Java

Related Word Details Successfully Inserted.....

Fig 9.4 Adding Related word details

Add Removing Words


Phishing Website Classification and Detection Using Machine Learning - Windows Internet Explorer
http://localhost:6326/PhishingWebsiteClassification/AdminAddRemovingWords.aspx
Phishing Website Classification and Detection Using Machine Learning
Word Details
Wesite Details
Provider
View User
View Files
View Feedback
Logout
Done
Trusted sites | Protected Mode: Off
100%

Add Removing Word

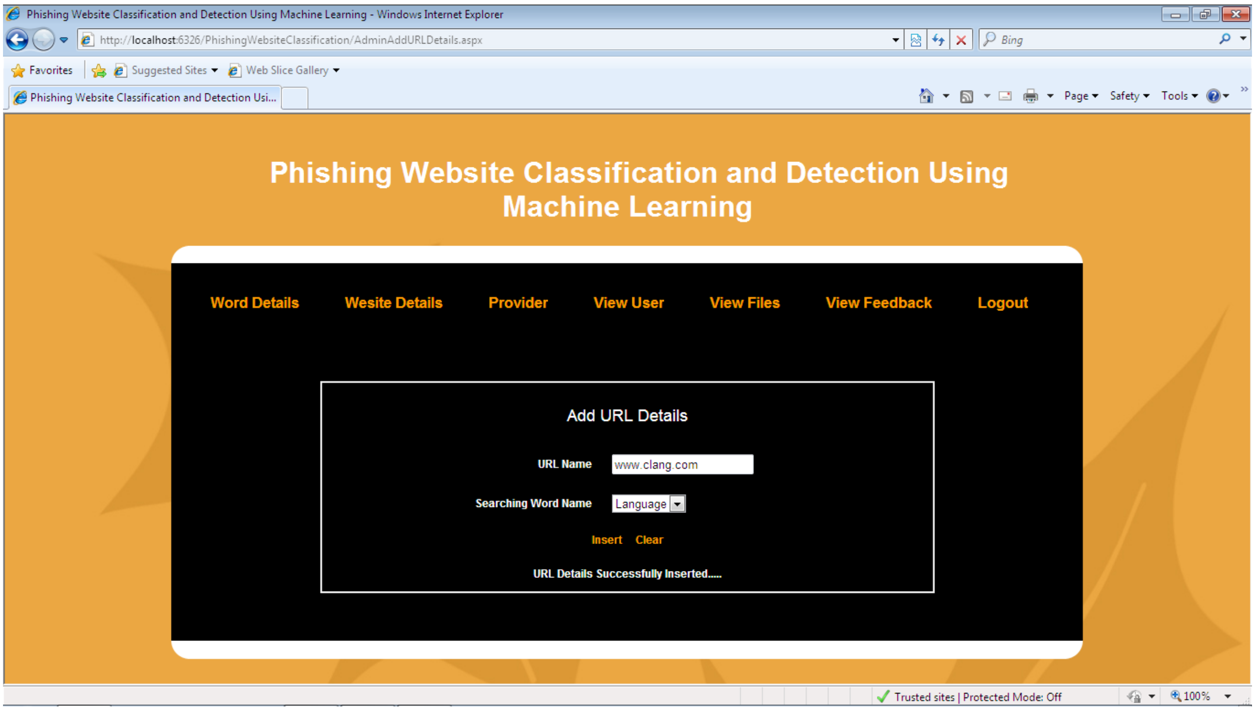
Removing Words: that

Add

Removing Word	Delete Record
are	Delete
hai	Delete
is	Delete
was	Delete

Fig 9.5 Add Removing word

Add URL Details


Phishing Website Classification and Detection Using Machine Learning - Windows Internet Explorer
http://localhost:6326/PhishingWebsiteClassification/AdminAddURLDetails.aspx
Phishing Website Classification and Detection Using Machine Learning
Word Details
Wesite Details
Provider
View User
View Files
View Feedback
Logout
Trusted sites | Protected Mode: Off
100%

