ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 5, Special Issue 14, April 2018

REAL TIME DETECTION AND PREVENTION OF PHISHING ATTACKS USING LINKGUARD

Prof. ASHA JOSEPH[1], ASHISH MAHARJAN[2], DIPESH GUPTA[3], KRISHNA PAUDEL[4], RAM KUMAR SHRESTHA[5]
Department of Computer Science and Engineering
BTI, Bangalore-35, India

ABSTRACT

An attack that is made by attackers using spoofed emails and fake website with a motive of tricking people to give their personal information is known as phishing. In this paper we are trying to detect the fake websites using LinkGuard algorithm to prevent from such kind of attacks. LinkGuard algorithm detects both known and unknown phishing attacks. Our experiments verified that LinkGuard is effective to detect phishing attacks with minimal false negatives.

I. INTRODUCTION

Initially emerged in 1990s, Phishing is derived from 'fishing' which means that the attacker allure users to visit a fake website by sending them fake emails by which they can get the victim's personal information like username, password, account number, etc[3]. Some of the attacks that has been frequently used is sending emails to potential victims, that looks like as if it has been sent by some bank or any kind of organization. Here the attackers may create any situation in which we will get a cause to enter our personal information in the particular website. So due to this we are giving them our information by ourselves, unknowingly. Nowadays phishing is commonly used by the phishers so it is creating a number of problems with the risk of financial loss of victims as well as the loss of some valuable information. Using LinkGuard algorithm as a key tool to detect the phishing attack we can successfully detect the phishing mail with an accuracy of 97%.

In this approach we compare the common characteristics of hyperlinks in phishing mails and identify whether those links are produced by a phisher or not. Some of the characteristics of the hyperlink in phishing mails are:

1. There is difference between visual and the actual link.
2. There is a presence of dotted decimals IP address instead of DNS name.
3. In order to make it real the attackers will be using same DNS name as that of the real system.

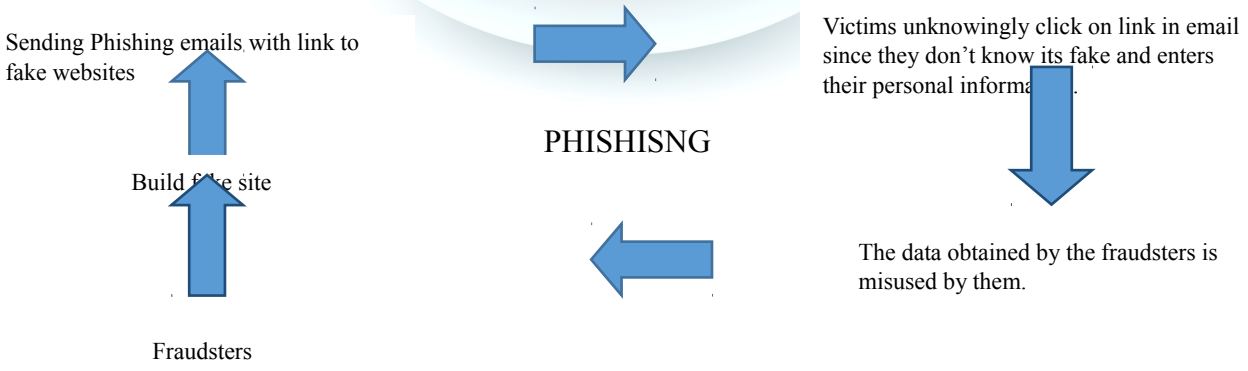

Fig. 1 Process of phishing a website

Fig. 1 shows the process of phishin

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 5, Special Issue 14, April 2018

We have conducted a detailed survey on this topic, further, in the rest of the paper we point out some of the limitations and propose a model to show how to overcome the limitations.

II. LITERATURE SURVEY

Several literature survey regarding the phishing detection has been made. The paper published by (Abdulghai, 2016, IEEE)had drawbacks of studying and checking only few URL characteristics for the detection, so ensuring the prevention against different types of hazardous attacks were difficult [1]. The other paper published (Yanhui Du, 2014, IEEE) based on the topic Research of Anti-Phishing Technology could only detect the traditional type of phishing attacks which could not fit new circumstances [2]. The paper published (Juan Chen, IEEE) could detect only the known types of phishing attacks [3]. The Fig. 2 shows the summary of the literature review.

Work/ Published	Content based Approach	Experimental Data Approach	Spam Filters Approach	Drawbacks
Abdulghai, 2016, IEEE	√	-	-	Dataset Limitation
Yanhui Du, 2014, IEEE	-	√	-	Limited to traditional sites
Juan Chen, 2006,IEEE	-	-	√	Cross site scripting not allowed

Fig. 2 Summary of Literature Review.

III. EXISTING SYSTEM

The existing systems use various techniques for prevention of phishing attacks which are listed below:

1. Detect and block the phishing websites in time.
2. Enhance the security of the website.
3. Block the phishing emails by various spam filters.
4. Install online anti-phishing software in user's computer.

IV. PROPOSED SYSTEM

Various approaches have been proposed for preventing the website or link from phishing attack. For collecting useful information from the victims phisher will allure the victims to click on hyperlink embedded in phishing email so in our model we are trying to sort this out by classifying the hyperlinks of phishing emails. A hyperlink has a structure as:

Anchor text

Where “URI” is used for getting the information that user need to access the networked resources. Anchor text is the text displayed in the user web browser.

In our model,initially we create a mail server from where we can either send or receive the mails. So user first need to login into the server. Whenever we encounter any kind of suspicious websites we will check its hyperlink using the mail server so if any particular hyperlink consists sufficient amount of phishing websites characteristics then it will be concluded as a phishing site.

IV. METHODOLOGY

A. Creation of mail system and database system.

Here we deal with user interface for home page, sign-in, sign-up and forgot your password pages. It also enable new user to sign-up and for existing user sign-in.whenever user forgets his/her password they can retrieve their password by using forget password link. The users are managed by database operation. The database is updated every time new user signs in.

Fig 3 shows the creation of mail system and database system.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 5, Special Issue 14, April 2018