Add URL Details

URL Name: www.clang.com

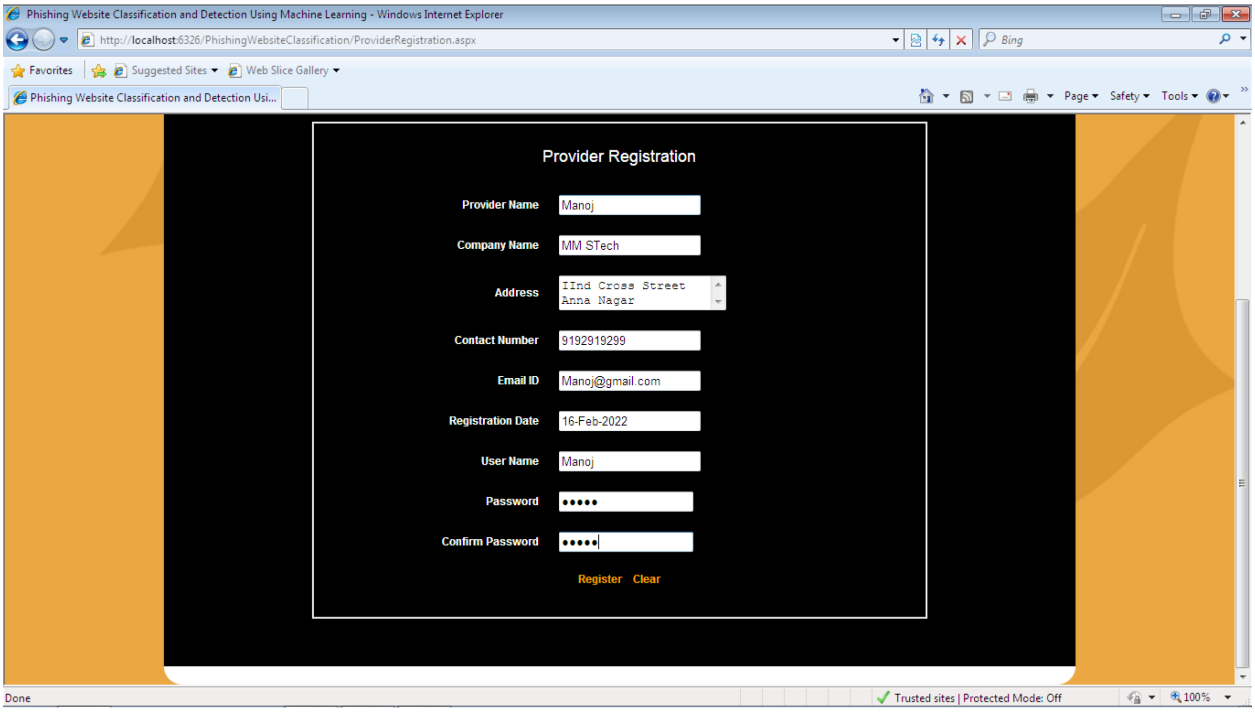
Searching Word Name: Language

Insert Clear

URL Details Successfully Inserted.....

Fig 9.6 Adding URL Details

Provider Registration


Phishing Website Classification and Detection Using Machine Learning - Windows Internet Explorer
http://localhost:6326/PhishingWebsiteClassification/ProviderRegistration.aspx
Favorites
Suggested Sites
Web Slice Gallery
Page
Safety
Tools
Done
Trusted sites | Protected Mode: Off
100%

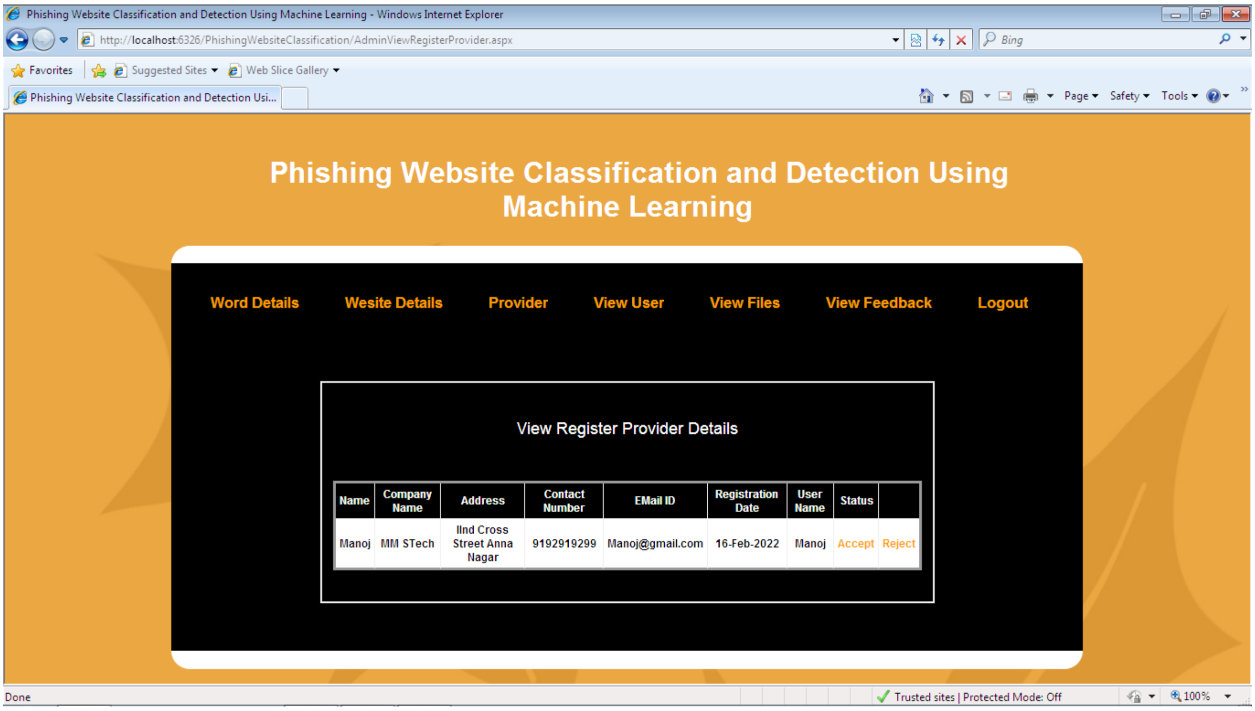
Provider Registration

Provider Name	Manoj
Company Name	MM STech
Address	IInd Cross Street Anna Nagar
Contact Number	9192919299
Email ID	Manoj@gmail.com
Registration Date	16-Feb-2022
User Name	Manoj
Password	•••••
Confirm Password	•••••