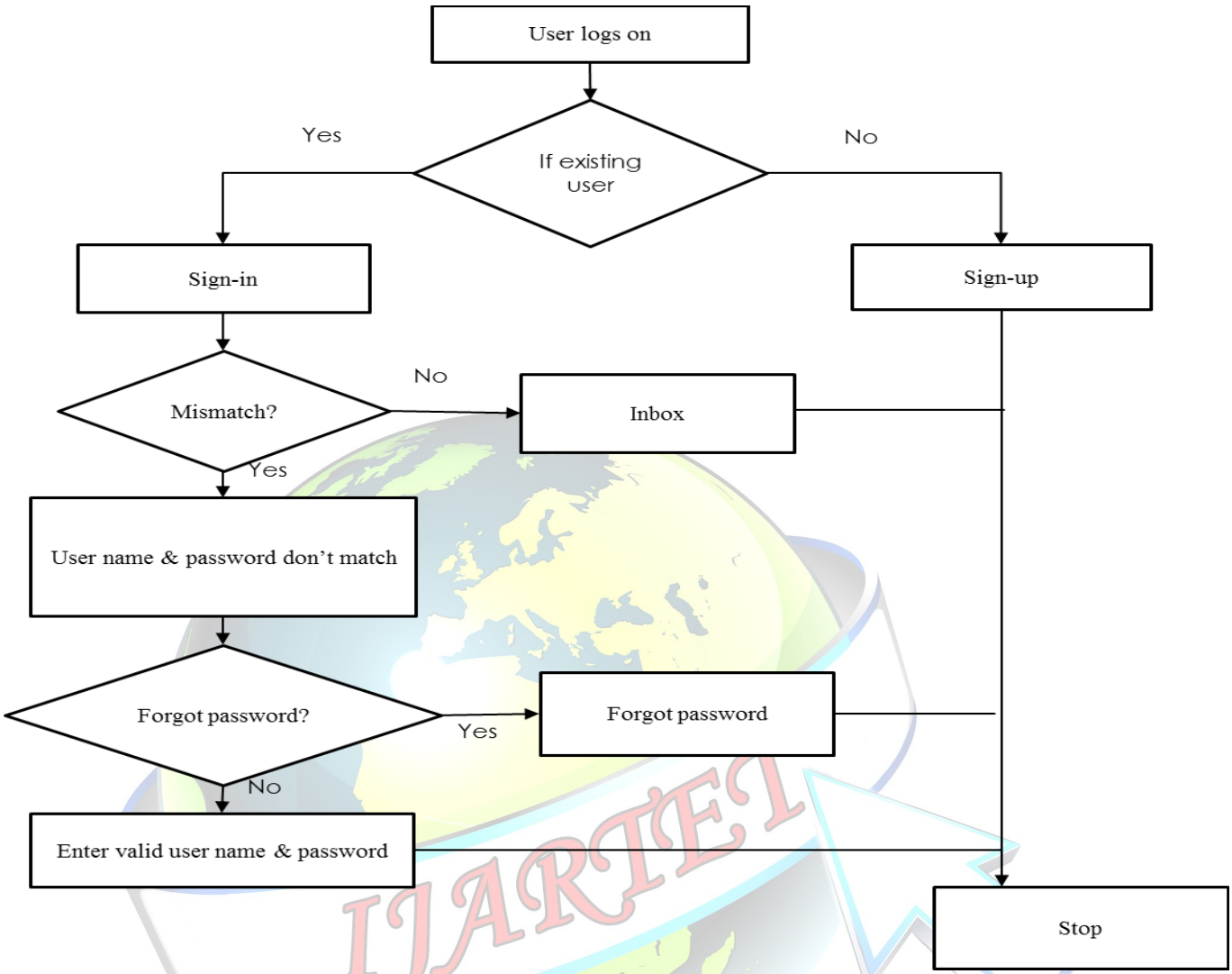

Fig. 3Creation Of A Mail System And Database Operation

B. Compose, Send and receive a mail

This module shows how to compose and send a mail. After sending a mail the date and the subject of the mail is displayed. Then we check into the receive mail whether it is a phishing or not.
Fig 4 shows how to compose, send and receive a mail.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 5, Special Issue 14, April 2018

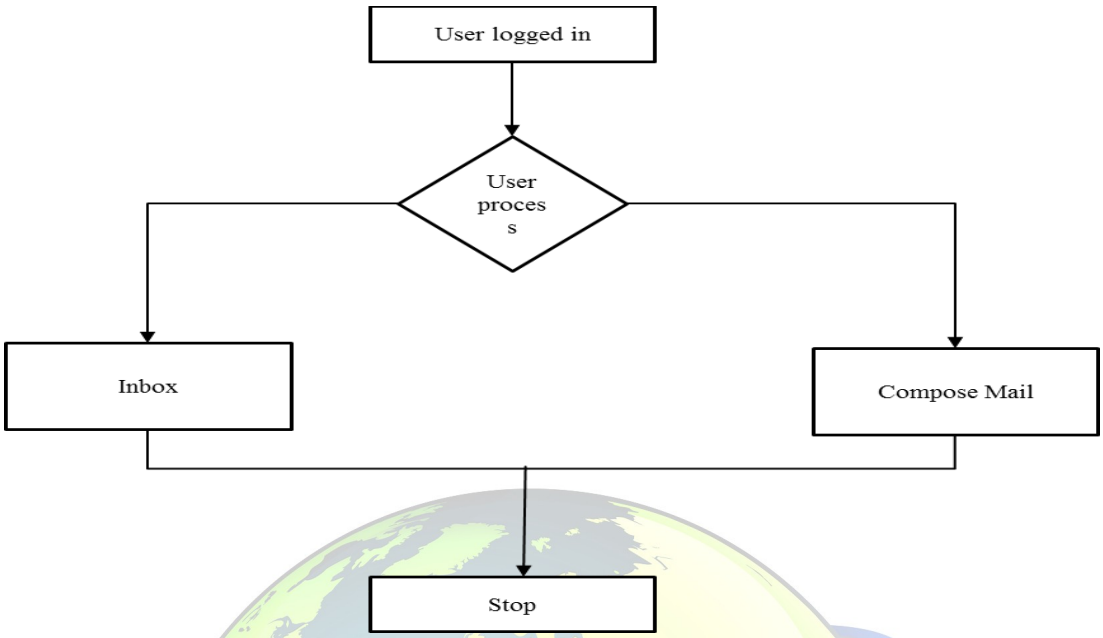

Fig. 4Compose, Send And Receive A Mail

C. Implementation of LinkGuard Algorithm

User can add domain names and categorize them as whitelist or blacklist. When a particular mail is confirmed to be phishing then that domain name automatically gets added to blacklist. Also the domain name are checked by LinkGuard algorithm to make sure if the domain names falls under any categories of hyperlink for phishing emails. In this way using this algorithm we can detect whether the emails is phishing or not and if it is a phishing user should be aware about not opening the particular link.
Fig. 5 shows the implementation of the LinkGuard Algorithm