Register Clear

Fig 9.7 Provider Registration

Admin View Register Provider Details

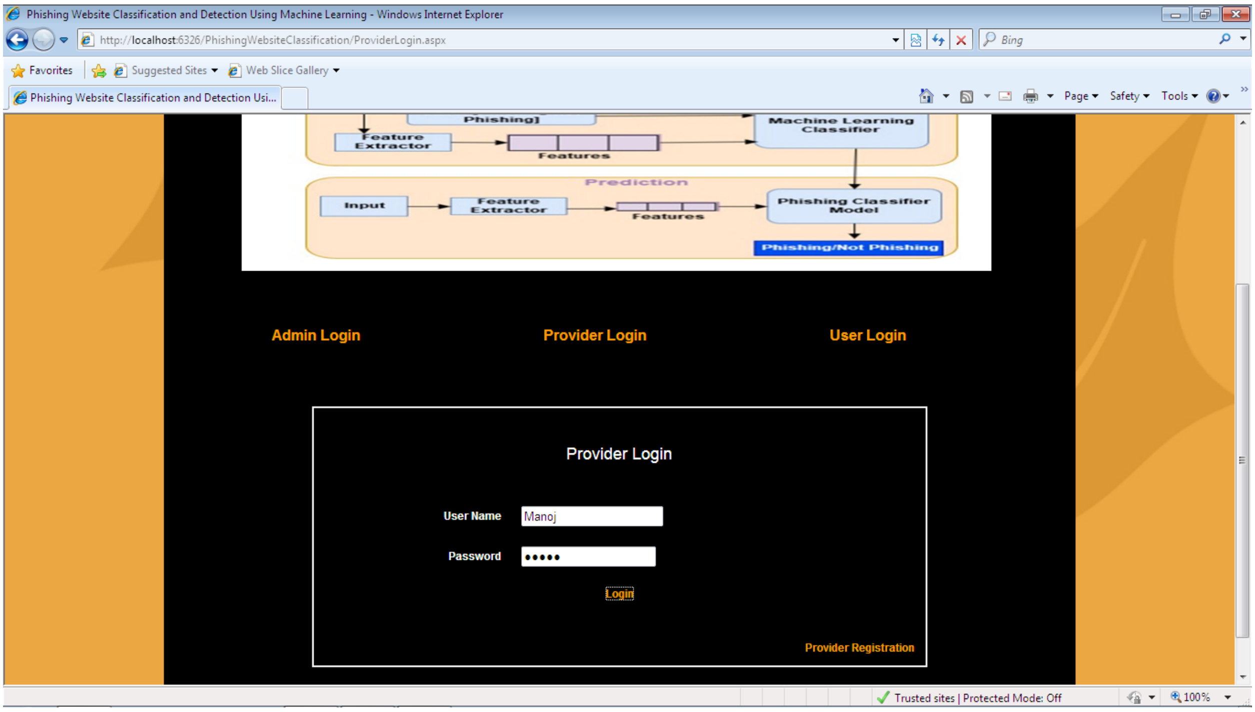

Phishing Website Classification and Detection Using Machine Learning - Windows Internet Explorer
http://localhost:6326/PhishingWebsiteClassification/AdminViewRegisterProvider.aspx
Favorites
Suggested Sites
Web Slice Gallery
Page
Safety
Tools
Phishing Website Classification and Detection Using Machine Learning
Word Details
Wesite Details
Provider
View User
View Files
View Feedback
Logout
Done
Trusted sites | Protected Mode: Off
100%

View Register Provider Details

Name	Company Name	Address	Contact Number	EMail ID	Registration Date	User Name	Status	
Manoj	MM STech	IInd Cross Street Anna Nagar	9192919299	Manoj@gmail.com	16-Feb-2022	Manoj	Accept	Reject

Fig 9.8 Admin View Accepted Provider Details

Provider Login


Phishing Website Classification and Detection Using Machine Learning - Windows Internet Explorer
http://localhost:6326/PhishingWebsiteClassification/ProviderLogin.aspx
Bing
Favorites
Suggested Sites
Web Slice Gallery
Phishing Website Classification and Detection Usi...
Page
Safety
Tools
Phishing]
Feature Extractor
Features
Machine Learning Classifier
Prediction
Input
Feature Extractor
Features
Phishing Classifier Model
Phishing/Not Phishing
Admin Login
Provider Login
User Login
Login
Provider Registration
Trusted sites | Protected Mode: Off
100%