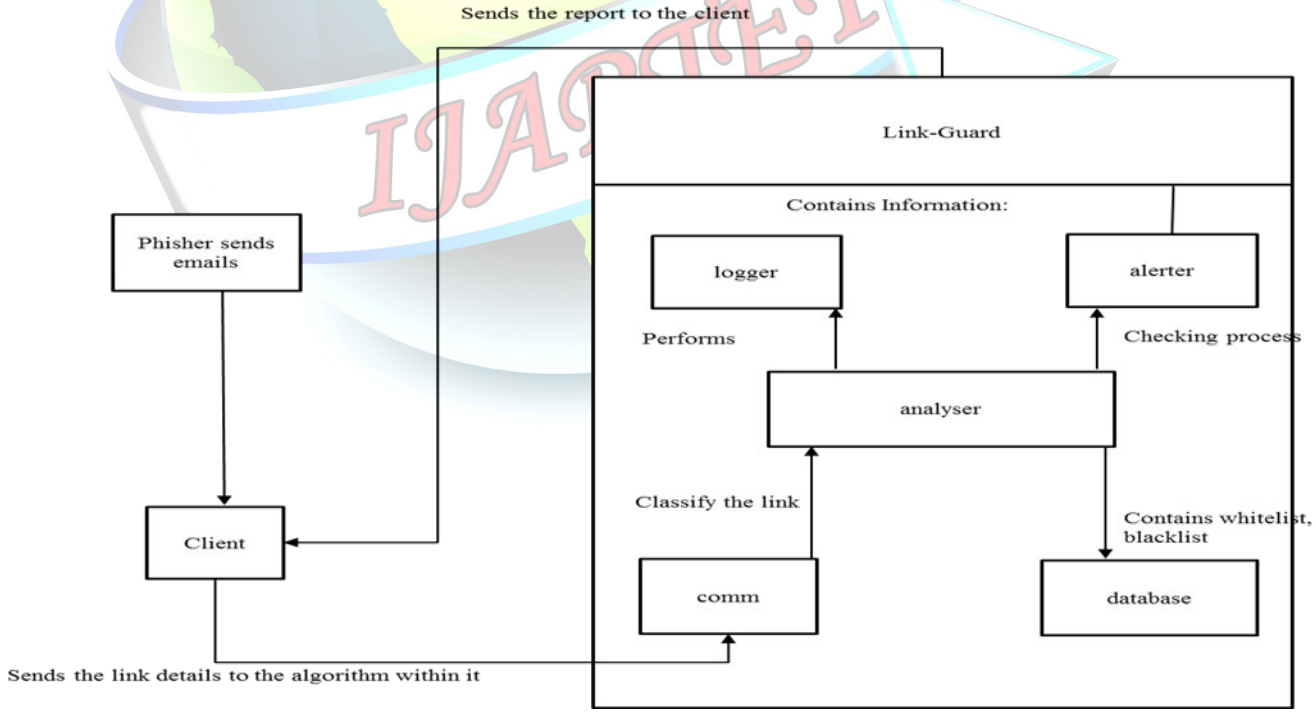

Fig.5Implementation Of Linkguard Algorithm

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 5, Special Issue 14, April 2018