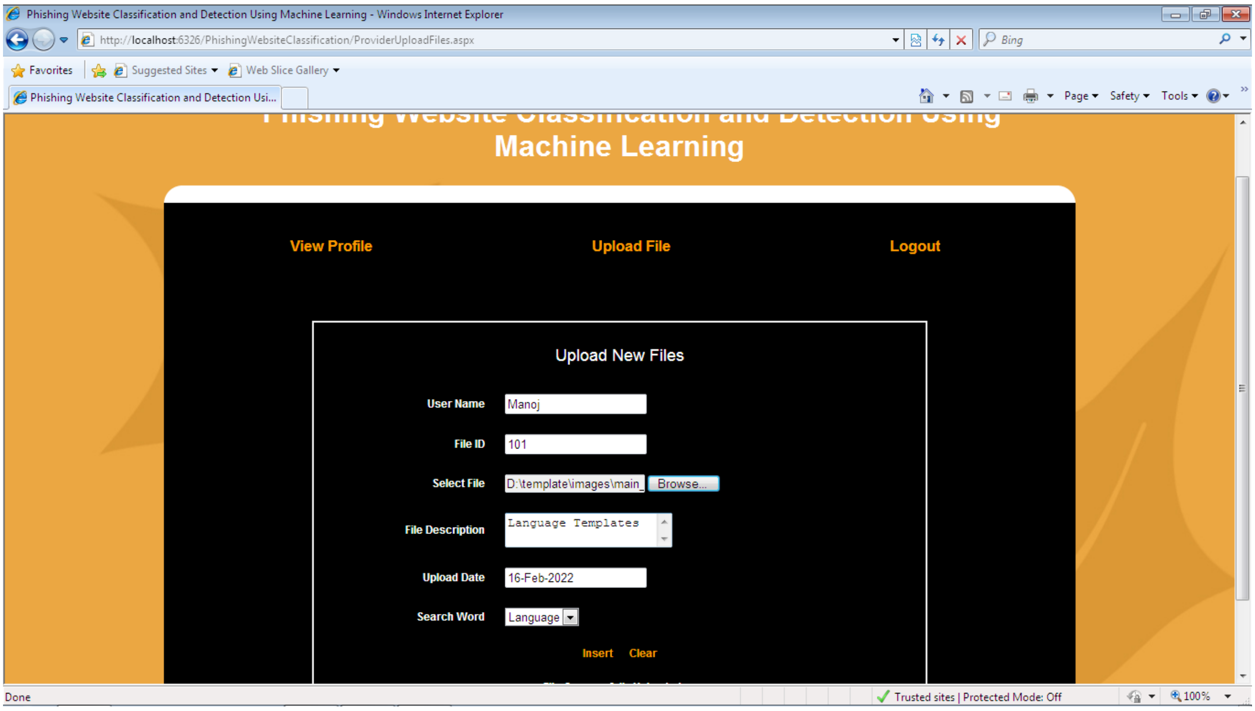
Provider Login

User Name: Manoj

Password: •••••

Fig 9.9 Provider Login

Upload New Files


Phishing Website Classification and Detection Using Machine Learning - Windows Internet Explorer
http://localhost:6326/PhishingWebsiteClassification/ProviderUploadFiles.aspx
Bing
Favorites
Suggested Sites
Web Slice Gallery
Phishing Website Classification and Detection Usi...
Page
Safety
Tools
Phishing Website Classification and Detection Using
Machine Learning
View Profile
Upload File
Logout
Browse...
Insert
Clear
Done
Trusted sites | Protected Mode: Off
100%

Upload New Files

User Name: Manoj

File ID: 101

Select File: D:\template\images\main_

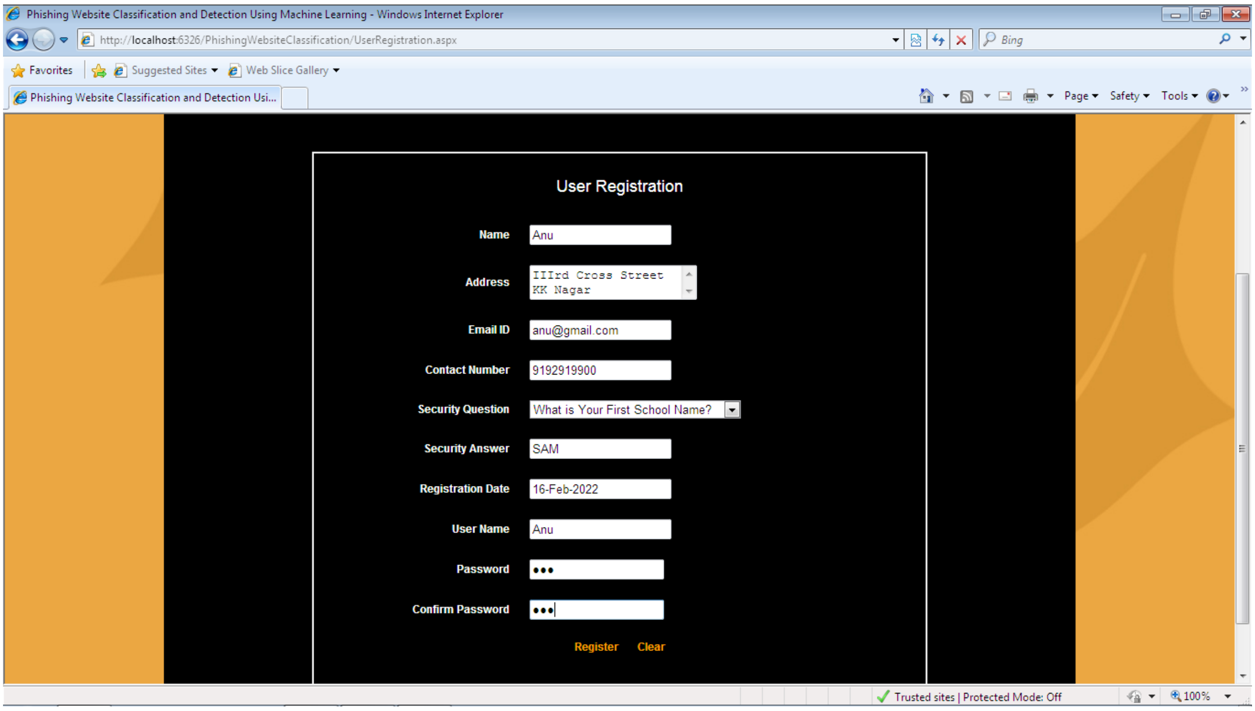
File Description: Language Templates

Upload Date: 16-Feb-2022

Search Word: Language

Fig 9.10 Uploading New files

User Registration


Phishing Website Classification and Detection Using Machine Learning - Windows Internet Explorer
http://localhost:6326/PhishingWebsiteClassification/UserRegistration.aspx
Bing
Favorites
Suggested Sites
Web Slice Gallery
Phishing Website Classification and Detection Usi...
Page
Safety
Tools
Register
Clear
Trusted sites | Protected Mode: Off
100%

User Registration

Name: Anu

Address: IIIrd Cross Street KK Nagar

Email ID: anu@gmail.com

Contact Number: 9192919900

Security Question: What is Your First School Name?

Security Answer: SAM

Registration Date: 16-Feb-2022

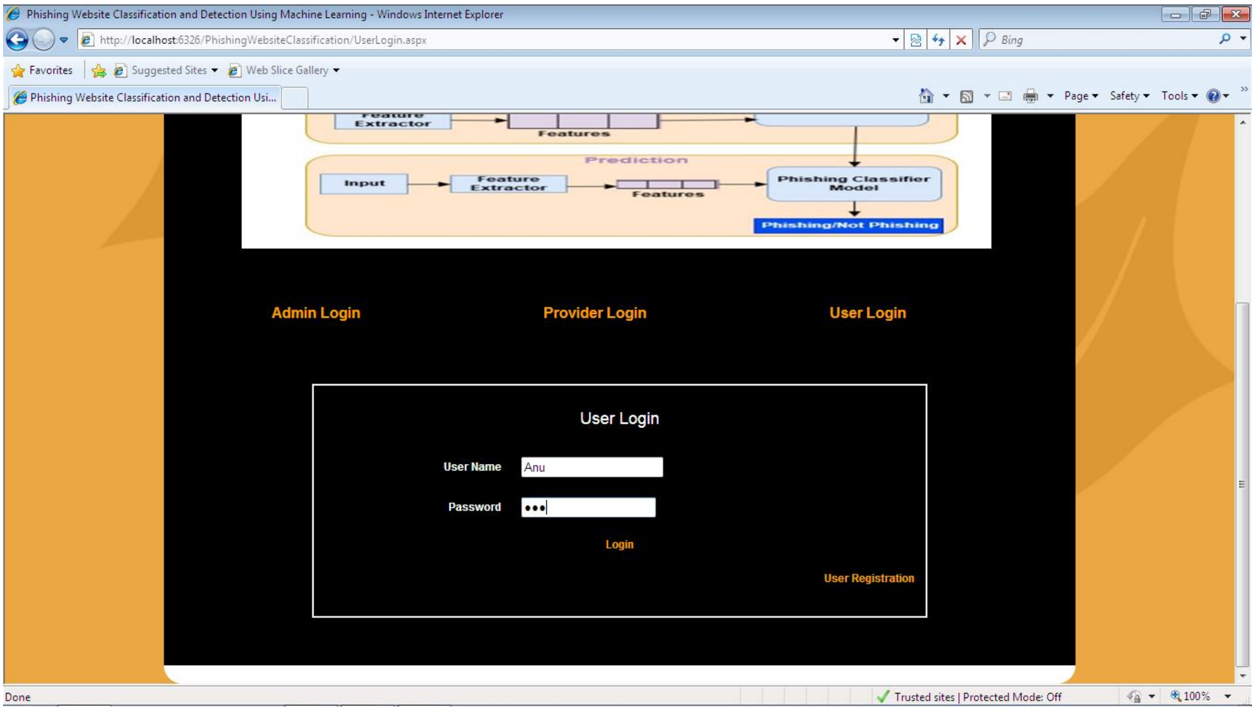
User Name: Anu

Password: •••

Confirm Password: •••

Fig 9.11 User Registration

User Login


Phishing Website Classification and Detection Using Machine Learning - Windows Internet Explorer
http://localhost:6326/PhishingWebsiteClassification/UserLogin.aspx
Bing
Favorites
Suggested Sites
Web Slice Gallery
Phishing Website Classification and Detection Usi...
Page
Safety
Tools
Feature Extractor
Features
Prediction
Input
Feature Extractor
Features
Phishing Classifier Model
Phishing/Not Phishing
Admin Login
Provider Login
User Login
Login
User Registration
Done
Trusted sites | Protected Mode: Off
100%

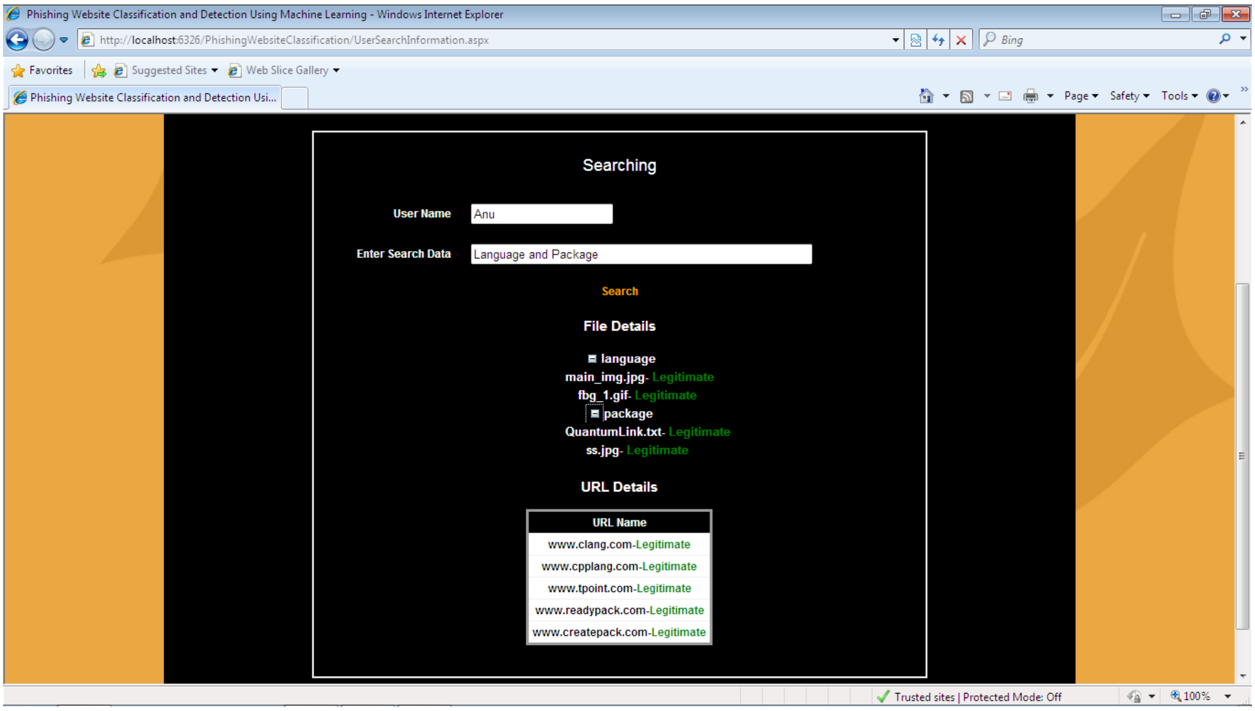
User Login

User Name: Anu

Password: •••

Fig 9.12 User Login

User Search Information


Phishing Website Classification and Detection Using Machine Learning - Windows Internet Explorer
http://localhost:6326/PhishingWebsiteClassification/UserSearchInformation.aspx
Favorites
Suggested Sites
Web Slice Gallery
Page
Safety
Tools
Search
Trusted sites | Protected Mode: Off
100%