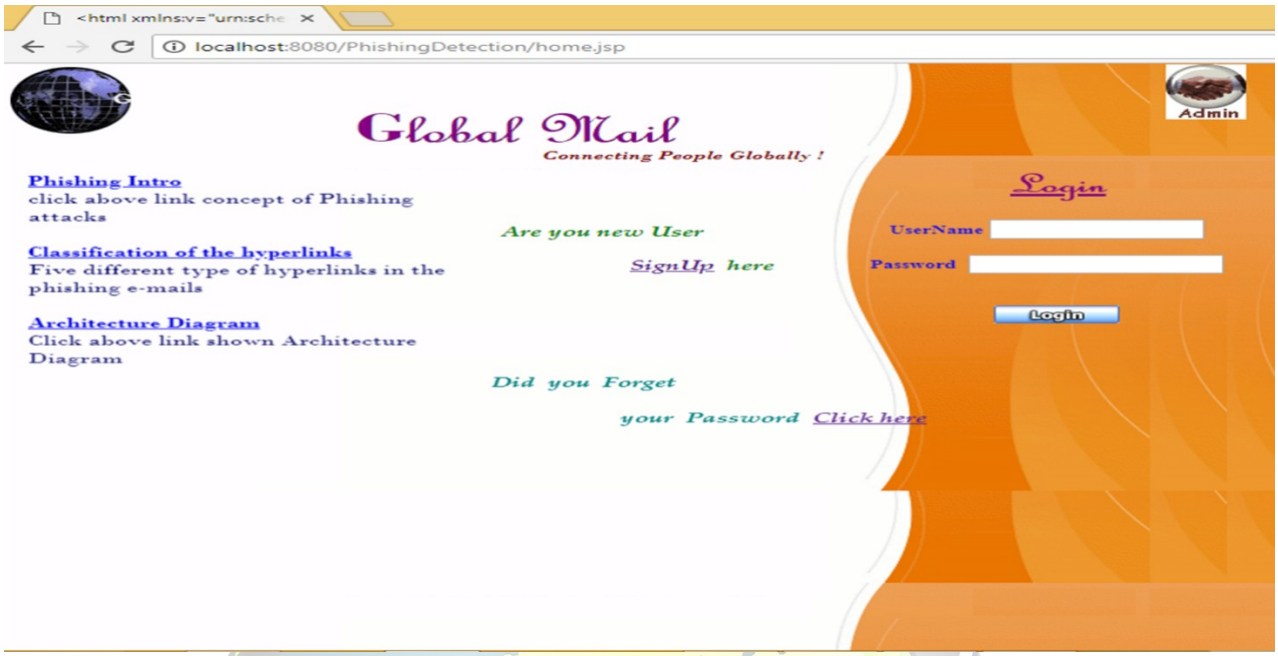

Fig. 6 Login page

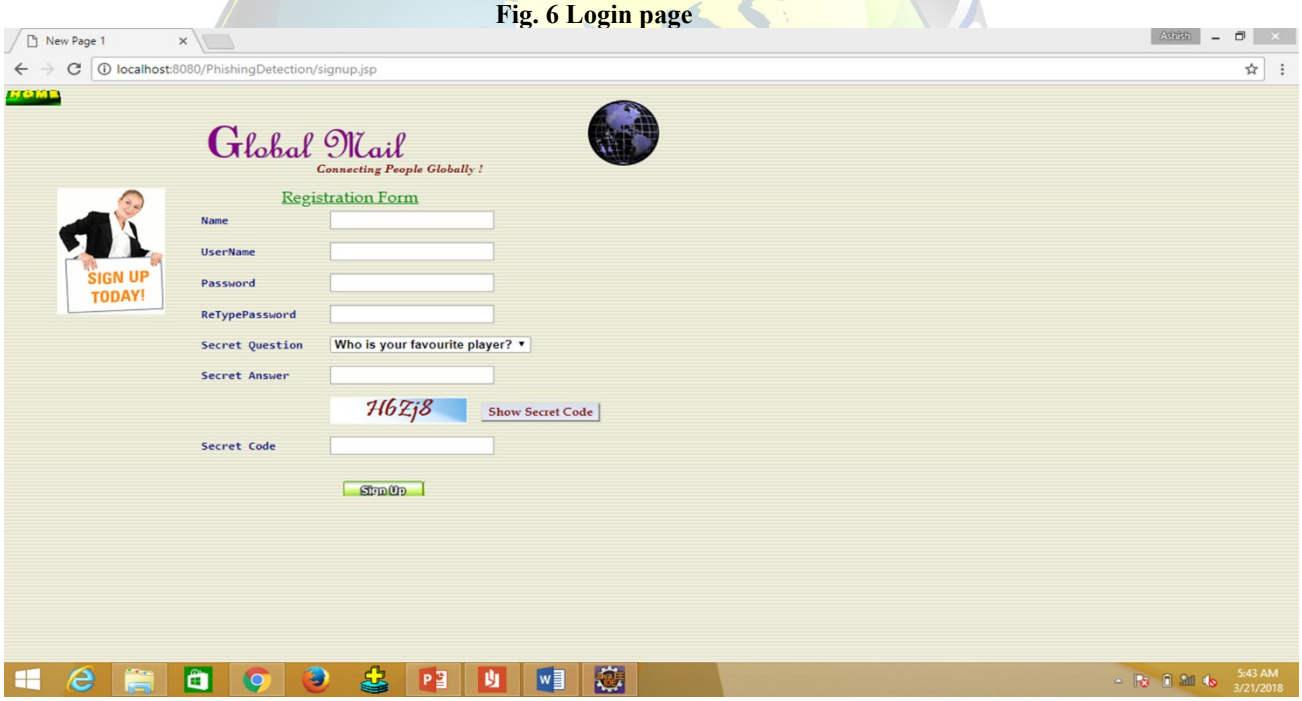

Fig. 7 Sign-up page

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 5, Special Issue 14, April 2018