Searching

User Name: Anu

Enter Search Data: Language and Package

File Details

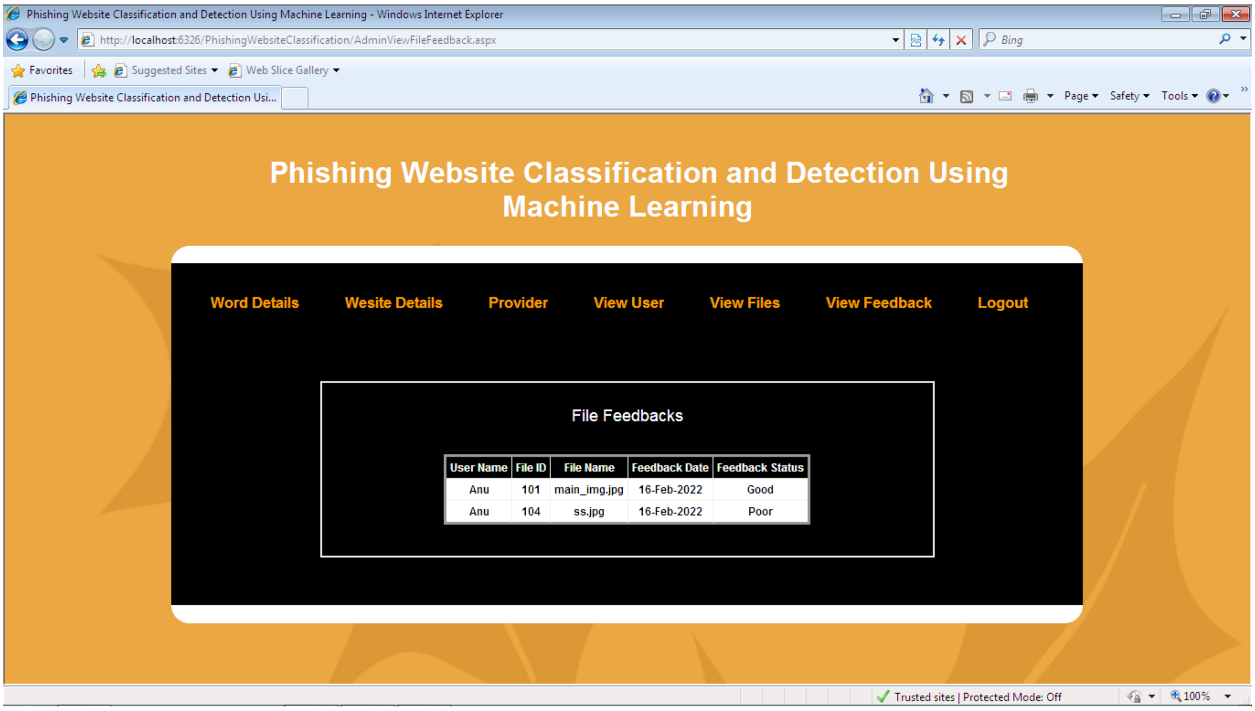
- language
  - main_img.jpg- Legitimate
  - fbg_1.gif- Legitimate
  - package
    - QuantumLink.txt- Legitimate
    - ss.jpg- Legitimate

URL Details

URL Name
www.clang.com-Legitimate
www.cpplang.com-Legitimate
www.tpoint.com-Legitimate
www.readypack.com-Legitimate
www.createpack.com-Legitimate

Fig 9.13 User Searching Information

Admin View File Feedbacks


Phishing Website Classification and Detection Using Machine Learning - Windows Internet Explorer
http://localhost:6326/PhishingWebsiteClassification/AdminViewFileFeedback.aspx
Favorites
Suggested Sites
Web Slice Gallery
Page
Safety
Tools
Word Details
Wesite Details
Provider
View User
View Files
View Feedback
Logout
Trusted sites | Protected Mode: Off
100%

Phishing Website Classification and Detection Using Machine Learning

File Feedbacks

User Name	File ID	File Name	Feedback Date	Feedback Status
Anu	101	main_img.jpg	16-Feb-2022	Good
Anu	104	ss.jpg	16-Feb-2022	Poor

Fig 9.14 Admin View File Feedbacks

CHAPTER 10

CONCLUSION AND FUTURE SCOPE

We have explored how well to classify phishing URLs from the given set of URLs containing benign and phishing URLs. We have also discussed the randomization of the dataset, feature engineering, feature extraction using lexical analysis host-based features and statistical analysis. We have also used different classifiers for the comparative study and found that the findings are almost consistent across the different classifiers. We also observed dataset randomization yielded a great optimization and the accuracy of the classifier improved significantly. We have adopted a simple approach to extract the features from the URLs using simple regular expressions. There could be more features that can be experimented and that might lead to improving further the accuracy of the system. The dataset used in this paper contains the URLs list which may be a little old, hence regular continuous training along with a new dataset would enhance the model accuracy and performance significantly. In our experiment we have not used the contentbased features as the main problem with the content-based strategy for detecting phishing URLs is the non-availability of phishing web-sites and the life span of the phishing website is small, and it is difficult to train an ML classifier based on its content-based features.

FUTURE ENHANCEMENT

In the future, we would like to incorporate a rule-based prediction based on the content analysis of a URL. Hence, the combination of classification based lexical analyzer along with a rule-based URL content analyzer for phishing URL detection would provide a comprehensive solution.

APPENDIX-I

CODING

Admin Login

```
public partial class AdminLogin : System.Web.UI.Page
{
    protected void Page_Load(object sender, EventArgs e)
    {
        try
        {
            Label1.Text = "";
            Menu m1 = (Menu)Master.FindControl("Menu1");
            m1.Visible = true;
        }
        catch (Exception ex)
        {
            Label1.Text = ex.Message;
        }
    }
    protected void LinkButton1_Click(object sender, EventArgs e)

}
```

Add Root Words

```
using System.Data.SqlClient;
using System.Configuration;
public partial class AdminAddRootWords : System.Web.UI.Page
{
    SqlConnection con;
    SqlCommand cmd;
    SqlDataReader rs;
    protected void Page_Load(object sender, EventArgs e)
    {
        try
        {
            Label1.Text = "";
            Menu m2 = (Menu)Master.FindControl("Menu2");
            m2.Visible = true;
            con = new
SqlConnection(ConfigurationManager.ConnectionStrings["connection"].Conne
ctionString);
            con.Open();
        }
        catch (Exception ex)
        {
            Label1.Text = ex.Message;
        }
    }
    protected void LinkButton1_Click(object sender, EventArgs e)
    {
        try
        {
            cmd = new SqlCommand("select * from wtable where
wname=@wname", con);
            cmd.Parameters.AddWithValue("wname", TextBox1.Text);
            rs = cmd.ExecuteReader();
            bool b = rs.Read();
            rs.Close();
            cmd.Dispose();
            if (b)
            {
                Label1.Text = TextBox1.Text + " Root Word Details Already
Inserted....";
                return;
            }

        catch (Exception ex)
        {
            Label1.Text = ex.Message;
        }
    }
```

Add Removing Word Details

```
using System.Data.SqlClient;
using System.Data;
using System.Configuration;
public partial class AdminAddRemovingWords : System.Web.UI.Page
{
    SqlConnection con;
    SqlCommand cmd;
    SqlDataReader rs;
    SqlDataAdapter adp;
    DataTable dt;
    protected void Page_Load(object sender, EventArgs e)
    {
        try
        {
            Label1.Text = "";
            Menu m2 = (Menu)Master.FindControl("Menu2");
            m2.Visible = true;
            con = new
SqlConnection(ConfigurationManager.ConnectionStrings["connection"].Conne
ctionString);
            con.Open();
            if (!IsPostBack)
                bindgrid();
        }
        catch (Exception ex)
        {
            Label1.Text = ex.Message;
        }
    }
    void bindgrid()
    {
        adp = new SqlDataAdapter("select * from rewtable", con);
        dt = new DataTable();
        adp.Fill(dt);
        GridView1.DataSource = dt;
        GridView1.DataBind();
    }

    protected void GridView1_RowCommand(object sender,
GridViewCommandEventArgs e)
    {
        try
        {
            string rword =
GridView1.DataKeys[int.Parse(e.CommandArgument.ToString())].Value.ToStr
ing();
            if (e.CommandName == "dr")
            {
                cmd = new SqlCommand("delete from rewtable where
rword=@rword", con);
                cmd.Parameters.AddWithValue("rword", rword);
                cmd.ExecuteNonQuery();
                cmd.Dispose();
                bindgrid();
            }
        }
```

Add URL Details

```
using System.Data.SqlClient;
using System.Configuration;
public partial class AdminAddURLDetails : System.Web.UI.Page
{
    SqlConnection con;
    SqlCommand cmd;
    SqlDataReader rs;
    protected void Page_Load(object sender, EventArgs e)
    {
        try
        {
            Label1.Text = "";
            Menu m2 = (Menu)Master.FindControl("Menu2");
            m2.Visible = true;
            con = new SqlConnection(ConfigurationManager.ConnectionStrings["connection"].ConnectionString);
            con.Open();
            if (!IsPostBack)
            {
                cmd = new SqlCommand("select wname from wtable", con);
                rs = cmd.ExecuteReader();
                DropDownList1.DataSource = rs;
                DropDownList1.DataTextField = "wname";
                DropDownList1.DataBind();
                rs.Close();
                cmd.Dispose();
                DropDownList1.Items.Insert(0, "Select");
            }
        }
        catch (Exception ex)
        {
            Label1.Text = ex.Message;
        }
    }
            cmd = new SqlCommand("insert into ptable values(@pname,@cname,@caddress,@cno,@emailid,@rdate,@uname,@pword,@status)", con);
            cmd.Parameters .AddWithValue ("pname",TextBox1 .Text );
            cmd.Parameters .AddWithValue ("cname",TextBox2 .Text );
            cmd.Parameters .AddWithValue ("caddress",TextBox3 .Text );
            cmd.Parameters .AddWithValue ("cno",TextBox4 .Text );
            cmd.Parameters .AddWithValue ("emailid",TextBox5 .Text );
            cmd.Parameters .AddWithValue ("rdate",TextBox6 .Text );
            cmd.Parameters .AddWithValue ("uname",TextBox7 .Text );
            cmd.Parameters .AddWithValue ("pword",TextBox8 .Text );
            cmd.Parameters .AddWithValue ("status","Register");
            cmd.ExecuteNonQuery ();
            cmd.Dispose ();
            Label1 .Text ="Register Provider Details....";
        }
        catch (Exception ex)
        {
            Label1.Text = ex.Message;
        }
    }
```