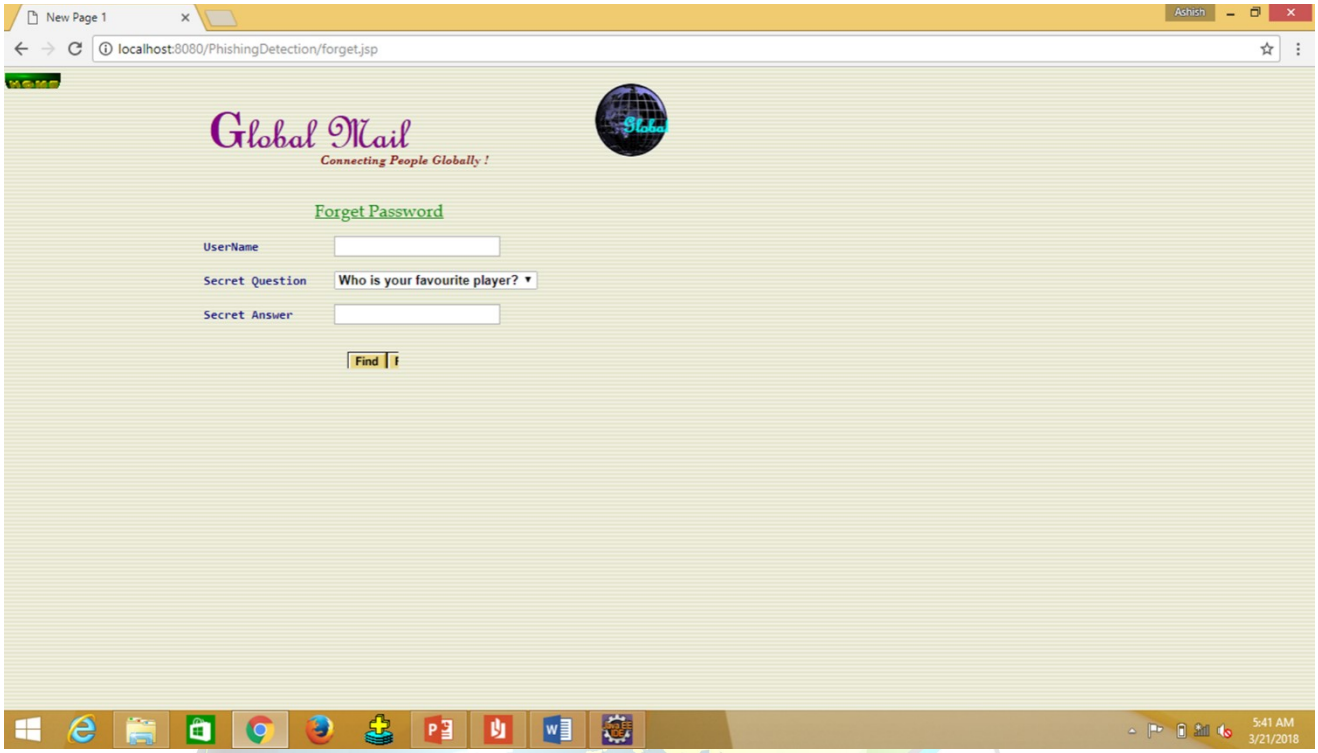

Fig. 8 Account Recovery page

VII. CONCLUSION

In this paper we propose a model for detecting phishing attacks using LinkGuard algorithm implemented in java platform. With an accuracy of 97% it is effective enough to detect the major phishing attacks. Although this model is not capable enough to detect the phishing attacks in the form of images and videos, we can use it to detect the fake websites. The results of our work completed half way through are shown in section snapshots.

Phishing attack if ignored can result in huge loss of financial aspects as well as loss of some valuable information. So, this approach should be prioritized and certain awareness should be created to minimize and eliminate such attacks as far possible. As a future enhancement, we propose to extend the work to include the identification of attacks in the form of images and videos and may be later real time attacks at the time as and when it happens and further we try extend it to be identified by the Operating system level itself as a digital forensic model[6][7].

VIII. REFERENCES

[1] Abdulghai ali Ahmed, Nurul Amirah Abdullah. Real Time Detection of Phishing attacks in 2016
[2] Yanhui Du, Fu Xue. Research of anti-phishing technology based on email extracion and analysis in 2014
[3] Jun chen, Chuanxiong guo. Online detection and prevention of phishing attacks in 2006
[4] www.1000projects.org/online-detection-and-prevention-phishing-attacks
[5] www.codeproject.com
[6] Joseph, Asha, Singh K John, Review of Digital Forensic Model and a proposal for operating system enhancement in 2016
[7] Joseph, Asha, Singh K John, Digital Forensic in distributed environment, IGI Global, 2018