Admin View Register Provider Details

```
using System.Data.SqlClient;
using System.Data;
using System.Configuration;
using System.Net.Mail;
public partial class AdminViewRegisterProvider : System.Web.UI.Page
{
    void bindgrid()
    {
        adp = new SqlDataAdapter("select * from ptable where status='Register'",
con);
        dt = new DataTable();
        adp.Fill(dt);
        GridView1.DataSource = dt;
        GridView1.DataBind();
    }
    void MailCoding(string remailid, string mess, string semailid, string pword)
    {
        MailMessage m = new MailMessage();
        m.From = new MailAddress(semailid);
        m.To.Add(remailid);
        m.Subject = "<b>Verification Status:</b><br>";
        m.IsBodyHtml = true;
        m.Body = mess;
        SmtpClient sclient = new SmtpClient();
        sclient.Host = "smtp.gmail.com";
        sclient.Credentials = new System.Net.NetworkCredential(semailid,
pword);
        sclient.EnableSsl = true;
        sclient.Send(m);
    }
```

Provider Upload Files

```
using System.Data.SqlClient;
using System.Configuration;
public partial class ProviderUploadFiles : System.Web.UI.Page
{
    SqlConnection con;
    SqlCommand cmd;
    SqlDataReader rs;
    void autonumber()
    {
        cmd = new SqlCommand("select isnull(max(fid),100)+1 from ftable",
con);
        TextBox2.Text = cmd.ExecuteScalar().ToString();
        cmd.Dispose();
    }
            if (!IsPostBack)
            {
                if (Session["PUserName"] != null)
                {
                    TextBox1.Text = Session["PUserName"].ToString();
                    autonumber();
                    TextBox4 .Text =DateTime .Now .ToString ("dd-MMM-yyyy");
                    cmd = new SqlCommand("select wname fr", con);
                    rs = cmd.ExecuteReader();
                    DropDownList1.DataSource = rs;
                    DropDownList1.DataTextField = "wname";
                    DropDownList1.Items.Insert(0, "Select");
                }
        }
```

APPENDIX-II

REFERENCE

[1] Jitendra Kumar, Balaji Rajendran, A. Santhanavijayan, Bindhumadhava, B. Janet, “Phishing Website Classification and Detection Using Machine Learning” 2020 International Conference on Computer Communication and Informatics (ICCCI -2020), Jan. 22-24, 2020, Coimbatore.

[2] Mohammed Nazim Feroz,Susan Mengel, “Phishing URL Detection Using URL Ranking,” IEEE International Congress on Big Data, July 2015

[3] Mahdieh Zabihimayvan, Derek Doran, “Fuzzy Rough Set Feature Selection to Enhance Phishing Attack Detection,” International Conference on Fuzzy Systems (FUZZ-IEEE), New Orleans, LA, USA, June 2019

[4] Moitrayee Chatterjee,Akbar-Siami Namin, “Detecting Phishing Websites through Deep Reinforcement Learning,” IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), July 2019

[5] Chun-Ying Huang,Shang-Pin Ma,Wei-Lin Yeh,Chia-Yi Lin,ChienTsung Liu, “Mitigate web phishing using site signatures,” TENCON 2010-2010 IEEE Region 10 Conference, January 2011

[6] Aaron Blum,Brad Wardman,Thamar Solorio,Gary Warner, “Lexical feature based phishing URL detection using online learning,” 3rd ACM workshop on Artificial intelligence and security, Chicago, Illinois, USA, pp. 54-60, August 2010

[7] Mohammed Al-Janabi,Ed de Quincey,Peter Andras, “Using supervised machine learning algorithms to detect suspicious URLs in online social networks,” IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017, Sydney, Australia, pp. 1104-1111, July 2010

[8] Erzhou Zhu,Yuyang Chen,Chengcheng Ye,Xuejun Li,Feng Liu, “OFSNN:An Effective Phishing Websites Detection Model Based on Optimal Feature Selection and Neural Network,” IEEE Access(Volume:7), pp. 73271-73284, June 2019

[9] Ankesh Anand,Kshitij Gorde,Joel Ruben Antony Moniz,Noseong Park,Tanmoy Chakraborty,Bei-Tseng Chu, “Phishing URL Detection with Oversampling based on Text Generative Adversarial Networks,” IEEE International Conference on Big Data (Big Data), [10] Justin Ma,Lawrence K. Saul,Stefan Savage,Geoffrey M. Voelker, “Learning to detect malicious URLs,” ACM Transactions on Intelligent Systems and Technology (TIST) archive Volume 2 Issue 3, April 2011

[11] Youness Mourtaji,Mohammed Bouhorma,Alghazzawi, “Perception of a new framework for detecting phishing web pages,” Mediterranean Symposium on Smart City Application Article No. 11, Tangier, Morocco, October 2017 Authorized licensed use limited to: Auckland University of Technology. Downloaded on June 04,2020 at 16:10:36 UTC from IEEE Xplore. Restrictions apply. 2020 International Conference on Computer Communication and Informatics (ICCCI -2020), Jan. 22-24, 2020, Coimbatore, INDIA

[12] Akihito Nakamura,Fuma Dobashi, “Proactive Phishing Sites Detection,” WI '19 IEEE/WIC/ACM International Conference on Web Intelligence), pp. 443-448, October 2019 [13] https://www.phishtank.com/developer_info.php, [Online]. Available: https://www.phishtank.com/developer_info.php [Accessed: 27- September- 2019].

[14] https://openphish.com/, [Online]. Available: https://openphish.com/ [Accessed: 27- September- 2019].

[15] https://majestic.com/reports/majestic-million [Online]. Available: https://majestic.com/reports/majestic-million [Accessed: 27- September- 2019].

[16] Preethi, '14 Types of Phishing Attacks That IT Administrators Should Watch For', [Online]. Available: https://blog.syscloud.com/types-ofphishing [Accessed: 10- November- 2019].

[17] Ebubekir Büber, ' Phishing URL Detection with M', [Online]. Available: https://towardsdatascience.com/phishing-domaindetection-with-ml-5be9c99293e5 [Accessed: 10- November- 2019].

[18] scikit-learn, , Machine Learning in Python, [Online]. Available: https://scikit-learn.org/stable/ [Accessed: 10- November- 2019].